SECOND

INTERNATIONAL SYMPOSIUM

ON DIGITAL FORENSICS AND SECURITY

Edited By: Prof. Dr. Peter Cooper & Assist. Prof. Dr. Murat Karabatak

---

MAY 12 – 13, 2014

SAM HOUSTON STATE UNIVERSITY

HUNTSVILLE, TX

2ND INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY

12-13 MAY 2014

SAM HOUSTON STATE UNIVERSITY

Houston-TX-USA

Proceding Book

Edited By

Prof. Dr. Peter COOPER
Assit. Prof. Dr. Murat KARABATAK

ISBN : 978-975-394-076-4

Houston-Texas - USA

2014

PREFACE

The Second International Symposium on Digital Forensics and Security Takes place in May 2014, at Sam Houston State University and is a milestone in encouraging activity the area of information assurance and digital forensics. This event is conducted as a consortium including Firat University, Sam Houston State University, Gazi University, Police Academy in Turkey, Petru Maior University, University of Arkansas at Little Rock, and The Polytechnic Institute of Cávado and Ave.

Crimes are no longer limited to physical or emotional acts that break the law. Cyber crimes, which refer to crimes that involve digital devices and networks, are also increasing rapidly. In addition, many traditional crimes now have cyber evidence associated with them. Digital Forensics is the acquisition of digital evidence, examination, and reporting of the findings on digital devices and networks that pertain to a criminal investigation. The importance of Digital Forensics is increasing for the law enforcement community for a number of reasons, not the least of which is that computers, tablets, smart phones and the Internet represent the fastest growing technology tools used by criminals. This trend is expected to continue for the foreseeable future.

It is evident that the investigators in this area need to be equipped the necessary skill set to effectively write and request warrants, handle digital evidence in an manner that maintains the quality of evidence throughout the chain of custody, ad effectively transmit the evidence to a legal system, as yet not equipped properly to understand digital evidence. Not only are the numbers of qualified cyber crime investigators limited, but also Digital Forensics education programs and scholarly activities in this area are rare around the world. As a result, the Digital Forensics Engineering Technology program, a collaborative venture between Sam Houston State University and Firat University and the ongoing International Symposia on Digital Forensics and Security are a necessary and timely development.

Despite the relative youth of our field in comparison with most other academic fields there is beginning to emerge a significant body of work that encompasses, the digital forensic processes, law and the development of techniques to address emerging threats, in particular infrastructure threats and cyber warfare. This symposium will hopefully serve to make people aware of the threats of cyber crimes and latest research findings with bridging different countries and cultures.

I sincerely would like to thank for all contributors and participants for the ISDFS'14.

Prof. Dr. Peter COOPER
Chair of the Consortium

HONORARY BOARD

Calin Enachescu	Rector, Petru Maior University
Dana Gibson	President, Sam Houston State University
Jaimie Hebert	Provost, Sam Houston State University
Joel E. Anderson	Chancellor, University of Arkansas at Little Rock
Kutbeddin Demirdağ	Rector, Fırat University
Remzi Fındıklı	President, Police Academy
Süleyman Büyükberber	Rector, Gazi University
Joao Carvalho	President, Polytechnic Institute of Cavado and Ave

EXECUTIVE COMMITTEE MEMBERS

Prof. Dr. Coskun Bayrak	UALR, Little Rock, AR, USA.
Prof. Dr. Vahit Bicak	National Police Academy, Turkey.
Prof. Dr. Peter Cooper	Sam Houston State University, Huntsville, TX, USA.
Assoc. Prof. Dr. Haller Piroska	Petru Maior University, Romania
Prof. Dr. Seref Sagiroglu	Gazi University, Ankara, Turkey
Prof. Dr. Asaf Varol	Firat University, Elazig, Turkey.
Prof. Dr. Maria Manuela Cruz Cunha	Polytechnic Institute of Cavado and Ave, Portugal

LOCAL ORGANIZING COMMITTEE MEMBERS

Prof. Dr. Peter COOPER, Chairman

Assoc. Prof. Dr. Lei CHEN

Assist. Prof. Dr. Cihan VAROL

Assist. Prof. Dr. Murat KARABATAK

Andy Bannett

SCIENTIFIC COMMITTEE MEMBERS

Abzettin Adamov	Qafqaz University	Azerbaijan
Alejandro Villegas	Microsoft	United States
Ali Shahintash	Qafqaz University	Azerbaijan
Asaf Varol	Fırat University	Turkey
Bernd Krieg-Bruckner	Bremen University	Germany
Bojan Cukic	West Virginia University	United States
Brian Woerner	West Virginia University	United States
Chengjun Wang	Vermont Technical College	United States
Chris Bowerman	Sunderland University	United Kingdom
Cihan Varol	Sam Houston State University	United States
Coşkun Bayrak	University of Arkansas at Little Rock	United States
Esref Adali	İstanbul Technical University	Turkey
Guofei Gu	Texas A&M University	United States
Gongjun Yan	University of Southern Indiana	United States
Haller Piroska	Petru Maior University	Romania
Hamadou Saliah-Hassane	Teluq University	Canada
Jie Wu	Temple University	United States
Larisa Zaiceva	Riga Technical University	Latvia
Lei Chen	Sam Houston State University	United States
Ming Yang	Southern Polytechnic State University	United States
Murat Karabatak	Fırat University	Turkey
Narasimha Shashidhar	Sam Houston State University	United States
Peter Cooper	Sam Houston State University	United States
Ruhai Wang	Lamar University	United States
Qingzhong Liu	Sam Houston State University	United States
Seref Sagiroglu	Gazi University	Turkey
Shengli Yuan	University of Houston-Downtown	United States
Shaoen Wu	Southern Mississippi University	United States
Tamara Kachala	Cherkasy State Technological University	Ukraine
Vahit Bicak	Police Academy	Turkey
Weiping Wang	Central South University	Canada
Yiming Ji	University of South Carolina Beaufort	United States

KEYNOTE SPEAKERS

Chris Morales

Director of Research at NSS Labs

Topic: The need for a mind shift from one of prevention to one of resiliency

Chris Morales, Practice Manager, Architecture and Infrastructure, has over 17 years of IT and information security experience and joins NSS from 451 Research where he was Senior Analyst, Enterprise Security. At NSS, his areas of research include mobile security, data security, vulnerability management, malware detection and host protection.

Prior to 451, Morales was the Technical Partner Manager at Accuvant, where he developed position strategies for new offering areas such as mobile device security, data security and malware threat analysis. He developed integration strategies for security products in key client accounts in his role as a Security Architect at McAfee, and he also served as a Security Architect with IBM Internet Security Systems. Earlier in his career, Morales held the role of Senior Systems Administrator with Delta Technology, and he also cofounded a company that developed business finance software and small-business networks.

David Morgan

US Attourney's Office IT Manager

Topic: Management by Methodology - Problems in the Enterprise. Organizations, to include civilian, federal, and contracting entities, all have the same critical problem: A lack of foundational knowledge in the workforce. This wastes time, costs money and destroys resources, all of which weaken the overall organization.

David has over 30 years' collective experience working with security in both physical as well as virtual environments. He currently serves as the Supervisory Information Technology Specialist at the Office of the U.S. Attorney, Southern District of Texas.

During his career David has worked with the Texas Department of Criminal Justice as a Correctional Officer, with the U.S. Marine Corps as a military police watch commander, Special Operations Response Team Leader (aka SWAT), Evidence Custodian, Special Enforcement, Chief Criminal Investigator, Protective Service Detail Team Leader, and with the FBI as an Information Technology Specialist and Information Systems Security Officer.

When David isn't at work he enjoys teaching. He has taught various topics which include operating systems, network infrastructure, and network security.

Noel Due FBI Cyber Crime Division **Topic:** Bot Net Threat Focus Group, an international Law Enforcement effort to take down botnets in the wild.	
Noel Due has been an FBI Special Agent focusing on Cyber matters for eight years and is currently assigned to work computer intrusion matters. Noel has over twelve years in Cyber investigations including network and host based forensic investigations and is based in Houston, Texas.	

TABLE OF CONTENTS

A Case Study on Intellectual and Industrial Property Rights in Turkey

A. Özbilen, U. Yavanoğlu, C. Seyrek, B. Çağlar, O. Milletsever, Ş. Sağiroğlu *001*

A Research on Software Security Vulnerabilities of New Generation Smart Mobile Phones

N. Yıldırım , R. Daş , A. Varol *006*

A Survey on Operating Systems for Wireless Sensor Networks

A. Akbaş, M. Gültekin *017*

Adli Döküman İnceleme İçin Otomatik Hiperspektral Luminesans Görüntüleme Sistemi

A. Kholmatov, F. Hacizade, G. Bektaş *021*

Advanced Dynamic Analysis of Cryptolocker

J. Lang, N. Shashidhar *026*

AES, LSB and Huffman Encoding Based Steganography in Telemedecine

U. Kas, E. Tanyildizi *032*

An Approach for Cyber Security Experimentation Supporting Sensei/IoT for Smart Grid

B. Genge, P. Haller, A. Gligor, and A. Beres *037*

Biometric Authentication Systems

L. Chen, C. Hale *043*

Toplumsal Olaylarda Sosyal Medyanın İletişimsel Rolü

Necati Türkay *047*

Computer Forensics in Turkey: A Macro Analysis

M. Çolak, M. Karaman, M.U. Eren, S. Çakır, A.B. Gökalp *051*

Consequences of Using Weak Functions of Old EPC Global C-1 G-2 Standard for Obscuring Secrets

M.H. Özcanhan, G. Dalkılıç, O. Yarımtepe *058*

Counter-Digital Forensics and Relationship with National Security

Ş. Sağıroğlu, M. Karaman *063*

Hastanelerde Biyomedikal Cihaz Takibi

M. H. Özcanhan, G. Dalkılıç, S. Utku *067*

Hukuk Öğretiminde Adlî Bilişim: Türkiye Örneği Bağlamında Bir Değerlendirme

Çetin Arslan *073*

Implementing Secure Communication on Short Text Messaging

A. Chandragari, P. Cooper, F. Liu *077*

Legal Concerns and Challenges in Cloud Computing

L. Chen, S. Krishnan *081*

Mobile Biometric Security Systems for Today and Future

N. Yıldırım, A. Varol *086*

New Method For Automatic Fingerprint Recognition System: Entropy And Energy – Adaptive Network Based Fuzzy Inference System (EEANFIS)

A. Varol, E. Avci *092*

Providing Patient Rights with Consent Management

E. Olca, O. Can *101*

Risk Management Methods in Small Scale Companies

F. Mastjik, C. Varol *105*

SQL Injection: Hardening MYSQL

N. Nevarez, B. Zhou *110*

Steganalysis of Quality Pair JPEG Steganography

K. Tasdemir, F. Kurugollu, S. Sezer *113*

The Importance of Keeping Network Devices under Control in Big Networks for Network Forensics

F. Ertam, T. Tuncer, E. Avci *119*

The Road Map for Digital Forensic Law of Turkey

İhsan Baştürk *124*

The Role of Database Forensics in Cyberspace Law Enforcement

M. S. Metzger, B. Zhou *130*

Üniversitelere Yapılan Siber Saldırılar ve Üniversite Yönetimi Tarafından Yapılması Gerekenler

S. Karabatak, F. Özmen, M. Karabatak *139*

A Case Study on Intellectual and Industrial Property Rights in Turkey in Perception of Forensics

Uraz Yavanoglu[1], Alper Ozbilen[2], Ceydacan Seyrek[3],
Busra Caglar[4], Ozlem Milletsever[5], Seref Sagiroglu[6]
Gazi University, GUTIC, Ankara /Turkey,
[1]uraz@gazi.edu.tr, [2]ozbilen@gmail.com, [3]ceydacanseyrek@gmail.com,
[4]busracaglar992@gmail.com, [5]milletseverozlem@gmail.com, [6]ss@gazi.edu.tr

***Abstract*—Intellectual and industrial property rights in Turkey are becoming significant more than ever putting efforts into developments and research activities. Using any material which is subject to intellectual and industrial property rights requires permission given by its author. Like many counties, using copyrighted materials or materials which are considered industrial property without permission or license result in violating Turkish law. It can be said that Turkish law relating Intellectual and industrial property rights are mostly compatible with international law. The fact is that there is a strong connection between the importance of intellectual property rights and economic activities based on technological advances [1]. In this paper, scope of intellectual and industrial rights in Turkey is discussed. [2].In this study, intellectual property rights in Turkish legal framework are introduced in addition to piracy and imitation activities in the context of forensics. Intellectual and industrial property rights in Turkey and some other countries are compared with each other. In order to make sure that having proper understanding about these violations in Turkey, some expert's case reports mostly related to unlicensed software, copyright infringement, breach of trademark and domain violation are reviewed .**

Keywords—forensic, intellectual property, industrial rights, security, criminal complaint, court cases

I. INTRODUCTION

Intellectual property rights including patents, utility models, trademarks, industrial designs and geographical indications are important to provide encouragement to their inventions [3].
Intellectual and industrial property rights may involve scientific and literary works, films, music, artistic works such as drawings, sculptures, photographs as well as computer programs. All kind of legal protections relating to intellectual and industrial property rights stimulate new invention and new ideas.

Definitions relating intellectual and industrial rights are given below;

Industrial properties include innovations, inventions, artistic works and original designs rights. Rights under this category mainly refer to protection of industrial inventions such as authentic which are used in a certain industry.

A patent refers to royalty right for an invention. Document showing these rights is called patent. A patent allows its owners to maintain the features of the invention. The patent owners are granted special privilege. This privilege is mainly about using this invention legally. Patent owners may allow someone else to use any invention under certain conditions which are mostly called licenses. In the other way, as patent owner may sell the patents' rights to someone else if required.

Utility model basically refers to invention owner who has set of rights such as produce invention's product and marketing for 10 years. Utility model certificate process is generally easier than patent process especially in microcredit and research organizations. Utility model protection functions as an option are realized more quickly than patent protection function.

A trademark is a distinguish sign which defines goods or services produced by the company. There are many features including a word, letter, form or pack. Trademark system makes consumers to identify different products based on their characteristics. Different products produced by different company indicated by unique characteristic feature called trademark. Trademark may obtain combination of symbols, drawings, 2-D or 3-D shapes, etc.

Industrial design covers wide variety products to be produced by machines or hands. Industrial design includes parts of product, set of tools and products involving graphic symbols and typographic characters.

Geographical indication signs have geographical origin. Mostly, geographical indication sign includes name of origin of products. These indication signs are usually used for agricultural products.

Creators protect their works with copyright. Novels, poems, plays, newspapers, advertisements, computer programs, films, drawings, paintings and photographs are within the scope of copyright protection.

This paper consists five sections. Section 2 mentions the studies in the literature. Section 3 clarifies procedures in the field of forensics. Section 4 explains expert's case reports about the issues explained above. Section 5 discusses the study, presented in this article.

II. CASE STUDIES

Intellectual property and industrial property rights are protected under Turkish laws. Investigations are considered under different issues. Thus, the works need to be classified. The sections in tables include the details on this topic [2].

Table 1: Scope of Intellectual and Industrial Property Rights [2, 4, 5]

Content of Intellectual Property	**Protection tool**	**Protected Areas**	**Used Areas**
Creative Contents	Copyright and Patents	Authors' rights and Producers' rights	Each area under production
Sounds and Videos	Copyright and Trademark	Distinctive brand and symbols	All sectors, especially the music and Media
Signs and Logos	Trademarks	Distinctive brand and symbols	All sectors
Webpage and Interfaces	Copyright and Industrial Design	Product visualization	Authors' rights, Media and Companies' rights
Software	Trademark and Patents	New industrial inventions and Distinctive brand and symbols	Companies' rights and Individual rights
Databases	Industrial Design	Product visualization	Companies' rights
Identities	Industrial Design	Product visualization	All areas
Geographical indications	Geographical Tools	Descriptive place names	Food and drinks and Historical monuments

Table 2: International agreements for intellectual and industrial property rights [4, 5]

Content of Intellectual Property	**International Agreements**	**Advertising Elements**	**Protected by**
Signs and Logos	TRIPS, Madrid Agreement, Nice Agreement, Vienna Agreement,	Business names, Logos, Product names, Domain names	Trademarks
Creative Contents	Bern Convention, Rome Convention, Geneva Convention, Brussels Convention, WIPO Copyright Convention, WIPO Phonograms Convention, Universal Copyright Convention, Paris Convention, Patent Cooperation Agreement, Budapest Convention, Strasbourg Agreement, European Patent Convention	Written material, photographs, art, graphics, music and videos	Copyright
Sounds and Videos	Paris Convention, Patent Cooperation Agreement, Budapest Convention, Strasbourg Agreement, European Patent Convention, TRIPS, Madrid Agreement, Nice Agreement, Vienna Agreement	Sounds in the advertising	Copyright and/or by trademark law
Webpage and Interfaces	The Hague Agreement, Locarno Agreement, Bern Convention, Rome Convention, Geneva Convention, Brussels Convention, WIPO Copyright Convention, WIPO Phonograms Convention, Universal Copyright Convention	Computer-generated products	Industrial design law, website by copyrights
Software	Paris Convention, Patent Cooperation Agreement, Budapest Convention, Strasbourg Agreement, European Patent Convention	Digital advertisements	Copyright and/or patents
Databases	Washington Agreement	Consumer profiles	Copyright
Identities	The Hague Agreement, Locarno Agreement	Name, photograph, image, voice or signature	Publicity or privacy rights
Geographical indications	Lisbon Agreement	Sign used on goods that have a specific geographical origin and possess qualities or a reputation that are due to that place of origin	Laws against unfair competition, consumer protection laws, laws for the protection of certification marks

Table 3: Companions for intellectual and industrial property rights

Type of Violation Countries	**Turkey**	**United States of America**	**European Union [6]**
Copyright	The law of intellectual and artistic works [7] -Article 21 right to work. -Article 22 right of duplication. -Article 23 the right to emit. -Article 71 of criminal case.	Copyright act of 1978 [8]. -Article 408 registered in general terms. -Article 409 applications for copyright registration procedure. -Article 410 registration application and registration certificated -Article 411 relation with registration and rape case. -Article 412 rape of registration is a prerequisite.	92/100 numbered and dated November 19, 1992 Renting of Intellectual Property, Lending and Related Rights Council Directive Concerning.
Unlicensed Software	The law of intellectual and artistic works [7] -Article 22 right of duplication. -Article 38 of personally use. -Article 52 of opportunity to benefit. -Article 71 of criminal case. -Article 81 of prevention of infringement of rights	The United State Standard Computer Information Transfer Law (Software and Information licensing standards) [9].	91/250 dated May 14, 1991 Council Directive on the Protection of Computer Programs Legal.
Breach of Trademark	No. 556 decree law on the protection of trademarks [10]. -Article 61 infringements of trademark rights.	-American Competition Law [11].	-93/98 dated 29 October 1993 Author's Rights and Related Rights with the Council Directive on the harmonization of the protection period.
Domain Violation	The law of intellectual and artistic works [7] -Article 22 right of duplication. -Article 23 the right to emit. -Article 71 of criminal case.	U.S. Federal Law No. 18 of the Criminal Code in 2323 article [12].	2001/29 numbered and dated 22 May 2001 and Related Rights in the Information Society Author of the Parliament and Council Directive on the Harmonization of Rights.

III. PROCEDURES

Criminal complaints or claims can be made to law enforcement officers or attorney generalship. Criminal complaints or claims procedure regulated to Article 158 of Turkish Criminal Procedure Code [13]. According to Article 158 of Turkish Criminal Procedure Code "Report or claim related to the crime may be submitted to the office of the public prosecution or the offices of the security forces" [13].

File a criminal complaint or claims against a person or legal identity about copyright in music works used without purchase, forgery of CD, use unlicensed software, breach of trademark, domain or photography and use without permission from Torrent network. The prosecution offices launch an investigation about complaint. If law enforcements get a criminal complaint; turn to prosecution about event and law enforcers continue to research according to the orders of the prosecutor.

After the investigation, law enforcers raided the scene under the orders of the prosecutors and take a crime scene report. If law enforcers need to confiscate item in scene of crime, related operations are regulated by Article 119 of Turkish Criminal Procedure Code [14]. Article 119 covers Turkish Criminal Procedure Code "The members of the security forces shall conduct searches upon the order of the judge, or if there is peril in delay, upon a written order of the public prosecutor, if the public prosecutor is not reachable, upon a written order of the superior of the security force.

The proceedings will be considered by the attorney generalship. The prosecutors prepare an indictment according to 5271 Turkish Code of Criminal Procedure 170/2 Article [15]. Then, attorney generalships launch an investigation.

After investigation, the court case files according to indictment. The parties may reconcile scope of the Turkish Criminal Code [4]. The judges rescind the trial herein. If the parties are not reconciling, the court file is sent to the experts.

The experts consider the court case. After then, the expert prepares report according to Intellectual and Industrial Property Rights Law to be used for is presented the judge by the expert.

Figure 1 also gives more detail about the procedure.

IV. CASE REPORTS

This part of article focuses on case reports on various topics within the scope of Intellectual and Artistic Works. The investigation of this article is based on real cases in Turkish Courts. The steps followed for enlightened any court case require more investigations to decide the case. A report in the direction of need or order given by court an expert can prepare it and present it to the court.

After above procedures which are mentioned in Section 3, experts express technical facts and his /her opinions about the case. The

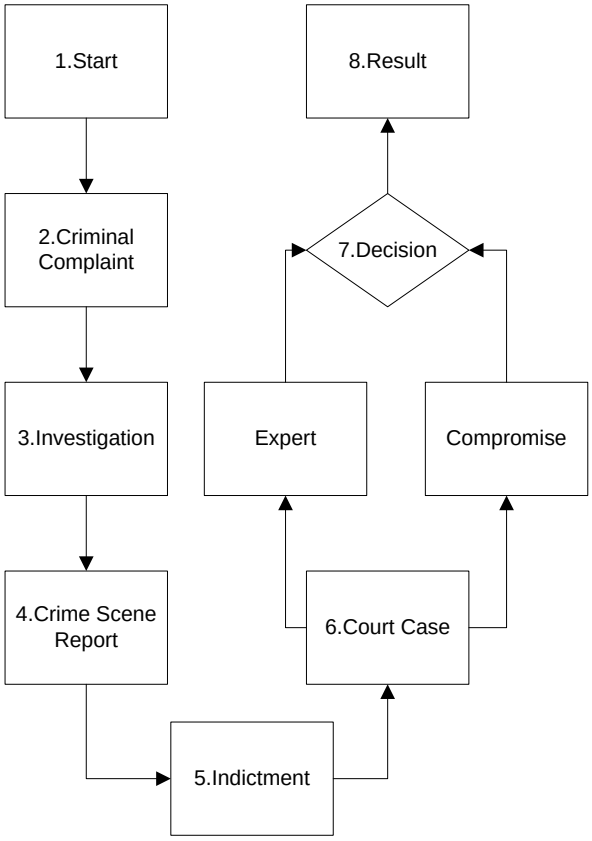


Figure 1: Block Diagram of Procedure

A. Unlicensed Software

In this section, experts' reports are examined about the use of unlicensed software. In the reports which are prepared by experts, files are criminal complaint against business organization about using unlicensed software.

As a result of the reports, computer software in business organization are in the nature of the work protected by Turkish Law No. 5846 within Intellectual and Artistic Works [7]. In this case, violations of reproduction rights according to Article 22 protection covers installed computer environment illegal replication.

For this reason, this action is violation of the unlicensed software without license according to Article 71 of the Law No. 5846 within Intellectual and Artistic Works [7].

Invoices and documents are the most significant evidence of the original software that require the license fee. In line with this information, experts examine invoices and documents belonging to the software. Article 52 of the Law No. 5846 on Intellectual and Artistic Works have been violated by the absence of invoices and documents related to the software [7].

Article 81 of the Law No. 5846 within Intellectual and Artistic Works have been violated due to reproduction of programs on computer environment and use without banderole [7].

B. Copyright

Other case is copyright violation. In Turkey, musical works are protected by Turkish Law No. 5846 within Intellectual and Artistic Works [7]. Non-profit Turkish organizations which are called MESAM and MUYO-BIR support to product digital rights of musical rights. The foreign musical rights are also protected by the same organizations according to the international ownership agreements among international bodies. These organizations follow copyright violations and take necessary actions.

If the parties are not reconciling in the case, the court file is sent to the experts. MESAM's computers and CISAC's databases are examined by the experts. Subsequently, the experts evaluate the result of the examination.

The result evaluated according to Article 71 of the Law No. 5846 within Intellectual and Artistic Works. Afterwards, the databases are checked in the presence of Financial Rights Transfer Agreement.

C. Breach of Trademark

In this section, expert's reports are examined about breach of trademark that is prepared by trademark-patent expert and computer expert. In the expert's report, experts were studied whether there was violation of the company trademark rights or not.

Criminal complaint mentions about products of the trademark without the knowledge of company was marketed via the web site and this action constitutes unfair competition.

First of all, experts research whether it is a registered trademark or not. After this stage, they were examined use of the trademark on web site. On the web site about the trademark of content to determine who shared information security elements are needed. Besides that, in order to detect whether the content published by whom, require knowledge of e-signatures or mobile signature.

In case of failure is to provide elements of information security, the trademark's products which were sold on the internet as to whether the original certain information can not available or not.

D. Domain Violation

Domain Rights are protected by the same law. In this case, a patent expert, quality control experts and computer experts will make an examination together.

Holders of rights are researched by experts. A financial and moral rights infringement offense within the scope of the report is written.

The result is evaluated by Article 22, Article 23 and Article 71 of the Law No. 5846 within Intellectual and Artistic Works. The Article 22 protects work in unauthorized reproductions. The Article 23 includes of the works in unauthorized distribution and the other article is protected the works without permission to go public [7].

V. Conclusion

Intellectual and industrial properties rights have vital role to protect not only the properties' owners but also economical development .For that reason, there is great responsibility of international, national and local lawmakers to protect these properties against illegal use. To minimize issues like using unlicensed software, illegal copy, or domain violation, there are international - local agreements and laws available across the word. Turkey is one of them where have full respect of copyrighted materials. Turkish laws regarding intellectual and industrial properties have been covered computer software.

There is a number of ongoing cases regarding unlicensed software in Turkey in order to make a right decision, related courts which are primarily deal with copyrighted materials, prefer to work with computer experts. In this paper, as a part of Turkish criminal process, methods which experts follow in order to find out if there is a use of unlicensed software has been summarized. At the end of the study we offer the digital forensic case reports which can be mainly used in a range of violation such as unlicensed software, unauthorized use of copyrighted materials, breach of trademark and domain violation.

Overall, in Turkey, there is no specific digital forensics steps which can be followed to find out if there is a violation of intellectual and industrial properties rights. To broaden this study and create an awareness regarding violation of intellectual and industrial properties rights,

APPENDIX

GUTIC is Gazi University Technology and Innovation Center. GUTIC was established on 2012. Professor Sagiroglu currently holds the chair position.

REFERENCES

[1] U. Gokovalı and K. Bozkurt, "Fikri ve Sinai Mülkiyet Hakkı Olarak Patentler: Dünya ve Türkiye Açısından Tarihsel bir Bakış,"Mugla University Journal of Social Sciences, vol. 17, Mugla, 2006

[2] O. Kacar Akman and B. Can Karahasan, DIME Working Papers on Intellectual Property Rights, Istanbul,2008

[3] Z. Bicer Ozcelik and C. Ozcelik, "Türkiye'de Sinai Mülkiyet Hakları," Mühendis ve Makina, sayı. 629, Bursa

[4] Turkish Criminal Procedure Code (Art. 158, Law No. 5271 of December 4, 2004)

[5] World Intellectual Property Organization (WIPO), www.wipo.int(31.01.2014)

[6] A. Yarayan, "Fikir ve Sanat Eserleri Kanunu'nun Avrupa Birliği Mevzuatına Uyumu", Türkiye, 2006

[7] Law No. 5846 of December 5, 1951 on Intellectual and Artistic Works (as last amended by Law No. 5728 of January 23, 2008)

[8] O. Nacakcı, P. Bahtiyaroglu, "Fikir Ve Sanat Eserlerinin Zorunlu veİhtiyari Tescili" , Türkiye, 2007

[9] Internet: http://www.ucitaonline.com/ (31.01.2014)

[10] Internet:http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.8042 &MevzuatIliski=0&sourceXmlSearch= (31.01.2014)

[11] Internet: http://en.wikipedia.org/wiki/Competition_law (31.01.2014)

[12] B. Yeh, "Intellectual Property Rights Violations: Federal Civil Remedies and Criminal Penalties Related to Copyrights, Trademarks,and Patents", CRS Report for Congress, 2012

[13] Turkish Criminal Procedure Code (Art. 158, Law No. 5271 of December 4, 2004)

[14] Turkish Criminal Procedure Code (Art. 119, Law No. 5271 of December 4, 2004)

[15] Turkish Criminal Procedure Code (Law No. 5271 of December 4, 2004)

Alper OZBILEN works in Turkish Information and Communication Authority. He received BSc, M.Sc. and PhD .degree from Gazi University. He received the double MSc. degree from Boston University. He is leading researcher of Gazi University Technology and Innovation Center. His research interest are information technology, cyber security.

Ceydacan SEYREK was born in Ankara, Turkey. She currently continues her B.Sc. in Gazi University Department of Computer Engineering. Her research interests are Information Security; internet,web and information systems and applications and Artificial Neural Networks, Forensic Analysis.

Busra CAGLAR was born in Ankara, Turkey. She currently continues her B.Sc. in Gazi University Department of Computer Engineering. Her research interests are Information Security, Bioinformatics and Artificial Neural Networks, Forensic Analysis.

Uraz YAVANOGLU was born in Ankara, capital city of Turkey. He is research assistant of Gazi University Department of Computer Engineering. He received his M.Sc. degree in Gazi University Department of Computer Engineering and Ph.D. degree in Gazi University Faculty of Technology. His research interests are Artificial Intelligence, Data Mining, Information Security, Forensic Analysis and Social Media Mining.

Ozlem MILETSEVER was born in Ankara, Turkey. She received her B.Sc. degree from Gazi University Department of Computer Engineering. Her research interests are Information Security, Pattern Recognition, Biometric and Artificial Neural Networks. She is currently pursuing her M.Sc. degree in Hacettepe University, Department of Computer Engineering.

Seref SAGIROGLU is professor Department of Computer Engineering at Gazi University. His research interests are intelligent system identification, recognition and modeling, and control; artificial neural networks and artificial intelligence applications; heuristic algorithms; industrial robots; analysis and design of smart antenna; internet, web and information systems and applications; software engineering; information and computer security; biometry, electronic and mobile electronic signature and public-key structure, malware and spyware software. Published over 50 papers in international journals indexed by SCI, published over 50 papers in national journals, over 100 national and international conferences and symposium notice and close to 100 notice are offered in national symposium and workshops. He has three patents and 5 pieces published book. He edited four books. He carried out of a many national and international projects. He hold the many conferences and continues academic studies

A Research on Software Security Vulnerabilities of New Generation Smart Mobile Phones

N. Yıldırım, R. Daş and A. Varol

Firat University, Technology Faculty, Software Engineering Department, Elazig/Turkey,
nilyildirim87@gmail.com, resuldas@gmail.com, varol.asaf@gmail.com

***Abstract*— Mobile device world has now become an unavoidable habitat for people. For this reason, hackers and attackers have created a new threat and malicious area in the world of smart mobile devices and they continue to defraud victims, to steal information and to cause losses as material and moral of mobile users. In this paper mobile security vulnerabilities and mobile application attacks (malware, direct attacks, data interception, and exploitation) are handled by different mobile operating systems. Later, needs for mobile security, testing of mobile systems and automated mobile testing tools to find security vulnerabilities have been investigated.**

***Keywords*— Mobile vulnerability, mobile attacks, security testing, Android, iOS**

I. INTRODUCTION

Information security means ensuring the security of personal data and knowledge in information society. With the importance of computer technology, the majority of information about the personal lives has been propelled to the virtual systems. In this case, securing of information in computers and mobile systems has a great importance for people. Information security basically targets (1)confidentiality which can be defined as closed to unauthorized access, (2) integrity means protecting content from threats of changing or deleting knowledge and (3)availability means to be ready of knowledge when needed [1].

Mobile technologies are used more than other computer systems because of being portable and providing people to access the information from anyplace. With the popularization and improvement of smart phones, all personal virtual transactions are begun to realize with these devices.

Popular operating systems used in smart phones are known as Android, iOS, BlackBerry OS, Windows Phone OS and Symbian. Mobile systems as seen on Table 1, while android-based sale percentage of Smartphones was 72.6 in 2012, it is seen that the percentage rate has reached 81.9 in the third quarter of 2013. Although iOS is in the second sequence with 12 percentages, iOS and the Smartphones which use the other OS (BlackBerry, Microsoft, Symbian, etc.) sales rates are decreasing.

Table 1: Worldwide Smartphone sales to end users by operating system in 3Q13 (Thousands of Units) [2]

Operating System	**3Q13 Units**	**3Q13 Market Share (%)**	**3Q12 Units**	**3Q12 Market Share (%)**
Android	205,022.7	81.9	124,552.3	72.6
iOS	30,330.0	12.1	24,620.3	14.3
Microsoft	8,912.3	3.6	3,993.6	2.3
BlackBerry	4,400.7	1.8	8,946.8	5.2
Bada	633.3	0.3	4,454.7	2.6
Symbian	457.5	0.2	4,401.3	2.6
Others	475.2	0.2	683.7	0.4
Total	**250,231.7**	**100.0**	**171,652.7**	**100.0**

With the increasing use of smart mobile devices, hackers have started to produce malicious software or to look for vulnerabilities for smart phones. The reason of benefit from these malicious apps or phone vulnerabilities are listed as seizing user information (to sell the information to companies for gaining money), damaging to the phone or the operating system (to sell the anti-virus software), harming the user moral. According to Pocatilu, malicious applications' goals and objectives are in following and these harm users or smartphones in following ways [3]:

- Annoying alerts or messages;
- Advertising popups opened;
- Unwanted web pages opened;
- Malicious programs send unwanted messages (SMS, MMS), make phone calls and this causes higher invoices;
- Unauthorized use of personal information data;
- Altering or removing data stored in the file system, contacts, messages etc.;
- Confidential data transferred to a remote location;
- Monitoring SMS messages and listening telephone calls.

In this article, we work on an investigation of mobile security threats and security testing tools. In the first section we will focus on security threats for mobile phones with general and operating systems (Android, iOS). In the second section we will focus on security analysis of new generation smart mobile phones and testing tools by operating systems (Android, iOS).

II. THE SECURITY VULNERABILITIES OF SMART MOBILE PHONES

In the past, malicious softwares are mostly threating computer systems, but now, exceedingly threaten the safety of users. The purpose of the computer security involved in computer technology (PC, tablet PC, mobile technologies, Smartphones, etc.): "To make investigations for threats and hazards which can encounter while individuals and organizations are using these technologies" [1]

With growing numbers of Smartphones, hackers or attackers tend to mobile technologies. Smartphone users increasingly use online banking, online shopping andother operations with mobile phones which requires a credit card and so there are likely to be more threats designed to produce profits for the attackers [4]. Users don't take into account that smart device cannot be safe when realizing these important transactions (online banking, using a credit card, etc.) therefore not informed enough about mobile security. Whereas, more users download and install third party apps for Smartphones and the risk of installing malicious programs is rapidly increasing [4]. In addition to users, most of mobile application developers don't understand the security aspect of the application or they don't focus on the security properties of the application.

The main attack methods that threaten mobile devices are malware (malicious software), direct attacks, data interception (intervention), exploitation (using weakness) and social engineering [5].

Malware is a kind of hostile, annoying and uninvited software or program code designed to use a device without the owner's assent [4]. Types of malware are listed below;

- *Virus:* It is a program or a code that is loaded to the mobile system (or generally to the computer) without the user's knowledge. The virus is dangerous for mobile users because it can copy itself to another device quickly and use memory, change data and crash system.
- *Worm:* It means "Write Once, Read Many" and it is a kind of virus. It processes same as a virus because it can copy itself to another device quickly and use memory, but it doesn't change files.
- *Trojan:* It is a program that often used to gain backdoor access. It doesn't copy or replicate itself as a virus or worm.
- *Spyware:* It is a spy software which hides in an application or software. It monitors victim's activities after installed and sends activity report to the attacker.

In *Direct Attack*, the attacker uses a common application vulnerability or an opening system vulnerability and aims to gain unauthorized access and information [5]. By *Data Interception*, traffic flow is followed by the attacker and attacker seizes the data. When a mobile user sends data by Wi-Fi, this is an advantage for the attacker.

According to Polla et al. [4], the methodologies for realizing attacks to Smartphones are categorized in following classes:

- Wireless;
- Break-in;
- Infrastructure-based;
- Worm-based;
- Botnet;
- User-based

Malicious programs use Bluetooth and the wireless connection feature of smartphone, short messaging and telephone calling services to spread and to harm other smartphones. When using an open Wi-Fi, hackers wait for sniffing for realizing banking and shopping activities by victims.

In addition to malicious software, malicious sites are important threats for smartphones. In 2012 most dangerous and risky place was pornography, as seen in Figure 1, more than 20 percent of the time that a user who were coming from a pornography site, went to a malicious site [6]. Also social engineering and phishing attacks which realize through web pages for mobile phones threat users. Mobile phone users' bank details can be seized by directing users to fake sites of banks or the attacker robs the user information that is important for its own.

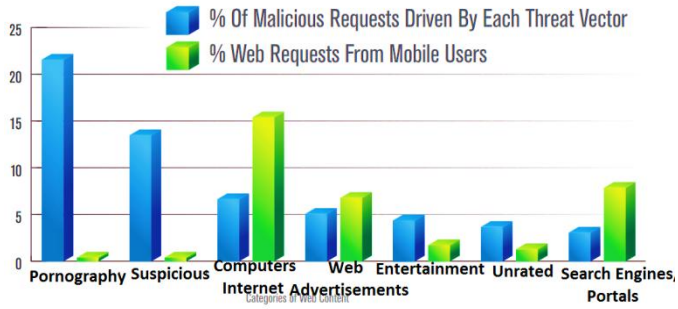


Figure 1: Percentage of malicious requests driven by each category compared to requests for content in that category [6].

A mobile device can be used by attackers for collecting and selling personal data, accessing information of device owner or may use the device like a gateway between enterprise data and resources and in addition the device can be used for botnet [7] (a botnet is a set of devices that are affected by a virus which provides to attacker the ability of devices to remotely control [4]). Attackers also want to gain money from user's banking transactions via banking application vulnerabilities. Also the level of security systems is increasing by the banks for not to be affected from malwares but malware programmers are producing new codes to break this security level [8].

Delac et al. [9] define attacker-centric threat model for mobile platforms to analyze attacker's goals, motives and attack strategies. This model includes 3 issues [9];

- *Attack goals:* That item determines the attacker's interests and the reasons for attacking. Attacker aims to collect private data, utilizing computing facilities and making harmful malicious actions.
- *Attack vectors:* That item focuses on threat's spreading ways on mobile platforms. These ways handling on 4 categories; mobile network services, Internet access, Bluetooth and USB and other devices.
- *Mobile malware:* That item describes mobile malware and indicates that mobile attacks generally occurs multiple variants of Trojans, botnet, worms, rootkits.

A. Security Vulnerabilities on Android Based Systems

Android is an open source and free mobile operating system based on the Linux kernel [10] and developed by the free software community, Google, Open Handset Alliance. Android market platform is growing faster and can be said this is the fastest growing mobile application platform, but unlike the Apple's App store, the applications on Android market go through no scanning process [10]. This state leads to Android OS to be a grace operating system for attackers.

In this section Android vulnerabilities are handled by application and operating system features.

a. Vulnerabilities of Android Operating Systems

Investigating Android OS architecture is the first way to understand its security. Android OS architecture separates into four main levels (applications, application framework, libraries, Android runtime and Linux kernel) and these levels can communicate between them. Figure 2 shows Android architecture.

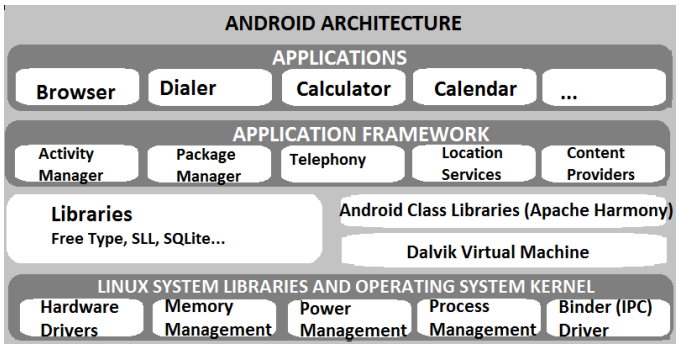


Figure 2: Android architecture [11].

Android OS is built on the Linux kernel and the Linux kernel is responsible for accessing memory, processor and network management, accessing physical devices [9]. Since 2003, Linux 2.6 kernel version which is considered safe is used in Android OS and this operating system includes these mechanisms; process isolation, interprocess communication security (IPC) and user-based authorization [5]. They can be sorted as below [12] ;

- User-based application permissions model,
- Extensible mechanism for secure IPC,
- Process isolating.
- The feature for removing risky parts of kernel for security.

In Linux mechanism, each application has a unique Linux user ID so this prevents distributing the other applications [13]. In the next layer Android native libraries which are written with C / C++ are located and applications acquire them via Java native interfaces [13]. The next layer is the Android runtime and it contains Android specific virtual machine (Dalvik virtual machine) and some core libraries [11]. The application framework layer provides device and application connection and application layer includes installed applications.

Android specific security mechanism is examined in four sections; sandboxing, application signing, permissions and accessibility of components [10]. Sandboxing means an application only access or use their files or other applications' open accessed files. Application sandboxing includes permissions, privileges, kernel access and authorizations for a mobile application [14]. The Sandbox for Android isolates each app's data and codes from other apps [15] and so it prevents buffer overflows, remote code execution, and stack smashing [13] .

Every developed application must be signed with a certificate whose private key is held by the application's developer and the Android system uses the certificate for determining of the application's author and for establishing a trust correlation between apps [16]. Also signature permission can be given to applications signed with the same certificate [9]. For instance vendors can use same certificate in different applications and application updates can be signed with same certificate [17]. Thus, application vulnerabilities can consist through software signatures.

Permission mechanism is required for some apps that perform special process and URI (Intent permission flags) permissions which required giving ad-hoc access to specific pieces of data [10]. Each application on Android has a unique sandbox folder and should be accepted the permissions for access to applications [14]. This prevents application to perform malicious behaviour [13].

Android applications are formed by combination of several separate components which can be called individually [18]. Application components can be set as private or public; public component can be accessed by other apps and private components are accessible only within the same application [10].

Android is an open accessed operating system and can be understood that Android OS cannot always safe. Operating system permissions are given to the actions can cause malicious programs to take advantage of certain features in the operating system or can cause greater damage. Especially due to Android is an open-accessed operating system, malicious applications can cause the following with operating system characteristics [3], these features are at Application Framework layer:

- reading and writing contacts and calendar entries;
- reading or sending e-mail messages, SMS and MMS;
- making phone calls;
- getting location;
- accessing the internet;
- accessing other smartphones using Bluetooth connection;
- reading and writing on file system.

Android is a multi-tasking operating system and therefore multiple applications can stay open. For this reason, malware authors can run their codes in the background and the codes run in the background until the end of battery power [19]. When considering, laptop and computers are turned off when not using but mobile devices should be always remained open.

Android operating system also allows using USB device for installing application; thus, many android users install applications from a USB device [7] which creates ways to malwares for spreading.

b. Vulnerabilities of Android Applications

According to the research on 400.000 android apps taking by Bit9, 72 percentage of all Android apps access at least one high-risk permission; %42 of apps access location data (GPS), %31 of apps access phone calls or phone, %26 of apps have access to personal info, %9 of apps use permissions that can cost and %1 of apps have access to account info [20]. That introduction is for understanding the big security risk of Android applications. Applications download from Android Market, Google Paly Store or an unknown source by innocent Android users and they always think "everything is ok" but a malware programmer or attacker is not innocent enough.

The user cannot find enough protection at Android security mechanism when he or she installed an app which infected a malware [21]. Since the Android market adopts the "anything goes" opinion, applications are not very closely monitored [4]. The android application review process is not strong like iOS and applications downloaded outside from Google Play Store are very risky despite applications downloaded from the Google Play Store [14].

Presenting such threats by attackers to user who installs the application is important. Vulnerabilities occurring in Android applications consist of configuration errors that made by developers or errors that caused from system users [22]. Privilege escalation attack is a good example for Android vulnerabilities. A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws. An application which has less permission (non-privileged) wants to access components of a more privileged application (privileged) to have the same privilege [10]. Making components of the application accessible by other components of applications causes of privileged escalation attack [10].

Attackers use reverse engineering for changing existing applications and application repackaging for writing malicious applications. For example,(1) a popular application is downloaded by an attacker, (2) the application is decompiled, (3) malicious code is inserted in it, (4) the application is signed again, (5) and published again with a similar or a different name on the Android Market or on a web page [3]. This operation, called *repackaging* is the most important technique to make malware installation to users with tricking [23]. They use repackaging especially banking applications and people always knows that mobile applications of these business companies are highly secure. Figure 3 shows a banking attack scenario by repackaging.

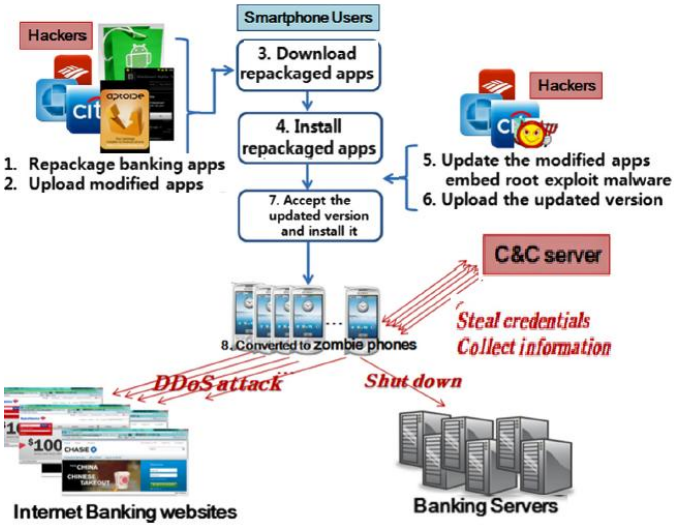


Figure3: Banking attack scenario [23].

There is a dozen of Android malware which affects users or devices in today's mobile world. A few mobile malware are investigated by affecting aspect in Table 2.

Table 2: Android Malwares

Malware	**What does it cause to?**
Exploit: MasterKey.a [8]	This malware takes advantage of Masterkey vulnerability and it makes changes to an app's code without affecting the cryptographic signature.
Trojan: FakeDefender.a	FakeDefender is a fake anti-spyware program for mobile devices.
Trojan: obad.a [8]	Obad variants gain administrator privileges wants to break the Android operating system's security layer. Obad collects and sends the following details about the device to a remote C&C server: the Media Access Control (MAC) address and IMEI, the operator name, the time and root access.
Trojan: sxjolly.a	It receives commands to send SMS messages or subscribe the device to a premium-SMS service
Trojan: tramp.a [8]	This malware monitors the user's SMS messages and steals all phone numbers from the user's phone. It can cause sending message, blocking call, getting current location, observing and contacting from Google Cloud Messaging [8]
Trojan: uten.a [8]	The malware obscures itself as a mobile analytic platform used by developers, "Umeng" SDK library.
Trojan: FakePlayer [19]	That looks like only a media player, but also send text messages without user's knowledge.
Exploit: Lotoor.g and Lotoor.j [24]	Also known as DroidDream – they were capable of executing without the user knowledge. The malware affects earlier versions of the Android OS and exploits known privilege escalation vulnerabilities to gain root access.

Trojan: Android.Pjapps [24]	This sends SMS messages to rate numbers and earning a commission for the cyber-criminals by user's bill. That Trojan also has botnet specialties.
Exploit: HippoSMS, [23]	That malware sent SMS messages to a coded premium-rated telephone number
Spyware: JackeeyWallpaper [23]	This spyware collects phone numbers, email addresses, IMEI numbers from infected device and hackers sell them to spammers.
Trojan: Geinimi [25]	It performs a lot of malicious behaviours such as using personal data, malicious advertising, and it has capable of create botnet and it causes to produce malware by repackaging applications.
Trojan: GGtracker [26]	Direct users to fake app stores to premium rate SMS services
Trojan: SMSspy [8]	It is used for monitoring banking application SMS
Trojan: Zitmo	Bank sends a confirmation message to Android user which Zitmo Trojan infects. Zitmo Trojan directs the confirmation message to the attacker.
Trojan: SMSZombie [27]	It seems like only wallpaper, but it collects SMS messages from China Mobile Payment system.
Trojan: Cawitt.A [27]	It causes turning compromised devices into botnet zombies via using Twitter connection. It collects data from the zombie device like IMEI number.

Using needed system resources and features, apps must request to AndroidManifest.xml [15]. AndroidManifest.xml includes permissions which applications and also malicious applications can use. Malware authors create crowded and complicated permission list for a normal mobile user, after than they ask for accessing permissions to users. After obtaining permissions, they can access their goals via the application. When the user installs the application, the permissions which are required to accept by the user are collected under the "Permissions" title. The required permissions in Android are indicated in Table 3.

Table 3: Android Permissions

Action	**Required Permission**
Read and write contacts [3]	Read_contacts Write_contacts
Read and write Calendar items [3]	Read_calendar, Write_calendar
Send SMS, read and write (all SMS functions) [3] [25]	Send_sms, Read_sms / write_sms Receive_sms Broadcast_sms
Access the Internet [3]	Internet
Use the telephony [3]	Call_phone
Access the camera device [10]	Camera
Access the external storage [3]	Read_external_storage Write_external_storage
Get location [17]	Access_fine_location, Access_coarse_location, Access_mock_location
Get some phone information (phone numbers, IMEI, IMSI, etc.) [25].	Read_phone_state
Read and write the user's browsing history and bookmarks [10]	Read_ history_bookmarks Write_history_bookmarks

Relationships between applications and permissions are shown in Figure 4.

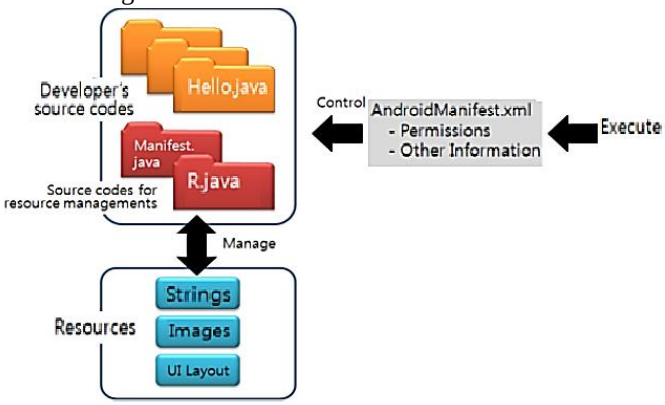


Figure 4: Relationships between applications and permissions [15].

Zhou and Jiang [28] observed 1260 malware samples and 49 malware families form Android markets in their research and 86% of malwares are formed repackaging apps, 36.7% of them contain privilege escalation and 93% from them have botnet capability. They use accessing internet, reading phone state, accessing network state, writing external storage and accessing Wi-Fi state permissions mostly. Top 20 permissions which are used by 1260 malware samples are shown in Figure 5.

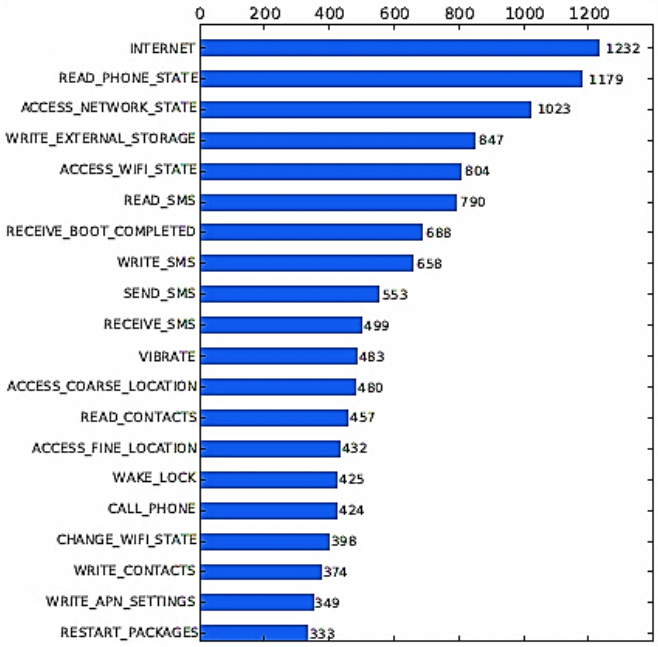


Figure 5: Top 20 permissions which are used by 1260 malwares [28].

B. *Security Vulnerabilities on IOS Based Systems*

A lot of malicious applications and vulnerabilities which affect iOS and iPhone users are available but they are not much as Android's. In this section iOS vulnerabilities are handled by application and operating system features.

a. *Vulnerabilities of OS Operating Systems*

Before handling iOS security, to examine the iOS architecture is useful. iOS have 4 abstraction layer; Core OS (kernel) layer to provide low-level network and common operating system services, the iOS Core Services Layer which is the foundation framework, Media Layer which provides graphics, audio and video technologies , Cocoa touch layer which is the basic framework for developing iOS applications (with multitasking, touch-based input technologies etc.) [14] . The layers are shown in Figure 6.

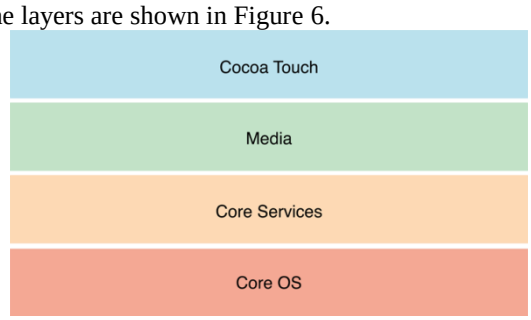


Figure 6: iOS architecture [29].

iOS security by operating system can be handled by system architecture. System architecture is discussed by Apple [30] with four aspects:

- *Secure Boot Chain:* Each step of boot up is cryptographically signed by Apple for ensuring chain of trust. The chain moves in this way; BootRom->LLB->iBoot->kernel->file system.
- *System Software Personalization:* It is used for prevent devices from being downgraded to older versions that lack the latest security updates.
- *App Code Signing:* iOS requires every code must be signed with Apple-issued certificate to ensure the apps comes from trusted and known source. It prevents unauthorized apps and malwares.
- *Runtime Process Security:* After applications are trusted and installed, iOS checks code signature of all executable memory pages to ensure that applications run without modified and the system works correctly. Sandboxing for iOS has been defined by Apple and accessing to system, network and hardware by applications has been controlled with limitations [14]. iOS is more secured than Android about sandboxing because each permissions on iOS sandboxing is protected by iOS and don't depend on applications.

In addition to these security features, iOS keychain is important for storing all passwords, keys and important short data. iOS keychain uses SQLite database [30] and keychain services uses the Common Crypto dynamic library [9]. iOS platform provides developers to write secure codes using iOS secure API and prevents malwares to infiltrate the App Store; iOS secure API located in Core Services layer and this based on Core OS Layer [9].

As discussed above, it is understood that iOS has a strong security infrastructure. It means iOS's doors are closed to malware and vulnerabilities with a large proportion.

b. *Vulnerabilities of iOS Applications*

When Apple iOS applications is thought about security, it can be seen clearly that iOS is quite safe from Android. Apple does not require an antivirus program because an iOS user only downloads applications from the App store and every application is carefully examined before being accepted into the App Store [14]. This indicates, iOS is quite safe from Android OS. Mobile malware doesn't affect iOS as Android devices because Android platform is an open platform but Jailbreaking is a big threat for Iphone and so iOS users, because jailbroken phones exposed to attacks by hackers.

Every app for iOS must be signed by Apple, and if a code doesn't carry Apple's signature or the signature doesn't match the code, iOS doesn't run this code [27]. Apple urges on every application must be signed distributed through its App Store, users want to use all applications from other stores like unofficial Cydia store and they make jailbreaking [26]. In July 2010 U.S. Libraray of Congress added jailbreaking to their lists which do not violate copyright protections and only a week later JailbreakMe 2.0 has emerged for Iphone users to jailbreak their phones [4].

There is important iOS malwares are available and as an example of iOS malwares iSAM has been selected. According to Damopoulos et al.(2011) iSAM is important iOS malware that can connect back to its boot master to update programming logic and iSAM includes 6 different malware specifies [4]:

- propagation logic;
- botnet control logic;
- denial of application services;
- denial of network services;
- collect confidential data stealthily;
- send a large number of malicious SMS.

Some of iOS threats are handled in Table 4.

Table 4: iOS threats

Threat	What does it cause to?
Data collecting: Aurora Feint [31]	This application removed from Apple store due to privacy concerns because it identifies online users to match their friends and send it unencrypted to the servers.
Data collecting: Storm8's iSpy [32]	"This makes use of the 'backdoor' method to access, collect, and transmit the wireless phone numbers of the iPhones on which its games are installed"
Vulnerability : libtiff [31].	It allows attackers to seize iPhone by vulnerabilities which found in TIFF processing library of the Safari browser
Worm : Ikee [33]	This is the world's first iPhone worm which targets jailbroken iPhones. It have Apple's default root password of "alpine". Also it shows to victims a message on wallpaper "ikee is never going to give you up".
Vulnerability : JailbreakMe	It is a security bug for Iphone users to access their phones completely

III. Security Analysis of New Generation Smart Mobile Phones

Guaranteeing the safety of mobile applications and test them has become imperative because of the proliferating malicious processes for mobile. Technically, the main problem is assessing the security of applications delivered to the market rapidly and another main problem is that security testing is expensive and manual process [34]. Because of this reason, mobile application writers don't care about the application's security if it is not about an application which requires security in real sense. In this section testing of mobile systems are handled.

A. *Testing of Mobile Systems*

As in the PCs, there are many testing techniques as penetration, fuzzing and automated testing tools. Also, many companies are available to perform these tests.

At first *fuzzing* can be handled. Fuzzing is a test technique, have been created towards applications by random or oriented. The purpose of fuzz testing is fuzzing the application automatic, semi-automatic or manual way, then identifying the system response and display the collapse status [35]. Security testing is a hard task because it is a form of negative testing. Fuzzing is a form of negative testing because that feeds unexpected input data to detect security vulnerabilities [21]. There are not enough successful techniques for fuzz testing apps for smartphone platforms [21].

Penetration testing is a test method used to provide information guarantee and testing is made by white hat hackers who are using the same tools as black hat hackers but with necessary permissions [36]. Penetration testing is increasingly required for Mobile Platforms (Android, iOS and BlackBerry) to help organizations or users understand risks and flaws of their mobile applications [36].

Mobile device and mobile application penetration test provides measuring mobile device security and that is useful for [37] ;

- making mobile application more secure,
- removing vulnerabilities from the mobile devices,
- securing mobile applications from all types of attacks.

For an example of automated Android testing tools, Droid Analyzer is important about its process. It first (1)decompresses the APK files of apps to extract permission information (2) parses the assembly codes to subtract risky APIs, strings and keywords associated with dubious cases. It detects mobile botnets, information leakage, and monetary loss by sending SMS or calling of premium services [23]. Processing of Droid Analyzer shown in Figure 7:

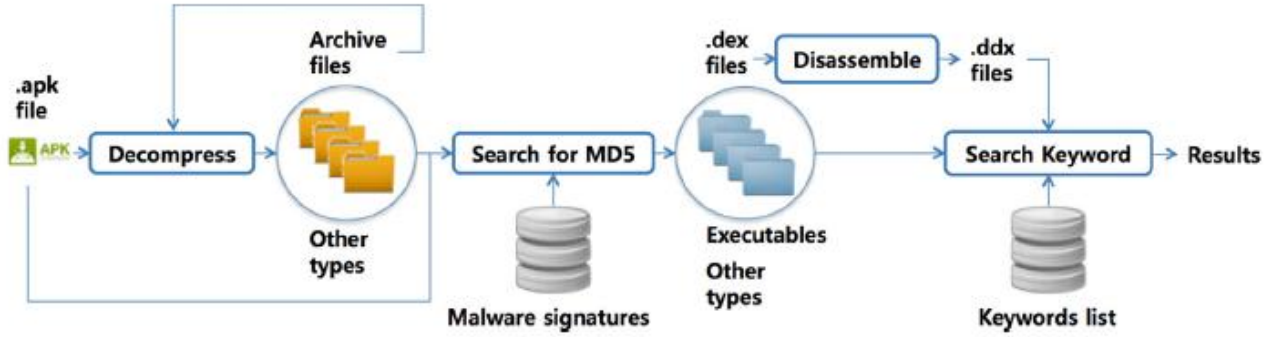


Figure 7: Process of Droid Analyzer which is a testing tool for Android [23].

Some of automatic testing tools and their process methods are shown in Table 4:

Table 4: Testing tools based on operating system

Testing Tool	Mobile OS	Process Method
DroidVulMon [38].	Android	Its functions are following running applications, services, process, network and routing status. DroidVulMon detects malicious applications which hides in mobile terminal and It determines that if an application makes attack to the terminal
Clang Static Analyzer [39]	iOS	It is used for analyse C and C++ codes for to find bugs and that can be used for decompiled iOS applications.
Flawfinder [40]	iOS	It is a program that examines source codes and reports to identify possible security weakness by risk levels. It can be used for identify C and C++ codes.
GNU Project debugger [41]	iOS	It allows to see what is going on `inside' another program while it executes
AppSec Labs iNalyzer [42]	iOS	It automates penetration test for iOS and attacks logic and forwards it to the targeted iOS application. It includes BruteForce, Fuzzing, SQL injection tests.
Testdroid (enterprise, cloud, recorder) [43]	Android and iOS	It provides managing server, application and recorded user actions with all aspects of automated testing on multiple real Android and iOS devices simultaneously.
Android SDK (Software Development Kit) [44].	Android	It includes a few GUI test tools but creating automation is limited because of Android's security properties.
Android Security Evaluation Framework (ASEF) [45]	Android	It detects unusual activities of apps, exposes vulnerable components and tests the apps on Android Virtual Device. It is helpful for android developers.
APSET [46]	Android	It is a model based security testing approach to detect data vulnerabilities in Android apps.

B. *Testing of Android Systems*

Malek et al. [34] focused on testing the security of Android apps and they submit a framework for developing tool-suite that realizes numerous test cases for detecting security vulnerabilities. They have created a framework because of the lack of fuzz testing apps frameworks and the framework presents automated test techniques for Android devices to find vulnerabilities quickly and properly. First step is to identify input – output interfaces; these may include GUIs, network interfaces, files, APIs, messages. Second step, input generators provides strengths for test cases so the framework tests a wide-range of conditions. The Test Execution Environment is used for executing the tests on lots of samples of the same application. The Exception Analysis engine researches on Runtime Error Repository and so this correlates the executed test cases with identified vulnerability problems. The last engine, The Interactive Reporting Environment uses Test Report Repository which stores the results of test analyses and enables the security analyst to evaluate the application' vulnerabilities.

For making penetration test for Android system, first issue to have a PC or laptop which installed web proxy. The main aim to enter between mobile device and server by PC with proxy installed and gain all control. A web proxy application like Charles web debugging proxy application can be installed. The certificate which is sent by Charles should be taken between trust certificates. For this operation, the certificate should be saved to SD card. After that, the certificate should be taken between trusted certificates. After these processes, Android application which is wanted to test can be opened and all the traffic can be analyse and data can be scanned for vulnerabilities.

C. *Testing of IOS Systems*

For making penetration test for iPhone, pre-requisites are [31];

- Mac Book running Snow Leopard OS
- Apple iOS (for testing iPhone applications)
- Charles Proxy21.
- SQLite Managers

The penetration testing processes explained by Shah [31] are disclosed with items according to priority;

- Installing the iOS SDK; Simulator is not available for download. It comes with iOS SDK and it must install.
- Using the correct iOS version for matching the development environment and test environment is important
- Setting up a proxy with a proxy tool (WebScarb, Paros, Burp etc.) than inserting SSL certificate in the keychain.
- Decompiling the application: This process is necessary to make more thorough security assessment by analysing the codes.
- Client based data is stored by iOS applications in SQLite database on the device. Information is unencrypted in the database and that can contain important data. SQLite Manager Firefox can be used for analyse SQLite database.
- To obtain the application's daily activities information, analysing log files is important.

IV. Comparison of some intelligent mobile phone operating systems for security

For comparing security differences between Mobile OS, Table 5 has been created.

Table 5: Different OS's general security features compares

Feature	Android OS	iOS OS	Blackberry OS
Data Storage	Have an external storage which can be accessible for treats [14]	Have no external storage and difficult for threats to access the storage [14]	Have an external storage and that can cause to spread malicious aps or codes.
Application Sandboxing	Each app has a different sandbox [14].	All aps use the same sandbox [14]	Each application process runs in its own sandbox
Application Permissions	Kernel and IPC enforced	Multiple sandboxing	JME class based
Application Access	Apps can't communicate directly with other apps, or access the other application directories.	Applications can communicate with other apps by their components.	-
App Stores	Android market or Google Play store divulges the permissions of apps.	Apple App store doesn't divulge the permissions of apps.	Blackberry App world divulges the permissions of apps.

For comparing some smart phone OS (IPhone 4s for iOS, Blackberry Bold 9700 for Blackberry, Samsung Galaxy S4 for Android OS were selected) for general security settings Table 6 has been created from Oh et al. [47] study:

Table 6: General Security Settings Compares of Different OS [47].

	(1) iOS	(2)Android	(3)Blackberry
Setting a device password to defen against any unauthorized physical access	(1) Settings _ General _ Passcode (2)Settings _ Location & Security _ Set password Settings _ Location & Security _ Set up screen lock Settings _ General _ Passcode (3)Users should protect the Blackberry device's individual PIN.		
Disabling unknown sources for application Installation to avoid third party applications	(2)Settings _ Applications _ Unknown sources (3) Options _ Security Options _ Application Permissions		
Turning off wireless properties (GPS, Bluetooth, Wi-Fi) when not in use to prevent serious threats.	(1)Settings _ General _ Network _ Wi-Fi Networks Settings _ General _ Bluetooth (2)Settings _ Location & Security _ Use GPS satellites Settings _ Wireless & network _ Wi-Fi/ Bluetooth		
Backing up data on the device to prevent loss of information	(1)Settings _ iCloud (2)Settings _ Privacy _ Back up my data		
Turning off location info to avoid applications to access location information.	(1) Settings _ Location Service (2) Disable- Allow Google's location service to collect anonymous location data. Collection will occur even when no applications are running.' (3) Options _ Security Options _ Application Permissions _ Location (GPS) = Deny		

V. Conclusion

Entering internet and mobile technologies into our lives has provided to complete works quickly and easily but it has opened the doors of new threats. Especially, attackers and hackers started to focus on seizing mobile systems or harming mobile user due to realizing mobile banking transactions with mobile smart phones and storing private correspondence and confidential data in the mobile phone.

In this paper, today's mobile threats and vulnerabilities were discussed via iOS and Android operating system. When hardware as well as software-security features of iOS operating system are handled, it is seen that every prevention method have been taken against malware and vulnerabilities. To not to allow installing applications without Apple signature and to check every code's signature when they are running reduce the risk of security. Also, to not installing applications any store except Apple App Store reduces the security risk greatly.

Android allows applications to be downloaded from every platform because of it is an open accessed free software. Security audits of loaded applications to Android Market or the Google Play Store are not analysed attentively. In addition, the risk of spreading malicious codes are pretty much due to Android operating system provides applications to access components of other applications.

Testing techniques and automated testing tools were also examined to ensure the security of applications and protect them from threats. Application testing process is important for the user towards all kinds of vulnerabilities which developers will not realize.

Dye et al. [48] has addressed the vulnerabilities for smart phones in application vulnerabilities, operating system vulnerabilities, cryptography concerns and other security concerns, and these can be useful for to be protected from vulnerabilities:

Application Vulnerabilities [48]*:* One of the most common sources of vulnerabilities for smart phones is the vulnerabilities in apps themselves. To not to be faced with application vulnerabilities, the things which should be done are below:

- The app code must not include external resources like external IP address.
- The programmer should limit input areas without weakness for example in a phone number field must be possible to input only numbers 0-9 rejecting the other words or symbols.
- When the application initializing if it fails, the behaviour of the app must be set to prevent the exploitation by a third party.
- All the temporary files which consist during operation of the app should be removed to prevent unauthorized access, to protect the integrity of stored data on the device and to preserve denial of service attacks.
- The external codes must validate the signature on all ActiveX and script languages.

Operating system (OS) vulnerabilities [48]*:* OS vulnerabilities are often the basis important security problems for smart phones or mobile devices. To not to be faced with application vulnerabilities, the things which should be done are below:

- An application should not change file permissions except that are required for its own work or should not cause the other applications change them.
- Any app using GPS must not forward the user's location to an external resource unless the user did not know where to go the data
- The app must not share permanent memory with other apps, must not read it from OS resources unless needed from app functions.
- Applications must be controlled to prevent maliciously accessed and used as a proxy to cause further damage to the device by using unauthorized code or reading susceptible data.

REFERENCES

[1] M. Baykara, R. Daş and İ. Karadoğan, «Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi,» %1 *1st International Symposium on Digital Forensics and Security (ISDFS'13),*, Elazığ, 2013.

[2] Gartner, «Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in Third Quarter of 2013,» November 2013. [Online. Available: http://www.gartner.com/newsroom/id/2623415. [accessed January 2014].

[3] P. Pocatilu, «Android Applications Security,» *Informatica Economica,* vol 15, no. 3, pp. 163-171, 2011.

[4] M. L. Polla, F. Martinelli and D. Sgandurra, «A Survey on Security for Mobile Devices,» *IEEE Communications Surveys & Tutorials,* vol 15, no. 1, pp. 446-471, 2013.

[5] Ö. F. Acar, «Mobil Cihazlarda Güvenlik Android and IOS Karşılaştırması,» Tübitak Bilgem, 9 June 2013. [Online. Available: http://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-cihazlarda-guvenlik-android-ve-ios-karsilastirmasi.html. [18 January 2014].

[6] Blue Coat, «Blue Coat Systems 2013 Mobile Malware Report,» November 2013. [Online. Available: http://www.bluecoat.com/sites/default/files/documents/files/BC_2013_Mobile_Malware_Report-v1d.pdf. [accessed January 2014].

[7] Q. Li and G. Clark, «Mobile Security:A Look Ahead,» *Security & Privacy, IEEE,* vol 11, no. 1, pp. 78-81, 2013.

[8] f-secure, «Mobile Threat Report,» November 2013. [Online. Available: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf. [accessed January 2014].

[9] G. Delac, M. Silic and J. Krolo, «Emerging Security Threats for Mobile Platforms,» %1 *Proceedings of the 34th International Convention*, Opatija, 2011.

[10] P. P. Chan, L. C. Hui and S. Yiu, «A Privilege Escalation Vulnerability Checking System for Android Applications,» %1 *Communication Technology (ICCT), 2011 IEEE 13th International Conference on Digital Object Identifier*, 2011.

[11] S. Khan, M. Nauman, A. T. Othman and S. Musa, «How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms,» %1 *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, Kuala Lumpur, 2012.

[12] R. J. G. Vargas, R. G. Huerta, E. A. Anaya and A. F. M. Hernandez, «Security Controls for Android,» %1 *Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, Sao Carlos, Brazil, 2012.

[13] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev and C. Glezer, «Google Android:A Comprehensive Security Assessment,» *Mobile Device Security,* pp. 35-44, March /April 2010.

[14] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan and N. E. Othman, «Comparison Between Android and iOS Operating System in terms of Security,» %1 *8th International Conference on Information Technology in Asia (CITA)*, Borneo Malaysia, 2013.

[15] T. Cho, J.-H. Kim, H.-J. Cho, S.-H. Seo and K. Seungjoo , «Vulnerabilities of Android Data Sharing and Malicious Application to Leaking Private Information,» %1 *Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, Da Nang, 2013.

[16] Android Open Source Project, «Signing Your Applications,» April 2011. [Online. Available: http://developer.android.com/tools/publishing/app-signing.html. [accessed January 2014].

[17] W. B. Tesfay, T. Booth and K. Andersson, «Reputation Based Security Model for Android Applications,» %1 *11th International Conference on Trust, Security and Privacy in Computing and Communications* , Liverpool, United Kingdom, 2012.

[18] Android Open Source Project, «Introduction to Android,» android.com, 2013. [Online. Available: http://developer.android.com/guide/index.html. [accessed 2 February 2014].

[19] S. Gold, «Android insecurity,» *Network Security,* pp. 5-7,

October 2011.

[20] Bit9, «Pausing Google Play: More Than 100,000 Android Apps May Pose Security Risks,» October 2012. [Online. Available: https://www.bit9.com//files/1/Pausing-Google-Play-October2012.pdf. [accessed January 2014].

[21] R. Mahmood, N. Esfahani, T. Kacem, N. Mirzaei, S. Malek and A. Stavrou, «A Whitebox Approach for Automated Security Testing of Android Applications on the Cloud,» %1 *Automation of Software Test (AST), 2012 7th International Workshop on Digital Object Identifier*, Zurich, Switzerland, 2012.

[22] F. Şengül and A. Varol, «Ağ Saldırı Yöntem and Tekniklerinin İstatistiksel Analizi,» %1 *1st International Symposium on Digital Forensics and Security*, Elazig/ Turkey, 2013.

[23] S.-H. Seo, A. Gupta, A. M. Sallam, E. Bertino and K. Yim, «Detecting mobile malware threats to homeland security through static analysis,» *Journal of Network and Computer Applications*, vol 38, pp. 43-54, 2014.

[24] Computer Fraud & Security, «Android marketplace hit by malware,» *Computer Fraud & Security*, p. 3, March 2011.

[25] W. Tang, G. Jin, J. He and X. Jiang, «Extending Android Security Enforcement with A Security Distance Model,» %1 *Internet Technology and Applications (iTAP)*, Wuhan, 2011.

[26] Computer Fraud & Security, «More mobile security glitches,» *Computer Fraud & Security*, vol 2011, no. 7, p. 3, 2011.

[27] S. Mansfield-Devine, «Android malware and mitigations,» *Network Security*, pp. 12-20, November 2012.

[28] Y. Zhou and X. Jiang, «Dissecting Android Malware: Characterization and Evolution,» %1 *33rd IEEE Symposium on Security and Privacy*, San Francisco, CA, 2012.

[29] Apple Inc., «About the iOS Technologies,» Apple.com, 2013. [Online. Available: https://developer.apple.com/library/ios/documentation/miscellaneous/conceptual/iphoneostechoverview/Introduction/Introduction.html. [accessed 2 February 2014].

[30] Apple Inc., «iOS Security,» Apple Inc., U.S., 2012.

[31] K. Shah, «Penetration Testing for iPhone / iPad Applications,» 2012. [Online. Available: http://www.mcafee.com/au/resources/white-papers/foundstone/wp-pen-testing-iphone-ipad-apps.pdf. [accessed 20 January 2014].

[32] D. Goodin, «Backdoor in top iPhone games stole user data, suit claims,» The Register, 6 November 2009. [Online. Available: http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/. [accessed 13 January 2014].

[33] D. Goodin, «World's first iPhone worm Rickrolls angry fanbois,» The Register, 8 November 2009. [Online. Available: http://www.theregister.co.uk/2009/11/08/iphone_worm_rickrolls_users/. [accessed 18 01 2014].

[34] S. Malek, N. Esfahani, T. Kacem, R. Mahmood, N. Mirzaei and A. Stavrou, «A Framework for Automated Security Testing ofAndroid Applications on the Cloud,» %1 *2012 IEEE Sixth International Conference on Software Security and Reliability Companion*, Maryland, USA, 2012.

[35] İ. Baliç, «Fuzzer/Fuzzing Kavramı and Güvenlik Zâfiyetleri Bölüm 1,» 15 11 2013. [Online. Available: http://ibrahimbalic.com/2013/fuzzerfuzzing-kavrami-ve-guvenlik-zafiyetleri-bolum-1/. [accessed 01 2014].

[36] J. Yeo, «Using penetration testing to enhance your company's security,» *Computer Fraud & Security*, vol 2013, no. 4, pp. 17-20, 2013.

[37] Codec Networks, «Mobile Application penetration testing,» 2012. [Online. Available: http://www.codecnetworks.com/Services%20Flyer/Mobile%20Application%20Penetration%20Testing.pdf. [accessed 12 January 2014].

[38] Y. J. Ham, H.-W. Lee, J. D. Lim and J. N. Kim, «DroidVulMon - Android based Mobile Device Vulnerability Analysis and Monitoring System,» %1 *Seventh International Conference on Next Generation Mobile Apps, Services and Technologies*, Prague, Czech Repulbic, 2013.

[39] Clang Sataic Analyzer, «Clang Sataic Analyzer,» Clang Sataic Analyzer, [Online. Available: http://clang-analyzer.llvm.org/. [accessed 18 January 2014].

[40] Dwheeler, «Flawfinder,» dwheeler, [Online. Available: http://www.dwheeler.com/flawfinder/. [accessed 22 January 2014].

[41] GNU Project Debugger, «GDB: The GNU Project Debugger,» gnu.org, 08 January 2014. [Online. Available: https://www.gnu.org/software/gdb/. [accessed 22 January 2014].

[42] App Sec Application Security Lab, «AppSec Labs iNalyzer,» App Sec Application Security Lab, 2014. [Online. Available: https://appsec-labs.com/iNalyzer. [accessed 21 January 2014].

[43] Testdroid, «Testdroid Application,» testdroid, 2014. [Online. Available: http://testdroid.com/. [accessed 20 January 2014].

[44] T. Takala, M. Katara and J. Harty, «Experiences of System-Level Model-Based GUI Testing of an Android Application,» %1 *Fourth IEEE International Conference on Software Testing, Verification and Validation*, Berlin, Germany, 2011.

[45] P. Patel, «ASEF - Android Security Evaluation Framework,» Qualys, 2013. [Online. Available: https://code.google.com/p/asef/. [accessed 2 February 2014].

[46] S. Salva and S. R. Zafimiharisoa, «Data vulnerability detection by security testing for Android applications,» %1 *Information Security for South Africa, 2013*, Johannesburg, 2013.

[47] T. Oh, B. Stackpole, E. Cummins, G. Carlos , R. Rahul and S. Lim, «Best Security Practices for Android, BlackBerry, and iOS,» %1 *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT)*, USA, 2012.

[48] S. M. Dye and K. Scarfone, «A standard for developing secure mobile applications,» *Computer Standards & Interfaces*, vol Article in Press, 2013.

A Survey on Operating Systems for Wireless Sensor Networks

A. Akbaş[1] and Muaz Gültekin[2]

[1]Yalova University, Istanbul/Turkey, ahmetakbas@yalova.edu.tr
[2]Yalova University, Istanbul/Turkey, muaz.gultekin@gmail.com

***Abstract*— Wireless sensor nodes consisting of sensors, systems, wireless communication equipment and operating system have rapid development and become an exciting new technology. Recently, use of Wireless Sensor Networks (WSNs) which consist of many sensor nodes that provide collection of data and transmission of information to sinks is growing highly. There are many constraints on wireless sensors such as battery management, processing capacity, memory etc. In this study, we try to present brief information about operating system of WSNs. We analyze the most popular WSN operating systems in many aspects.**

***Keywords*— Operating System, TinyOS, EPOS, Wireless Sensor Networks.**

I. Introduction

A WSN consists of many sensors that randomly placed required areas, communicate with sink and between each other (Figure 1). These sensors gather physical data depending on features of different locations separately process the data and by transmitting those to the neighbor sensor send to the upmost layer sink. Sink which has more advanced features than other sensors collects all incoming data and via the internet or satellite convey to the user by transmitting from physical to virtual environment.

WSNs are generally used such as nature monitoring (plants, animals etc.), weather forecasting, keeping under control far places, in the health sector following up patient, controlling harmful environment to human health, in military enemy tracking, intelligent agriculture, environmental monitoring and protection areas [1].

A. Advantages and Disadvantages of WSNs

Due to the easy locating, WNSs can be placed dangerous to human regions and any other places. Normally a single sensor can work in a short distance but many sensors provide communication in a big area since they work simultaneously. The sensors got tiny proportions and more features with the development of technology and the rapid development of the radio frequency (RF) while communicating with environment in real time they consume less energy.

When any sensor deteriorated, data loss doesn't occur thanks to too much data that collected with many sensors. Despite there are a lot of sensors, the cost is low so that the sensors are small and easy locating [2]. WSNs do not require cabling and infrastructure. So moving them to other areas is quite easy.

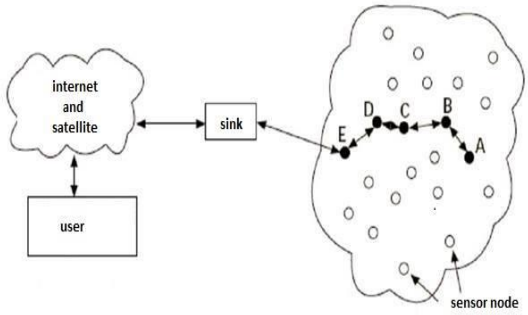


Figure 1: Structure of a Wireless Sensor Network.

So far, many studies have been submitted about WSNs. In this study, we try to present brief information about operating system of WSNs. The most known operating systems of WSNs are TinyOS, SOS and EPOS [1].

B. WSN Security

WSN security has great importance for using in military and transmitting critical data. Since the sensors are communicate in a wireless environment, external interference or routing the data packets is easier. This requires giving more importance to the security.

Due to the sensors' structural features such as low-capacity memory, low-energy, limited band width, limited processing power and hardware-related problems, they are incline to malfunction. By reason of couldn't calculate bit operations of Processor's computational unit and limited computational power, traditional security algorithms couldn't be used. So security vulnerability occurs.

Sensors can exist in places where physical environment conditions unfavorable such as sea, open-air, destruction zone. These physically insecure environments, makes possible the sensors are taken by malicious people. Due to the low cost usage is preferred and also they can be used in hazardous areas so that does not require maintenance.

Implemented different security counter-measures to prevent problems such as loss of data packets during the communication between nodes, changed data content, data integrity. In data security stages, data encryption is encoding data with private keys. Data authentication is used to control weather the data transmitted to the other sensor and controlling the data whether is changed is data integrity. Data freshness

ensures whether the data is recent. But, because of the structural features of sensors, all security solutions can't be implemented properly.

II. MANAGEMENT OF WSNs

Any WSN operating system should handle basic operations such as functionality, power management, simple process mechanisms, sensing hardware abstraction and a configurable communication stack.

The operating system handle the resources on each node, supply a layer of abstraction for the hardware, and offer the system developer a programming interface which allows SW applications to be efficiently implemented. Figure 2 and Figure 3 show the hardware organization of a sensor node and organization of a software layers, respectively.

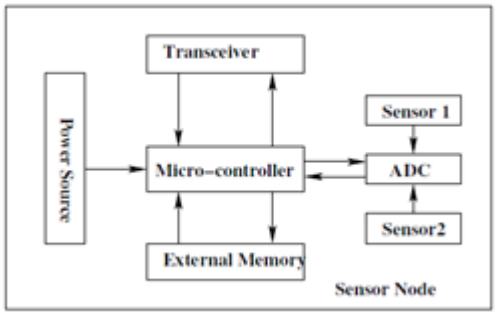


Figure 2: Sensor node architecture.

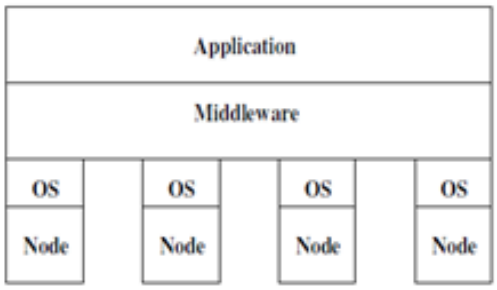


Figure 3: Software layers.

The main activities of a sensor node are listed below

- Processor management
- Memory management
- Device management
- Scheduling policies
- Multi-threading
- Multitasking
- Proper concurrency mechanisms
- Application Programming Interface (API)

The most known WSNs operating systems are; TinyOS, Contiki OS, Lorien OS, MANTIS OS (Multimodal networks of in-situ sensors) and EPOS (Embedded Parallel Operating System). While an operating system of WSN is developed some issues must be considered. These are:

A. Power Management

Battery management is the main issue of WSN. The aim of the power management is long life battery regard to restricted resources. So operating system is provide necessary mechanisms in order to consume the power in optimized way to extend the life of the WSN.

Wireless sensor operating system should adjust power consumption periodically. In order to save energy WSN has three main phase in idle or sleeping state. These phase are Power down, power save and idle. Thanks to these mechanisms operating system provision a clean and brief abstraction for power management [1, 3].

Wireless sensors act as transceiver and receiver state. Wireless sensors consume more energy in receiver position according to receiver position. On the other hand wireless sensors consume more energy in idle phase according to transceiver position. So this mechanism should be handled by Operating system efficiently.

B. Processing Power

WSNs consume power while try to accomplish some task. Some processes consist of many computational transactions while some consist of few computational transactions. Many task handled at the same time. That's why operating system should have schedule policy which operates process efficiently according to the policy.

C. Memory Management

Memory is one of the main concerns of wireless sensors. The main issue of memory in wireless sensor is limited memory. Due to limited memory, operating system should handle memory management efficiently. Another problem is Sensor nodes also have nonvolatile external data storage mechanism. That's why every program module stored in the memory and executed from here. So operating system should handle this mechanism efficiently [1].

D. Portability

Portability can be summarized as making software run on the different hardware platform. So operating system should be easily applied and portable. Another expectation is operating system should be easily configurable to different customized hardware platform [2].

E. Multitasking

At certain time wireless sensors should perform more than one task. For instance a node of WSN while collecting data from neighbor sensor the node sends message to the main. According to D Janakiram, these operations can be listed as shown below [4]

1. Sense the data
2. Collect data from other neighborhood sensor nodes
3. Aggregate the data based on the certain conditions provided
4. Encrypt/decrypt the data before processing forwarding

5. Route the data to the sink node

III. OPERATING SYSTEMS FORWSNs

A. TinyOS

TinyOS is open source project and developed at the University of California in Berkeley [2]. TinyOs is event based operating system. Event-driven properties provide TinyOS using CPU efficiently. In TinyOS, when an event is triggered, all the tasks related to the event that send out the signal are disposed rapidly. After that event and all the related tasks are disposed over, the untapped CPU will be turned into the IDLE Mode rather than searching the next dynamic event actively [5]

TinyOS operating system is developed using NesC. TinOS's program also developed in nesC environment. TinyOS operating system using split phase execution model. Thanks' to this model microcontroller sends signal to I/O (hardware) and handled independently from microcontroller. TinyOS also provide a concurrency system which accomplish by task scheduler. Thanks' to the scheduler mechanism no task preempt each other. Each task runs until completion and the next task is started after that (Figure 4).

TinyOS does not use multi-threading mechanism. That means every task use the same stack and task scheduler based on first in first out (FIFO) approach. Using the same stack at runtime bring memory perseveration. If there is no more task in stack TinyOS sets the system into sleep mode [5].

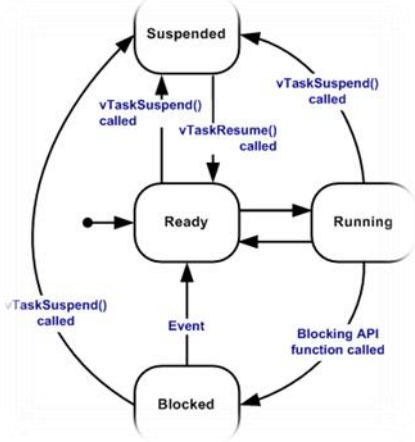


Figure 4: TinyOS event handler

The communication architecture of TinyOS uses the concept of Active Messages (AM) these are small packets of size 36 bytes and a one byte handler ID.

TinyOS operating system use event-driven model. So this approach has some disadvantages like low programming flexibility, non-preemption. According to experiment TinyOS operating system has three limitations. New platform support, application construction, and reliable operation are the main three issue of TinyOS that have to be considered.

B. SOS

SOS is event based an operating system and developed in C programming environment. SOS operating system using component based approach so, SOS operating system similar to TinyOS with many aspects. SOS operating system usees run to completion concurrency mode.

On the other hand TinyOS more flexible than SOS [4, 5 and 7]. TinyOS operating system use the single stack structure, SOS also use the same approach but SOS provides stack priority mechanism.SOS also allow dynamically new component contribution thanks to dynamic linking mechanism. In Figure 5 how dynamic linking is handled in SOS environment is shown.

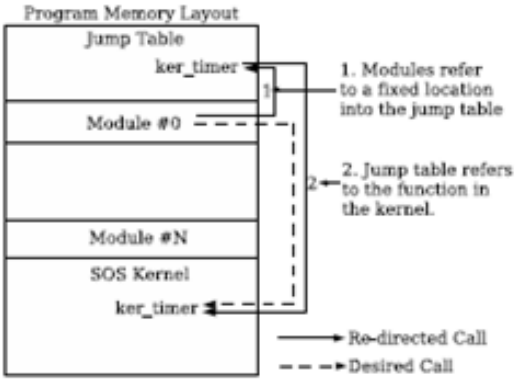


Figure 5: Linking in SOS

Distribution protocol listens for ad of new modules if a new model catches insertion module initialized. If Distribution model get an ad of a module

- It checks if the module is an updated
- It checks version of a module already installed on the node
- It checks the node is interested in the module and has free program
- It checks memory for the module
- It checks the module and immediately examines the metadata (contains the Unique identity for the module, the size of the memory)

If the steps that listed below is not handled SOS kernel is unable to allocate memory for the local state of the module.

Dynamic linking is handled by using a script. Metadata file contain ID, packet header information and packet memory information. This linking script using pointer addresses to the packet. All these operations are invoked by SOS kernel.

C. Mantis (MOS)

Mantis is an open source and thread based operating system. Mantis operating system is developed in C-programming language environment for wireless sensor networking platform. MANTIS gets its name from Multi-modal system for Networks (Figure 6).

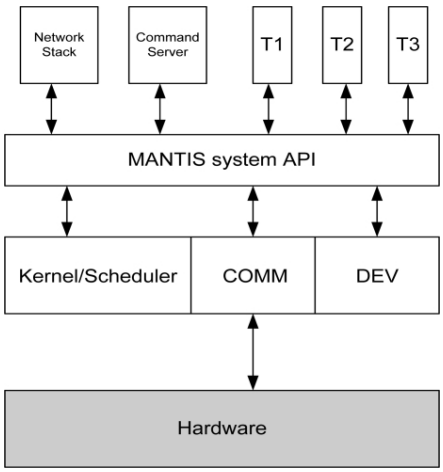


Figure 6: Mantis OS

The main features of MOS (Mantis Operating System) are as follows:

- Developer friendly C API with Linux and Windows development environments
- Automatic preemptive time slicing for fast prototyping
- Different platform support such as MICA2, MICAz, and TELOS motes
- Energy-efficient scheduler for duty-cycle sleeping of sensor node
- Small footprint (less than 500B RAM, 14KB flash)

The last version of MOS provides multi-threading cross platform for WSN. While the event driven based model considering task's size is mandatory, the thread driven based model supplies flexible environment [6 and 7].

MOS provide en efficient energy power mechanism. It provides sleep function which save energy by activate microcontroller sleep mode. MOS provide

- multimodal prototyping
- dynamic reprogramming
- remote shells
- management of in-situ sensors through dynamic reprogramming and remote login.

IV. CONCLUSION

In this survey study WSN operating systems was discussed in many aspects. Another contribution of this paper is discussing operating system technical structural. There are lots of open problems that need further investigation to make the OS provide stronger support for WSNs. providing a convenient programming model and a suite of useful system services on the resource constrained sensor nodes is a continuing focus of current research. However, design trade-offs among small footprint, energy efficiency, reliability, Real-time guarantees, configurability, and programming convenience, need to be made with respect to different application scenarios.

REFERENCES

[1] Indian Institute of Technology Madras: Operating Systems for Wireless Sensor Networks. May, 2007
[2] TinyOS: An Operating System For Sensor Networks , pp. 570–578
[3] University of California, A Dynamic Operating System for Sensor Nodes, http://nesl.ee.ucla.edu/projects/sos/.
[4] J. Raj Kumar, Goel Institute of Technology, A Comparative Analysis of Wireless Sensor Network Operating Systems, Int J EnggTechsciVol 1, pp.41-47, 2010,
[5] Fakultät für Informatik, Comparison of Operating Systems TinyOS and Contiki, April 2011
[6] Federal University of Santa Catarina, Operating System Support for Wireless Sensor Networks , Wireless Sensor Networks Department of Computer Science: A Note on Scaling Wireless Sensor Network. December, 2005
[7] Berkley: T2: A Second Generation OS for Embedded Sensor Networks, Mar. 2003

Adli Doküman İnceleme İçin Otomatik Hiperspektral Luminesans Görüntüleme Sistemi

A. Kholmatov, F. Hacizade, G. Bektas

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
TÜBİTAK-BİLGEM, Gebze/Kocaeli
{ alisher.kholmatov, fikret.hacizade, gokhan.bektas}@tubitak.gov.tr

***Abstract*— Forensic document investigation possesses a wide arsenal of tools and techniques aimed at analyzing questioned documents for their authenticity, integrity, ownership, revelation of covert information as well as analysis of age and restoration of other associated document properties. Hyperspectral image processing based document investigation systems are widely adopted for pen ink comparison as well as for disclosure of erased and covered writings. Such systems are being appreciated for having non-destructive nature and fast processing time. Luminescence analysis, where document is excited by a certain light wavelength and then inks are expected to emit light at other wavelengths, is also commonly used to compare document inks. However, luminescence analysis in its classical form is prone to error as comparison is based on the amount of emanation not the spectrum of the luminescence. In this work, we present a device and a method for automatic hyperspectral luminescence imaging. Luminescence spectrums are obtained at a high spatial resolution within a field of interest, which are then compared using developed spectrum analysis algorithms. The output of the realized system is a color coded image indicating proximity of underneath luminescence spectra.**

***Özet*— Adli belge inceleme biliminde, incelenen belgenin, orijinalliği, bütünlüğü, aidiyeti, yaşı ve diğer ilgili öğelerinin analiz edilmesi için oldukça geniş bir yelpazede yöntemler kullanılmaktadır. Hiperspektral görüntüleme sistemleri, mürekkep karşılaştırmada ve silinmiş yada karartılmış yazıların ortaya çıkarılmasında sıklıkla kullanılmaktadırlar. İncelenen belgeye zarar vermemesi ve hızlı işleme zamanı bu tür sistemlerinin başlıca üstünlükleridir. Luminesans analizi (incelenen numunenin belirli bir dalgaboyundaki ışıkla uyarıldıktan sonra başka dalgaboylarında ışıma yapması) de mürekkepleri karşılaştırmak için sıklıkla kullanılmaktadır. Fakat, luminesans spektrumunu incelemek yerine sadece belirli bir dalga boyundaki ışıma miktarına bakılan klasik yöntemle yapılan analizlerde hatalar ortaya çıkabilmektedir. Bu çalışmada otomatik hiperspektral luminesans görüntüleme cihazı ve ilgili yöntemleri tanıtılmaktadır. İncelenen bölgenin luminesans spektrumu yüksek uzamsal cözünürlükte elde edilerek geliştirilen yöntemlerle işlenerekanaliz edilmektedir. Geliştirilen sistem analiz sonucu olarak spektrum benzerlikleri renkle kodlanmış bir görüntü üretmektedir.**

I. GİRİŞ

Adli doküman inceleme kapsamında değerlendirilen belgenin maruz kaldığı veya belge üzerinde yapıldığı iddia edilen tahrifatın türüne göre inceleme yöntemleri ve ekipman kullanılmaktadır. Hiperspektral görüntüleme i) sonradan eklenen, değiştirilen, silinen veya karartılan yazı ve işaretlerin tespitinde, ii) resmi belgelerdeki güvenlik unsurlarının doğrulanmasında (ör. pasaport, vize ve paralardaki şifrelenmiş saklı görüntü ve optik işaretlerin çözümlenmesi ve doğrulanmasında), iii) belgelerdeki mürekkep ve baskı malzemelerinin tespitinde, iv) belgeler üzerinde bırakılan parmak izi, lif ve benzeri delillerin tespitinde yaygın olarak kullanılmaktadır. Hiperspectral görüntülemenin ana avantajları incelenen belgeyi tahrif etmemesi, çabuk sonuç vermesi ve göreceli olarak fazla uzmanlık gerektirmemesi olarak özetlenebilir.

Adli doküman inceleme laboratuvarlarında sıkça kulanılan Video Spektral Karşılaştırıcı (VSC) yöntemine dayalı cihazlardan farklı olarak hiperspektral görüntüleme teknolojisine dayalı cihazlar belge üzerindeki farklı mürekkepleri birbirinden ayrıştırma işleminde mürekkeplerin yansıma (reflectance), yutulma (absorbance) ve geçirgenlik (transmittance) spektrumu ölçerek analiz yapmaktadırlar. Ayrıca, mürekkeplerin luminesans özelliği de incelenebilmektedir. VSC yöntemiyle çalışan cihazlar luminesans spektrumunu değerlendirmek yerine sadece tek bir dalga boyundaki luminesans şiddete bakılarak karar verilmektedirler. Bu durum, özellikle aynı kalemin, farklı basınç uygulanarak kullanıldığı yazılarda, yazıların farklı kalemlerle yazılmış gibi algılanmasına ve dolayısıyla hatalı karar verilmesine neden olabilmektedir.

Bu çalışmamızda luminesans spektrumu tarama yöntemi ve analiz algoritmaları irdelenmektedir. Ayrıca, belgelerdeki sonradan eklenen, değiştirilen, silinen veya karartılan yazı ve işaretlerin tespiti için hiperspektral luminesans görüntüleme sistemi geliştirilmiştir.

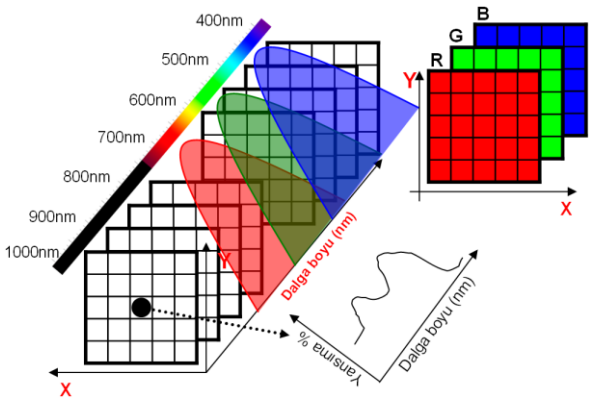
II. HİPERSPEKTRAL GÖRÜNTÜLEME

Mürekkeplerin maruz kaldığı ışığı saçılmalı (diffuse) yansıtma karakteristikleri, mürekkepleri oluşturan temel maddelerin yutulma katsayılarıyla (absorbance coefficient) orantılıdır. Farklı maddelerden üretilen mürekkepler belirli dalga boylarındaki ışığı soğurmaktadırlar (absorbance). Işığın yutulmayan spektral bileşenlerinin bir kısmı ise saçılmalı yansıtmayla geri dönmektedir. Ölçülen dalgaboyu aralığındaki yansıtma ve soğurma spektrumları maddelerin (bu çalışma kapsamında ise mürekkeplerin) bir çeşit imzası olup bunların tespiti ve sınıflandırılmasında yaygın olarak

kullanılmaktadırlar. [1].

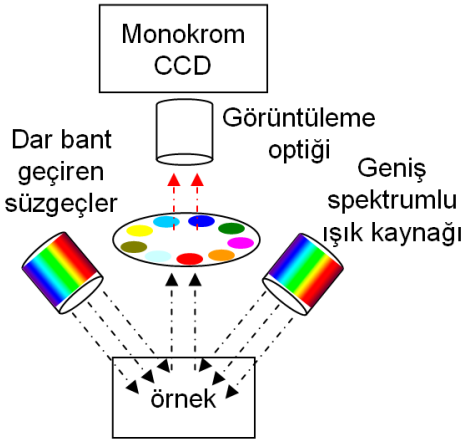
İncelenen belgenin (yada bir bölümünün) hiperspektral görüntüsünü elde etmek için morötesi dalga boyu bölgesinden (~350nm) başlayıp yakın kızılötesi dalgaboyuna kadar (~1100nm) 10-20nm dalgaboyu adımlarla peş peşe sayısal görüntüler çekilerek istiflenmektedir. Çekilen bu görüntü serisine yaygın olarak hiperspektral görüntü küpü de denilmektedir. Öte yandan, multispektral görüntü de bu minvalde sıkça duyulan bir tabir olup, hiperspektral görüntüden farklı olarak sadece birkaç (multi) dalgaboyuna karşılık gelen bant imgeleri içermesinden, bazı durumlarda ise bant imgelerinin sürekli olmayan (not continuous) dalgaboyu aralığından elde edildikleri ve belirli spektrumları kapsamadıkları için bu adı almaktadır. Hiperspektral görüntülerde sürekli dalgaboyu aralığına karşılık gelen onlarca hatta yüzlerce bant imgesi mevcut olduğundan her bir piksel için spektrum elde edilmekte ve spektral analiz uygulanabilmektedir.

Hiperspektral görüntü, belgenin uzamsal (spatial) ve spektral içeriğini bir arada barındırmaktadır. Küp içerisindeki her çerçeve belgenin belirli bir dalgaboyundaki görünümüne karşılık gelirken, aynı pozisyondaki piksel değerleri ise belgenin o noktasındaki maddenin (mürekkep, kağıt, lif vs.) spektrumunu oluşturmaktadırlar. Buna karşılık, geleneksel sayısal renkli kameralar ışık spektrumunu genişçe örtüşen kırmızı (R), yeşil (G) ve mavi (B) kesitlere ayırarak kaydetmekte ve bunları birleştirdiğinde göze hoş gelen gerçekçi görüntüler oluşturmaktadırlar. Hiperspektral görüntüden alıştığımız renkli görüntüyü elde etmek mümkündür (tersi ise mümkün değildir). Şekil 1'de hiperspektral görüntü küpü ile geleneksel renkli kameranın görüntüsü şematik olarak gösterilmektedir.



Şekil 1: Hiperspektral (solda) ve geleneksel 3 kanallı (RGB) renkli (sağda) görüntülerin şematik gösterimleri. Hiperspektral görüntü küpü belgenin uzamsal içeriğinin yanısıra her piksel için spektral verileri de içermekte, RGB gürüntüsü ise görünür dalgaboyu spektrumunu genişçe örtüşen 3 süzgeçle örneklemektedir.

Yansıma spektrumu tabanlı hiperspektral görüntü tarama cihazlarının değişik çalışma prensipleri vardır [2]. Bu çalışmada Şekil 2'de gösterilen yönteme benzer bir tasarım benimsenmiştir. Geniş spektrumlu ışık kaynağı kullanılarak incelenen belge aydınlatılmaktadır. Düzgün (uniform) aydınlatma sağlamak için ise ışık kaynakları belirli açılarda ayarlanmaktadırlar. Belgenin yansıma spektrumunu elde etmek için görüntüleme optiği önünde dar bant geçiren süzgeçler (narrow bandpass filter) değiştirilerek ışınımın çok ince spektral bant imgeleri tek renk CCD kamera kullanarak peş peşe kaydedilmektedir. Kullandığımz filtre 1nm hassaslığında adımlarla ışınım spektrumunun örneklenebilmesini sağlamaktadır. Alternatif tasarım olarak, spektrograf ve mekanik tarama düzenekleri de kullanılabilmektedir. Spektrograf, örneğin üzerindeki tek çizgiye karşılık gelen tüm spektrumu aynı anda örneklemektedir. Tüm örneğin hiperspektral görüntüsünü elde etmek için ise mekanik tarama kullanılmaktadır [2].



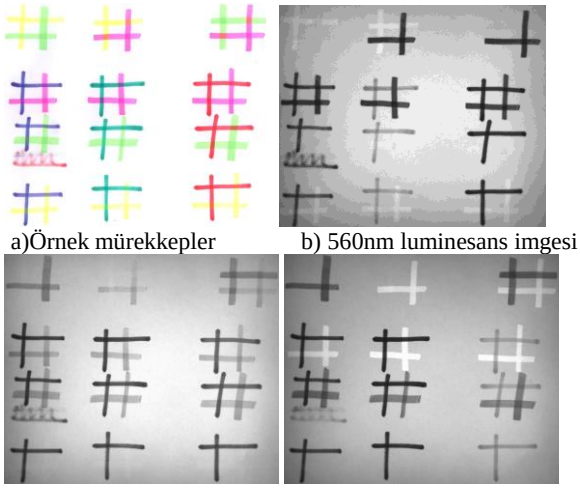
Şekil 2: Hiperspektral görüntüleme sisteminin ana bileşenleri ve temel çalışma prensibi.

Gerçek hayatta doküman inceleme uzmanları, belgenin hiperspektral görüntüsünü elde etmek için videospektrograf cihazları kullanılmaktadırlar. Buna örnek olarak şekil 6'da gösterilen ve TÜBİTAK BİLGEM-UEKAE tarafından geşiltirilen ForensicXP-4010D cihazı gösterilebilir [3, 8]. Cihaz 350-1050nm geniş spektral aralığında çalışmaktadır ve 1 nm'lik spektral adımlarlarla örnekleme yapabilmektedir. Otomatik tarama esnasında ise spektral bant görüntüleri 20 nm adımlarla ve 12-bit çözünürlükte gri seviyeli imgeler şeklinde kaydedebilmektedir. Sistemde 1360x1024 pixel yüksek çözünürlüklü CCD kamera ve 10x Zoom özellikli parfocal lens kullanılmıştır. Cihazın en küçük spektral inceleme alanı 6x6µm2 olduğundan belgelerde normalde çıplak gözle görülemeyen ayrıntıların spektrumların ölçülmesi mümkündür.

A. Luminesans

Eski tür sarmal teli olan lambalardan yayılan ve akkor (incandescence) tabir edilen ısınma sonucu yayılan ışık türüne hepimiz alışığızdır. Buna karşın, ısınmaya bağlı olmayıp maddeden yayılan ışık türüne ise genel olarak luminesans denilmektedir. Kimyasal reaksiyonlar, bazı yarı iletkenlere uygulanan elektrik enerjisi (örneğin LED'ler) ve bir çok başka etken luminesansa sebeb olabilmektedir. Herhangi bir maddenin foton soğurmasından sonra yayıdığı ışık türüne ise fotoluminesans denilmektedir. Luminesan olayı maddenin moleküler yapısından kaynaklandığından dolayı maddeleri ayrıştırmasında yardımçı olabilmektedir.

Adli doküman inceleme kapsamında incelenen belge, belirli dalga boyundaki ışığa maruz bırakılarak daha uzun dalgaboylarında oluşan luminesans incelenmektedir. Örneğin, şekil 3-a)'da gösterilen numune 470nm dalga boyundaki ışık ile uyarılmış ve sırasıyla 560nm, 600nm ve 620nm dalga boylarında elde edilmiş, örnek üzerindeki mürekkeplerin luminesans özelliğini gösteren bant imgeleri şekil 3-b), 3-c) ve 3-d)'de gösterilmişlerdir. Görüldüğü gibi 560nm dalga boyunda en çok ışımayı sarı mürekkep yapmakta, buna karşın 620nm dalga boyunda ise en çok ışımayı pembe mürekkep yapmaktadır.



a)Örnek mürekkepler b) 560nm luminesans imgesi

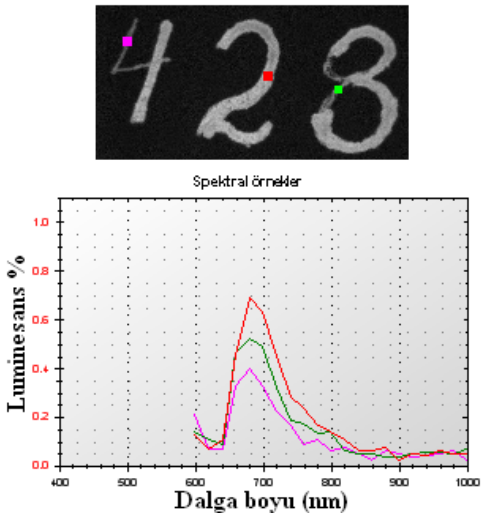
c) 600nm luminesans imgesi d) 620nm luminesans imgesi

Şekil 3: Örnek mürekkepler a) ve b) 560nm, c)600nm, d)620nm dalgaboyunda luminesans imgeleri.

VSC cıhazı kullanan doküman inceleme uzmanları farklı murekkepleri birbirinden ayırt etmek için bu mürekkeplere karşılık gelen luminesans şiddetleri arasında en büyük farkı bulunduran bant imgesini göz önüne alarak karar vermektedirler. Maalesef bu seçenek bir takım koşullarda yanlış kararlar vermelerine neden olabilmektedir. Örneğin, yazım sırasında kaleme farklı basınç uygulayarak yazılan yazılar yada yazının üstünden aynı kalemle birkaç kez geçilen yerler farklı luminesans şiddeti verebilmektedir. Şekil 4'ün üst satırında 470nm dalga boyunda elde edilen luminesans görüntüsü gösterilmektedir. Görüntüde aynı kalemle yazılmış yazının 4 ve 8 rakamlarının bazı bölgelerine yazım sırasında daha az basınç uygulanmıştır. Eğer gösterilen bu tek bant luminesans imgesine bakılarak karar verilseydi, yazının farklı kalemlerle yazılmış olduğu sonucu çıkarılabilirdi. Bir diğer sorunda, en uygun luminesans bant imgesini bulmak için manuel tarama yapılmakta ve uygun imge göz kararı belirlenmektedir. Bu da zaman kaybına ve insandan kaynaklı hatalara neden olmaktadır. Biz bu çalışmada tek bant luminesans imgesine bakılarak karar vermek yerine bir çok dalga boyunu içeren luminesans spektrumunu değerlendirmeyi önermekteyiz. Şekil 4 üstte bahsedilen yazıdaki ihtilaflı bölümler için elde edilmiş luminesans spektrumunu göstermektedir. Görüldüğü gibi bu bölgelerin spektral imzaların FWHM (full width at half maximum) hemen hemen aynıdır sacede tepe genlikleri arasında fark vardır. Bu çalışmada otomatik lüminesans spektrumu tarama tekniği ve ilgili spektrum analiz yöntemlerini önermekteyiz. Önerilen yöntemler var olan doküman inceleme cihazına kazandırılarak sahada kullanıma sunulmuştur.

III. SPEKTRUMU ANALIZI VE GÖSTERIM

Cihazımızda incelenen belgenin luminesans spektrumunu elde etmek için şekil 2'de gösterilen geniş spektrumlu ışık kaynakları yerine halka şeklinde dizilmiş LED'lerden yapılmış ışık kaynağı kullanılmaktadır. İncelenen örnekleri değişik dalgaboyundaki ışıklarla uyarabilmek için 455-850nm arasında değişen 8 LED grubu kullanılmıştır. Tarama sırasında, incelenecek olan belge, seçilen dalgaboyuna uygun LED grubuyla uyarılmakta ve görüntüleme optiği önündeki spektral süzgeç yardımıyla, oluşan luminesans spektrumu 5nm'lik dalgaboyu adımları ile taranmaktadır. Elde edilen luminesans spektrumu hiperspektral görüntü küpü şeklinde saklanmaktadır.



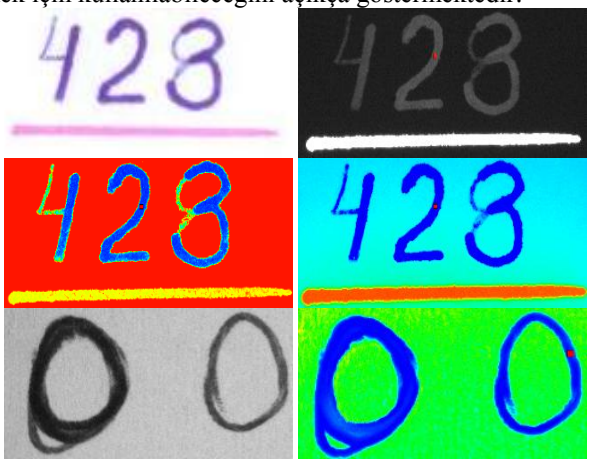
Şekil 4: 470nm dalgaboyu ışıkla uyarılarak 680nm dalgaboyunda elde edilen luminesans imgesi (üst), renkli işaretleyicilerle gösterilen bölgelerdeki ortalama luminesans spektrumları (alt).

Hiperspektral görüntüleri işlemek için değişik yöntemler mevcuttur [4-6]. Adli belge inceleme kapsamında kullanılan hiperspektral görüntü analiz ve gösterim yöntemleri hakkında daha önceki çalışmamızda [4] detaylı bilgi verilmiştir. Bu çalışma kapsamında ise mürekkepleri spektral imzaların genliklerine bakılmaksızın karşılaştırma yapabilmek için imzalar arasındaki doğrusal ilintiyi ölçen Pearson katsayısı (r) kullanıldı [7]:

$$r = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}}$$

burada $X, Y, \overline{X}, \overline{Y}$ sırasıyla karşılaştırılacak iki n adet bileşene sahip spektral imzaları ve bunlara karşılık gelen ortalamaları ifade etmektedirler. Katsayının değeri -1 (ters

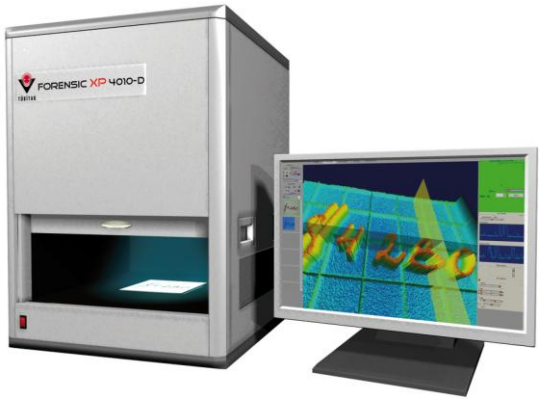
ilinti) ile 1 (pozitif ilinti) arasında değişmektedir. İnceleme sırasında referans spektral imza seçilerek (ör. sistemimizde görüntüdeki mürekkep üstüne işaretleyici koyarak) geri kalan bütün spektrumların referans imza ile olan ilintilerini hesaplanabilmektedir. Analiz sonucunun kolay algılanabilir olması için sistem tarafından yapay renklendirilmiş görüntü üretilmektedir (mavi ve tonları pozitif ilintiyi yada yakınlığı ifade etmektedir). Örnek olarak şekil 5-üst-sol'da farklı kalem basınçlarıyla yazılmış yazı örneği (4 ve 8 sayları) gösterilmektedir (alttaki çizgi ise farklı bir kalemle çizilmiştir). Yazı, 470nm dalgaboyunda ışıkla uyarılıp yukarıda anlatıldığı şekilde luminesans spektrumları elde edilmiştir. Şekil 5-üst-sağ'da 680nm dalgaboyunda elde edilen luminesans görüntüsü gösterilmektedir. şekil 5-orta-sağ'da kırmızı işaretleyici referans spektral imzanın yerini belirtmektedir. Yapay renklendirme ise geri kalan spektrumların referans imzaya Pearson katsayısına göre olan benzerliğini kodlamaktadır. Görüldüğü gibi farklı basınçla yazılan yerlerin lüminesans spektrumlarının genlikleri farklı olmalarına rağmen beklenen sonuç elde edilmiştir. Şekil 5-orta-sol ise Pearson katsayısı yerine Öklid uzaklığı kullanılarak elde edilmiştir. Bu nedenle farklı basınçla yazılan yerler farklı bir kalemle yazılmış gibi görünmektedir. Şekil 5-alt satır ise aynı kalemle birkaç kez üstünden geçilen yazıyı ve analiz sonucunu göstermektedir. Ayrıca iki farklı mürekkeple yazılmış yazının yansıma ve luminesans spektrum analizleri Şekil 7 ve 8'de sırasıyla, gösterilmektedir. Şekil 8 farklı mürekkeplerin farklı luminesans spektruma sahip olduklarını ve mürekkepleri ayirt etmek için kullanılabileceğini açıkça göstermektedir.



Şekil 5: Farklı kalem basınçlarıyla yazılmış yazı örneği (üst-sol), 470nm dalgaboyu ışıkla uyarılıp 680nm dalga boyunda elde edilen luminesans görüntüsü (üst-sağ), referans spektral imzaya Öklid uzaklığına (orta-sol) ve Pearson katsayısına (orta-sağ) göre spektrum analizi. Alt satır aynı kalemle yazının üstünden birkaç kez geçilerek (sol) ve Pearson katsayısına göre analiz sonucunu (sağ) göstermektedir.

IV. SONUÇLAR

Bu çalışmada otomatik hiperspektral luminesans görüntüleme sistemi geliştirilmiştir. Geliştirilmiş cihaz şekil 6'da gösterilmektedir. Elde edilen luminesans spektrumlarını analiz etmek için spektral imzalar arasındaki ilintiye dayalı karşılaştırma algoritması gerçeklenmiştir. Sistemimizi kullanan belge inceleme uzmanlarının algısını güçlendirmek ve kullanım kolaylığı sağlamak için ise elde edilen spektrum karşılaştırma sonuçlarının yapay renklendirmesi sağlanmaktadır. Geliştirilen sistemin tek bant luminesans imgesine bakılarak yanlış kararların verilmesi olasılığının önüne geçilmesinde etkili olduğu gösterilmiştir. Örnek olarak aynı kalem fakat farklı basınç yada birkaç kez aynı kalemle yazı üstünde geçilen durumlarda, tek bant luminesans imgesini göz önüne almak yerine spektrumu analiz etmenin daha doğru bir yöntem olduğu gösterilmiştir. Geliştirilen sistem sahada adli doküman inceleme uzmanlarının kullanımına sunulmuştur.



Şekil 6: TÜBİTAK-BİLGEM tarafından geliştirilen Forensix XP-4010D hiperspektral görüntüleme sistemi.

V. TEŞEKKÜRLER

Forensic XP adli belge inceleme cihazının geliştirilmesinde katkısı bulunan tüm BİLGEM-UEKAE çalışanlarına teşekkürlerimizi sunarız.

VI. KAYNAKÇA

[1] G. Vane and A. F. H. Goetz, "Terrestrial imaging spectroscopy," Remote Sens. Environ., vol. 24, pp. 1–29, 1988.

[2] A. F. H. Goetz, "Imaging spectrometry for remote sensing: Vision to reality in 15 years," Proc. SPIE—Imaging Spectrometry, vol. 2480, pp. 2–13, 1995.

[3] Forensic XP 4010 Doküman İnceleme Cihazı. http:// www.uekae.tubitak.gov.tr.

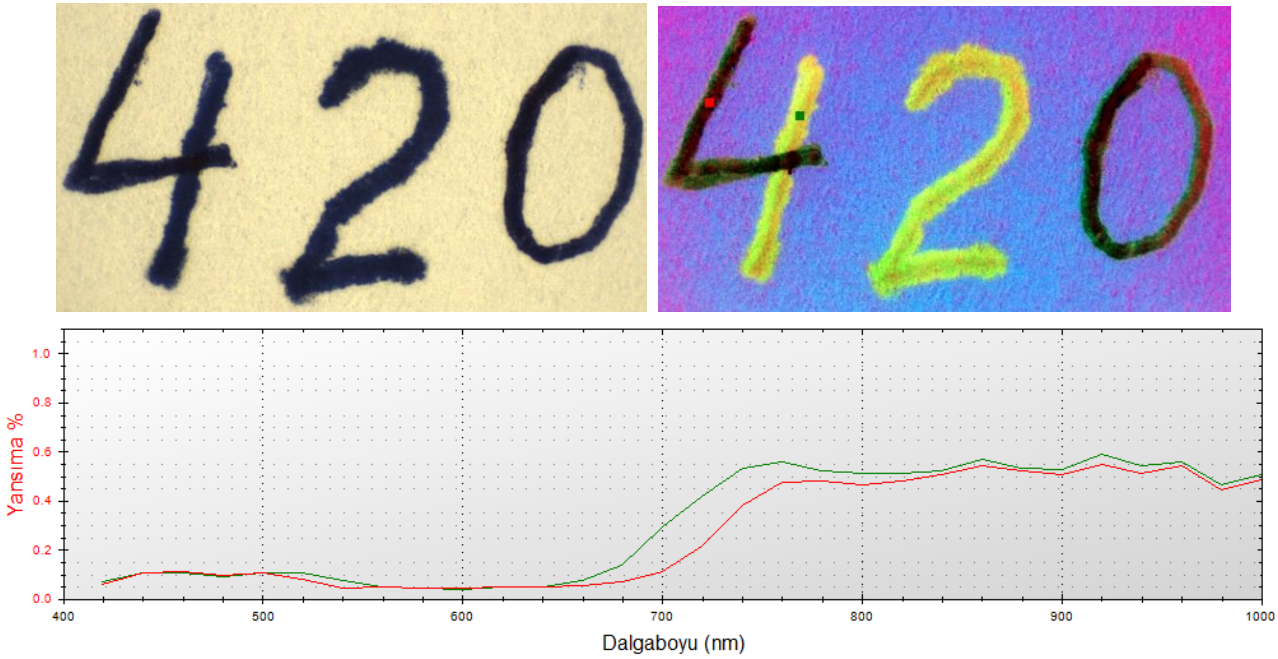
[4] Kholmatov, A. Nasibov, H. Hacizade, F., "Hyperspectral image processing and display techniques in the context of forensic document investigation," Signal Processing and Communications Applications (SIU), Turkey, 2012

[5] J. S. Tyo, A. Konsolakis, D. I. Diersen, R. C. Olsen, "Principal-Components-Based Display Strategy for Spectral Imagery", IEEE Trans. on Geoscience and Remote Sensing, Vol. 41(3), pp. 708- 718, 2003

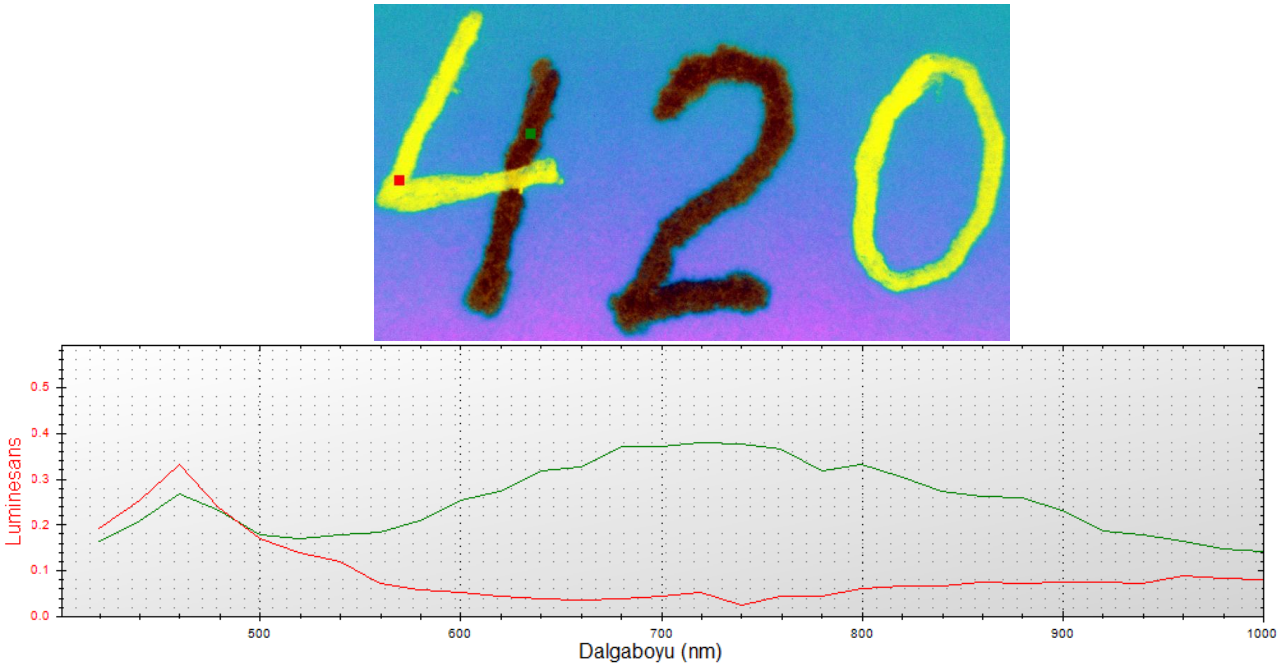
[6] N. P. Jacobson and M. R. Gupta, "Design Goals and Solutions for Display of Hyperspectral Images", IEEE Trans. on Geoscience and Remote Sensing, Vol. 43(11), pp. 2684-2692, 2005

[7] J. L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient", The American Statistician, 42(1):59–66, February 1988.

[8] TÜBİTAK 2013 Faaliyet Kitabı, ss.67-68.



Şekil 7: Farklı üreticilere ait iki değişik kalemle yazılmış yazının RGB görüntüsü (sol-üst), PCA kullanarak analiz edilmiş hiperspektral yansıma spektrumu görüntüsü (sağ-üst), kırmızı ve yeşil işaretleyicilere karşılık gelen farklı mürekkeplerin yansıma spektrumları (alt).



Şekil 8: Şekil 7'de gösterilen örnek yazıya karşılık gelen luminesans spektrumu PCA kullanarak analiz edilmiş. Analiz sonucu elde edilen hiperspektral luminesans görüntüsü (üst), kırmızı ve yeşil işaretleyicilere karşılık gelen farklı mürekkeplerin luminesans spektrumları ise altta gösterilmektedir.

Advanced Dynamic Analysis of Cryptolocker

J.Lang, N. Shashidhar

Sam Houston State University, Huntsville, TX
{jdl016, karpoor}@shsu.edu

***Abstract*— Cryptolocker and other crypto viruses can cost organizations and users significant time and money. To help understand this issue in greater detail, we isolate Cryptolocker and perform advanced dynamic malware analysis in an effort to learn its behavior. We assert that this knowledge will be very useful in building a proactive approach of protecting computing systems from the Cryptolocker family of malware.**

***Keywords*—Cryptolocker, analysis, malware, crypto virus**

I. Introduction

IMAGINE coming into work one day and booting up your work station, only to discover that all of your files have been encrypted by an unknown attacker. The attacker demands that you pay a ransom of $300 in exchange for a private key that will allow you to decrypt your files. This typical scenario is played out because of a piece of malware named Cryptolocker.

Cryptolocker can be transmitted by malicious email or by a drive-by download. After a machine is infected, the malware encrypts files that are accessible through a drive letter such as C:\, D:\, etc. Once the files are encrypted, the malware changes the background on the targeted machine, and the countdown clock begins. If the user fails to pay the ransom, the private key will be deleted, leaving the encrypted files unrecoverable.

There are many ways to prevent data loss from Cryptolocker and other types of malware, such as safe computing practices and up-to-date backups. To be successful at combating Cryptolocker, security professionals need to understand how this malware behaves. In this work, we conduct advanced behavioral analysis of cryptolocker to explore the actions and behaviors of this malicious piece of code. At the end, we suggest potential weaknesses that an IT administrator can possibly safeguard to protect their systems.

II. Prior work

The topic of dynamic malware behavioral analysis has been researched thoroughly. Some of the research has been directed at specific tools [1]. In this paper, the author presents an overview of Anubis and discusses how it helps automate malware analysis. A second type of automation is TWMAN [2] [3]. Although we initially use automated analysis, it has some drawbacks. The drawbacks to any automation of analysis are that the results can lack in completeness and may produce information that may be not useful. To help with the usefulness of automation, some researchers have implemented activity graphs in an attempt to clarify their results [4]. This is a great solution to show management who may not be technically inclined about what exactly is happening.

Another attempt at analyzing malware is putting an infected machine in an isolated network that mimics the Internet [5]. This will help researchers gain more knowledge of malware that changes its behavior if it discovers it is located in a virtual environment or a system without Internet access [6]. We use this approach with the implementation of FakeNet. FakeNet will allow us to mimic a DNS server and monitor network packets.

Hybrid approaches combine an automatic analysis with a hands-on analysis. A typical hybrid approach consists of an automated part to get a large overview, then a hands-on approach to clarify the results from the automation. This is the approach that we take, in this work, to understand Cryptolocker. Initially we subject the executable to automated analysis and then pursue advanced dynamic analysis using the automated results as the starting point for our analysis. Such hybrid analysis is common in the literature and was used in identifying the largest network threat by Zolkipli et.al. [7].

Once malware is discovered, it needs to be classified. Extensive research has been conducted on this issue. One method is a two-part approach that consists of behavior identification and malware classification [8]. A second approach proposes three stages: "(a) behavior of collected malware is monitored in a sandbox environment, (b) based on a corpus of malware labeled by an anti-virus scanner, a malware behavior classifier is trained using learning techniques and (c) discriminative features of the behavior models are ranked for explanation of classification decisions" [9]. This technique attempts to use machine learning to help identify different strands of malware. We can easily classify Cryptolocker as ransomware, so the need of classification for this analysis is not required.

A basic overview of ransomware, including, what it is and its goals is explained in the work done by Bridges et.al. [10]. In this work, the author outlines the basics and the background on malware. Despite being basic and elementary, this research enables one to understand why ransomware can be a significant problem. To delve a little deeper into the different types of ransomware, Gazet et. al [11] conduct a comparative analysis of various ransomware virii, and study several different types of ransomware. In this work, we build upon these ideas and use them to understand more deeply how Cryptolocker behaves as ransomware.

To analyze ransomware, firstly, we need to set up a secure environment. There are several resources available in the literature which outlines the techniques and approaches to establish secure analysis environments, setting up both physical and virtual testing environments, what tools to use and how to obtain copies of malware [12], [13], and [14]. Since we are unable to describe the processes involved in establishing secure malware analysis environment in greater detail here, due to space restrictions, we refer the interested reader to these references.

III. Analysis

In this section, we outline the set of tools that we have used in this research. Firstly, to conduct an effective analysis, we have assembled the following set of standard malware analysis tools. These tools, that we have chosen, are free and readily available online and are considered fairly standard and accepted in malware analysis. These tools include 1. Process Monitor, 2. Process Hacker, 3. FakeNet, 4. RegShot and 5. Sysinternals' Strings.

Malicious code can be obtained by setting up a honeypot, getting a sample from an infected machine or browsing malware research websites to find specific instances of malware. We obtained our copy of Cryptolocker from http://www.kernelmode.info. Kernel Mode contained two samples of Cryptolocker that were downloaded to the host machine.

The first specimen that was found was labeled *clilock.rar*. The second specimen we obtained was labeled *0388.zip* with an MD5 signature of bbb445901d3ec280951ac12132afd87c. We decided to focus on 0388.zip because this instance was the latest rendition of Cryptolocker.

First, the files were submitted to different dynamic analysis sites to determine if these samples were copies of Cryptolocker and what we might learn about them. On https://www.virustotal.com, the submitted files were analyzed to determine if different antivirus software could detect this particular instance of the virus. The zipped copy of Cryptolocker-0388 was detected by 4 out of 48 anti-virus vendors, while the unzipped version fared better, with detection by 42 out of 48 antivirus software programs.

The next step taken is to run *Strings* on the executable. *Strings* is a part of Microsoft's Sysinternals' utilities. Strings searches for ANSI and UNICODE strings within an executable. When a program is compiled, the instructions are converted into machine language. However, the literal strings are not converted and are left in human readable format. Strings searches through all of the machine code and finds these literal strings. These strings can provide key items, such as hard-coded IP addresses, URLs and Microsoft Windows function calls. Sometimes the results of strings can be lacking because a common technique to evade analysis is to pack the executable contents so that the string literals are not exposed. Sysinternal Strings is a quick way to discover possible ways the malware will behave.

After performing these preliminary investigation steps, the next step is to run the malware, i.e., conduct dynamic analysis. We set up our lab environment on a MacBook Pro with 8 GB of RAM, with Windows 7 running under BootCamp. We installed VMWare Workstation on Win 7. Caution should be taken as some malware look for the VMWare client and attempts to take advantage of it [14]. To prepare the environment, a Windows 7 virtual machine was created on VMWare Workstation. All of the tools that could be used to analyze malware were loaded onto the virtual machine. A snapshot of the clean virtual machine was created to allow an analyst to quickly revert back to the point at which the snapshot was taken. From a clean snapshot of the virtual machine, Process Monitor, Process Hacker, Process Explorer and FakeNet are started.

Process Monitor is part of Windows Sysinternals. It shows real-time file system, Registry and process thread activity. Process Hacker is a free multi-purpose tool that helps monitor system resources and detect malware. Process Explorer is also part of Windows Sysinternals. It shows what .DLLs and handles a process has opened or loaded. All of these utilities help to determine what processes are running and how they are behaving on the machine. These tools are useful for monitoring what a suspicious program is doing, what .DLLs it has utilized, how much memory it is using, what threads the process have spawned and verifying if the process is signed and legitimate.

To simulate a network, FakeNet is configured and started. FakeNet is a tool that mimics a network so that malicious software believes that it is interacting with a real network. When a piece of malware sends a DNS request, FakeNet will respond with a "200 Found" response. When malware asks for a .jpg, .txt, etc., FakeNet responds by sending the malware the type of file it requested. Before FakeNet was developed, an analyst had to run several tools to accomplish all the tasks that FakeNet does.

Once all of the process monitoring tools are started and FakeNet is running, RegShot is opened and the first shot is initialized. RegShot is an open source project that takes a snapshot of a registry before an installation and compares it to the registry after a user installs a piece of software. Naturally this is useful for malware analysis because an analyst can use RegShot to establish a registry baseline before an installation of a suspicious piece of software. After the installation of the suspected file, a second shot is performed. RegShot does the comparative work, by returning a list of changes that was made between the first and second shots.

Finally, after the framework is set, the binary is executed. The first thing we noticed was that the executable deleted itself. FakeNet shows that Cryptolocker begins making several DNS queries. For these queries, FakeNet, replies back to Cryptolocker with a "200" response that informs the malware that the DNS query was resolved. After letting FakeNet run for a few minutes, a pattern is noticeable. All of the URLs Cryptolocker was seeking, seem random, but the extensions --biz, .ru, .org, .co.uk and .info seem to occur in a specific order.

After allowing the malware to run for a few minutes, we

took a second shot with RegShot. The first shot and the second shot were then compared. We saved these results for later analysis. Next, Process Monitor is shut down and its log files are saved as well. After all of the log files and pertinent information were saved to a removable drive the virtual machine was reverted back to its clean snap shot.

IV. ANALYSIS RESULTS

A. Automated Analysis

When 0388.exe was submitted to Anubis, we received the following results. We would like to note that, even though the file names are different, the MD5 remains the same. The reason for this is that Anubis recognized this as a previously submitted file and the report we received was a copy of the report submitted earlier.

- Filename: 6a1e32af2e.exe
- MD5 -bbb445901d3ec280951ac12132afd87c
- Load-Time DLLs
- ntdll.dll
- C:\WINDOWS\system32\ kernel32.dll
- Run-Time DLLs
- gdiplus.dll
- UxTheme.dll
- comctl32.dll
- MSIMG32.dll
- OLEAUT32.dll
- WININET.dll
- ole32.dll
- CRYPT32.dll
- MSASN1.dl
- msvcrt.dll
- ADVAPI32.dll
- RPCRT4.dll
- Registry values read

Key	Name	Value
HKLM\ SYSTEM\ CurrentControlSet\ Control\ Session Manager	CriticalSectionTimeout	2592000
HKLM\ SYSTEM\ Setup	SystemSetupInProgress	0
HKLM\ Software\ Microsoft\ Windows NT\ CurrentVersion\ Windows	AppInit_DLLs	
HKLM\ Software\ Policies\ Microsoft\ Windows\ Safer\ CodeIdentifiers	TransparentEnabled	1
HKLM\ System\ CurrentControlSet\ Control\ Terminal Server	TSAppCompat	0

B. Strings

Strings located several interesting strings in the executable. We list a brief overview below and is not to be construed as an exhaustive list.

- 184.164.136.134 - This hard-coded address is probably the preferred Command and Control server. Currently an nslookup command returns that the server could not be found.
- RSA1 - RSA is a public key cipher/cryptosystem. We believe this to be the encryption method for Cryptolocker. More research is needed to determine if this is the case.
- 71 file extensions - This list includes the types of files that Cryptolocker looks for to encrypt.
- A list of cash amounts - These amounts are used by Cryptolocker to alert the user of an infected machine of their ransom price demand. 300 USD, 300 EUR, 300 AUD, 600 BRL, 300 CAD, 6000 CZK, 3000 DKK, 300 GBP, 3000 MXN, 4500 NOK, 600 NZD, 1500 PLN, 600 RON, 4500 SEK.
- Several Windows functions, including Windows encryption functions.
- Markup language that informs the victim of what has happened and how to pay the ransom.
- Due to the amount of strings available, one can assume that the Cryptolocker executable was not packed to hide itself from malware analysts.

C. RegShot

- We determined that 109 keys were added. Not all of these keys are due to the infection. An analyst needs to look through the results to find entries that relate to Cryptolocker. A few of these entries are:
    1. HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing \Vvrlupvcbbdz_RASAPI32
    2. HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\Vvrlupvcbbdz_RASMANCS

- 367 values added to keys including 12 updates to HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\Vvrlupvcbbdz_RASAPI32
- These entries gives a good place to look for information. Although the naming of these entries gives us a good guess at what they are used for, a more in-depth analysis is needed to determine how they are truly used.
    1. EnableFileTracing: 0x00000000
    2. EnableConsoleTracing: 0x00000000
    3. FileTracingMask: 0xFFFF0000
    4. ConsoleTracingMask: 0xFFFF0000
    5. MaxFileSize: 0x00100000
    6. FileDirectory: "%windir%\tracing"
- These two entries are important because it gives us the location that the executable is stored. With this information we can monitor this location for future infections. Also, one of the techniques to prevent Cryptolocker from executing is to not allow any programs to execute from the AppData folder or its children.
    1. HKU\S-1-5-21-1661378203-3683921125-1189639900-1000\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker: "C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe"
    2. HKU\S-1-5-21-1661378203-3683921125-1189639900-1000\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker: "C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe"

D. FakeNet

Once Cryptolocker is launched, it begins to produce many DNS queries. The formats of these URLs were the name being 14 characters long, followed by one of the following extensions: .net, .biz, .ru, .org, .co.uk, .info. FakeNet also stores all of the network packets for later analysis. The format of these packets is .pcap and can be analyzed through Wireshark. In the analysis we see several DNS calls and calls to the /home/ directory. However, since the VMWare machine is isolated from the Internet, there is no way that Cryptolocker can connect to a Command and Control server. A future analysis can be to allow Cryptolocker to access the Internet and interact with its Command and Control server. That analysis would be beneficial to determine how the interaction between the Command and Control servers and Cryptolocker operate.

E. Process Monitor

Process Monitor can be set only to allow processes with a certain name. The filters were set to only pull actions of processes named 0388.exe (name of file with Cryptolocker). After the 0388.exe started to execute, several operations were performed. One was to create a file named Vvlupvcbbdz.exe. Vvlupvcbbdz.exe was started and created its own processes. The process named 0388.exe continued on until finally deleting itself and closing its process. Process monitor showed that Vvlupvcbbdz.exe was saved at C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe. Viewing that area, we were unable to see this file, even though we had the option to see hidden files enabled. In the Process Monitor log file, the process Vvrlupvcbbdz.exe cycles through a short sequence:

- RegOpenKey HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- RegSetInfoKey HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- RegQueryValue HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker
- RegCloseKey HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnces

Cryptolocker is opening a key and looking for a value. To determine what that value is, a static analysis could be performed on the executable.

F. Process Hacker

Thread ID	Start Address	Priority
304	Vvrlupvcbbdz.exe+0x9bbd	Normal
788	Vvrlupvcbbdz.exe+0xbee0	Normal
956	GdiPlus.dll!GdipCreateSolidFill+0x817	Normal
1344	rasman.dll!RasAddNotification+0x384	Normal
1408	Vvrlupvcbbdz.exe+0xbee0	Normal
1432	ntdll.dll!RtlLoadString+0x430	Normal
1500	Vvrlupvcbbdz.exe+0xbee0	Above Normal
1568	ntdll.dll!RtlDosSearchPath_Ustr+0x69a	Normal

Thread ID	Start Address	Priority
2128	ws2_32.dll!WahQueueUserApc+0x5c	Normal
2244	mswsock.dll+0x62ee	Above Normal
2260	Vvrlupvcbbdz.exe+0xbee0	Time Critical
2596	ntdll.dll!RtlDosSearchPath_Ustr+0x69a	Normal
2860	ntdll.dll!RtlDosSearchPath_Ustr+0x69a	Normal
2868	Vvrlupvcbbdz.exe+0xbee0	Normal

G. Process Explorer

The process Vvrlupvcbbdz.exe is easily identified inside Process Explorer. The description for this process says Cvent and the company that is listed is *Wave*. A quick Google search does not reveal anything particularly helpful. Other useful information pulled with Process Explorer:

- **Path**: C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe
- **Command line**:

  "C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe" "-rC:\Users\Jeremy\Desktop\0388.exe"
- **Current Directory:**

  C:\Users\Jeremy\AppData\Local\

V. RESULTS INTERPRETATION

After we complete the analysis, we used the gathered information to exploit weaknesses within the malware.

The first thing to note is the MD5 hash, bbb445901d3ec280951ac12132afd87c. We can use this hash to positively identify this flavor of Cryptolocker.

When using Systinternals Strings, we see a hard-coded IP address of 184.164.136.134. This is probably a preferred Command and Control server. The systems administrator can block this IP address, making it difficult for the malware to contact its Command and Control server. It does not completely stop. As seen when we used the FakeNet tool, Cryptolocker creates random URLs and attempts to contact each of them. The URLs that are created are derived from an algorithm, so if the algorithm is discovered, a security professional can attempt to block all of the future URLs. This is what researchers discovered, so they began a DNS sinkhole campaign [15]. A DNS sinkhole is a DNS server that gives out misinformation in response to a DNS request, in hopes of thwarting malicious activity, such as bonnets or in this case, Cryptolocker.

Strings also returned RSA1. We believe that RSA is the cipher used to encrypt the victim's device. Clearly, it isn't practical to brute force, in an effort to obtain the key. However, there may be a chance that the encryption wasn't set up properly, allowing a researcher to defeat the encryption, such as by finding what happened to the Bitcrypt Ransomware [16].

Regshot noted the location that the executable was saved.

- HKU\S-1-5-21-1661378203-3683921125-1189639900-1000\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker: "C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe"
- HKU\S-1-5-21-1661378203-3683921125-1189639900-1000\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker:"C:\Users\Jeremy\AppData\Local\Vvrlupvcbbdz.exe"

This shows us that Cryptolocker is launching from the \AppData\Local\ folder. To keep Cryptolocker from launching, an administrator can set policies that block apps in \AppData\Local\ from executing or he can create a whitelist of known good applications that are allowed to start within that folder.

A final item to check is how the file is named. In this case the executable file was named Vvrlupvcbbdz.exe. We can assume that the creators of this malware didn't want the name to be the same during each execution. The name staying the same would allow for easier discovery by the victim. If the algorithm could be discovered on how the name is generated, we could create a simple script that could check the \AppData\Local\ folder for files with that name. However, it can be noticed that the name never changed with each execution of the malware. The assumption can be made that the malware would have the same name because each execution is done on the exact same machine. This assumption leads to the idea that what remains the same between each snapshot can be the seed for the random name generator.

The assumption we were working under is that if we can find the seed to the random name generator, we would perhaps then take be able to take the information of what changed in the random name generator seed and how it affected the name of the executable. The next step would be to take this knowledge and reverse the random name generating algorithm.

To attempt to discover the random name generator seed, we created three separate virtual machines. We assigned each machine a different IP Address, a different MAC address and a different time. The executable 0388.exe was started that allowed Cryptolocker to be installed on the virtual machines. Unfortunately, the result was that there was no change in the name, ruling out that the system time, MAC address or the IP address had anything to do with the random name generation.

Future tests can include using different Windows product IDs, since all of the virtual machines were clones and therefore had the same product ID.

VI. Conclusion

In this work, we conducted some basic and advanced dynamic behavioral analysis of the malware known as Cryptolocker. This analysis armed us with several possible ways to combat Cryptolocker and other types of similar malware. We showed that taking a proactive approach to dealing with Cryptolocker can save large amounts of man hours due to lost work.

Future analysis of Cryptolocker would be to perform a static analysis on the executable, as well as to run the executable in a debugger. One of the goals of the next two steps would be to determine how the file is named. If the seed random name generator is discovered, the naming algorithm could be discovered as well.

Although a proactive approach to combat Cryptolocker is good; not getting infected is even better. So practicing safe computing is always paramount. Also, if all else fails, having up-to-date backups will minimize the potential damage.

References

[1] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda and C. Kruegel, "A View on Current Malware Behaviors".

[2] H.-D. Huang, C.-S. Lee, H.-Y. Kao, Y.-L. Tsai and J.-G. Chang, "Malware Behavioral Analysis System: TWMAN".

[3] H.-D. Huang, T.-Y. Chuang, Y.-L. Tsai and C.-S. Lee, "Ontology-based Intelligent System for Malware Behavioral Analysis," WCCI 2010 IEEE World Congree on Computational intellegence, Barcelona Spain, 2010.

[4] A. R. A. Grégio and R. D. C. Santos, "Visualization Techniques for Malware Behavior Analysis".

[5] K. Yoshioka, Y. Hoshizawa, D. Inoue, M. Eto and K. Nakao, "Malware Behavior Analysis in Isolated Miniature," IEEE, 2008.

[6] H. Shinotsuka, "Malware Authors Using New Techniques to Evade Automated Threat Analysis Systems," Symantec, 26 October 2012. [Online]. Available: http://www.symantec.com/connect/blogs/malware-authors-using-new-techniques-evade-automated-threat-analysis-systems. [Accessed 16 11 2013].

[7] M. F. Zolkipli and A. Jantan, "Malware Behavior Analysis: Learning and Understanding Current Malware Threats," Second International Conference on Network Applications, Protocols and Services, 2010.

[8] M. F. Zolkipli and A. Jantan, "An Approach for Malware Behavior Identification and Classification".

[9] K. Rieck, T. Holz, C. Willems, P. D¨ussel and P. Laskov, "Learning and Classification of Malware Behavior".

[10] L. Bridges, "The changing face of malware," January 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485808700102. [Accessed 15 12 2013].

[11] A. Gazet, "Comparative analysis of various ransomware virii," 2008.

[12] M. Sikorski and A. Honing, Practical Malware Analysis, No Starch Press, 2012.

[13] E. Skoudis and L. Zeltser, Malware: Fighting Malicious Code, Upper Saddle River, New Jersey: Pearson Education, Inc., 2008.

[14] J. M. Aquilina, E. Casey and C. H. Malin, Malware Forensics: Investigating and Analyzing Malicious Code, Burlington, MA: Syngress Publishing, Inc., 2008.

[15] Grinler, "DNS Sinkhole campaign underway for CryptoLocker," Bleeping Computer, 24 October 2013. [Online]. Available: http://www.bleepingcomputer.com/forums/t/511780/dns-sinkhole-campaign-underway-for-cryptolocker/. [Accessed 28 November 2013].

[16] M. Grooten, "Researchers crack ransomware encryption," Virus Bulletin Ltd, 21 February 2014. [Online]. Available: http://www.virusbtn.com/blog/2014/02_21.xml?rss. [Accessed 1 April 2014].

AES, LSB and Huffman Encoding Based Steganography in Telemedicine

U.Kas[1] and E. Tanyildizi[2]

[1]Fırat University, Elazig/Turkey, Elazig/ TURKEY, umitkas04@gmail.com
[2]Firat University, Technology Faculty,Software Engineering Department,23119,Elazig / TURKEY, etanyildizi@gmail.com

***Abstract*—Privacy of patient's information is vital for telemedicine applications. This paper presents protecting the transferring of medical images. The classic algorithms carried out to images. This study presents a new method which pieces methods of encryption, data compression and data hiding for the purpose of confident medical image transmission. In this method we compress patient's information with Huffman algorithm then encrypt the compressed patient's information with the advanced encryption standard (AES) finally embed the encrypted patient's information to the original image. When the message arrives to receiver side, we carry out the reverse methods to get patient's information. This study shows that a possible amount of information can be embedded into an image with imperceptible changes.**

***Keywords*— Medical Images, Image Steganography, Data Hiding, AES, Huffman, Cryptology.**

I. GİRİŞ

Günümüzde bilgisayarlar ve internet, dünyanın farklı noktalarını birbirine bağlayan en önemli iletişim araçlarıdır. İletişim araçlarının gelişmesi ile mesafe artık bir engel olmaktan çıkmaktadır. Aynı zamanda iletişim araçlarının gelişmesiyle insanlar bilgiyi kolaylıkla değiştirebilmektedirler. Bununla birlikte gelişen teknoloji, iletişimde kullanılan bilginin güvenliği problemini ortaya çıkarmaktadır [1].

Bilgi güvenliğini gerektiren önemli süreçlerden birisi de doktor-hasta bilgi güvenliğidir. Doktor, hastaya yarar sağlarken aynı zaman da hasta haklarını da ihmal etmemelidir. Hasta bilgi gizliliğinin önemi 1995 tarihli Bali Hasta Hakları bildirgesinin gizlilik hakkı bölümünde vurgulanmaktadır [2]. Bu bildirgede hastaya ait korunması gereken önemli bilgilerden biri de hastaya ait tıbbi verilerdir.

Tıbbi verilerin sayısal verilere dönüşmesi ve bilgisayar dünyasındaki gelişmelerle birlikte tıbbi verilerin aktarımı konusu ortaya çıkmıştır. Farklı ortamlar arasında bilişim teknolojileri kullanılarak teşhis, tedavi, araştırma ve insan sağlığını iyileştirmeyi hedefleyen sağlık hizmetine teletıp denir [3]. Teletıp kavramının geçmişi 1920'lere dayanmakta ve tıp dünyasındaki yaygınlığı sürekli artmaktadır [4]. Teletıbbın amacı,hastalara ucuz ve kaliteli sağlık hizmeti sunulmasına yardımcı olmaktır [3].

Teletıbbın faydaları aşağıdaki gibi özetlenebilir [3]:

- *Bilgi Erişimi*: Hasta bilgileri çeşitli veri saklama ortamlarında saklandığı için bu bilgilere anlık ulaşım sağlanır
- *Hasta Erişimi:* Sağlık hizmetlerinin gidemediği yerlere erişim sağlanır.
- *Ekonomik:* Hastaların uzak mesafelerdeki sağlık merkezlerine gidebilmek için harcayacağı masraflar ortadan kalkar
- *Zaman:* Sağlık merkezlerine gitme, giriş işlemi yaptırma, muayene sırası bekleme gibi işlemlerde harcanan zaman azaltılır.

Teknolojik gelişmeler düşünüldüğünde, teletıp alanındaki verilerin güvenliğini sağlamak için ya verileri gizlemek ya da şifrelemek gerekmektedir. Bu sebeple, veri güvenliğini arttırma ile ilgili son zamanlarda önemli çalışmalar yapılmaktadır. Bu çalışmalardan veri gizleme yaklaşımlı çalışmaların başarılı sonuçlar verdiği görülmektedir. Veri gizleme yaklaşımlarından en sık kullanılan yaklaşımlardan birisi de steganografi tabanlı yaklaşımdır.

A. Steganografi

Steganografi, özel veya hassas verilerin başka bir nesne içerisinde saklanmasıdır. Steganografi yönteminde verinin gizlendiği nesneye örtü verisi, oluşan nesneye stego-nesnesi denir. Gizlenecek veri açık veri olabileceği gibi şifrelenmiş veri de olabilir [5].

Steganografi, dilbilim steganografi ve teknik steganografi olmak üzere iki alt gruba ayrılmaktadır. Dilbilim steganografi, taşıyıcı verinin metin olduğu, teknik steganografi ise taşıyıcının metin yerine görünmez mürekkepler, gizli yerler, bilgisayar tabanlı yöntemler gibi birçok aracın olduğu steganografi koludur.

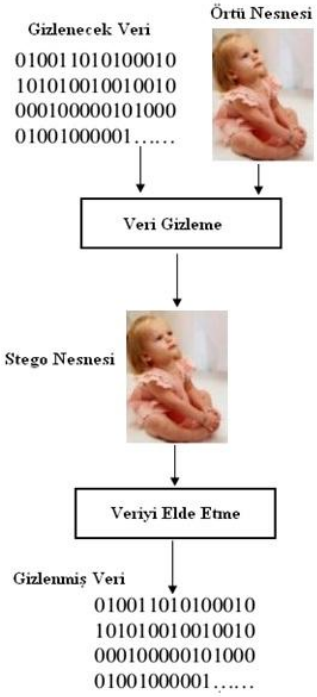
Steganografi kullanım alanları açısından üç gruba ayrılmaktadır:

- Metin steganografisi
- Ses steganografisi
- Görüntüsteganografisi

Metin steganografisi, örtü verisinin metin olduğu steganografi alanıdır. Taşıyıcı metin olduğu için saklanacak veri miktarı sınırlıdır. Çünkü metin içindeki gereksiz alan ve boşluk sayısı yeterince fazla değildir [6].

Ses steganografisi, örtü verisinin dijital ses olduğu steganografi alanıdır. Dijital seslere bilgiyi yerleştirmek görüntü içerisine bilgiyi yerleştirmekten daha zordur [7].

Görüntü steganografisi örtü verisinin dijital görüntü olduğu steganografi alanıdır. Verinin örtü verisine gizlenmesini sağlayan farklı yöntemler bulunmaktadır [8]. Bu çalışmada en önemsiz bite ekleme yöntemi kullanılmıştır. Görüntü steganografisinin genel işleyiş yapısı Şekil 1'de gösterilmektedir.



Şekil 1. Görüntü steganografisinin genel işleyiş yapısı

B. En Önemsiz Bite Ekleme

En önemsiz bite ekleme(LSB-Least Significant Bit), veri gizleme yöntemlerinden biri olup uygulanması basit olduğundan oldukça sık kullanılan bir yöntemdir. Ancak kullanımındaki dikkatsizlikler veri kayıplarını beraberinde getirebilmektedir [9]. En basit veri gizleme tekniği verinin bitlerini kaplama nesnesinin zeminine belirlenen sıra ile gömmektir.

En önemsiz bitin değişimi insan tarafından algılanamaz çünkü bu değişimin etkisi çok küçüktür. Bu yöntemde gömülecek veri kapasitesi en önemsiz ikinci, üçüncü bitler kullanılarak arttırılabilir. Bunun sonucu olarak gizlenmiş verinin istatistiksel olarak tespit edilme riskini arttırmakla beraber resmin doğruluğunu da azaltmaktadır [10].

Bu yöntemde, resimdeki her pikselin her baytının en önemsiz biti, gizlenecek olan verinin biti sırasıyla değiştirilir. Bu işlem sıra ile yapılabileceği gibi rastgele de yapılabilir [9].

LSB yöntemi ile gerçekleştirilen steganografi uygulamalarının güvenliğini arttırmak için bazı anahtarlar kullanılabilir. Bunlar;

- *Steganografik anahtarlar:* Veri gizleme ve gizlenen veriyi elde etme denetimi için kullanılan anahtarlar,
- *Kriptografik anahtarlar:* Verinin gizlenmeden önce şifrelenmesi ve gizlendikten sonra deşifre edilmesi için kullanılan anahtarlardır [9].

C. LSB Yönteminin 24-bit Renkli Resimlere Uygulanması

24 bitlik renkli resimlerin her pikselinde 3 bayt kullanılmaktadır. Bir pikselin rengini kırmızı, yeşil ve mavi renklerinin yoğunlukları belirler. Bu üç rengi kullanarak resimlerde gördüğümüz her rengi elde edebiliriz. Kullanılacak resmin sadece son bitinin değiştirildiğini ve resmin *yükseklik*genişlik* piksele sahip olduğu düşünülürse*3*yükseklik*genişlik* bitlik veriyi kaydedecek alana sahip olunur. Örneğin, 24 bitlik derinliğe ve 1280x800 piksel boyutuna sahip bir resim 384.000 bayt veri gizleyebilir. Veriyi gizlemeden önce veri dosyasının adı, veri dosyası adının boyutu ve veri boyutu yazılmalıdır. Aşağıdaki örnek 24 bitlik renkli bir resmin üç pikselinin ilk sekiz baytına C harfinin nasıl gizlendiği gösterilmektedir.

Pikseller: (01010001 10100111 00100100)

(10000100 01010111 11001010)

(00110001 10111110 01010111)

C: 10000011

Sonuç: (01010001 10100110 00100100)

(10000100 01010110 11001010)

(00110000 10111111 01010111)

Piksellerin baytları içerisinde sadece altı çizili son dört bit değiştirilmiştir.

Yüksek kalitedeki resimlerin sıkıştırılarak kullanılması birçok uygulama için daha uygundur ancak sıkıştırma esnasında gizlenen verinin kaybolmaması gerekmektedir [6]. Bunun için veri sıkıştırılırken kayıpsız bir sıkıştırma yapılmalıdır.

II. HUFFMAN VERİ SIKIŞTIRMA ALGORİTMASI

Sıkıştırma yöntemleri kayıplı ve kayıpsız sıkıştırma olmak üzere iki gruba ayrılır. Kayıplı sıkıştırmada sıkıştırılan dosya tekrar açıldığında dosyada veri kaybı oluşurken kayıpsız sıkıştırmada bu durum söz konusu değildir.

Kayıplı sıkıştırma bir miktar veri kaybının insanın duyu organlarının ayırt edemeyeceği durumlarda kullanılır. Kayıplı sıkıştırmaya MP3(Mpeg-1 AudioLayer 3) teknolojisi örnek olarak verilebilir.

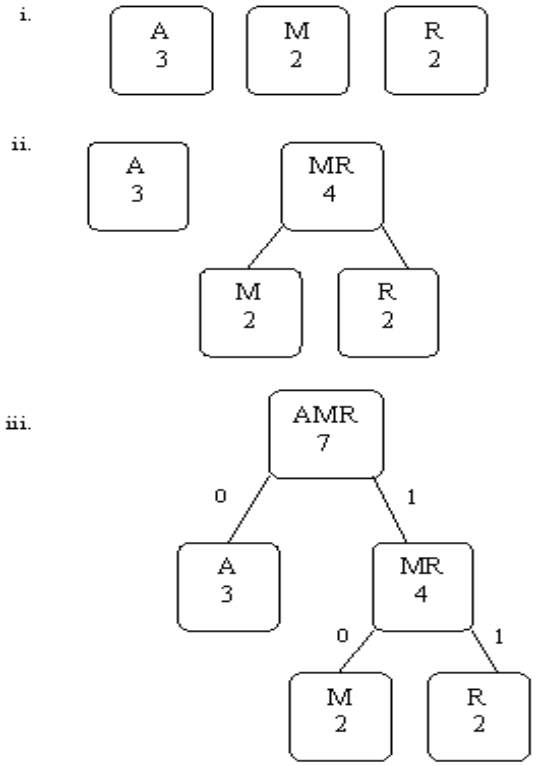
Kayıpsız sıkıştırmaya Huffman algoritması, örnek olarak verilebilir. Huffman veri sıkıştırma algoritması veri kümesindeki karakterlerin tekrar sayısı fazla olanı daha az alanla tekrar sayısı az olanı ise daha fazla alanla ifade edilmesine dayanmaktadır. Veri içerisindeki karakter sayısına ve bu karakterlerin tekrarlanma sayısına göre %10 ile %90 arasında sıkıştırma oranı elde edilebilir. Bu algoritma ile veriyi sıkıştırmak için verideki karakterlerin tekrar etme sayılarının bilinmesi gerekir. Bu tekrar sayıları frekans tablosu ile gösterilirler. Bu algoritmada ilk olarak frekans tablosu, daha sonra karakterleri ifade edecek bitleri temsil eden Huffman ağacı oluşturulur[11].Aşağıdaki verilen örnekte MARMARA

verisinin Huffman algoritması ile nasıl sıkıştırıldığı gösterilmektedir.

Tablo1: "MARMARA" için frekans tablosu

Karakter	Frekans
A	3
M	2
R	2

i. En son düğümleri oluşturacak bütün karakterler frekanslarına göre küçükten büyüğe doğru sıralanır.
ii. En küçük iki frekansa sahip iki karakterin frekansları toplanarak yeni bir düğüm oluşturulur. Oluşturulan düğüm mevcut düğümler arasında uygun yere yerleştirilir.
iii. Bir önceki adımdaki işlemler tekrarlanır. Huffman ağacının kodu oluşturulurken ağacın kök düğümünden başlanır. Şekil 2'de görüldüğü gibi kök düğümün soluna ve sağına sırasıyla 0 ve 1 yazılır [11].



Şekil 2: "MARMARA" için Huffman ağacı

Huffman Ağacı yardımıyla her karaktere ait belirlenen Huffman kodları Tablo 2'de verilmiştir.

Tablo2: "MARMARA" verisinin Huffman kodları

Karakter	Frekans	Bit Sayısı	Huffman Kodu
A	3	1	0
M	2	2	10
R	2	2	11

Bu veri ASCII kodu ile kodlandığında toplam 56bit yer kaplarken Huffman algoritması ile 3x1+2x2+2x2=11bitlik yer kaplar. Böylece %80.36 oranında sıkıştırma yapılmış olur.

Sıkıştırılmış verinin geri elde edilmesinde ise sıkıştırılmış verinin ilk biti alınır. Eğer bit bir karaktere karşılık geliyorsa, ilgili karakter yerine konur.Eğer alınan bit bir karaktere karşılık gelmiyorsa sonraki bitle birlikte alınıp karşılaştırma yapılır. Bu şekilde devam edilerek orijinal veri elde edilir[8].

III. AES-GELİŞMİŞ ŞİFRELEME STANDARDI

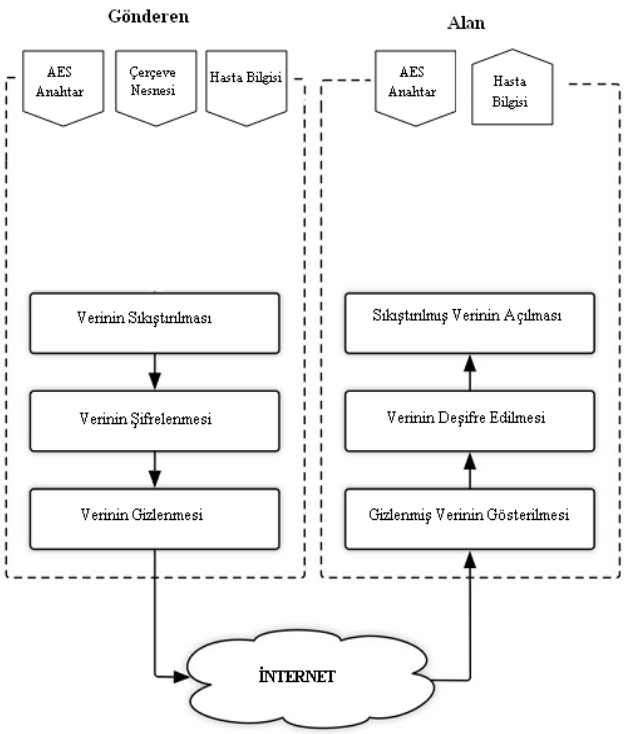
Tüm modern şifreleme algoritmaları şifreleme ve deşifreleme işlemlerinde bir anahtar kullanmaktadır [12]. Veri şifrelenirken ve deşifre edilirken aynı anahtarı kullanan algoritmalar simetrik, kullanmayan algoritmalar ise asimetrik algoritmalardır.

Simetrik algoritmalara AES standardında yer alan Rijndael algoritması örnek verilebilir. Rijndael Algoritması,128 bitlik veri bloklarını 128, 192, 256 bitlik anahtarla şifreleme yapar. Asimetrik algoritmalara ise RSA(RIVEST-SHAMIR-ADLEMAN) algoritması örnek verilebilir. RSA algoritması, tek yönlü bir fonksiyonla şifreleme işlemini gerçekleştirdiği için fonksiyon bilinmeden algoritmayı çözmek oldukça zordur. Rijndael algoritmasına göre daha güvenli, ancak daha yavaştır.

Hem simetrik hem de asimetrik algoritmalar tasarlanırken kırılmaması düşünülerek tasarlanmalıdır. Teorik olarak, tüm şifreleme algoritmalarının kullandığı anahtar tüm anahtarlar denenerek bulunabilir [12]. Ancak bu işlemde kaba kuvvet algoritması kullanılırsa, anahtarı kırmak için gerekli hesaplama gücü üssel olarak artar. *n* bitlik bir anahtarı kırmak için gerekli kombinasyon sayısı 2^n olarak hesaplanır. Örneğin; 56 bitlik bir anahtarlı bir sistem, kaba kuvvet algoritması yardımıyla $721*10^{14}$ adımda çözülür. Bu işlem çok sayıda kişisel bilgisayarın güç paylaşımı yardımıyla birkaç ay içerisinde kolaylıkla gerçekleştirilebilir. 128 bitlik bir anahtara sahip bir sistem kaba kuvvet algoritması yardımıyla $34*10^{68}$ adımda çözülür. Bu işlemin günümüz teknolojisine sahip bilgisayarlarla gerçekleştirilmesi zordur. Birçok yöntemin avantajı kullanılarak geliştirilen sistemlerle bile kırılamaz anahtar üretmek çok zordur [12].

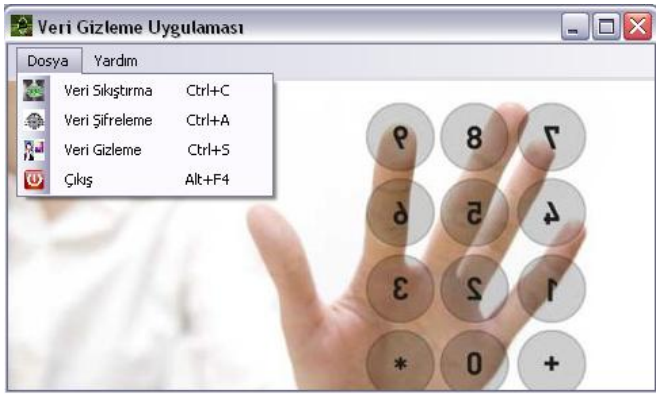
IV. ÖNERİLEN SİSTEM

Bu çalışmada, sisteme gelen hasta verisi öncelikle Huffman veri sıkıştırma algoritması ile sıkıştırılır. Daha sonra elde edilen sıkıştırılmış hasta verisi AES ile şifrelenir. Son olarak şifrelenmiş hasta verisi orijinal görüntü dosyasına gömülür. Mesaj alıcı tarafa ulaştığında yukarıda belirtilen sıranın tersi kullanılarak hasta verisi elde edilir. Gerçekleştirilen çalışmanın veri gizleme işleminin temel akış şeması Şekil 3'te verilmiştir. Önerilen sistemde her modülün görevi mantıksal olarak ayrıktır. Ancak gerçek uygulamada tüm kullanıcılar bu modülleri kullanmaktadır. Bu modülleri kullanan doktor, içerisine hasta verisini gizlediği resmi bilgisayarına kaydettikten sonra internet yoluyla başka doktorlarla paylaşabilmektedir.



Şekil 3: Veri gizleme uygulamasının akış şeması

Yapılan uygulamada, doktorun işlem yapabilmesi için sisteme giriş yapması gerekmektedir. Sistem yöneticisi tarafından verilen kullanıcı adı ve şifre bilgileri yardımıyla doktor sisteme giriş yapabilir. Sisteme giren doktorun karşısına dosya ve yardım menüleri gelmektedir. Dosya menüsünde veri sıkıştırma, veri şifreleme, veri gizleme alt menüler bulunmaktadır (Şekil 4). Yardım menüsünde ise yapılan uygulamanın kullanımı ile ilgili bilgiler yer almaktadır.



Şekil 4: Dosya menüsü görünümü

Doktor, hasta bilgisini sıkıştırıp şifreledikten sonra veri gizleme ekranından hasta bilgisini Şekil 5'te gösterilen veri gizleme formunu kullanarak gizleyebilmektedir. Doktor, içerisine hasta bilgisini gizlediği resmi bilgisayarına kaydettikten sonra internet yoluyla başka doktorlarla paylaşabilmektedir. Bu verilerin gönderimi sırasında istenmeyen kişilerin hasta bilgisini görmesi önerilen yöntemle oldukça güçtür.

V. DENEYSEL SONUÇLAR

Geliştirilen uygulamada, doğruluk oranını belirleyebilmek için İşaret-Gürültü Oranı(PSNR : Peak Signal - to - Noise Ratio) değerleri hesaplanmıştır. Veri gizleme işlemi sonucu elde edilen görüntülerin, orijinal görüntüden farkı doğruluk oranı hakkında bilgi vermektedir. PSNR değerlerinin hesaplanması için gerekli formül aşağıda verilmiştir.

$$MSE = \frac{1}{M \times N} \times \sum_{i=0}^{M} \sum_{j=0}^{N} [I(i,j) - K(i,j)]^2 \quad (1)$$

$$PSNR = 20 \times log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (2)$$

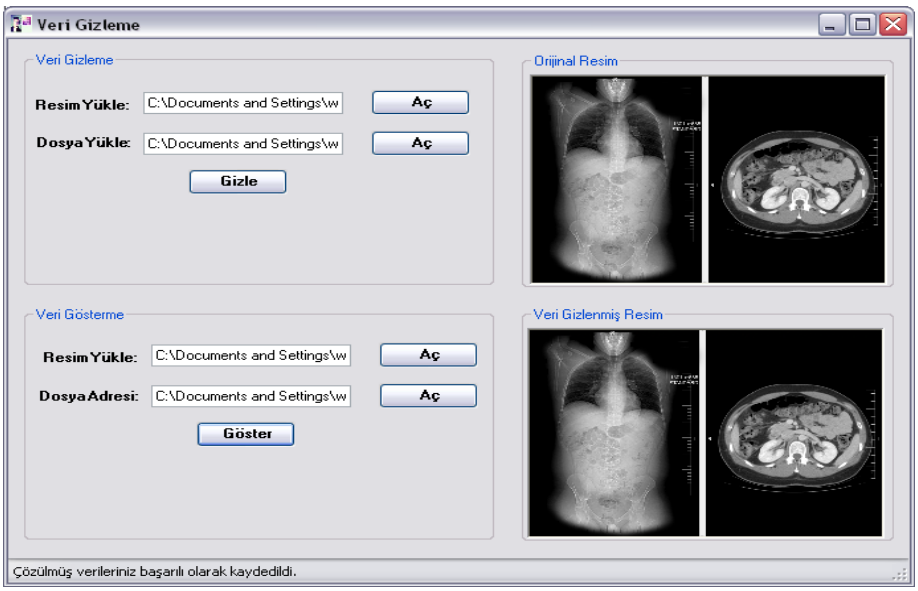
36dB üzerinde bir PSNR değeri, insan gözü tarafından fark edilemeyen bir bozulma olarak kabul edilir [13]. Yapılan uygulamada hastaya ait verilerin bulunduğu üç farklı metin gizlenmiş ve geliştirilen uygulama ile elde edilen görüntüler ile orijinal görüntüler için PSNR değerleri Tablo 3'te gösterilmiştir. Elde edilen sonuçlar 36dB değerinin üzerinde olduğu için oluşan bozulma insan gözü tarafından fark edilememektedir.

Tablo3: Orijinal ve stego görüntüleri için PSNR tablosu

Resim Boyutu	Metin Boyutu	Mesaj Gizleme	Mesaj Alma	PSNR Değeri
1407KB	0.92KB	√	√	50.35dB
1407KB	1.34KB	√	√	40.25dB
1407KB	2.41KB	√	√	37.67dB

VI. SONUÇLAR

Bu çalışmada, Huffman veri sıkıştırma algoritması, AES ve LSB veri gizleme algoritması beraber kullanılmıştır. Yapılan uygulamada, farklı boyutlardaki resimler içerisine farklı boyutlarda veriler gizlenmiştir. Orijinal resim ile veri gizlenen resim arasında gözle görülebilir bir değişim olmadığı gözlenmiştir. LSB yöntemi ile yapılan çalışmalarda gizlenecek veri boyutunun çerçevenin boyutuna bağlı olmasından dolayı daha fazla veri gizleyebilmek için veri sıkıştırıldıktan sonra resmin içerisinde gizlenmiştir. Ayrıca veri gizlenmeden önce şifrelendiği için veri iletişimi daha güvenli olmuştur. Sonuç olarak, önemli verilerimizi koruyabilmek için farklı güvenlik tekniklerini birlikte kullanmak daha etkili olmaktadır. Bu çalışmada önerilen yöntem, bilgi gizlemenin gerektiği her alanda rahatlıkla kullanılabilir.



Şekil 5: Veri Gizleme formuna ait pencerenin görünümü

KAYNAKLAR

[1] N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi "Image SteganographyTechniques: An Overview", International Journal of Computer Scienceand Security (IJCSS), Volume (6) : Issue (3), p168-187 2012.

[2] (09.03.2014) http://sbu.saglik.gov.tr/hastahaklari/bali.htm

[3] (09.03.2014) http://www.datamed.com.tr/telemedicine.html

[4] (09.03.2014) http://bolibo.typepad.com/blog/2009/04/history-and-evolution-of-telemedicine.html

[5] V. Bayraklı, E. Güvenoğlu,"Medikal Görüntülerde Doktor-Hasta Bilgi Gizliliğinin Sağlanması",Akademik Bilişim 2013,Antalya,23-25 Ocak 2013.

[6] (13.03.2014) http://andacmesut.trakya.edu.tr/bgt/Ders1.ppt

[7] (13.03.2014) http://andacmesut.trakya.edu.tr/bgt/Ders6.ppt

[8] *D.Sellars,"An Introduction to Steganography", Student Papers, 1999* http://www.zoklet.net/totse/en/privacy/encryption/163947.html

[9] A. Şahin, E. Buluş, M.T. Sakallı,"24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme", Trakya Üniversitesi Fen Bilimleri Dergisi, Edirne, Haziran 2006.

[10] A.Maity,"A new technique to hide information with in image file",MCA Thesis, October 2010.

[11] (11.03.2014)http://members.comu.edu.tr/boraugurlu/courses/bm223/content /week6/hafta6.pdf

[12] K. A. Navas, S. A. Thampy, M. Sasikumar,"EPR Hiding in Medical Images for Telemedicine",International Journal of Biomedical Sciences, January 1, 2008.

[13] Uğur Erdoğan, "**İleri Şifreleme Standardı (Advanced Encryption Standard – AES) Algoritmasının Bir Mikroişlemci Üzerinde Gerçeklenmesi**", Lisans Tezi, Elektronik ve Haberleşme Mühendisliği Bölümü, İstanbul Teknik Üniversitesi, Türkiye, 2008.

An Approach for Cyber Security Experimentation Supporting Sensei/IoT for Smart Grid

B. Genge, P. Haller, A. Gligor, and A. Beres

Petru Maior University of Tg. Mures, Mures, Romania
bela.genge@ing.upm.ro, phaller@upm.ro, agligor@upm.ro, adela.beres@gmail.com

***Abstract*—We propose SCYAMIX, a middleware aimed at facilitating cyber-physical security experimentation with Sensei/IoT* standard proposal and physical processes for Smart Grid. Sensei/IoT* represents the first joint effort involving ISO, IEC, and IEEE to provide a Semantic Web 3.0 standard for Sensor Networks, M2M and IoT. The proposed middleware fuses together distributed Sensei/IoT*-compliant communication architectures and protocols with real-time software simulators to enable disruptive cyber security experiments. A case study is presented to demonstrate SCYAMIX's ability to recreate Smart Grid architectures involving complex physical processes and cyber security scenarios.**

***Keywords*—Smart Grid, security, middleware, Sensei/IoT*.**

I. Introduction

NOWADAYS, Smart Grid is commonly recognized as the next generation power grid. Through the pervasive adoption of modern Information and Communication Technologies (ICT), Smart Grid improves operational benefits of control, reliability and safety, and provides advanced two-way communication, more flexible integration of heterogeneous measurement and sensor-actuator networks.

Although the adoption of generic off-the-shelf ICT in Smart Grid provisions indisputable advantages and benefits, it raises several issues concerning the reliability and security of communications and control systems – the core infrastructure of Smart Grid. The impact of generic malware on the normal functioning of Industrial Control Systems (ICS – part of Smart Grid core) can be devastating if we simply consider the published attack reports on ICS. Of course, the construction of a comprehensive list of events and attacks is difficult to achieve in the industrial setting, mainly because of non-disclosure policies adopted by different stakeholders. Therefore, most reported events cannot be chronologically ordered, since the actual discovery date of malware does not coincide with the actual infection time of the system.

Nevertheless, the year 2010 can be seen as a turning point in the perception of security in the industrial setting. This is mainly attributed to the discovery of Stuxnet [1], the first malware specifically designed to attack ICS. Stuxnet is also the world's first (discovered) malware capable to rewrite the control logic of ICS hardware and to actually hide its presence by exploiting several zero-day vulnerabilities. Unfortunately, the discovery of systems infected with Stuxnet malware is not limited to the year 2010 and other Stuxnet targets have been discovered at different power plants and installations from southern Iran in 2012 [2]. The potential impact of cyber attacks in the power sector has been highlighted by the Tempe, AZ incident [3] from 2007. In this particular case an improper configuration of load shedding programs caused the opening of 141 breakers and a loss of significant load, which subsequently led to a 46 min power outage affecting almost 100 000 customers.

In this context, the deployment of effective protective mechanisms for future infrastructures such as Smart Grid requires novel testing facilities with complex features embodying the cyber and physical dimension of these critical infrastructures. To address this issue, a substantial number of approaches have been documented in research publications. As such, we find a wide range of testbeds and middleware aimed at facilitating cyber-physical security experimentation with Smart Grid and other industrial infrastructures [7-12]. In the particular case of Smart Grid, a commonly addressed problem is the actual architecture and protocols which will enable the deployment of large-scale infrastructures consisting of a wide variety of devices and systems such as Customer Energy Management Systems (CEMS), Distributed Energy Resources (DER), Advanced Metering Infrastructures (AMI), and so on.

To alleviate the aforementioned issues, this paper proposes *SCYAMIX*, a middleware combining the distributed communication features of HERMIX platform [4] with the real-time simulation capabilities of AMICI [5]. In a nutshell, SCYAMIX enables real-time cyber-physical security experimentation with the recently proposed Sensei/IoT* standard [6]. It implements basic communication and architectural features defined within Sensei/IoT*, and it enables the execution of disruptive experiments against physical infrastructures through the adoption of distributed simulation software.

Although, as shown in the following section, in the literature we find several approaches and middleware for Smart Grid, to the best of our knowledge, the approach presented in this paper is the first attempt aiming at providing experimentation features combining a Sensei/IoT* standard-compliant

architecture and protocols with simulated physical processes.

The remaining of this paper is organized as follows. Section II provides an overview of related work. The proposed approach is presented in Section III and experimental results concerning a specific cyber security case study is presented in Section IV. The paper concludes in Section V.

II. Related Work

In this section we provide an overview of the state-of-the-art for Smart Grid architectures. AMI (Advanced Metering Infrastructure) is an important part of the Smart Grid system and several researches have been carried out for making it scalable and operational during outages.

In the work of Zaballos, *et al.* [7], an architecture based on wireless networks and communication power lines for Smart Grids is proposed. The authors concentrate on the communication infrastructure and on the importance of integration of different communication protocols and standards. The paper also documents the successful adoption and application of International Telecommunication Union (ITU) USN/NGN to Smart Grid architecture.

SeDAX (Secure Data-centric Application eXtensible platform) is the platform proposed by Young-Jin Kim, *et al.* [8, 9]. SeDAX uses Delaunay Triangulation (DT) graphs to provide and information-centric communication in the grid. Its architecture focuses on data availability and communication resilience by using a geographic hash forwarding algorithm and a DT-based data replication scheme. The algorithm is evaluated and compared with other geometric-based alternatives based on route tables size, message overhead, delivery performance and replication cost.

Zhou, *et al.* [10] introduced a new performance metric – Accumulated Bandwidth Distance Product (ABDP) to evaluate communication architectures for AMI in Smart Grid. The metric, based on greedy algorithm, was tested on Distributed MDMS (Meter Data Management System) architecture, a fully distributed architecture and centralized communication architecture. Results proved that distributed architectures have more benefits compared to centralized ones.

Athreya and Tague [11] proposed a self-organizing mesh hierarchy to assure the operability of AMI during outages based on a distributed Time Division Multiple Access (TDMA). The model's performance was evaluated using a wireless TDMA modeler, which proved to assure consistent performance during outages.

Finally, we mention the work of Siaterlis, *et al.* [12], where a generic testbed was proposed to enable security studies with cyber-physical systems. The approach employed emulation testbeds to recreate ICT hardware and software and the AMICI simulation software to recreate the behavior of physical processes.

Compared to the previously mentioned approaches, the novelty of the middleware proposed in this paper is that it enables cyber security experiments with an emerging standard, i.e., Sensei/IoT*, ensuring at the same time an accurate recreation of cyber and physical dimension of Smart Grid.

III. Architecture and Description of the Proposed Middleware

In this section we provide a description of the proposed middleware. We start with an overview of the emerging Sensei/IoT* standard and we continue with a brief presentation of the two main components of the proposed middleware: HERMIX and AMICI. Finally, we present the proposed architecture which fuses several technologies and software to enable a wide range of features for cyber security experimentation with Smart Grid.

A. Sensei/IoT: from XMPP to Smart Grid*

The Extensible Messaging and Presence Protocol (XMPP) protocol, developed in 1999 by the Jabber open-source community was intended for near real-time instant messaging, presence information, and contact list maintenance.

The XMPP is an open Extensible Markup Language (XML) protocol which defines the way of XML content streaming. It has been used in many applications, most importantly the Smart Grid in the case of the Internet of Things applications.

Since 2002 the XMPP working group established by Internet Engineering Task Force (IETF) has made efforts for standardization. Initially, four specifications (RFC 3920, RFC 3921, RFC 3922, RFC 3923) were created that lead in 2004 to a Proposed Standard. In 2011, first specifications were replaced by RFC 6120 and RFC 6121, and new ones were added such as RFC 6122.

Besides the mentioned core protocols, the XMPP Standard Foundation takes part at the new open XMPP extensions development also known as XEP stanzas. These are not singular and therefore joint attempts for global, open standards among global players are noticed. We mention here the ISO/IEC/IEEE P21451-1-4 XMPP standard, outlined in the following sub-sections.

1) ISO/IEC/IEEE P21451-1-4 XMPP Overview

ISO/IEC/IEEE P21451-1-4 XMPP Interface Standard is also known as *Sensei/IoT** and represents the first joint effort amongst ISO, IEC, and IEEE to design a Semantic Web 3.0 Sensor Standard for Sensor Networks, M2M and IoT.

The main goal of the Sensei/IoT* standard is to demonstrate the assured interoperability, scalability, and security using the XMPP protocol. The scope of the standard concerning Smart Grid can be summarized in the following main points: (i) electric power generation by offering access to data sharing on energy usage, primary energy cost or greenhouse gas emission; (ii) renewable energy based generation and storage systems by offering access to data concerning the primary energy and stored energy availability; (iii) transmission system on lines and busses fault detection; (iv) distribution system on microgrid integration and substation controls; (v) consumer side on using smart metering, the management of the local generation and storage capabilities.

2) Sensei/IoT Main Features*

Smart grid implementation based on Sensei/IoT* standard

must answer a series of key challenges concerning: effectiveness of Internet usage, interoperability, scalability, session persistency, cyber vulnerability, cyber exposure, presence detection, security, etc. Many of these challenges are covered by the new proposed standard. We mention some of these features:

- Technology agnostic and protocol independent.
- The use of the Transport Layer Security (TLS) for data traffic encryption built into the protocol.
- Meta Data Isolation (MDI) and intrusion protection against cyber-attacks.
- Usage of the Semantic Web 3.0 based on XML metadata for providing semantic conversation between devices.
- Usage of a Service Broker as a trusted intermediary to establish a trust relationship between users, applications, and devices.
- Possibility to use an Identity Provider (IdP) in order to provide Single Sign On (SSO).
- Support end-to-end digital signing and encryption based on RFC 3923 Efficient XML Interchange (EXI).

3) Remarks on Using Sensei/IoT standard*

Adopting in the existing or newly emerging Smart Grid the Sensei/IoT* standard can provide a series of benefits such as interoperability, scalability and security. It can be used at any level of a Smart Grid allowing the harmonization of protocols by enabling operation between new and legacy protocols.

Many advantages are given by the characteristics of the XMPP protocol: the technology and protocol independence allows decreasing costs and complexity; XMPP can facilitate a transition to new IEC standards; XMPP offers trusted messages transmission solutions and an easy usage in case of dynamic addressing issues; it has built-in cyber security protection mechanisms.

B. HERMIX Platform

The HERMIX platform [4] developed by Vitheia consortium was designed to collect, store and analyze large amount of data coming from a diversity of nodes, ranging from sensors to high resolution cameras.

The platform can be viewed as a set of interconnected nodes (physical resources, users, automation scripts, services) with a layered architecture. Every node represents an information provider or a consumer. The logical management layer has a service oriented architecture and it is responsible for formatting and extracting the data, for automatic analysis and processing. This layer also manages the proper authentication, authorization and access control mechanisms and assures the interconnection with other systems. The lower communication layer uses the event-driven architecture that follows a publish-subscribe pattern for small and structured data exchanges between nodes. The data storage layer hides the used underlying database system and at the same time it provides storage support for this hybrid communication model.

The features embedded within XMPP, including federation across domains, authentication, end-to-end signing, object encryption and its security support even for mobile endpoints make it a good candidate for industrial applications. The platform uses XMPP for meta-data exchange (like session initiation, device managing requests, etc.) and small structured data generated by endpoints (e.g., events: a switch changes its state, an alarm sensor detects movement). For high quantity, binary data, e.g., video and audio streams, an out-of-band protocol is used depending on the type of stream. At the highest level there is a set of interconnected XMPP servers running over the Internet. The distribution of the XMPP servers ensures proper load distribution, interconnection between resources managed by different authorities.

On the XMPP server level the proposed platform features are implemented in a server side component which exposes basic and common functionalities to be used by the other modules. Those functionalities include: communication with the XMPP server and message routing between the connected nodes; node management; interconnection with the physical bus; authorization management; and persistent storage.

To assure the interoperability between different vendors' specific devices a dedicated module needs to be created for every type of industrial bus (e.g., LON, CAN, EIB, Modbus, etc.). The module communicates with the specific bus and transforms the physical devices information into node representation. The node is not necessarily hosted on the resource itself, it acts as a host for a set of resources connected to the same bus. The module and the delegate nodes assure the protection of the low capability resources, e.g., low power sensor nodes, from external attacks implementing proper authorization and encryption mechanism.

A node identified in XMPP world by a unique *JID* (Jabber ID) is defined by a set of features, status information, received commands, and generated events. Taking into account the heterogeneity of existing protocols, new types can be described, but the main goal of this resource model is to provide homogeneity at the description level. A node can be dynamically created by the Node Manager based on an XML description or based on the image saved in the database. The Node Manager collects and saves automatically every modification in the registered node data in the Object Archive. When a saved data is required, it is loaded into memory and transformed into its runtime C++ representation.

The discovery mechanism is used to obtain information about devices, their features or events, using the standard Service Discovery protocol defined in the XMPP extension XEP-0030 [13]. The state is divided into several parts to assign different privilege levels to the state variables. The events are also organized hierarchically and different events require different privileges to subscribe to them. A user subscribing to a collection node (an event node tree) will receive events generated by all the descendants of the collection node.

The transport of the binary data from a source to multiple destinations is handled by the Controller nodes. The access to the binary archives is also done indirectly, through the controllers. The Controller poses two types of communication

channels: one for controlling the way data is distributed based on XMPP protocol; other for actual large data transport. The controller is exposed in middleware as a delegated node attached to a component.

The Object Manager also enforces permission policies managed by an Authorization Manager. Permission attached to an object is represented as a set of tuples (object id, list of permission types, a set of bare JIDs, set of groups). When the Object Manager needs to authorize access to an object, it will request the object's access control list (if not already cached) from the Authorization Manager. The maximum caching interval is imposed by the Authorization Manager and must be invalidated if it is changed. Separation between permission validation and permission management assures the third-party integration.

C. AMICI Platform

The *Assessment platform for Multiple Interdependent Critical Infrastructures* (AMICI) [5] provides software simulators to recreate the physical dimension of critical infrastructures such as Smart Grid. AMICI was developed from the need to provide real-time multi-model experimentation capabilities supporting cyber security studies concerning critical infrastructures. Its architecture, depicted in Figure 1, includes two main components: a simulation unit denoted as *Sim*; and a proxy unit, denoted as *Proxy*.

The main role of the simulation unit (Sim) is to run the physical process model in real-time. This is achieved by coupling the model time to the system in such a way to minimize the difference between the two. Models are constructed in Matlab Simulink from where the corresponding 'C' code is generated using Simulink Coder. These are then integrated using an XML configuration file that provides the required flexibility so that researchers do not need to modify AMICI's source code.

From the *Sim* unit's point of view each model is seen as a set of inputs and outputs. These are mapped to an internal memory region (I/O MEM) that is read/written by other software modules as well. The Sim unit allows an open access to its I/O MEM by implementing OS level shared memory operations. This way, AMICI enables interaction with ad-hoc software that can write specific model inputs, i.e., OPEN/CLOSE a valve, and can read the status of the model, i.e., measured voltage. Interaction with other Sim units is enabled by implementing not only RPC (Remote Procedure Call) server-side operations but client-side calls as well. By using only the XML configuration file, the Sim unit can be configured to read/write inputs/outputs of models run by remote Sim units. These are mapped to the inputs/outputs of the model running locally, enabling complex interactions between models running in parallel on different machines. The Proxy unit has several roles within AMICI. First of all, it is able to run remote control code, thus enabling the integration of more complex control hardware emulators. At the same time, it can be used to handle Modbus protocol calls, transforming them to RPC calls and finally sending requests to the Sim unit.

As demonstrated in [12], AMICI can be applied to a wide range of security experiments. Its software units have been tested with several physical process models such as oil-fired electrical power plants, chemical processes, railway systems, and large-scale power grid models. AMICI's software units are available as open source under EUPL license and can be freely downloaded from SourceForge (http://sourceforge.net/projects/amici/).

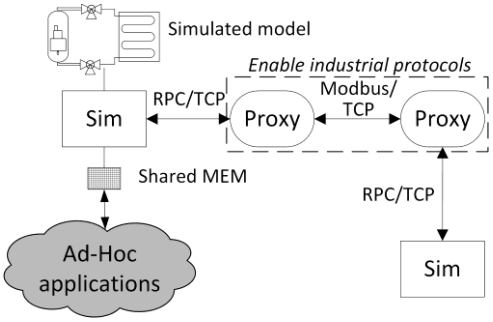


Figure 1: Architectural overview of AMICI.

D. SCYAMIX: Fusing HERMIX With AMICI

We propose *Smart grid CYber security assessment platform based on AMIci and hermiX (SCYAMIX)*, which fuses together the communication features provided by HERMIX with the physical process simulation capabilities brought by AMICI. SCYAMIX is thus able to provide realistic communication architectures and protocols which have been proved to be well-adapted to large infrastructures such as the Smart Grid [4]. At the same time SCYAMIX brings additional capabilities to enable the recreation of the physical dimension, which constitutes a significant component of any industrial system.

Fundamentally, from an architectural point of view, SCYAMIX provides capabilities to recreate the cyber and physical dimension of Smart Grid. For the cyber dimension SCYAMIX adopts HERMIX to provide real software and protocols running on real networking infrastructures. This approach is well established in the field of cyber security, since the use of real infrastructures provides high fidelity of results and in many cases it can capture not only whether a system will fail but also how it will fail. In contrast, the use of simulation to recreate the cyber dimension of Smart Grid would provide an effective approach to model normal network and software conditions, but it would fail to capture the way computer networks fail. This aspect has been well documented and studied by previous work [12, 14, 15, 17].

For the physical dimension SCYAMIX uses simulation since this provides an efficient, low-cost and safe approach to recreate the physical dimension. Apparently, this might be interpreted as a lack of realism and low experiment fidelity, however, the use of software simulation for cyber security experimentation scenarios enables disruptive experiments on multiple heterogeneous physical processes.

This is not possible with production systems since security and resilience tests entail risks of potential side effects to mission critical services [16]. Furthermore, today several complex models are freely available and are actually applied in different industries. For example, in the energy sector

simulation has become so accurate and trusted that it is commonly used to aid decision making between transmission system operators.

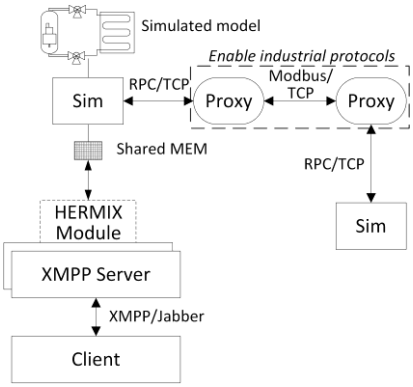


Figure 2: SCYAMIX architecture.

The architecture of SCYAMIX, as a result of fusing HERMIX and AMICI is depicted in Figure 2. The procedure followed for this purpose exploits the features provided by each of the two software platforms. As such, we implemented an additional HERMIX module to access the shared memory region created by AMICI's simulation unit. Model inputs and outputs are written and read by the implemented module, ensuring the required communication between cyber components and the simulated physical processes.

Devices exposed by simulated models, e.g., valves and sensors, are given different JIDs and are accessed through standard XMPP stanzas. Each device is registered in the HERMIX database (MongoDB) and users (client software) can subscribe to receive events. The proposed platform is thus compatible with any client software implementing an XMPP communication interface according to the standard description. This provides a powerful feature and enables the integration of heterogeneous software which can interact with simulated physical processes in a wide range of scenarios.

IV. Case Study

In this section we present a case study showing the applicability of the proposed middleware. We start by presenting a description of the experiment setup and scenario, and we continue with the presentation of results.

A. Experiment Setup and Scenario

The aim of this particular scenario is to illustrate the interdependence property of physical processes and how this property can be used to detect attacks/faults by indirect monitoring of process parameters. The experiment also shows the applicability of the proposed middleware in constructing realistic Smart Grid scenarios and conducting realistic cyber security experiments.

For the physical process we adopted the IEEE 39-bus New England system [18], representing a portion of the American Electric Power System as of early 1960. The model is run by a simulator unit and includes 39 buses, i.e., substations, together

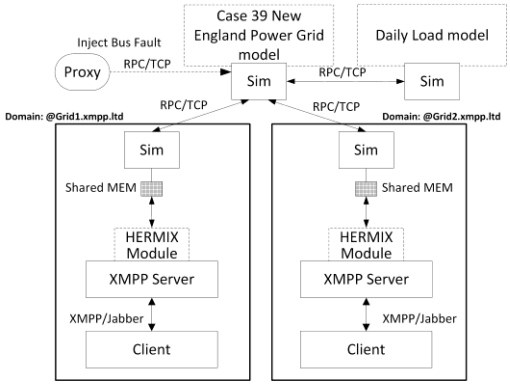


Figure 3: Experiment setup.

with 10 generators. The daily load applied to our system derives from real data [19] and is run in parallel with the power grid model by a separate simulation unit.

We defined two separate XMPP/Jabber domains: *@Grid1.xmpp.ltd* and *@Grid2.xmpp.ltd*. As it would happen in reality, we used each domain to monitor a subset of substations. More specifically, client applications in *@Grid1.xmpp.ltd* monitored buses 1 to 18 while client applications in *@Grid2.xmpp.ltd* monitored buses 19 to 39.

The disturbance we applied to the grid consisted of a 100ms bus fault issued with the help of Proxy unit from AMICI software. The fault replicates the effect of an attack on the power grid which causes circuit breakers to trip, which finally leads to a brief disconnection of a specific bus from the grid. The experiment setup is depicted in Figure 3.

B. Experimental Results

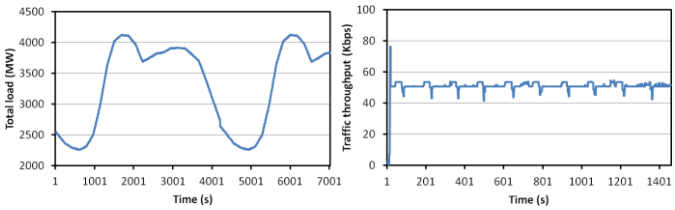
The daily load applied to the grid during this scenario is similar to a typical daily load curve and is depicted in Figure 4 (a). The XMPP traffic measured in both domains is highly regular and mostly constant, as shown in Figure 4 (b). The visible bursts in the same figure are caused by concentrator timer mechanisms implemented within HERMIX modules.

In Figure 5 we have depicted the measured voltages in the two power grid domains. As shown in both sub-figures, voltages are highly sensitive to the injected disturbance. The bust fault is applied to bus 1, belonging to the first domain, and the effect of this action is clearly visible in Figure 5 (a).

The injected disturbance is highly visible in the second domain as well (see Figure 5 (b)). Here we recorded voltage collapse for only one bus (bus 39), which is directly connected to bus 1. Nevertheless, the effect is also visible on the voltage level of all the other buses.

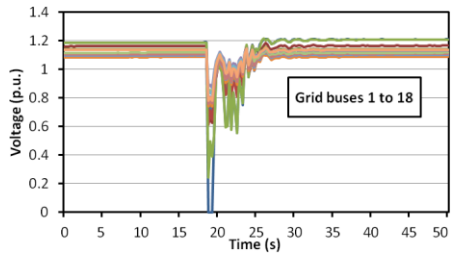
This close relationship between different power grid substation voltages comes from the interconnections and interdependencies between different buses. Electricity grids require the establishment of a certain balance between the generated and consumed power. When this balance is disturbed, there can be serious consequences leading to power failure and massive black-outs. Cyber attacks might have a similar effect to the one reported in this study, since circuit breakers and control mechanisms have the ability to respond to

commands issued remotely. These can lead to severe loss of load which can have a similar effect to the Tempe, AZ incident [3] from 2007, as mentioned earlier in this paper.

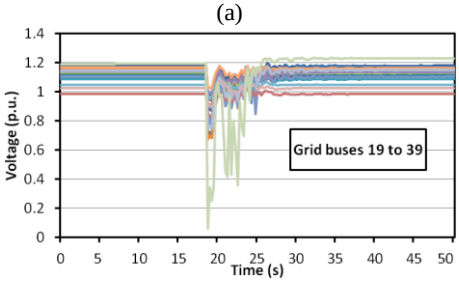


(a) (b)

Figure 4: Daily load (a) and XMPP traffic throughput in the first domain (b)



(a)



(b)

Figure 5: Measured disturbance on power grid by client in *@Grid1.xmpp.ltd* (a) and by client in *@Grid2.xmpp.ltd* (b)

V. Conclusion

The middleware proposed in this paper provides a suite of software components and protocols to enable cyber security experimentation with the recent Sensei/IoT* standard proposal. The approach builds on cyber security experimentation capabilities that glue together the cyber and physical dimensions of Smart Grids. The XMPP/Jabber-compliant cyber architecture of SCYAMIX is complemented by physical process simulation capabilities, which enable disruptive experiments on complex process models.

We believe that SCYAMIX advances the state of the art from several perspectives: (i) the approach fuses a XMPP/Jabber-compliant implementation with software simulators in order to provide a complex set of features; (ii) the middleware is highly scalable, supporting scalable cyber and physical dimensions of Smart Grid; and (iii) to the best of our knowledge SCYAMIX is the first reported approach providing a Sensei/IoT* compliant implementation combining communication architectures and protocols with real-time software simulation. As future work we intend to extend SCYAMIX's capabilities and to test its performances in scenarios including real sensor networks.

Acknowledgment

This research was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme.

References

[1] T. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, April 2011.

[2] BBC News, *Iran 'fends off new Stuxnet cyber attack'*, 22 December 2012.

[3] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*, New York, Momentum Press, May 2010.

[4] P. Haller, A. Bica, and I.C. Szanto, "Middleware for heterogeneous subsystems integration in health care services," *Interdisciplinarity in Engineering International Conference*, Tirgu Mures, pp. 349–354, 2012.

[5] B. Genge, C. Siaterlis, and M. Hohenadel, "AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures," *7th International Conference on Critical Information Infrastructures Security*, Lillehammer, Norway, Lecture Notes in Computer Science 7722, pp. 228–239, 2012.

[6] M. Presser, P.M. Barnaghi, M. Eurich, and C. Villalonga, "The SENSEI project: integrating the physical world with the digital world of the network of the future," IEEE Communications Magazine, vol. 47, no. 4, pp. 1-4, April 2009.

[7] A. Zaballos, A. Vallejo, and J.M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Network*, vol. 25, no. 5, pp. 30–37, 2011.

[8] Young-Jin Kim, Jaehwan Lee, G. Atkinson, Kim Hongseok, and M. Thottan, "SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1119-1136, July 2012.

[9] M. Hoefling, C.G. Mills, and M. Menth, "Analyzing storage requirements of the resilient information-centric SeDAX architecture," *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 306-311, Oct. 2013.

[10] Jiazhen Zhou, R.Q. Hu, and Yi Qian, "Scalable Distributed Communication Architectures to Support Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1632-1642, Sept. 2012.

[11] A.P. Athreya and P. Tague, "Self-organization of a mesh hierarchy for smart grid monitoring in outage scenarios," *2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1-6, Feb. 2013.

[12] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, Dec. 2013.

[13] XEP-0030: Service Discovery, 2008, http://xmpp.org/extensions/xep-0030.html.

[14] R. Chertov, S. Fahmy, B. Ness Shroff, "Fidelity of Network Simulation and Emulation: A Case Study of TCP-targeted Denial of Service Attacks," *ACM Trans. Model. Comput. Simul.*, vol. 19, no. 1, pp. 4:1-4:29, Jan 2009.

[15] B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera, "A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems," *Computers and Electrical Engineering*, Elsevier, vol. 38, no. 5, pp. 1146-1161, 2012.

[16] D. Duggan, "Penetration testing of industrial control systems," Technical Report, SAND2005-2846P, Sandia National Laboratories, 2005.

[17] B. Genge and C. Siaterlis, "Analysis of the effects of distributed denial-of-service attacks on MPLS networks," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 87-95, 2013.

[18] University of Washington – Electrical Engineering, "Power Systems Test Case Archive," http://www.ee.washington.edu/research/pstca/

[19] M. Manera and A. Marzullo, "Modelling the load curve of aggregate electricity consumption using principal components," *Environ. Model. Softw.*, vol. 20, no. 11, pp. 1389-1400, Nov 2005.

Biometric Authentication Systems

An Evaluation of Current Technologies and Study of Asus SmartLogon Face Recognition

Christopher Hale, Lei Chen

Salesforce.com Portland, OR chale@salesforce.com
Sam Houston State University, Huntsville, TX, chen@shsu.edu

***Abstract*— Biometrics is emerging as an effective and efficient technology in industry for authentication and access control. It has been shown to perform acceptably well and has multiple advantages, such as low false acceptance rate, over traditional authentication technologies. It is also emerging as a means of authentication for personal use, and many notebook computers and mobile devices come equipped with the hardware and software to utilize biometrics. This paper seeks to evaluate common biometric practices and their effectiveness. It also analyzes one specific personal biometric solution: Asus SmartLogon face recognition and catalogs its performance in the real world, demonstrating where this system excels and where it falls short.**

Keywords - Biometrics, performance, evaluation, Asus, SmartLogon, authentication, digital, security.

I. Introduction

We live in a computer age. As time progresses, we become increasingly dependent on computers and related technologies for our daily lives. These technologies make seemingly menial and basic tasks streamlined and easier to handle. Even complex and involved activities are being bestowed upon computer systems due to their convenience and expediency. With the growing amount of information and responsibility placed on computer systems comes an increased threat of misuse and abuse of these systems. Safeguards must be developed in conjunction with technology in order to ensure its safety. One such safeguard is the field of biometrics.

In the realm of security, authentication is one of the largest problems faced by software engineers. By design, computer interfaces do not take into account the individuals using them, but rather the credentials they provide. Illegitimate users who have obtained false credentials are a threat to this system. Luckily, biometrics offers a way to eliminate this problem effectively in most scenarios. There are several authentication methods that are accepted throughout the industry. These authentication protocols typically use three methods of authentication: something you have, something you know, and/or something that you are. Biometrics uses the latter of these three.

Biometrics is a means of personal identification that uses physical characteristics to authenticate users of a system. Biometrics may use a number of different authentication mediums, such as fingerprint, retina and iris scans, face, voice, hand geometry, handwriting, body odor, ear, and lip geometry. By using these unwavering physical characteristics, we gain several advantages over more traditional methods of authentication such as a username/password combination or keycards.

Before any emerging technology can hope to see industry-wide success and implementation, it must certainly undergo thorough testing and evaluation. As one of these newcomers to the field of authentication and security, biometrics is also subject to this scrutiny. What follows is an examination of current biometric technologies, their functions, and an analysis of personal user-based biometric software.

II. Background

A. Advantages of Biometric Systems

Biometrics possesses several key advantages for use as an authentication mechanism. Biometrics can be more reliable because an individual's biometric identity normally is unique. Consider the example of fingerprints: no two people have an exact matching set of fingerprints. This simple fact creates an advantage over passwords, as there are common passwords such as 'password' or '12345' that are common amongst many users [1]. This makes an attack on weak passwords possible by malicious attackers, while biometrics does not face the same threat. Another key benefit of biometric systems is that of persistence. A biometric signature is always with the user, and it cannot be forgotten. Users often have to write down passwords in order to remember them, especially in systems that require advanced alphanumeric passwords, which may lead to theft or loss of the password. This scenario is not possible with advanced biometrics systems and technologies. A user cannot forget their iris or misplace their fingerprints, and compared to stealing passwords, it is generally more difficult for hackers to steal clear iris scans (e.g. from a HD photo) and good quality fingerprints (e.g. from a glass). Biometrics, such as facial scanning, is also advantageous because they are universal. Every typical user has the features

that the system utilizes. These features are also relatively constant. Throughout a user's life, their retinal and fingerprint signatures will not change naturally.

B. Biometric Data Gathering and Comparison

A biometric scan typically begins as an image file. However, using images for storage and authentication often proves to be problematic. To store high resolution images of all users in a system would require extremely large amounts of storage space. Worse yet, performing comparisons on this data are even more problematic. To demonstrate this, consider the fingerprints in Figure 1.

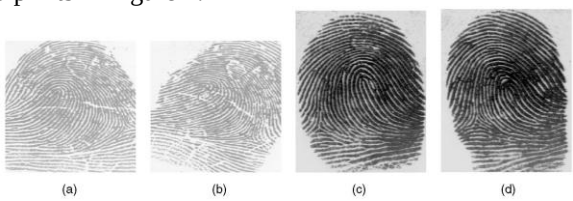


Figure 1. Examples of fingerprints.

These are typical scans from users of a fingerprint based biometric system. Prints (a) and (b) belong to the same user, while prints (c) and (d) each belong to different users. Performing a simple query into a database of employee fingerprints (employees) on the given fingerprint (print) such as 'SELECT name FROM employees WHERE print = fingerprint' will fail. Although prints (a) and (b) belong to the same user, the images appear to be quite different. Similarly, performing a modified query such as 'SELECT name FROM employees WHERE print LIKE fingerprint' will also not work. Although prints (c) and (d) belong to different users, they appear to be quite similar. An efficient biometric system must be able to differentiate among such scenarios. If images are used, this task is impossible or extremely difficult. How then do biometric systems perform these comparisons? The answer is minutiae.

Minutiae are small attributes within a fingerprint or other biometric scan [2]. These attributes deviate from the normal ridges, blood vessels, or face geometry found in a biometric scan and can be used to form a unique signature for each individual. In biometric systems that use fingerprints, there are a multitude of different minutiae that can be used. These include bifurcation, double-bifurcation, trifurcation, and opposed bifurcation, etc. When a scan is made, the biometric system identifies the minutiae and uses them to calculate the signature of the image [3]. Depending on the medium used, exact procedures for this phase may differ, however the algorithms perform essentially the same function. One of the most widely accepted algorithms for calculating fingerprint signatures is the Delaunay Triangle, which makes use of the minutiae by calculating angles of their relationship to one another [4]. Based on these calculations, a biometric signature is created. This method helps solve several problems within a biometric system. First of all, the size of the database needed to store biometric data is greatly reduced. Switching from several megabytes of image data for each scan to at most 64 bits for numeric data vastly cuts down on size. Comparisons of data are also much easier to perform, as comparing numbers is much faster and more efficient than an image comparison.

III. Biometric Applications

Any well conceived and implemented biometric system may look great on paper, but performance in the real world is the true test of its applicability and effectiveness. A recent study was conducted to evaluate several different biometric systems in the workplace in order to establish a baseline for performance and a means of comparison.

A. Previous Studies

In the realm of biometrics, there are two main figures used to evaluate the effectiveness of a system or implementation: False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR measures how often a system allows an illegitimate user to be authenticated under the guise of a legitimate user, while FRR measures how often a legitimate user is falsely denied access into the system. Of these two, as far as security is concerned, FAR is clearly the most critical statistic. Allowing users to be authenticated who should be denied is much worse of a security problem than denying legitimate users. False acceptance brings with it a drastic security risk. A good biometric system should be able to minimize or completely eliminate these numbers. In practice, however, this is difficult to achieve.

A recent study [5] was conducted in order to evaluate the effectiveness of biometric systems in the real world in terms of their FAR and FRR rates. For this study, the five most widely used biometric systems were compared: face, fingerprint, hand, iris, and voice based biometrics. In order to determine effectiveness, these systems were rated on false acceptance and false rejection rates as well as efficiency of enrolling. Enrolling involves getting a quality scan for the baseline in the system. This experiment was conducted under a normal office setting, which is a typical environment for biometric systems. During enrolment, all technologies performed very well. The only errors were two individuals with fingerprints that were damaged to the point of enrolment failing and a user with a blind eye that was not able to enroll via an iris scan.

An important variable in calculating false acceptance and false rejection was the threshold of error for the biometric system. All biometric systems have a level of 'tolerance' for matches. As the level is raised, fewer false rejections are made. On the other hand, if the tolerance is set too low, the system is prone to false rejection. Each test began with a subject attempting to access the system three times in each medium with a high tolerance. As the test progressed, the tolerance was raised. The clear winner was the iris biometric system. It achieved only a 1.8% false acceptance rate, even with the tolerance set at its highest [5]. A close second was fingerprint scans, which performed well one the tolerance was lowered slightly. As the tolerance lowered, all of the systems began to perform equally well. This test served to demonstrate the performance of biometric system in real life, and their applicability to workplace security.

Biometrics does not always have to be applied to workplace security. India is at the forefront of a system called Universal ID [6]. This system seeks to keep biometric data on all of Indian citizens. This makes for rapid identification of all individuals in a manner more efficient than ID cards or other documents. The NSA also uses facial recognition biometrics through public transportation and terminals for monitoring and surveillance.

B. *ASUS SmartLogon*

The computer hardware and software manufacturer ASUS has taken a step forward in applying biometrics to operating system security. Many of their notebook computers and netbooks come bundled with SmartLogon, which utilizes the integrated or attached webcam to conduct biometric facial recognition and authentication. This feature replaces the usual username and password fields at the operating system logon screen in Windows based systems. A base scan is set up by the system administrator, and this scan is used to compare the provided scans at logon. By authenticating using facial recognition, it is assumed to be a more secure means of logging on. This method is not susceptible to password theft or cracking, and ensures that the person logging on is the user allowed by the operating system. In an ideal environment, this solution would be foolproof and prone to no errors. But how does this system perform in the real world? How does it hold up against malicious attacks? This research and testing seeks to answer those questions.

IV. Experimentation and Results

In order to evaluate SmartLogon, the FRR and FAR values were computed in varying lighting and environmental conditions as well as varying tolerances. To begin, the system was tested with optimal conditions: ample lighting, static facial expression, and good base scan across the tolerance ranges. As expected, these conditions produced favorable results. These tests were continued with degrading conditions and scans across the tolerance levels. To compute each value, 100 login attempts were attempted at each tolerance and condition level.

A. *False Rejection Rate*

Figure 2 shows a summation of the results of testing at each tolerance level and it's computed FRR. These tolerance levels were preset in SmartLogon and are not able to be granularly controlled other than high, medium, and low.

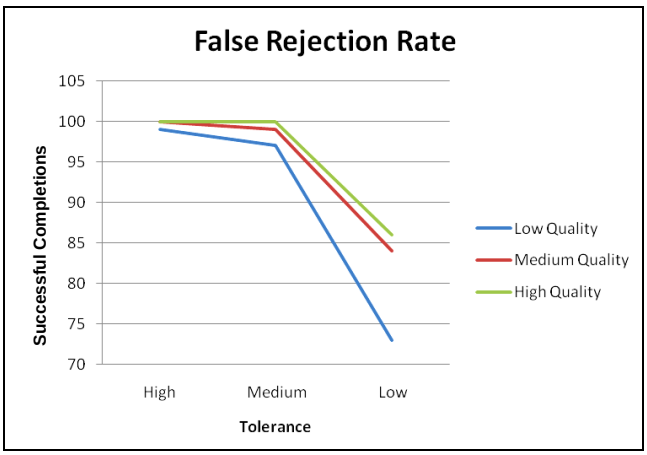


Figure 2. False Rejection Rate (FRR) test results.

As expected, each quality of scan had fewer false rejections when the tolerance was greater. As the tolerance decreased, each of the scans began to degrade in performance. Even one of the scans conducted in perfect conditions failed at the highest scrutiny associated with low tolerance.

B. *False Acceptance Rate*

The next figure to determine the performance of SmartLogon is the FAR. This test was conducted similarly through the varying condition and tWWolerance levels. The main difference is that instead of attempting to log in as a registered user, an attempt to log in as a malicious user was made.

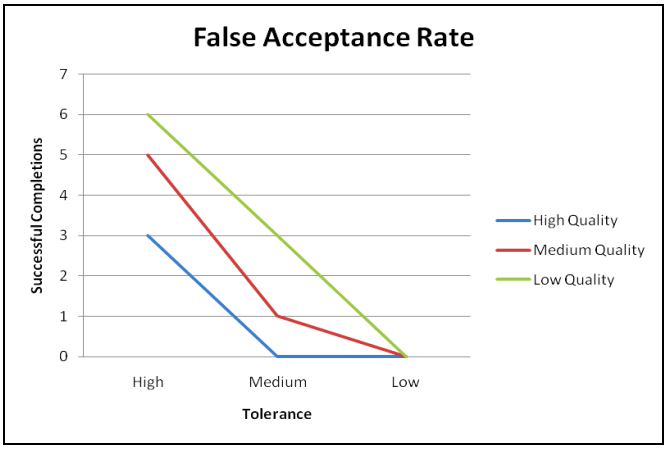


Figure 3. False Acceptance Rate (FAR) test results.

As indicated in Figure 3, SmartLogon has a decently low FAR when using high quality scans. When quality decreases, the FAR increases tremendously, almost doubling for medium quality and going as high as 6% for low quality. In the worst conditions and lowest tolerance, a substantial percentage of malicious users were allowed to log on. On the left side of the graph, we can see that with a high tolerance, a few false acceptances are allowed. As the tolerance is increased, false acceptances are decreased and eventually completely eliminated.

C. System Flaws

While SmartLogon has demonstrated high quality figures for its FAR and FRR, there are still other areas to consider. One of these is the susceptibility to attacks. With any biometric system, there is a constant threat of users trying to fool the system in order to spoof identity. One of the ways of doing this is making a copy of legitimate user's credentials (mold of a fingerprint, copy of photo, etc.) and presenting them as their own. To achieve this with the SmartLogon system, a printed picture of a registered user of the system and presented to the webcam for authentication. Unfortunately, this technique worked flawlessly every time. The system happily accepted the photograph and logged in the user pictured. This flaw creates a large security gap. Any individual who knows of a registered user in SmartLogon can obtain his/her photo and use it to gain access to the system. If combined with another form of authentication such as a password in order to create a two-factor authentication system, this attack is thwarted.

SmartLogon has several other fatal flaws in its operation. Any user is able to open up the console and add users or change the base facial scans for a user. This means that if an illegitimate user was to gain access to the system through either a false acceptance or another exploit, he can add his own scans into the system, effectively creating a backdoor to the system. In this way, the attacker does not have to rely on these attacks in the future as he simply is authenticated as a normal user. Another concern for this software is that there is no limit for the number of logon attempts. This makes brute force attacks and false acceptances more likely. Many security systems have an upper bound that will only allow a predefined number of failed attempts before flagging the logon as malicious. The addition of this feature would increase the security of the SmartLogon application. Although it does not affect the security of the application, unusual behavior was observed from the program that could impact its viability as an authentication system for some users. Scans taken in which the user is wearing glasses fail to authenticate. This is true for both sunglasses and reading glasses. This would cause quite an inconvenience for users who require these aids.

V. Conclusions and Future Work

The need for security in a digital age is an ever-growing concern. Securing our valuable sensitive information has become the focus of many areas of study and software development. Biometrics is a proposed solution to this problem and can often be more reliable than the currently accepted technologies. ASUS has taken the concept of biometrics and brought it to the end user operating system level. SmartLogon authenticates users and logs them into Windows based OS through the use of facial recognition. This software performs within the expectations of a biometric system during normal and strenuous operating conditions. It is not, however, without fault. SmartLogon is still susceptible to a number of exploits that are easy to conduct, even without any previous computer knowledge. With these flaws present, SmartLogon is not viable as an end-all security system. It should not be relied on for security of highly secret documents. It does serve its purpose as a front line defense from unauthorized users into a computer system.

Asus SmartLogon is only one of several comparable different personal end user based biometric authentication systems. There are a number of other facial recognition utilities that can be integrated into personal computers and smart phones with the intention of providing an extra layer of security. Apple has incorporated a fingerprint scanner, utilizing the Touch ID technology, into their most recent mobile device, the iPhone 5S. Attacks against this protocol have been demonstrated as effective means of circumventing this security control [7]. Future research should include an analysis of these other competing technologies to determine not only their individual performance, but performance in comparison to similar services. This would allow for selection of the best non-enterprise biometric software currently on the market.

(1) References

[1] Neil Yager and Ted Dunstone, "The Biometric Menagerie," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 2, pp. 220-230, Feb. 2010, doi:10.1109/TPAMI.2008.291.

[2] Marios Savvides, Karl Ricanek Jr., Damon L. Woodard, and Gerry Dozier, "Unconstrained Biometric Identification: Emerging Technologies," Computer, vol. 43, no. 2, pp. 56-62, Feb. 2010, doi:10.1109/MC.2010.55.

[3] Ron Vetter, "Authentication by Biometric Verification," Computer, vol. 43, no. 2, pp. 28-29, Feb. 2010, doi:10.1109/MC.2010.31.

[4] Michal Choras, "Emerging Methods of Biometrics Human Identification," in proceedings of ICICIC, pp.365, Second International Conference on Innovative Computing, Information and Control, 2007.

[5] Tony Mansfield, “Biometric Authentication in the Real World,” The National Physical Laboratory, (NPR) The center for Mathematics and Scientific Computing, Middlesex, United Kingdom, 2005.

[6] Karl Ricanek Jr., "Dissecting the Human Identity," Computer, vol. 44, no. 1, pp. 96-97, Jan. 2011, doi:10.1109/MC.2011.17.

[7] Frank, "Chaos Computer Club Breaks Apple TouchID," http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, 2013.

Toplumsal Olaylarda Sosyal Medyanın İletişimsel Rolü

N. Türkay

necatiturkay@hotmail.com

***Abstract*—The era in which we live witnesses rapid improvements in science and technology. On the other hand, societies express their reactions against political and social events happened utilizing technology that is the characteristic of the era. Social networks which are the means of media with internet databases recently popular are used as the means of protest of the individuals. Thus, social events and organizations are spread through broad social masses quickly by this means communicatively. By way of social means of media used frequently by activist groups, small and medium sized social action ideas may transform into mass actions and public security and the basic rights and the freedoms of the individuals may be grabbed in an environment of anarchy. Information technologies provided for the benefit of humanity may be used concurrently as the area of organization of the social events ruining the social peace and threatening the public order.**

Key Words – Social Events, Social Media, Communication

ÖZET — Yaşadığımız çağ bilim ve teknolojideki hızlı gelişmelere sahne olmaktadır. Bununla birlikte toplumlar, gelişen siyasi ve sosyal olaylar karşısında tepkilerini çağın niteliği olan teknolojiden faydalanarak ifade etmektedirler. Son zamanların adından çokça söz ettiren internet veri tabanlı medya araçları olan sosyal ağlar, bireylerin birer protesto aracı olarak kullanılmaktadır. Böylece toplumsal olaylar ve organizasyonlar iletişimsel olarak bu sayede kısa sürede geniş halk kitlelerine yayılmaktadır. Eylemci gruplar tarafından sıkça kullanılan sosyal medya araçları sayesinde küçük veya orta ölçekli toplumsal eylem fikirleri kitlesel eylemlere dönüşmekte ve kamu güvenliği kişilerin temel hak ve özgürlükleri bir anarşi ortamında gasp edilebilmektedir. İnsanlık yararına sunulan bilişim teknolojileri aynı zamanda toplumsal huzuru bozan ve kamu düzenini tehdit eden toplumsal olayların organizasyon alanı olarak da kullanılabilmektedir.

Anahtar Kelimeler— Toplumsal Olaylar, Sosyal Medya, İletişim

I. GİRİŞ

Toplumun en küçük yapısal birimi bireylerdir. Bireyler toplum içerisinde çeşitli rollerde ve toplumsal statülerde yer alırlar. Bu durum; bireylerin eğitim seviyesi, kültürel yapısı ve temel ihtiyaçları gibi etkenlere göre çeşitlilik kazanabilmektedir. Bireylerin birleşimi sosyal grupları, sosyal grupların birleşimi ve etkileşimi de toplumları oluşturmaktadır. Bireylerin toplum içerisindeki rolleri, toplumların yapısal özelliklerini oluşturarak toplumsal farklılıkları meydana getirmektedir.

Belirli bir coğrafi bölge üzerinde temel ihtiyaçlarını karşılamak için örgütlenmiş aralarındaki etkileşimi ve iletişimi düzenleyen kuralları ve kurumsal ilişkileri olan hem biyolojik hem de kültürel olarak kendisini yeniden üretecek mekanizmalara sahip, büyük insan topluluklarına toplum denir. [1] Toplum kavramı insanlık tarihi kadar eski ve sistemli bir yapı olarak ortaya çıkmaktadır. İnsanların tabiatla mücadele etmesi; birlikte yaşama olgusunu sağlamıştır. Böylece bireyler arasındaki etkileşim bireylerin sosyalleşmesini sağlamış ve toplumun temelleri bu şekilde atılmıştır.

Yukarıdaki tanımdan da anlaşılacağı gibi bireylerin bir coğrafi bölgeyi paylaşması, kişiler arasındaki örgütlenmeyi ve toplum içindeki örgütsel iletişimi de beraberinde getirmektedir. Toplumların örgütsel yapıları ile iletişimleri zamana ve yaşanılan çağın özelliklerine göre farklılık göstererek bugüne kadar gelmiştir. Tarihin en eski çağlarındaki iletişim araçlarının nitelikleri ve kapsama alanıyla; günümüz haberleşme nitelik ve yöntemleri arasındaki büyük fark, insanlık tarihinin uzun serüveninin geldiği en son ve göz kamaştıran noktayı göstermesi bakımından oldukça önemlidir. Gelişen teknoloji sayesinde toplumsal gruplar arasındaki hızlı ve ekonomik iletişim olanakları, toplumları toplumsal olarak alabildiğine hareketlendirmiş; internet ve bilgi teknolojilerindeki hızlı gelişmeler, bireylerin veri ve bilgi aktarımı imkânını sağlamıştır. Yeni medya araçları olarak adlandırılan sosyal medya, toplumların hareketlenmesinde toplumsal eylem ve olaylarda belirleyici iletişimsel roller üstlenmektedir. Bu şekilde bireylerin toplumsal olayları organize eden marjinal gruplara katılması, sosyal ağlarda "takipçi" ve "çevrimiçi" olmaları sosyal eylemlerin iletişimsel yapısı için yeterli olmaktadır.

II. TOPLUM VE TOPLUMSAL OLAYLAR

Belirli bir fiziki mekânda yaşayan, temelde kendi kendini korumak ve yaşamsal gereksinimlerinin karşılanması için ortak değer ve dünya görüşüyle birlikte hareket eden topluluk içinde sosyal ilişkiler içinde örgütlenen insan topluluklarına toplum denilmektedir. [2] Toplumu meydana getiren bireyler arasında çeşitli sosyal ilişkilerin olması, bireylerin toplumsal yapıda örgütlenebilmesini sağlamıştır. Toplum içinde bireylerin iletişimi, toplumun kültürünü ve yapısını şekillendirmektedir. Bu da toplumun bir olay karşısında tepkisini ve hareketliliği toplum değerlerine göre şekillenmesini gösterir.

Bireylerin bir arada yaşamalarının beraberinde getirdiği en önemli sonuçlarından biri de duygu, düşünce ve heyecanlarını müşterek olarak dile getirme arzusudur. Bu durum çoğu zaman toplumun ideoloji ve kültürü ile şekillenerek gerçekleşmektedir. Toplumların duygu ve düşünce yoğunluğunu topluca ifade edilmesi toplumsal hareketliliği ortaya koymaktadır.

Toplumsal hareketler; geniş bir toplum içindeki tutumları, davranışları ve sosyal ilişkileri değiştirmek üzere uyumlu çabalara girmiş insanlardan meydana gelen bir gönüllü birlik olarak tanımlanabilir. Sosyologlar, bazı toplumsal hareketlerin mevcut düzeni tamamen değiştirmeyi ve yerine yeni bir düzen kurmayı hedef aldığını ifade etmiştir. Bunların bazılarını "devrimci sosyal hareketler," bazılarını da toplumun çoğunluğunun karşı olduğu bazı yanlarını değiştirmeye yönelik olduklarını kabul ede " reformcu sosyal hareketler" şeklinde değerlendirmişlerdir. [3]

Toplumsal hareketler, toplumsal eylemleri ve olayları da beraberinde getirmektedir; ancak toplumsal eylemlerle toplumsal olayları birbirine karıştırmamak gerekmektedir. Toplumsal olayları, Emniyet Genel Müdürlüğü Güvenlik Daire Başkanlığı Merkez ve Taşra Kuruluş ve Çalışmaları Yönetmeliğinin 4'ncü maddesi kamu düzenini bozan kişi hak ve hürriyetlerini kısıtlayan veya tehdit eden ve kitlesel olarak gerçekleştirilen toplantı ve gösteri yürüyüşleri ile eylem ve etkinlikler olarak tarif etmektedir. Toplumsal eylemler ise yasalar çerçevesinde yapılan toplantı, yürüyüş, basın açıklaması ve buna benzer toplulukların duygu ve düşüncelerini, kamu düzenini bozmadan, kamuya ait bina ve tesislere zarar vermeden başka kişilerin hak ve özgürlüklerine dokunmadan gerçekleştirilir. Bu eylemler, amaca ulaştıktan sonra kamu düzeni bozulmadan sonlanır. Böylece toplumda bir karışıklık ve düzenin bozulması gibi bir durum söz konusu olmaz. Bu da toplumda kişilerin düşünce ve eleştirilerinin özgürce dile getirmesi toplumsal rahatlamayı sağlamaktadır. Sağduyunun hâkim olduğu bu tarz eylemler, toplumun önemli demokratik davranış şekilleri olarak gösterilebilir.

Türkiye'de toplumsal eylemler 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu ile düzenlenmiştir. 1985 tarihli olan bu kanun çeşitli ekleme ve değişikliklerle bu güne kadar gelmiştir. Son şekliyle: "Toplantı yapılabilmesi için, düzenleme kurulu üyelerinin tamamının imzalayacakları bir bildirim, toplantının yapılmasından en az kırk sekiz saat önce ve çalışma saatleri içinde, toplantının yapılacağı yerin bağlı bulunduğu valilik veya kaymakamlığına verir." ibaresi taşımaktadır. Bu yolla kanuna uygun yapılan her türlü eylem, toplumsal eylem olarak değerlendirilebilmektedir. [4]

Toplumsal olaylar, toplumsal eylemler gibi değildir. Bu olaylarda yasalara ve kamu düzenine muhalefet ön plandadır. Kısa sürede göstericiler şiddete yönelir ve kamu düzenini bozmaya çalışırlar. Toplumda bir kaos ortamı meydana getirerek halkı korku ve şiddet ile sindirmek, toplumu yaşanamaz bir hale dönüştürmek amaçlanmaktadır.

Toplumsal olaylarda yer alan bireylerin geneline bakılacak olursa bunların sosyal seviyelerinin düşük, karakterlerinin fazla olgunlaşmadığı, kendi kişisel gücünü ve yeteneğini ispatlayacak ortam bulamamış kişilik tiplerinden oluştuğu görülmektedir. Bu nedenle söz konusu bireyler, kendilerini ait hissedebilecek bir gruba bağlı olmayı ve bu grup içerisinde kendini ispatlamayı bu uğurda kendine verilecek her türlü örgüt görevini kabullenmeyi ifade eden bir kişilik yapısı içerisinde olurlar. Böylece kendisine sunulan her türlü telkine açık eylem yapmaya ve olay çıkarmaya açık bir kişi profili ortaya çıkarmaktadırlar.

Başlangıçta bir toplumsal eylem hüviyetinde tamamen kişilerin çeşitli insani değerlerini ifade eden; çevre bilinci, hayvan hakları, insan ve tabiat sevgisi gibi toplumun kabul edilebilir nitelikli konuları eylem çerçevesini oluşturmaktadır. Ancak bu durum çeşitli provokasyonlarla çok daha geniş boyutlu kitlesel eylemlere dönüşebilmekte, bir anda ülke ve dünya gündemi bu olaylardan oluşabilmektedir. Bu tarz toplumsal olayların geniş halk kitlelerine yayılması ve bu kitlelerinden taraftar bulması çağımızın temel niteliği olan siber dünyadaki bilgi ve haberleşme teknolojileri sayesinde gerçekleşmektedir. Böylece provoke edilen her toplumsal olay, sosyal medya destekli uluslararası nitelik kazanabilmektedir.

Toplumsal olaylar yaşanılan çağın toplumsal yapısından kaynaklanan ve gündemde olan konulardan beslenir. Toplumsal olaylar; bu yönüyle incelenecek olursa olayları gerçekleştiren kitlenin birey, grup, topluluk yapılarını bireyler arası ve gruplar arası iletişim kavramlarını bir sosyal medya zemininde incelemek faydalı olacaktır.

III. BİREYLER ARASI İLETİŞİM VE SOSYAL MEDYA

Toplumu oluşturan bireyler, birlikte yaşamanın gereği olarak iletişim ve etkileşim halindedirler. Böylelikle toplumun devamlılığını sağlayan maddi ve manevi değer yargılarının tamamı olan kültürün devamlılığını iletişim yoluyla sağlarlar. İletişim insanlık tarihinin her evresinde var olan ve çağın karakteristik özelliklerini taşıyan bir yapı olarak kendini göstermektedir.

İçinde bulunduğumuz yüzyılda iletişim teknolojilerindeki hızlı gelişme, bireyler arasındaki iletişimi farklı noktalara taşımakta ve bireyler arasındaki mekânsal mesafeyi minimal seviyelere indirmektedir. Medya kavramı teknolojik ilerlemelerle, internet altyapılı bir düzen almakta ve toplumda "Yeni Medya" olarak adlandırılan sosyal medya kendini göstermektedir.

Bilgi alışverişi yapmak amacıyla, kişilerin çalıştığı sektörlerden ve ilgilendikleri alanlardan aynı fikri paylaştıkları insanlarla tanışmak için internet üzerinden oluşturulan sosyal ağ kanallarına sosyal medya denilmektedir.[5] Sosyal medya; temelde bireyler arasında bilgi alışverişini sağlamak amacıyla aynı fikre ve dünya görüşüne sahip bireylerin yaşamdaki çeşitli ortak paydalarından hareketle bir araya geldiği sanal bir platform olarak adlandırılmaktadır. Bu yönüyle sosyal medya; bireylerin fikri gruplarının oluşmasını sağlayarak grupların duygu ve düşüncelerini yansıtan verilerini kendi takipçilerine aktaran geniş dijital ağ sistemleri oluşturmaktadır.

A.TOPLUMSAL OLAYLARDA BİR PROTESTO ARACI OLARAK SOSYAL MEDYANIN KULLANILMASI

Toplumdaki medya algısı yeni medya araçları olan sosyal ağlarla yeni bir boyut kazanmıştır. Sosyal ağların kullanımından önce medya, bir kurumsal yapı çerçevesinde hedef kitleye tek yönlü bir veri aktarımı niteliği ile yayın yapmaktaydı. Ancak yeni medya araçları, yapısal yönüyle toplumda çokça tartışılan interaktif bir görünüm kazanmıştır. Böylece medya kavramı sadece bir kurumsal yapı ile hedef kitleye yayın yapmaktan öte, veri ve ileti paylaşımı yoluyla sosyal medya kullanıcılarına imkân sağlamıştır. Böylece bireyler medyanın yayın ağına yayın

yapan ve ileti aktaran kimliği ile katılmışlardır. Artık sosyal medya ile bireyler toplumsal hayattaki statülerine göre karşılıklı veri alış-verişi yapan yayın merkezlerine dönüşmüşlerdir.

Sosyal medyanın bireylere tanıdığı katılımcı yayın imkânı, beraberinde tepkisel olarak toplumsal hareketliliği de getirmektedir. İdeoloji ve klavye arasına sıkışmış sosyal medya kullanıcıları, bu şekilde kamusal denetimden uzak çeşitli yayınlar yaparak toplumun huzur ve güvenini zedeleyen yapılar içerisinde yer alabilmektedirler.

Toplumsal olaylar bir toplumsal hareketlilik içinde meydana gelmektedir. Toplumsal hareketler; geniş bir toplum içindeki tutumları, davranışları ve sosyal ilişkileri değiştirmek üzere uyumlu çabalara girmiş insanlardan oluşan örgütlenmiş grupların ortaya koydukları tavır ve davranışlar olarak değerlendirilebilmektedir. Bu tavır ve davranışların çeşitli şekillerde kanuna aykırı olarak ortaya koydukları gösteri şekilleri toplumsal olayları oluşturmaktadır. Toplumsal olayları düzenleyen grupların fikirlerinin kitlelerle paylaşılarak toplumsal olaylara dönüştürülmesi, provoke edilmiş eylemci kitlesine ulaşılması toplumsal olayların iletişimsel eksenini oluşturmaktadır. Bu aşamada eylemci grup içerisinde, eylem provokasyonunu geniş kitlelere bir ajitasyon söylemiyle yansımış ve eylemi kitlelere yayacak iletişim araçları etkin rol almıştır.

Bilgi ve teknolojinin en ileri aşamasında olduğu yaşadığımız yüzyıl, iletişim ve haberleşmede bütün dünyayı saran bir internet ağıyla ortak bir veri ağı altyapısını ortaya koymaktadır. İnternet zemini üzerinde haberleşme teknolojisi, medya kavramı arasına bir de sosyal medya araçlarını yerleştirmiştir. Sosyal medya bireylere bütün dünyaya aynı anda yazılı ve görüntülü veri aktarma imkânını sağlamaktadır. Bu yapı aynı zamanda bireylerin doğruluğu ispatlanmamış yanlış bilgileri kendi profillerinden bütün dünyaya duyurduğu, toplumsal olayları gerçekleştiren grupların bir istismar alanı olarak değerlendirilebilir. Böylece sosyal medyada teknolojik altyapısıyla yasadışı toplumsal olayların iletişim alanı olarak kullanılmaktadır.

Yeni medya, internetin etkileşimli iletişim gücünü tanımlayan soyut bir kavramdır ve bu gücü kullanan araçlar, sosyal medya araçları olarak tanımlanmaktadır. [6] Sosyal medya araçları son 15 yılda birçok sosyal ağın yayına başlamasıyla kendini gösterdi. Bu ağların birçoğu kişilerin birbirleriyle tanışmasını ve mesajlaşmasını hedefleyerek ortaya çıkmışlardır. 2004 yılına gelindiğinde Facebook ve 2006'da da Twitter yayına başladı. Bu iki sosyal medya aracı diğerlerinden farklı olarak kullanıcılarına resim ve mesaj paylaşma imkânı haricinde organizasyon kurmayı, organize olmayı bilgi ve fikir paylaşmayı, inançlar ve düşünceler etrafında gruplaşmayı sağlayan birer sosyalleşme platformu oldular. Böylelikle sosyal ağların yükselişi, organizasyonları çevrimiçi topluluklara dönüştürdü. Bu durum, sosyal medyanın toplumsal olaylardaki iletişim ve organizasyon gücünün, kanunsuz eylemlerin düzenlenmesinde ve kamusal düzene ve rejime başkaldırı faaliyetlerinde bir iletişim aracı olarak kullanılmasına ortam sağlamıştır. [6]

Sosyal medya araçlarının bireyler arasındaki kullanımı mevcut ülkenin internet altyapısıyla doğru orantılı olarak gelişmektedir. Bu durum Türkiye örneği ile incelenecek olursa; internete erişim imkânı hane olarak 2010 yılında %41,6 iken bu durum 2011 yılında %42,9' a yükselmiştir. 2010 yılında bireylerin internet kullanım oranı ise %45 olarak ölçülüştür. [7]

Yeni medya düzeninin yapısal durumu toplumsal olayların etki gücünü de etkilemektedir. Sosyal ağlarda doğruluğu kanıtlanmayan bilgiler geniş yankılar uyandırmakta, bu yanlış haberler bir sorgulamaya tabi tutulmadan ağ kullanıcıları tarafından ani reaksiyonlara da neden olmaktadır. Bu da sosyal ağların toplumu ilgilendiren siyasi ve sosyal konuların bir manipülasyon alanı olmasına neden olarak sosyal hareketliliği de beraberinde getirmektedir. Sosyal medyanın toplumsal olaylardaki iletişim ve organizasyon kabiliyeti şu şekilde sıralanabilmektedir:

- Sosyal medya takipçilerinin organize olmalarını kolaylaştırması.
- Bireyler arasındaki etkileşimi arttırması
- Fikir ve grup ideolojisinin yayılmasını sağlaması
- Organizasyon ve iletişim maliyetlerini düşürmesi
- Toplumsal olaylarda daha çok sayıda insanın siyasi ve sosyal olaylara daha kısa sürede reaksiyon göstermesini sağlaması[8]

Sosyal medyanın yukarıda belirtilen nitelikleri toplumsal olayların teknolojik iletişim faaliyetlerindeki etkinliğini belirtmesi ve gerçekleşen olayların kitlesel olaylara dönüşmesindeki rolünü belirtmesi bakımından oldukça önemli bir durum olarak değerlendirilmektedir.

B. SOSYAL MEDYANIN TOPLUMSAL OLAYLARI ORGANİZE ETME GÜCÜ

Bireylerin sosyalleşmesine etki eden, toplumun her kesimini sosyal bütünleşme ekseninde bir araya getiren kitle iletişim araçlarının en geniş ifadesine medya denir. Medyanın bu görevi bireylerin birbirleriyle iletişim kurarak toplumsal sürekliliği sağlama ihtiyacına bağlı olarak gelişmektedir. Bu durum, klasik medya araçlarının bireylere sunulan yayınlarında geliştirilen söylem ile sosyal medyanın takipçi kitlesinin sosyal ve siyasal eğilimlerinin niteliğini oluşturur.

Medya, toplumlarda benimsenen sosyal ve siyasal fikirler doğrultusunda gruplaşma imkânını ortaya koymaktadır. Televizyon kanallarının, gazete ve dergilerin hitap ettiği kitle sosyal ve siyasal nitelik olarak birbirinden farklılık gösterebilmektedir. Yeni medya araçlarında bu durum klasik medyanın sosyal ve siyasal olarak farklı söyleminin ötesinde kullanıcıya özel sosyal ve siyasal söylem geliştirme imkânı sağlamaktadır. Böylece bireyler sosyal ağlar üzerinden çok geniş, katılımcı ve karmaşık ağlar sistemi içerisinde veri alan ve aktaran bir yapı içerisinde yer almaktadır.

Sosyal medya kanalları, bireyin söylemini gruplara ve kitlelere çok kısa sürede ve ekonomik olarak aktarılabilmektedir. Bu durum sosyal ve siyasal temayülleri ortak olan bireyleri sosyal medya üzerinde "sanal gruplara" dönüştürmektedir. Bu sanal platformlar, toplumsal eylem ve olaylar dâhil her türlü organizasyonların düzenlenip belirlenebildiği bir dijital paylaşım alanı olabilmektedir.

Toplumsal olayların düzenlenmesi; grup sloganlarının sosyal ağlar üzerinden paylaşılması, eylemci grupların hangi

alanlarda eylem yapacaklarını ve eylemlerin hangi boyutlarda sürdürüleceği, grupların lider kadroları ile grup arasındaki iletişim ağıyla belirlenmektedir. Bu iletişim ağının en güçlü olduğu alan sosyal ağların sağladığı iletişimsel alanla mümkün olmaktadır. Bu alan yaşanılan son dönemlerde grupları ve kitleleri toplumsal olaylara sürüklemekte, devlete ve kamu düzenine başkaldıran grupları kitlesel olaylar çıkarmakta organize etmektedir.

Sosyal ağlar üzerinden paylaşılan bilgi, haber ve verilerin doğruluğunun sorgulanması üzerinde en çok durulması gereken kavramlar arasında yer almaktadır. Teknolojik birçok hilelerle ortaya konulan bireylerin kişilik haklarını rencide eden verilerin sosyal medya üzerinden aynı anda bütün dünyaya yayın yapması ve bütün sosyal medya takipçileri tarafından kendi profillerinden duyurulması, büyük çapta kitlesel olaylara kapı aralamakta, kamuoyu bu türlü provokatif eylemlerle uzun süre meşgul edilebilmektedir.

IV. SONUÇ VE ÖNERİLER

Yaşanılan yüzyılın toplumsal hareketlilik açısından en önemli niteliğini, bilgi ve medya teknolojilerindeki gelişmeler ortaya koymaktadır. Bu gelişmeler, bireylerin iletişim faaliyetlerine küresel olarak düşük maliyetle katılımını sağlamakta ve bireyler bütün dünya ile internet zemininde aynı anda çevrimiçi olabilmektedir.

Medya araçlarında meydana gelen yapısal değişim ve dönüşüm, yeni medya kavramı olan sosyal ağları ifade etmektedir. Sosyal ağlar, bireylere ve topluluklara kişilerin kendi profillerinden veri aktarma, bilgi paylaşma, çeşitli sosyal ve siyasal gruplarla iletişim kurma imkânı vermektedir.

Zamana bağlı olarak yaşanan toplumsal değişmeler, kişiler ve gruplar üzerinde etki yapmaktadır. Bu değişim süreci toplumda bazı kesimler tarafından kabul görürken başka kesimler tarafından da protesto edilmektedir. Bunlar kişilerin bireysel tercihlerine ve dünya görüşlerine göre farklı tutum ve davranışları ortaya çıkarmaktadır. Bireylerdeki çeşitli tutum ve davranışların farklı siyasal düşüncelerle desteklenerek ifade edilmesi, toplumsal eylem ve olayların oluşumuna zemin hazırlamaktadır.

Toplumsal eylem ve olayların içeriğini her ne kadar yaşanılan yüzyılın sosyal yapısı belirlese de çağın teknolojik yapısı da eylemlerdeki yöntemin niteliğini ortaya koymaktadır. Geçmişte klasik medya araçları üzerinden aktarılan haber ve bilgiyle siyasi tercihlere göre orta ölçekli şekillenen toplumsal olaylar, bugünlerde sosyal medya araçlarıyla küresel nitelikler kazanarak bütün dünya tarafından takip edilmekte ve geniş kitlesel eylemlere dönüşerek bir ülkede gerçekleşen toplumsal olaylar, dünya gündemini oluşturabilmektedir.

Meydana gelen toplumsal olaylar, kamu düzenini bozmakta ve bu eylemlere katılmayan kişilerin temel hak ve özgürlüklerini hedef almaktadır. Eylem süresince bireylerin hizmet aldığı kamuya ait mallar zarar görmekte toplumdaki huzur ve asayiş ortamı bozulmaya çalışılmaktadır.

Toplumsal olayların ortaya koyduğu şiddetin oranı, eyleme katılan taraf kitlenin niceliği ile ölçülmektedir. Toplumsal eylemlere gösterici temin etmek, toplumsal olayları organize eden eylemci grupların iletişim ve propaganda faaliyetleriyle yakından ilgilidir. Toplumsal olayları çeşitli propaganda faaliyetleriyle organize eden marjinal gruplar, hem toplumsal eylemlere propaganda yollu gösterici eleman kazanmak hem de grupları toplumsal olaylarda organize etmek için sosyal medyadan faydalanmaktadır. Sosyal medyanın veri aktarımındaki geniş iletişimsel ağ imkânı, eylemci gruplara kışkırtıcı sloganlar ve yanlış bilgilerle dolu verileri tüm dünyaya servis etme imkânı sağlamaktadır. Bu nedenle toplumsal olayların şiddete dayalı etkisi en yüksek seviyelere çıkartılmaktadır.

Sosyal medyanın iletişim gücünden faydalanarak geniş kitlesel olayların tertiplenmesi, bundan hareketle kamu düzenin bozulmasına ve devletin milletiyle olan bölünmez bütünlüğünün zedelenmesine yol açan kanunsuz eylemlerin organizasyonunda iletişim teknolojilerinin rolü büyüktür. Bu durumun temelinde sosyal medya araçlarını kullanan bireylerin toplumsal huzur ve barışa karşı sorumlu davranması ve yalan yanlış bilgilerin paylaşımında bu sorumlulukla hareket etmesi gerekmektedir.

Demokrasiyle idare edilen toplumların temel niteliklerinden biri de medya özgürlüğüdür. Ancak bu özgürlük kamu düzenini bozmak, devletin milletiyle olan bölünmez bütünlüğüne kasteden söylem ve eylemlerde bulunma yıkıcı ve bölücü faaliyetler kapsamında değerlendirilmelidir. Sosyal barışı bozan eylemlerin çıkış noktasında yer alan yanlış bilgi ve dokümanların paylaşımında bulunarak yasadışı eylemlere kaynaklık eden kişi veya gruplar, yasal düzenlemeler doğrultusunda adli makamlar tarafından adli takibe alınmalıdır.

Adli takibi gerektirecek sosyal medya içerikli söylem ve eylemlerin takibini sağlamak amacıyla çeşitli yazılımlar geliştirip adli makamların hizmetine sunulması, ülke güvenliğini sağlama adına önemli mühendislik faaliyetleri olarak değerlendirilebilir.

KAYNAKLAR

[1] Ö. Demir, M. Acar, “Sosyal Bilimler Sözlüğü” S.405, Adres Yayınları, Ankara,2005

[2] İ. H. Keskin, “İstanbul’da Meydana Gelen Olayların Değerlendirmesi” S.18, İstanbul Üniversitesi Adli Tıp Enstitüsü, İstanbul, 2012

[3] O. Türkdoğan, “Osmanlıdan Günümüze Türk Toplum Yapısı” S.225 İstanbul,2008

[4] A. Bozkurt, “ Siyasiler Sosyal Medyanın Farkında”S.51,Türkiye Bilişim Derneği Dergisi, Sayı 127 Aralık 2010

[5] L.M. Koçgündüz,”Ortadoğu’daki Ayaklanmalarda Bir Katalizör Olarak Al Jazeera ve Mısır Örneği” Ortadoğu Analiz Cilt:3 Sayı:29 (2011)

[6] D. Body& N.B Ellison, “Social Network Sities:Definition, History and Scholarship” Jornal of Computer Mediated Communication, Vol: 13 210-230 (2008)

[7] Türkiye İstatistik Kurumu, “2011 hane Halkı Bilişim Teknolojileri kullanım Araştırması” (No:180), Ankara, 2011

C. Çildan,M. Ertemiz, H. K Tumuçin, E. Küçük,D. Albayrak “ Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü” Bilkent Üniversitesi Bilgisayar ve Bilişim Sistemleri Bölümü, Ankara

Computer Forensics in Turkey: A Macro Analysis

Medine Colak[1], Mehmet Karaman[2],
Mustafa Ugur Eren[3], Semra Cakir[4], Ahmet Burak Gokalp[5]

GUTIC, Ankara/Turkey
[1]medinecolak@gmail.com, [2]karamanmehmet@yahoo.com,
[3]mustafaugureren@gmail.com, [4]cakir.semra1@gmail.com, [5]aburakgokalp@gmail.com

***Abstract*–This paper introduces a macro analysis of computer forensics in Turkey. This analysis is based on completed thesis in university academia and the departments established. It also helps us gain insight related with given courses in the departments and some activities such as conferences, seminars, workshops. The analysis has shown that there have been enough educational infrastructures to deal with forensic related issues.**

***Keywords*–Forensics, computer, macro analysis, information security,**

I. Introduction

Nowadays, depending on the development of technology people store and share their personal information electronically to provide them an easy life. Therefore, computer crimes, which are committing on computer by bad persons, increase significantly in the world. Because of more money, challenges in busy life, ambitions of achievement, economic dissatisfactions in stressful life, etc. people want to commit computer crimes. Like all over the world, especially in Turkey, computer crimes have reached a significant level.

In addition to computer crimes that occurred against either to a person or it can be for society. There are many kinds of computer crimes such as; sending e-mail on behalf of others; coping CD, selling, fake documents printing, personal computers or corporate computers by accessing the information of persons, etc. In Turkey on behalf of computer crime are the most seen cases; bank cards and credit cards fraud, interactive bank fraud crimes against information systems and qualified fraud through the internet.

To avoid these types of crimes, people should get a good education about computer crimes and they should conscious about computer crime when they faced this crime. Since 2006, forensic awareness has occurred and it can be prevent, protect this bad situation in Turkey. With these awareness conferences, seminars, workshops, training programs have been given to development of computer crime.

In university, forensic awareness of informatics began to be formed in the field of computer forensic and information security departments. Also some associations, groups have been established to contribute to developments of this field.

This article consists of six sections. Section 2 gives some definition about forensics and computer crime. Section 3 summarized master thesis and doctoral thesis completed in Turkey. With this analysis we examined subject of this thesis. Section 4 shows departments, institutions of forensic crime and information security in universities of Turkey. Section 5 gives conferences, seminars and workshops about forensic crime and information security in Turkey. Section 6 illustrates the results and evaluations about macro analysis study.

II. Computer Forensics

The main goals of computer forensic are discovery, collection identification, analysis and presentations of legal and electric evidence [1]. Academic studies, which are conferences, workshops, seminars, education in university help awareness of computer forensics in Turkey.

Computer forensics is a now general topic and it consists of some sub areas. These areas of computer forensics are as follows, respectively [2]:

- Computer
- Network
- Incident Response
- Cell Phone
- GPS
- Media Device
- Social Network and recently cloud to remarks

Software commercially available in Turkey:

- Encase forensic: Software is manufactured and marketed by Guidance Software. This software has many functions such as one-to-one copy operation, preliminary examination of the media in viewing mode, keyword search, electronic media is write-protected computer can be connected to the views, some needed operations can be done with the encrypted property[2-3].
- Forensic Tool Kit (FTK): FTK is made by Access Data. The software scans a hard drive looking for various information. The toolkit also includes a standalone disk imaging program. Electronic media with identical copies of files contained within these media can be taken with this software. In addition this function, which is taken verbatim copies read-

only mode, may be displayed and deleted files can be displayed with FTK [2-3].

- X-ways forensic: X-Ways Forensics comprises all the general and specialist features. These features are disk cloning and imaging, automatic identification of lost/deleted partitions, various data recovery techniques, etc. [2-3].
- iLookLEO&iLookPI: These software have a number of functions such as directly examining floppy disks and hard drives instead of via an image, Win9x direct floppy investigation facility, image hash function provides MD5 or SHA1 hash of any image set defined, etc. [2-3].
- SMART: Smart forensic software is Linux Computer forensic software from ASR Data. It is designed to support data forensic practitioners and information security experts [2-3].
- P2 Commander: P2 Commander is a comprehensive digital investigation tool used by forensic examiners. This software has many different features. For example; pornography detection, file sorting along with comprehensive reporting, Data Triage analysis, etc. [2-3].
- MacForensicLab: The software is designed to meet the demands of law enforcement and digital forensic investigators. Data recovery and fast and verifiable media acquisition can be achieved with this software [2-3].
- BlackLight Mac Analysis: BlackLight is a multi-platform forensic analysis tool. This software is capable of data analysis [2-3].

III. Completed Thesis in Computer Crime and Information Security in Turkey

Computer crime is really important topic for people, organizer, government, etc. In this literature review, total six different education institutions, 5 universities and one academy are considered.

So in that step of our survey, we gathered information from the universities, institutes and academies, which are being probed about that field in Turkey. So it can be useful in order to help us gain insight about survey that is being done and the necessities are regarded with the most committed computer crimes, its prevention methods and effects to the information security field. The survey is shown in seven different columns that are directly related with the researches which have been done in related universities, institutes or academies, etc.

Comparison literature survey is given below:

Table1: Master Thesis and Doctoral Thesis about forensic, information security

University Name	Institute Name	Department	Subject	Thesis	Year	Keywords	
Marmara	Science	Electronic and Computer	Within The Framework Of Computer Forensics Computer Based Information Technology Crime Investigations And Analysis	MSc	2013	Computer Forensic, Information Technology	[4]
Ankara	Health Unit	Interdisciplinary Forensic Sciences	Comparison of Open Source and Proprietary Software In Data Recovery	MSc	2013	Digital Forensic, Data Recovery, Open Source Coding, Closed Source Coding	[5]
Gazi	Social Science	Crime and Law of Criminal Procedure	The Search and Seizure of Computer, Computer Programs and Logs.	MSc	2011	Computer, Search, Seizure, Electronic Evidence, Computer Forensic	[6]
Firat	Social Science	Educational Sciences	Training Of The Police Against Cyber Crime	PhD	2008	Police, Cyber Crimes, Combatting Crimes, Internet, Education, Instructional Program	[7]
Ankara	Health Unit	Interdisciplinary Forensic Medicine, Physical Investigating and Criminalistics	Evidence Collection and Examination in IT Crimes	MSc	2006	Computer forensics, computer crime, digital evidence, crime Scene, law	[8]
Firat	Science	Electronic and Computer	Analysis Of Fingerprint And Voice Recognition Digital Evidence Processes	MSc	2013	Computer Forensic, Digital Evidence, Fingerprint Recognition, Speaker Recognition	[9]
Firat	Science	Electronic and Computer	Assessment of Data Recovery Methods and Performances	MSc	2013	Data Recovery, Information Security, Computer Forensics	[10]
Firat	Graduate School of Natural and Applied Sciences	Electronic and Computer Education	Software Development For The Removal Of The Web Access Logs	MSc	2013	Web Mining, Web Usage Mining, Log Analysis, Web Access Logs, Data Mining, Information Extraction	[11]

Ankara	Health Unit	Interdisciplinary Forensic Sciences	The Investigation of Email Headers into the Origins of Emails	MSc	2012	Criminal Email, Cyber Crimes, Email Headers, Email Tracking, Spam, Spam Email	[12]
Halic	Science	Computer Engineering	Building a Computer Forensic Laboratory in Our Country and it's Contributions on Struggle Against Computer Crime	MSc	2008	Computer Forensic, Cyber Laboratory, Computer Crime	[13]
Police Academy	Security Science	Security Sciences	The New Electronic Evidence Acquisition Methods in Computer Forensics	MSc	2009	Computer Forensics, Computer Forensics in Turkish Criminal Procedure Code, Hand Held Device Forensics, Flash Memory Forensics, Audio and Video Forensics	[14]
Police Academy	Security Science	Forensic Sciences	Alterability of Signatures Due to Time	MSc	2011	Signature, Signature Alterability, Signature Forgery, Genuine Signatures, Signatures In Form Of Writings.	[15]
Police Academy	Security Science	International Security	EU's Financial Interests Legal and Institutional Protection: Turkey's Adaptation to European Union and AFCOS	MSc	2009	EU's Financial Interests, Irregularity , OLAF, AFCOS, EUROJUST	[16]
Police Academy	Security Science	Criminal Justice	Forensic Control	MSc	2009	Forensic Control, Protective Pre-cautions, Alternative for Arresting, Principle of Proportionality, Obligation	[17]
Police Academy	Security Science	Forensic Sciences	The Research of Palynological Forensic Evidence: Characteristics Found from Various Materials	MSc	2011	Criminalistics, Forensic Palynology, Crime Scene Investigation, Forensic Palynological Evidence, Spore, Pollen, Palynomorph.	[18]
Police Academy	Security Science	Criminal Justice	Regulation and practice of probation in Turkish Law	MSc	2010	Probation, Protective Commissions, Forensic Control, Working for the Public Weal, Continue to Educational Institution	[19]
Police Academy	Security Science	Forensic Sciences	The Evaluation of Weight Change Effect on Facial	MSc	2012	Forensic Identification, Weight Change, Facial Morphology, Anthropometric Measurement	[20]
Police Academy	Security Science	Criminal Investigations	The Benefits of Personal Identification Elements in Terms of Forensic Science and The Assessment of Implementations in Turkey	MSc	2009	Crime, Physical Evidence, Personal Identification Element, Database.	[21]
Police Academy	Security Science	Criminal Investigations	Forgery In Bills Of Exchange In The View Of Turkish Criminal Law and Forensic Examinations	MSc	2008	Bills Of Exchange, Forensic, Forgery, Alteration.	[22]

Table 2: Universities, courses and trainings programs related with forensic science

Universities	**Departments**	**Institutes**	**No of Courses**	**No of Academics**	**Establishment Year**	
Gazi	Digital Forensic	Informatics	14	13	2013	[23]
Gazi	Information Security Engineering	Science	31	18	2013	[24]

Hacettepe	Information Security	Informatics	14	12	2003	[25]
Turgut Ozal	Digital Forensic Engineering*	Sciences	18	17	2013	[26]
Firat	Digital Forensic Engineering	Technology	N/A	3	2013	[27]
Ankara	Forensic Science	Forensic Science	38	68	2010	[28]
Karadeniz Technical	Forensic Science	Forensic Science	N/A	N/A	2012	[29]
Mustafa Kemal	Computer Science	Science	N/A	3	N/A	[30]
Yasar	Cyber Security	Science	5	10	2012	[31]
Istanbul Sehir	Information Security Engineering	Science	23	7	2013	[32]
Istanbul Bilgi	The Law of Informatics and Technology	Law of Informatics and Technology	19	30	2010	[33]
Bahcesehir	Cyber Security*	N/A	N/A	N/A	N/A	[34]
Police Academy	Security Sciences	Security Science	4	221	2001	[35]
Police Academy	Faculty of Security Sciences	Security Science	53	15	2002	[36]
Police Academy	Faculty of Security Sciences	Forensic Science	N/A	N/A	2012	[37]

* Master Program
N/A: Not Available

IV. Education in Computer Crime and Information Security in Turkey

This section gives more information about content of courses at department of graduate and undergraduate schools in Turkey's Universities which are name of university department, institutions, academic personals and establishment year, etc. There are many departments and many courses in this area in Turkey.

Number of academic person at most at Faculty of Security Sciences at police academy while the number of academic person at least digital forensic engineering at Firat University and computer science at Mustafa Kemal University. Please see Table1 for more details. The first department was established at Police Academy in 2001 and the latest one was established in 2013 at Gazi, Turgut Ozal, Firat and Istanbul City University.

In Table 2, when we compare course column, Police Academy provides more cavies than other universities. Also this academy includes 2 different institutes and department in this field. Gazi University supports similar courses with two different institutes and department in this field. Police Academy is the first establishment education center and Gazi University has the latest establish education center in our research.

Karadeniz Technical, Bahcesehir and Department of Forensics in Police Academy have not completed their establishments yet.

V. Conferences, Seminars and Workshops in Computer Crime and Information Security

This section summaries conference, seminars and workshops about information security, cyber security and forensics organized in Turkey in recent years.

Table 3: Conferences, seminars and workshops about information security, cyber security and forensics in Turkey

Type	Name	Field	
Conference	International Conference on Information Security an Cryptology	İnformation security, Cryptology	[38]
Conference	Cyber Security Conference	Cyber security, Cyber spy training policies, Cyber wars	[39]
Conference	ISTEC Information Security Conference	IT security strategies, IT security applications	[40]
Conference	IDC IT Security Roadshow	Information security, İnvestigation of vulnerability	[41]

		Forensics	
Conference	Defence and National Information Security Conference	National security, Information security, Cyber attacks	[42]
Conference	ISSA Turkey Grand Security Conference	National security strategies enterprise-professional information and IT security	[43]
Conference	NOPcon Security Conference	Exchange ideas, share experiences	[44]
Conference	Public Institution Information Technology Security Conference	Cyber crimes Information security	[45]
Conference	Cyber Security and Turkey	Cyber security	[46]
Seminar	Information Security and Electronic Signature	Information security	[47]
Seminar	Information and Computer Security	Information security IT security	[47]
Seminar	Information Security	Information security	[47]
Seminar	Cyber Security and Turkey	Cyber security	[47]
Seminar	Electronic Signature	Information security	[47]
Seminar	Information Security Academy University	Cyber security Information security	[48]
Seminar	Cyber threats and Protection ways from cyber threats	Cyber security science of cryptology	[49]
Workshop	ITMSDAYS	Information security management	[50]
Workshop	International Conference on Information Security an Cryptology	Information security, IT security	[38]
Workshop	International Conference and Exhibition of Computer Forensics	Information security	[51]
Workshop	NOPcon Security Conference	Exchange ideas, Share experiences	[52]
Workshop	Information Security Academy University	Ethical hacking	[48-49]

ISTEC: Ibero-American Science and Technology Education Consortium, IDC: International Data Corporation, ISSA: International Social Security Association, ITMSDAYS: IT Management System Days

The survey result given in Table 3 is shown under three different columns. Information security, cyber security and forensics are the main fields in conferences, seminars and workshops.

In recent years, 9 conferences, 7 seminars and 5 workshops were organized. It can be concluded that these activities help to establish better infrastructures to develop programs and courses to improve awareness, etc.

VI. Conclusion and Evaluation

This paper presents a number of reviews on researchers, universities, courses, and organizations on forensics. The reviews have shown that Turkey has not enough programs and infrastructures at the beginning level.

Recent events and news have depicted that these developments need to be improved and increased.

When organizations, regulations and related law instruments are considered computer crime are recent problems in general around the world. To fight with crimes, new techniques, technologies, approaches, models and methods need to be developed and new strategy and politics.

Bear in mind that international collaborations are needed to develop standards. Practical aspects of incidents are also important to apply and solve problems encountered.

VII. Discussions

There have been a number of issues to be discussed statements are controversial issues, which are expressed about so much.

No of Organization: There are 19 theses including 18 master theses and one doctoral thesis in Table 1. Also there are 7 different universities of which names are Marmara, Ankara, Gazi, Firat, Halic and one Police Academy to provide these theses. According to our research, there are 6 institutes and 12 departments in these universities to study of 19 theses.

As you see there are 9 conferences, 7 seminars and 5 workshops about cyber security, information security, and forensics in Turkey. Also these activities improved according to new technology and arrangement every year.

No of Courses: There are 12 universities and 10 departments related with information security, cyber security and forensics in Turkey.

No of Researchers: There have been many researches in forensics fields. It has been estimated approximately 417 academic personal doing research in this field.

Overall Evaluations: It is a non-deniable fact that there has been a great potential to handle the issues about computer forensics. Considerable amount of enterprises has being maintained their studies since they have been established. Thus in Turkey, there is a great effort to produce logical solutions and scientific ideas.

Acknowledgement

GUTIC is Gazi University Technology and Innovation Center. Also we would like to thank Prof. Dr. Seref SAGIROGLU for his encourages preparing this article for

ISDFS providing Facilities in Laboratories at Gazi University Faculty of Engineering.

REFERENCES

[1] H. Çakır, M. S. Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Turkish Journal of Police Studies*, pp. 23-44, 2013.

[2] M. Karaman, Ş. Sağıroğlu, "Adli Bilişim", *Telepati*, vol. 203, August, 2012.

[3] A. S. Şirikçi, N. Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi", *Journal Of Informatics Technologies*, vol: 5, no: 3, 2012.

[4] İ. M. Taş, "Within the Framework of Computer Forensics Computer Based Information Technology Crime Investigation and Analysis", M.Sc. Thesis, Dept. of Elect. and Comp., Marmara University, İstanbul, 2013.

[5] A. S. Şirikçi, "Comparison of Open Source and Proprietary Software in Data Recovery", M.Sc Thesis, Institute of Forensic Sci., Ankara University, Ankara, 2013.

[6] O. G. Ünal, "The Search and Seizure of Computer, Computer Programs and Logs, M.Sc. Thesis, Dept. of Public Law, Gazi University, Ankara 2011.

[7] Ç. Gümüş, "Training of the Police against Cyber Crime", Ph.D. dissertation, Dept. of Educational Sci., Fırat University, Elazığ, 1 – 388, (2008).

[8] K. Say, "Evidence Collection and Examination in IT Crimes", M.Sc. Thesis, Dept. of Interdisciplinary Forensic Sci., Ankara University, Ankara, 2006.

[9] G. Akkan, "Analysis of Fingerprint and Voice Recognition Digital Evidence Processes", M.Sc. Thesis, Dept. of Elect. and Comp., Fırat University, Elazığ, 2013.

[10]Ş. Kara, "Veri Kurtarma Yöntemlerinin Başarımlarının Değerlendirilmesi", M.Sc. Thesis, Dept. of Elect. and Comp., Firat University, Elazığ, 2013.

[11] D. Demirol, "Software Development for the Removal of the Web Access Logs", M.Sc. Thesis, Dept. of Elect. and Comp., Firat University, Elazığ, 2013.

[12]İ. Avlamaz, "The Investigation of Email Headers into the Origins of Emails", M.Sc Thesis, Dept. of Interdiscipliner Forensic Sci., Ankara University, Ankara, 2012.

[13] İ. Çiçek, "Building a Computer Forensic Laboratory in Our Country and It's Contributions on Struggle Against Computer Crime", M.Sc. Thesis, Institute of Science Management Information Systems, Halic University, İstanbul, 2008.

[14]H. Aydoğan, "The New Electronic Evidence Acquisition Methods in Computer Forensics", M.Sc Thesis, Institute of Security Sciences, Police Academy, Ankara, 2009.

[15]A. Gümüşsoy, "Alterability of Signatures Due to Time", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2011.

[16] M. Boşnak, "EU's Financial Interests Legal and Institutional Protection: Turkey's Adaptation to European Union and AFCOS", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2009.

[17]V. Yıldız, "Forensic Control", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2009.

[18]C. Doğan, "The Research of Palynological Forensic Evidence: Characteristics Found from Various Materials", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2011.

[19]C. İlgün, "Regulation and Practice of Probation in Turkish Law", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2010.

[20]G. Eslek, "The Evaluation of Weight Change Effect on Facial Morphology", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2012.

[21]M. C. Çubuk, "The Benefits of Personal Identification Elements in Terms of Forensic Science and the Assessment of Implementations in Turkey", M.Sc Thesis, Institute of Security Sciences, Police Academy, Ankara, 2009.

[22]O. Er, "Forgery In Bills of Exchange In The View Of Turkish Criminal Law and Forensic Examinations", M.Sc. Thesis, Institute of Security Sciences, Police Academy, Ankara, 2008.

[23]Available:http://be.gazi.edu.tr/posts/view/title/adli-bilisim-70721, (13.02.2014)

[24]Available:http://fbe.gazi.edu.tr/posts/view/title/bilgi-guvenligi-muhendisligi-abd-acildi-81264, (13.02.2014)

[25]Available:http://www.bilisim.hacettepe.edu.tr/index.php/anabilim-dallar/bilgi-guevenlii, (13.02.2014)

[26]Available: http://fbe.turgutozal.edu.tr/kategori/adli-bilisim-muhendisligi-yuksek-lisans-programi-131-114.html, (13.02.2014)

[27]Available: http://portal.firat.edu.tr/WebPortal/?BirimID=388, (13.02.2014)

[28]Available: http://adlibilimler.ankara.edu.tr/, (13.02.2014)

[29]Available: http://adlibilim.ktu.edu.tr/genel.html, (13.02.2014)

[30]Available:http://www.mku.edu.tr/main.php?page=readpage&id=4812&location=bm, (13.02.2014)

[31]Available: http://bilmuh.yasar.edu.tr/?p=471, (13.02.2014)

[32]Available:https://www.sehir.edu.tr/Pages/Akademik/Lisansustu/FBE/BilgiGuvenligiMuhYL.aspx?PageID=3&MenuID=2249, (13.02.2014)

[33] Available: http://bthukuku.bilgi.edu.tr/, (13.02.2014)

[34]Available:https://akts.bahcesehir.edu.tr/bilgipaketi/index/programtanimi/program_kodu/1241001/menu_id/p_29/ln/tr?submenuheader=2, (13.02.2014)

[35]Available: http://www.pa.edu.tr/?appcode=web_abe, (13.02.2014)

[36]Available: http://www.pa.edu.tr/?appcode=web_abe, (13.02.2014)

[37]Available: http://www.pa.edu.tr/?appcode=web_abe, (13.02.2014)

[38]Available: http://www.iscturkey.org/index.php?lang=tr, (17.02.2014)

[39]Available: http://www.siberguvenlikkonferansi.org/, (17.02.2014)

[40]Available: http://www.istsec.org/, (17.02.2014)

[41]Available:http://idc-cema.com/eng/events/50518-idc-it-security-roadshow-2013?g_clang=TR, (17.02.2014)

[42]Available:http://ictsummitnow.com/en-defence-and-national-information-security-conference-tr-savunma-ve-ulusal-bilgi-guvenligi-konferansi/?lang=tr, (17.02.2014)

[43]Available: http://www.bilgiguvenligi.org.tr/duyurular.html, (17.02.2014)

[44]Available: http://www.etkinlik.com.tr/nopcon-bilgi-guvenligi-konferansi-2807, (17.02.2014)

[45]Available:http://www.bilgiguvenligi.gov.tr/etkinlikler/6.-kamu-kurumlari-bilgi-teknolojileri-guvenlik-konferansi-sunumlari.html, (17.02.2014)

[46]Available:http://ceng.gazi.edu.tr/~ss/index.php?id=konferans, (17.02.2014)

[47]Available: http://ceng.gazi.edu.tr/~ss/index.php?id=seminer, (17.02.2014)

[48]Available:http://blog.bga.com.tr/2011/04/bilgi-guvenligi-akademisi-universite.html, available date: 17.02.2014

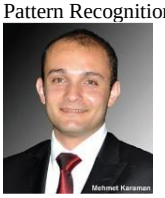
[49]Available: http://www.kararder.org/bilgi-guvenligi-semineri/, (17.02.2014)

[50]Available: http://www.itmsdays.com/info.php, (25.02.2014)

[51]Available:http://www.mertsarica.com/euroforensics-2011-ii-uluslararasi-adli-bilisim-konferansi-ve-sergisi/, (25.02.2014)

[52]Available:http://blog.bga.com.tr/2012/05/nopcon-istanbul-bilgi-guvenligi.html, (25.02.2014)

Medine COLAK was born in Ankara, Turkey. She has received BSc degree from Cankaya University Department of Computer Engineering and currently continues her M.Sc. in Gazi University Department of Computer Engineering. Her research interests are Information Security, Artificial Neural Networks, Pattern Recognition, and Biometrics.



Mehmet KARAMAN has been working for Information Technologies and Communication Authority in Turkey as a communication expert since 2008. He received BSc degree from Kocaeli University Department of Computer Engineering in 2004. He has received his M.Sc. degree from Gazi University Department of Computer Engineering and still continues his Ph.D. in Gazi University Department of Computer Engineering. His research interest are information security, digital forensics, counter-digital forensics, cyber security, advanced persistence threats and malware analysis.

Mustafa Ugur EREN was born in Ankara, Turkey. He currently continues his B.Sc. in Gazi University Department of Computer Engineering. His research interests are Internet and Web Based Systems and its Applications, Information Security, Information Retrieval.

Semra CAKIR was born in Ankara, Turkey. She currently continues her B.Sc. in Gazi University Department of Computer Engineering. Her research interests are Software Engineering, Project Management, Artificial Intelligence.

Ahmet Burak GÖKALP was born in Kayseri, Turkey. He currently continues his B.Sc. in Baskent University Department of Computer Engineering. His research interests are software engineering, information and computer security, electronic and mobile electronic signature and public-key structure, project management.

Consequences of Using Weak Functions of Old EPC Global C-1 G-2 Standard for Obscuring Secrets

M. H. Özcanhan[1], G. Dalkılıç[2] and O. Yarımtepe[3]

[1]Dokuz Eylül University, İzmir/Turkey, hozcanhan@cs.deu.edu.tr
[2]Dokuz Eylül University, İzmir/Turkey, dalkilic@cs.deu.edu.tr
[3]Dokuz Eylul University, İzmir/Türkiye, oguzyarimtepe@gmail.com

***Abstract*— Although there are numerous attacks launched against RFID authentication protocols using old EPC C-1 G-2 standard's functions for obscuring tag secrets, proposals are still coming. A recent protocol attempting to provide a secure and efficient mutual authentication protocol is using the same fallible strategy. The secrets of the protocol are fully exposed by an algebraic attack, in this work. The researchers of RFID tag security are advised to move to the lightweight cryptography support of the new version EPC C-1 G-2 standard. Only then the privacy and security of the users can be provided.**

***Keywords*— Patient safety, medication errors, RFID, authentication protocols, EPC Global.**

I. Introduction

RADIO Frequency Identification (RFID) is a growing technology that has matured, as it can be witnessed from the release of the second version EPC Global Class-1 Generation-2 standard (Gen-2) [1], and the integration of Near Field Communication (NFC) readers in almost every high-end mobile phone. The increasing popularity of mobile devices is also helping NFC to merge itself in many ubiquitous applications. Similarly, the growing number of big supply chains tracking their commercial commodities by using Gen-2 supported Ultra High Frequency (UHF) tags is making RFID the pervasive technology of our decade. Reports confirm that RFID is booming [2].

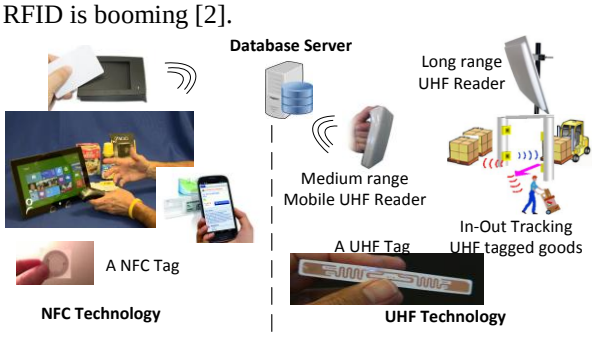
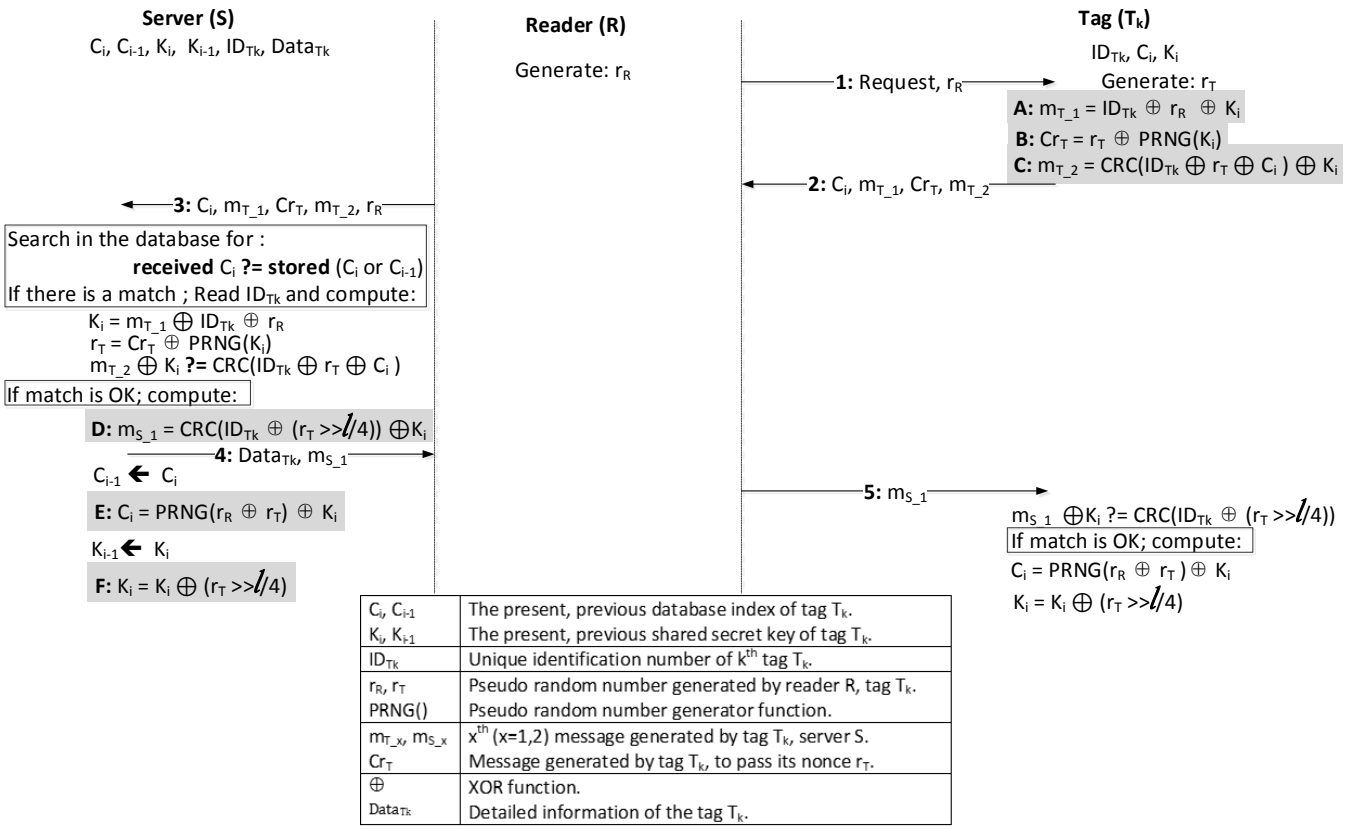


Figure 1: Reading NFC and UHF tags.

Although in all RFID applications, the tag's Electronic Product Code (EPC), in other words the unique identification number (ID), is read; UHF and NFC are in different categories [3]. The operating distance is the decisive difference. As its name suggests, NFC tags interact with their readers from a few cm, while UHF tags can be read from as far as few meters. Figure 1 shows the operating principles of UHF and NFC readers. Observe the very short distance between a NFC tag and its reader; while that of a UHF tag and its meters away reader. Because of their very short operating distance, NFC tags are sometimes named as proximity cards. The operating distance also differentiates the applications where the tags can be used. While NFC tags are used in individual identification applications like library cards, where each tag is read one by one; UHF tags are used for batch reading of many items like commercial goods, in a supply chain.

The operating distance is also a decisive factor in academic research. As the distance between a UHF tag and its reader is large, the communication through it can be eavesdropped. In fact, all academic works accept the air channel between the UHF tag and its reader as insecure. On the other hand, the communication between the wireless readers and the database server is accepted as secure, because the readers are known to have abundant resources for accommodating security tools that usually advanced personal computers have. Coupled with the insecure air channel, lack of sufficient support for security in the first version of Gen-2 has resulted in many weak authentication protocols to be proposed for the growing applications, as it can be witnessed by going through the vast number of RFID works enlisted at [4].

The expectation from RFID tags is to lead to unique identities for items which can be associated with buyers. Although it can be a positive intent, interference by a malicious eavesdropper can result in the loss of the privacy of the purchaser. No one wishes to share the information of the purchase which may lead to a clue on personal lifestyle. Many governments are trying to guarantee the privacy of their citizens by laws from improper use of RFID data. The U.S. Congress has introduced a bill "Opt Out of ID Chips Act" (H.R.4673), which requires warning labels on consumer products containing RFID devices [5]. California's State Senate has passed a measure (SB1834) in 2004, to set limits on the use of RFID technology that could lead to identify an individual, without his/her consent [6].



C_i, C_{i-1} K_i, K_{i-1}	The present, previous database index of tag T_k. The present, previous shared secret key of tag T_k.
ID_{Tk}	Unique identification number of kth tag T_k.
r_R, r_T PRNG()	Pseudo random number generated by reader R, tag T_k. Pseudo random number generator function.
m_{T_x}, m_{S_x} Cr_T	x^{th} (x=1,2) message generated by tag T_k, server S. Message generated by tag T_k, to pass its nonce r_T.
$\oplus$ $Data_{Tk}$	XOR function. Detailed information of the tag T_k.

Figure 2: Pang et al.'s proposed scheme: Pea [13].

In the rest of this paper, previous work is summarized in Section 2. A latest protocol proposal claimed to resist RFID attacks is analyzed in Section 3. A discussion follows in Section 4. A conclusion is given in Section 5.

II. Related Work

In order to take UHF tags to more complicated applications, instead of just reading the ID of a single tag (reading a tag), most research is on reading multiple tags simultaneously and matching the related ones, instantly. Hence, the matching of items and individuals are aimed. For example, matching of a patient with his medicine [7], generating evidence that the correct dosage has been administered to a patient [8], tracking valuable assets in a company; all require multiple tags on items and sometimes on humans, as well. One of the first researchers was Juels who proposed simultaneous reading of two tags [9]. Another proposal was careful to conform to Gen-2, while matching patients with their medicine [10]. According to the proposal, a daily dosage medicine package is tagged and the inpatient wears an RFID wristband.

Since then, many authentication proposals have been put forward to strengthen the security described by the old Gen-2. In old version Gen-2, messages are formed by just XORing ($\oplus$) generated nonces and secrets [11]. Apart from the XOR function, old Gen-2 uses a pseudo-random number generator (PRNG) for generating nonces and a cyclic redundancy check (CRC) function for checking message integrity. Some proposals chose to offer non-standard function upgrades, but most advocated the use of the available Gen-2 functions for obscuring messages, as well. Many attacks have been launched at proposals of this order, as it can be observed at [4]. The available functions have been shown to be weak and hence the protocols based on them demonstrated vulnerabilities summarized in some works [3, 12]. The applications using the vulnerable protocols put the safety and privacy of the user into the hands of a malicious attacker. To prevent the dangers to the user of the protocols, the researchers have to be informed about the weaknesses and the arrival of new tools. Our motivation is to convince the community to move on to the better enforced new Gen-2 standard.

A recent protocol repeating the same method, hence insisting on using XOR, CRC and PRNG is given in Pang et al.'s work [13]. The proposed protocol and its notation are depicted in Figure 2 and named as Pang et al.'s protocol (Pea). In a nutshell, Pea uses only CRC, PRNG and XOR function for obscuring the secrets that are passed to the server. The tag's index pseudonym C_i that is necessary to locate the tag in the database and a shared secret K_i are updated at the end of every session.

The authors of Pea make the following assumptions:

1. Tags are initialized with randomly generated parameters ID_{Tk}, C_i, K_i shown under the kth tag T_k in Figure 2, by trusted manufacturers.
2. Tag memories are secure and the tags can perform PRNG and CRC functions on their inputs.

3. The channel between the reader and the server is secure. But, the channel between the reader and the tag is insecure. Therefore, communication between the reader and the tag can be eavesdropped or modified.
4. The reader is trusted by the server.

The database is initialized with the values C_i, C_{i-1}, K_i, K_{i-1}, ID_{Tk}, $Data_{Tk}$ for each tag as shown in Figure 2, in accordance with the values stored on the tag. Initially, the previous (subscript i-1) values are set to present values and i = 0.

At the ith session, the reader starts the authentication process by sending a pseudo random number (nonce) r_R to the tag T_k. The energized tag generates its own nonce r_T and computes three values m_{T_1}, Cr_T and m_{T_2}. The reader receives (C_i, m_{T_1}, Cr_T, m_{T_2}) and appends r_R to it before sending (C_i, m_{T_1}, Cr_T, m_{T_2}, r_R) to the server. Using C_i, the server reaches the record of the tag. Using the fetched ID_{Tk}, the shared secret K_i is exposed. Next the tag's nonce r_T is calculated and used to test $m_{T\_2} \oplus K_i$. If the match is OK, the tag is authenticated and a reply m_{S_1} is prepared and sent to the tag via the reader. Without waiting for an acknowledgement, the server relegates the present values to C_{i-1}, K_{i-1} and updates C_i, K_i with new values. The tag validates $m_{S\_1} \oplus K_i$ to authenticate the server. Finally, the tag updates C_i, K_i, but does not keep old values. And that ends the mutual authentication of the two parties.

III. Security analysis of PEA

From the explanations of computation, it is obvious that although the PRNG function generates random numbers it is deterministic; otherwise the two sides cannot reach the same result for a given input. Hence, all of the functions XOR, CRC and PRNG are public and open to manipulations to the malicious listeners, as well.

Now, let the equations A, B, C, D, E, F of Figure 1 be appended with session number superscripts. For example, the m_{T_1} of equation A is represented as $m^i_{T\_1} = ID_{Tk} \oplus r^i_R \oplus K_i$. After eavesdropping two consecutive sessions starting with session i = 1, 10 equations are obtained.

A. Learning Phase

From equation A transmitted in step 2:

$$m^1_{T\_1} = ID_{Tk} \oplus r^1_R \oplus K_1 \tag{1}$$

$$m^2_{T\_1} = ID_{Tk} \oplus r^2_R \oplus K_2 \tag{2}$$

From equation B transmitted in step 2:

$$Cr^1_T = r^1_T \oplus PRNG(K_1) \tag{3}$$

$$Cr^2_T = r^2_T \oplus PRNG(K_2) \tag{4}$$

From equation C transmitted in step 2:

$$m^1_{T\_2} = CRC(ID_{Tk} \oplus r^1_T \oplus C_1) \oplus K_1 \tag{5}$$

$$m^2_{T\_2} = CRC(ID_{Tk} \oplus r^2_T \oplus C_2) \oplus K_2 \tag{6}$$

From equation D transmitted in step 5:

$$m^1_{S\_1} = CRC(ID_{Tk} \oplus (r^1_T >> l/4)) \oplus K_1 \tag{7}$$

$$m^2_{S\_1} = CRC(ID_{Tk} \oplus (r^2_T >> l/4)) \oplus K_2 \tag{8}$$

At the end of the first session, equation E:

$$C_2 = PRNG(r^1_R \oplus r^1_T) \oplus K_1 \tag{9}$$

At the end of the first session, from equation F:

$$K_2 = K_1 \oplus (r^1_T >> l/4) \tag{10}$$

B. Analysis Phase

XORing (1) and (2):

$$m^1_{T\_1} \oplus m^2_{T\_1} = K_1 \oplus r^1_R \oplus K_2 \oplus r^2_R \tag{11}$$

Substituting the value of K_2 from (10) into (11):

$$m^1_{T\_1} \oplus m^2_{T\_1} = K_1 \oplus r^1_R \oplus K_1 \oplus (r^1_T >> l/4) \oplus r^2_R \tag{12}$$

Simplifying (12):

$$m^1_{T\_1} \oplus m^2_{T\_1} = r^1_R \oplus r^2_R \oplus (r^1_T >> l/4) \tag{13}$$

XORing both sides of (13) with $r^1_R \oplus r^2_R$:

$$m^1_{T\_1} \oplus m^2_{T\_1} \oplus r^1_R \oplus r^2_R = (r^1_T >> l/4) \tag{14}$$

All values except ($r^1_T >> l/4$) are transmitted in clear text in steps 1 and 2 in Figure 2. Therefore, by shifting the value ($r^1_T >> l/4$) $l/4$ times to the left, r^1_T is exposed. Substituting r^1_T in (3), since Cr^1_T is passed in cleartext the value of $PRNG(K_1)$ is exposed:

$$Cr^1_T \oplus r^1_T = PRNG(K_1) \tag{15}$$

Substituting exposed r^1_T in $PRNG(r^1_R \oplus r^1_T)$ and then using (9), K_1 is exposed,:

$$C_2 \oplus PRNG(r^1_R \oplus r^1_T) = K_1 \tag{16}$$

Now the value of K_1 can be used to validate the previously captured $PRNG(K_1)$. But also by substituting K_1 in (10) directly, the value of K_2 can be exposed. The final secret remaining left to capture is ID_{Tk}, which can be obtained from either (1) or (2) and validated from (5) or (7) as follows. Inserting exposed K_1 in (1), ID_{Tk} is captured:

$$m^1_{T\_1} \oplus r^1_R \oplus K_1 = ID_{Tk} \tag{17}$$

The value of ID_{Tk} can be validated using (5) and (7). CRC function has a property announced in multiple works [12, 14]: CRC (X $\oplus$ Z) = CRC (X) $\oplus$ CRC(Z). Applying this property on (5) and (7):

$$m^1_{T\_2} = CRC(ID_{Tk}) \oplus CRC(r^1_T) \oplus CRC(C_1) \oplus K_1 \tag{18}$$

$$m^1_{S\_1} = CRC(ID_{Tk}) \oplus CRC(r^1_T >> l/4) \oplus K_1 \tag{19}$$

$m^1_{T\_2}$ and C_1 are transmitted in cleartext; r^1_T and K_1 were already exposed. $CRC(r^1_T)$, $CRC(r^1_T >> l/4)$ and $CRC(C_1)$ are easily calculated. Hence:

$$m^1_{T\_2} \oplus CRC(r^1_T) \oplus CRC(C_1) \oplus K_1 = CRC(ID_{Tk}) \quad (20)$$

$$m^1_{S\_1} \oplus CRC(r^1_T >> l/4) \oplus K_1 = CRC(ID_{Tk}) \quad (21)$$

IV. Discussion

The authors of Pea make a long description of the RFID privacy model based on numerous previous works. And then, the definition of untraceable privacy (UPriv) between a tag and a reader is given. Using the above two notions a net definition is provided: "A protocol is secure if the advantage $Adv^{Upriv}_A(k)$ of an adversary is negligible."; where ($Adv^{Upriv}_A(k) = |Pr(b' = b) - ½|$), k is the security parameter, $b' \in \{0,1\}$ is the guess value of b. In short, if an adversary cannot guess a tag $T_b \in \{T_0, T_1\}$ correctly, it means the probability Pr(b' = b) approaches ½. Hence, the value of $Adv^{Upriv}_A(k)$ approaches zero. Then, it can be concluded that the protocol is secure.

Basing their argument on the above definition of security, the authors defend the forward security and the privacy of Pea. It is demonstrated below that the claims are not true after the full disclosure attack demonstrated in the previous section, where ID_{Tk}, K_1, K_2, r^1_T have already been exposed. C_1, m_{T_1}, m_{T_2}, r^1_R, Cr_T, m_{S_1} are cleartext transmitted values. The parameters used have been augmented with superscripts T_b; as in r^{Tb}_T, meaning the nonce's originator is the superscripted tag.

A. Forward Security

It is claimed that it is infeasible to derive the previous secret key K^{Tb}_1 of tag T_b without the tag's nonce r^{Tb}_T. After exposing the static ID_{Tb} of the tag, using equation (1) the value of K^{Tb}_1 can be derived:

$$m^{Tb}_{T\_1} = ID_{Tb} \oplus r^1_R \oplus K^{Tb}_1 \quad (22)$$

Rewriting 22:

$$m^{Tb}_{T\_1} \oplus ID_{Tb} \oplus r^1_R = K^{Tb}_1 \quad (23)$$

Hence, Pr(b' = b) = 1 and $Adv^{Upriv}_A(k) = |Pr(b' = b) - ½| = ½$. And advantage $Adv^{Upriv}_A(k)$ is not negligible, therefore Pea does not satisfy the forward security criterion; therefore it is not secure.

B. Privacy

It is claimed guaranteeing that the values of m_{T_2} and Cr_T are different in each session because they depend on the changing nonce r_T and secret key K_i, also guarantees that an adversary cannot distinguish tag T_0 from tag T_1. Hence, advantage $Adv^{Upriv}_A(k)$ is negligible and Pea achieves untraceability. However, rewriting equations (3) and (5):

$$C^{Tb} r_T = r^{Tb}_T \oplus PRNG(K^{Tb}_1) \quad (24)$$

$$m^{Tb}_{T\_2} = CRC(ID_{Tb} \oplus r^{Tb}_T \oplus C^{Tb}_1) \oplus K^{Tb}_1 \quad (25)$$

Remembering that the secret nonce and the key (r^{Tb}_T, K^{Tb}_1) have already been exposed, $C^{Tb}r_T$ can be guessed with probability 1. The same is true for $m^{Tb}_{T\_2}$ as well. Therefore, an adversary can distinguish tag T_0 from tag T_1. Hence, advantage $Adv^{Upriv}_A(k)$ is not negligible meaning Pea does not achieve untraceability. Hence, the privacy of the beholder of a tag is not guaranteed.

The full disclosure attack launched in the previous section followed by the security analysis above, demonstrate yet again that protocols dependent on the weak functions of the old Gen-2 appear to be secure, but a thorough algebraic analysis of the exchanged data leads to the capture of the secrets. Our work merely uses the well-known algebraic properties of the used functions (CRC and XOR) one more time, to expose the secrets of the tag. The Learning and Analysis Phase methodology of our attack has been used in many previous works. Therefore, our attack is not a new type of attack.

Gen-2 ver2 standard; on the other hand, has support for lightweight encryption. This is a big improvement in low cost tags. It shows that more hardware and clock cycles have been allocated for better security algorithms, to satisfy the need for more secure applications. As an example, consider replacing the CRC and PRNG functions in Figure 2 with a lightweight encryption algorithm. The use of a secret key on some shared secrets could have better obscured the exchanged values. Thus, decrypting the transmitted values and exposing the secrets would depend on the strength of the encryption algorithm used. In short, the poor security level of Gen-2 ver1 functions has been upgraded to the security level of lightweight encryption algorithms. The choice of the proper lightweight encryption algorithm is out of the scope of this work, but the 64 bit support of Gen-2 ver2 is a good starting point.

V. Conclusion

A recent RFID protocol compliant to EPC Global Class-1 Generation-2 ver1 standard has been analyzed. The protocol uses the functions supported by the standard to hide the tag secrets, which have been proven to be weak for providing confidentiality. The insistence on providing more security by using an outgoing standard with weak security support has resulted in a meltdown of the proposed protocol, as the exposure of full shared secrets by our analysis demonstrates. The new version of EPC Global Class-1 Generation-2 ver2 standard supports lightweight encryption, which can be a better solution for protecting the tag secrets. Mere replacement of the functions used in the criticized protocol can show a big increase in the security level. This work can contribute to the work of the researchers, if insistence on using the weak functions of Gen-2 ver1 is relinquished and true encryption algorithms are brought into the new Gen-2 ver2 tags.

REFERENCES

[1] GS1. (2013) UHF Class 1 Gen 2 Standard v. 2.0.0. [Online]. Available: http://www.gs1.org/sites/default/files/docs/uhfc1g2/uhfc1g2_2_0_0_standard_20131101.pdf

[2] R. Das, P. Harrop, "RFID Forecasts, Players and Opportunities 2011-2021", *IDTechex*, 2011.

[3] M. H. Ozcanhan, G. Dalkilic, S. Utku "Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients," *Radio Frequency Identification*, pp. 19-33, 2013.

[4] Information Security Group. (2014) RFID Security and Privacy Lounge. [Online]. Available: http://www.avoine.net/rfid/index.php

[5] G. J. Kleczka. (2004). Opt Out of ID Chips Act. [Online]. Available: https://www.govtrack.us/congress/bills/108/hr4673

[6] D. Bowen, Senate Energy, Utilities and Communications Committee, (2004) Federal Law, SB 1834. [Online]. Available: http://leginfo.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1834_cfa_20040412_093616_sen_comm.html

[7] Joint Commission. (2010) National Patient Safety Goals (NPSGs). [Online]. Available: http://www.allhealth.org/BriefingMaterials/JointCommission-Oct2009-2010NationalPatientSafetyGoals-1722.pdf

[8] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J. C. A. Van der Lubbe, "A Comprehensive RFID Solution to Enhance Inpatient Medication Safety," *Int. J. of Med. Inform.*, vol. 80, no. 1, pp. 13–24, 2011.

[9] A. Juels, "Yoking-proofs for RFID tags", in *IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 138–143, 2004.

[10] H.-H. Huang, C.-Y. Ku, "A RFID grouping proof protocol for medication safety of inpatient," *Journal of Medical Systems*, vol. 33, no. 6, pp. 467-474, 2009.

[11] EPC Global Inc. EPC Global Class1 Gen2 RFID Specifications. (2008) [Online]. Available: http://www. alientechnology.com/docs/AT_wp_EPCGlobal_WEB.pdf

[12] T. Van Deursen, S. Radomirović, "Algebraic attacks on RFID protocols," *Information Security Theory and Practice*, pp. 38-51, 2009.

[13] L. Pang, et al., "Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1870-1875, 2013.

[14] P. Peris-Lopez, A. Orfila, J. C. Hernandez-Castro, J. C. A. Van der Lubbe, "Flaws on RFID grouping-proofs guidelines for future sound protocols," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 833–845, 2011.

Counter – Digital Forensics and Relationship with National Security

S.Sağıroglu [1], M. Karaman[2]

[1]Gazi University, Ankara /Turkey, ss@gazi.edu.tr
[2]Information Technologies and Communication Authority, Ankara/Turkey, mkaraman@btk.gov.tr

***Abstract*— With the increase in use of technology, today vast majority of people have digital devices to communicate with each other, to share something or to store digital data. The increasing use of these devices, such as notebook, mobile phone or pc, has led to the use them by criminals to plan their crime or keep illegal data like child pornography videos in these devices. Because of probability of existing such criminals, science of digital forensics has been born to help justice systems with its sophisticated ways. The main purpose of digital forensics is finding evidence from suspected digital devices and reporting all evidences to the court. Whole process is fulfilled by digital forensics experts. There is a crucial issue exist at this point, does digital forensics expert check whether counter digital forensics(C-DF) application is implemented or not ? At this study, we will focus on this issue and its side effects.**

Keywords—forensics, digital forensics, counter – digital forensics, anti-digital forensics, computer forensics

I. INTRODUCTION.

Today's world is getting more and more technological so more people are using new gadgets for various purposes such as communication, sharing something or keeping their data. With rising usage of these devices, many criminals also use them to keep their secrets. While some criminals are communicating to plan crime such as instant messaging tools, others are watching illegal videos like child pornography or storing secret data for selling it [1]. Digital forensics is a science that detects valuable evidences from criminal's technological gadgets and reports it to the court [2]. This process has some phases which are called as digital forensics methods.

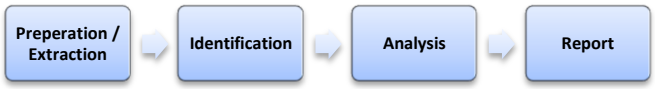


Figure 1: Digital Forensics Methodology

Preparation and Extraction Phase; this is the first step of digital forensics process [3 – 4]. Experts have to do sequential rules;

- Validate all hardware and software
- Duplicate forensic data
- Make a working copy
- Verify hash or fingerprint of data
- Extract data

Identification Phase; all extracted data are identified according to the chain of custody [5] by experts at this phase and experts make a relevant category of data. For example, after being examined, evidences are categorized by organizes crimes, child pornography or terrorism by experts.

Analysis Phase; in this step experts make a meaningful relations of all evidences and generate big picture to observe whole crime processes [6].

Report Phase; this is the one of the most important steps since judicial authorities cannot understand all technological information and also cannot make an exact decision because of complex and meaningless report [7]. For that reason, experts have to prepare their report clearly and understandable to help judicial authorities.

These mentioned phases are methodologies of digital forensics process. If there is no evidence dimming actions, these phases can clearly solve and examine forensically situation. But if it exists, which measurements expert has to take before examination?

Our study based on digital forensics evidence dimming which is called as counter – digital forensics. We will give C–DF definitions and applications area in Section II. Following this, we will focus on deeply C–DF methods and their implementations in Section III. Next section covers negative effects of C–DF to national cyber security. At the end of the study we will give some information's to create general awareness against C–DF techniques.

II. COUNTER - DIGITAL FORENSICS & METHODOLOGIES

Counter - digital forensics is a concept that aims of it are forensic evidence dimming, providing a lack of this evidences, defusing digital forensic experts/ tools or misleading the judicial authorities via scientific ways and technological tools by counter – digital forensics experts [8-10]. Besides, to make an excellent C-DF application experts and tools have to has specifications and capabilities. These are,

- C-DF experts or tools should not be determined by experts or tools,
- Evidences can be meaningless
- Evidences can be erased/wiped and cannot be recovered

- Used time of forensics experts can be extended
- Judicial authorities can be manipulated

C-DF experts have developed specific methods to perform their attacks. Now, we will mention these methodologies and tools through literature research.

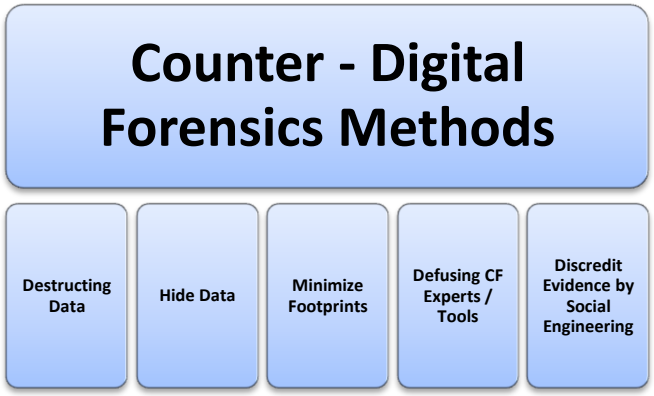


Figure 2: Counter – Digital Forensics Methods

Destructing Data; this method covers deleting, shredding or wiping whole storage with/without suspected digital device [11]. Data destruction can be performed numerous ways.
Data removal techniques;

- File deletion/shredding
- Formatting / reformatting hard drive
- Disk wiping
- Physical destruction
- Overwriting
- Metadata destruction
- User – based information deletion

Hiding Data is one of the most used methods to keep valuable information against digital forensics experts [12]. Keeping possible evidences hide, C-DF experts use several tools and techniques;

- Encryption
- Steganography
- Watermarking
- Image Encryption
- File Hiding in Slack Space and Bad Blocks
- SSL / SSH Encapsulation
- Package Encapsulation
- Cloud

Minimizing Footprint; after C-DF process C-DF experts have to hide remove their or used applications footprint because of being determination by DF experts [13]. Minimization footprint methods are;

- Virtual Machines
- Live CDs
- Live USBs
- Memory Injections
- Creating meaningless user/group accounts
- Deleting appropriate log files
- Using fake IP

Defusing DF experts or tools; manipulation of evidence or changing of contents in examined data/disk may cause vital problems that evidences can lose its judicial value. To make this effect, C-DF experts study on digital forensics (DF) experts' methodologies and DF tools running steps [14]. C-DF experts evaluate all process steps and DF applications capabilities before, in the course of study or after examination and then they perform C-DF one or multi methodologies to convince judicial authorities about evidence.

Discredit Evidence by Social Engineering; whether DF experts collect and report evidences with appropriate DF tools or not, C-DF experts can mislead judicial authorities through missing or wrong information. For example, C-DF experts can change prospective evidence files content or add extra evidence file with inappropriate content [15].

III. SIDE EFFECTS OF C-DF TO NATIONAL CYBER SECURTY

It's an indisputable fact that the rule of law in today's World. While judging individuals, Law decides by taking the constitution and legislation. In process of making decision, in order to be healthy, dozens of components to make a decision is helping law [16]. These assistant components are called forensic science in general terms and exemplified in the form of forensic medicine, forensic microbiology, forensic audio, computer forensics. At any stage of the legal process provided by the judicial authorities of forensic science is incomplete or flawed data or evidence contained in the report and to the legal system as well as social justice in our country will lead to injury [17]. Therefore experts working in forensic science need to be careful in process of forensic analysis and witness to the current study to oppose the concept of forensic science.

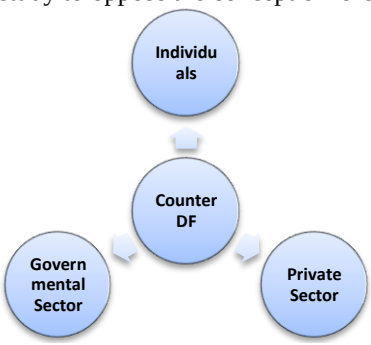


Figure 3: C –DF and its relation with individuals, private and governmental sectors

As our subject, digital forensics and its experts should always keep their mind that there might be opposite forensic studies during their studies due to the legal process and should refrain from giving their negative results analysis. These negative results starting from individuals, private and public sectors may cause many negative reflections. Besides the public

conscience and the law unscathed, national cyber security will be able to give rise to the formation of the weakness.

To show relation C-DF and individuals, private and governmental sectors, we will explain these relations separately.

Individuals; Day by day, data storage capacity of individuals using more active of communication technologies and by reason of having these devices that belongs to people are able to store data in the judicial sense of importance [18]. To get rid of the potential accusation as the result of methods of computer forensic applications that disrupt the judicial processes of individuals will lead to even greater wounds in public's conscience.

Besides hiding their data that might be forensic evidence, because of happening in cyberspace that computers belongs to people can exposure to cyber threats and attacks. As a result of cyber-attacks, that computers could be used in the shape of zombie or by unauthorized persons with different purposes that poses also an element of crime. Moreover, victim individuals can be taken into the custody if C-DF couldn't be detected because of hiding their footprint using C-DF techniques.

Private Sector; Six critical sectors have been identified for cyber security infrastructure that was prepared and published by the Board of Cyber Security in National Cyber Security Document in Turkey [19]. Critical sector structure is public, energy, telecommunications, banking and finance, water and transportation that is given in Figure 4.

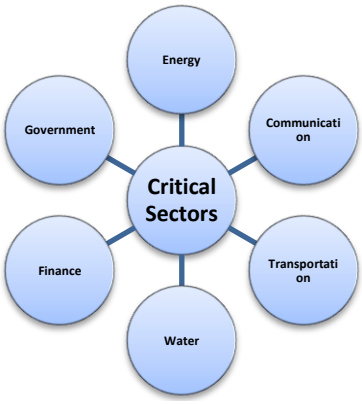


Figure 4: Critical Sectors in Turkey

In terms of Turkey perspective, vast majority of critical sectors companies are located in private sectors. It clearly means that majority of Turkish cyber space is located in private sectors. This can cause a problem such as industrial espionage, monitoring of critical financial data or stealing enterprise commercial data, if the guilty are not punished or detected through digital forensics or cyber security experts. According to this issues, private sectors cyber security experts have to know how to track cyber threats which are performed by cyber attackers or C-DF expert.

Governmental Sector; However individuals and private sectors are important components of national cyber security, governmental institutions such as intelligence agencies, foreign ministry units or military units are as much important as others, maybe much more. It is known that all national critical data are stored and transported on national cyber space [20]. Nowadays all data, from critical archive data of public, to military and intelligence data are stored on information systems. While cyber-attacks targeting individuals or private sector aims to gain reputation or pecuniary advantage, cyber-attacks targeting public sector aims to obtain strategically data belonging to public and damage the international reputation of the public. It is critical to determine the organizations, countries or at least individuals who committed the cyber-attack to protect the international reputation and security [21]. Considering that these attackers will be more Professional than the attackers belonging to the previous two groups, it is very important to analyze the cyber-attack source and results. Both digital forensics experts and cyber security experts who are responsible of public cyber security need to have information about counter digital forensics that will broaden their understanding of both digital forensics and cyber analysis capabilities.

IV. CONCLUSION

Digital forensics has vital role for judicial system because of increasing technology usage. Today criminals, illegal organized groups or enemy country intelligence agencies have been performing cyber-attacks or crimes via using digital devices. Many judicial decisions have to solve this crimes or threats through digital forensics implementations or cyber security protection tools to suspected digital devices or networks. While performing digital forensics process, DF experts have to find evidence via reliable and healthy way. During DF process, experts can face some issues that can affect such as damaged disc. Besides this, DF experts can face extra high level implementations or application provide evidence cannot be detected. These implementations or applications are called as C-DF implementations or applications and these tools or methods are developed by illegal computer security experts or criminals who have IT skills. C-DF application, experts or combined methods can cause side effects on judicial systems.

REFERENCES

[1] Karaman, M., Sağıroğlu, S., "Adli Bilişim Perspektifinde Siber Güvenlik – Adli Bilişim İlişkisi", International Symposium on Digital Forensics and Security, Elazığ, (2013).

[2] Wang, Y., Cannady, J., Rosenbluth, J., "Foundation of computer forensics: A technology fort he fight against computer crime", Computer Law & Security Report, 21/119-127, (2005).

[3] Peisert, S., Bishop, M., Keith, M., "Computer Forensics in Forensis", Third International Workshop on Systematic Approaches to Digital Forensic Engineering, (2008).

[4] Daniel, L., Daniel L., "Digital Forensic : The Subdisciplines", Digital Forensic for Legal Professions, S17-23, (2011).

[5] Garfinkel, S.L., "Digital forensics research: The next 10 years", Digital Investigation 7, S64-S73, (2010).

[6] Altschaffel, R., Kiltz, S., Dittmann, J., "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy", 2009 Fifth

International Conference on IT Security Incident Management and IT Forensics, (2009).

[7] Kim, Y., Kim, K.J.,"A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, (2010).

[8] Garfinkel, S., "Anti-Forensics: Techniques, Detection and Countermeasures", , 2nd International Conference on i-Warfare and Security, Naval Postgraduate School, Monterey, CA, USA, 2007.

[9] Liu, Brown, "Bleeding-EdgeAnti-Forensics", Infosec World Conference & Expo, MIS Training Institute, 2006.

[10] Liu, Stach ,"Defeating Forensic Analysis", CEIC 2006- Technical Lecture 1. Notes, 4. May.2006.

[11] Fruhwirht, C., "An anti-forensic, two level, and iterated key setup scheme", TKS1, 2009.

[12] Sartin, B., "ANTI-Forensics – distorting the evidence", Computer Fraud & Security, 2006.

[13] Albano, P., Castiglione, A., Cattaneo, G., Santis, A., "A Novel Anti-Forensics Technique for the Android OS" , International Conference on Broadband and Wireless Computing, Communication and Applications, 2011.

[14] Lee, S. S., Chang, K., Lee, D., Hong, D., "A new anti-forensic tool based on a simple data encryption scheme", Future Generation Communication and Networking, 114 – 118 (2007).

[15] Losavio, M. M., Hindi, M., "Boundary Conditions for the Digital Forensic Use of Electronic Evidence and The Need for Forensic Counter-Analysis", Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, 1 – 6 (2011).

[16] Krenhuber, A., Niederschick, A., "Forensic and Anti-Forensic on modern Computer Systems", Johannes Kepler Universität Linz, 2006.

[17] DeLooze, L. I., "Counter Hack: Creating a Context for a Cyber Forensics Course", Frontiers in Education Conference, 2008. FIE 2008. 38th Annual, T2H-1 - T2H-6 (2008).

[18] Harris, R., "Arriving at an anti-forensics consensus Examining how to define and control the anti-forensics problem", Digital Investigations, 44 – 49 (2006).

[19] Internet: Resmi Gazete "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf, 2013.

[20] Stamm, M. C., Wu, M., Liu, K. J. R., "Information Forensics: An Overview of the First Decade", IEEE Access, 2013

[21] Schlicher, B., "Emergence of Cyber Anti-Forensics", 4th Annual Cyber Security and Information Intelligence Workshp, Oak Ridge National Laboratory, 2008.

Seref SAGIROGLU is professor Department of Computer Engineering at Gazi University. His research interests are intelligent system identification, recognition and modeling, and control; artificial neural networks and artificial intelligence applications; heuristic algorithms; industrial robots; analysis and design of smart antenna; internet, web and information systems and applications; software engineering; information and computer security; biometry, electronic and mobile electronic signature and public-key structure, malware and spyware software. Published over 50 papers in international journals indexed by SCI, published over 50 papers in national journals, over 100 national and international conferences and symposium notice and close to 100 notice are offered in national symposium and workshops. He has three patents and 5 pieces published book. He edited four books. He carried out of a many national and international projects. He hold the many conferences and continues academic studies.

Mehmet KARAMAN has been working for Information Technologies and Communication Authority in Turkey as a communication expert since 2008. He received BSc degree from Kocaeli University Department of Computer Engineering in 2004. He has received his M.Sc. degree from Gazi University Department of Computer Engineering and still continues his Ph.D. in Gazi University Department of Computer Engineering. His research interest are information security, digital forensics, counter-digital forensics, cyber security, advanced persistence threats and malware analysis.

Hastanelerde Biyomedikal Cihaz Takibi

M. H. Özcanhan[1], G. Dalkılıç[2] ve S. Utku[3]

[1]Dokuz Eylül University, İzmir/Turkey, hozcanhan@cs.deu.edu.tr
[2]Dokuz Eylül University, İzmir/Turkey, dalkilic@cs.deu.edu.tr
[3]Dokuz Eylül University, İzmir/Turkey, semih@cs.deu.edu.tr

***Özet*—Hastanelerde kullanılan seyyar (mobil) biyomedikal teçhizat, cihaz ve aletlere (varlıklar) ihtiyaç duyulduğu zaman bulunamamalarından kaynaklanan sorunlar, tüm tıp çalışanları tarafından bilinen bir konudur. Genel varlık takibi konusunun bir alt başlığını oluşturan hastane varlıklarının etkin yer tespiti ve takibi günümüzdeki kablosuz teknolojilerle mümkün hale gelmiştir. Bu çalışmada, pahalı mobil hastane varlıklarının yüksek maliyeti olmayan radyo frekansı ile çalışan (RFID) ekipmanlarla yer takibi önerilmektedir. Öneri, somut bir yapı teklifi ve güvenli kimlik onayı protokolleriyle desteklenmektedir. Önerinin performans, maliyet ve güvenliği de bu çalışmada değerlendirilmektedir.**

***Anahtar Kelimeler*—RFID, Cihaz takibi, Güvenli kimlik onayı.**

***Abstract*— The problems encountered when the used mobile biomedical equipment, materials and tools (assets) go missing in a hospital are known, by all medical personnel. As a sub-title of the general real time location systems, efficient real time location and monitoring of hospital assets has become possible with today's wireless technologies. In this work, real time location and monitoring of valuable hospital assets by using non-expensive RFID equipment is proposed. The proposal is supported by a solid set-up and two secure authentication protocols. The performance, cost and security of the proposal are also evaluated, in this work.**

***Keywords*—RFID, Equipment tracking, Secure authentication.**

I. GİRİŞ

HASTANELERDE hastalara verilen sağlık hizmetlerinde, klasik ana-bilgisayar üzerinde koşan veri tabanı kayıt sistemleri (Hastane Sistemleri: HS) dışında, hasta tedavisi ve takibi için de mobil, bilgisayarlı elektronik araçların kullanımı yaygınlaşmaktadır. Birçok farklı özellik ve kapasiteye sahip mobil araç kullanımıyla ortaya çıkan teknik konuların, verilen sağlık hizmetinde hasta güvenliğinin tehlikeye atılmaması için uyulması gereken kurallar belirlenmiştir [1]. Bu ve benzeri yayınlarda önceliğin hasta güvenliğine verilmesi öngörülmektedir. Gömülü sistem veya direkt olarak bilgisayar ihtiva eden özelliklere sahip modern mobil ürünlerin kullanıldığı bazı sağlık hizmetleri şunlardır:

- Muayene, tahlil ve tanı konması,
- Hasta tedavisi,
- Otomatik ilaç dozaj paketi hazırlama (AMD: Automatic Medicine Dispenser),
- Doğru yatılı hastaya, doğru dozda, doğru zamanda ilaç uygulaması,
- Gerçek zamanlı hasta ve yeni doğan bebek konum (lokasyon) takibi (RTLS: Real Time Location System),
- Bilgisayarlı görüntüleme,
- Yapay kalp, bilgisayarlı protezler, vb.

Muayenede kullanılan veya hasta üzerine takılan (Holter cihazı gibi) bazı cihazların ortak özelliği pahalı ve mobil olmalarıdır. Kullanılan cihazlar, ihtiyaç bittikten sonra kullanıldıkları yerlerde unutulmakta veya alındıkları yere iade edilmemekte, hatta bulundurulmaları gerekli dolap veya depo dışındaki yerlerde unutulmaktadır. Oysa bu cihazların yeniden kullanımı için terk edildikleri yerde bulunmaları ve depolanmaları gereken yere geri getirilmeleri gerekmektedir. Varlıkların depolandıkları yerden alındıklarında otomatik not düşülmesi, hangi amaçla alındığı ve nerede kullanılacağı bilgisinin HS'ne kolayca girilmesi, hızlı şekilde geri getirilebilmeleri için önemlidir. Mobil hastane varlıklarının konum ve kullanım amacı bilgilerine sahip olunmadığı zamanlarda ortaya çıkan bazı sorunlar şunlardır:

- Yeni hasta muayene veya tedavi sürecine başlanamaması veya geciktirilmesi,
- Tahlil yapma, tanı konma, görüntüleme işlemlerinin yapılamaması veya gecikmesi,
- Yatılı hastaların veya yeni doğan bebeklerin ilaç uygulamalarında hata yapılması.

Bahse konu sorunlar, yönetmeliklerle korunan hasta güvenliğinin temininde ciddi ihlaller oluşturmakta ve birçok olumsuz sonuca sebep olmaktadır. Hastanelerde meydana gelen olumsuz ilaç etkilerinden (ADE: Adverse Drug Effects) dolayı, her yıl çok sayıda yatılı hasta hayatını veya sağlığını kaybetmektedir [2, 3]. Kayıplar sadece yatılı hastaların kayıplarıyla sınırlı kalmamakta, uzayan yatış süreleri ve ilave sağlık sigortası bedelleri yıl sonu toplamında çok büyük maliyetlere ulaşmaktadır. American Medical Association ve Eurobarometer'in yaptırdığı araştırmalar yüksek kayıp rakamlarını ortaya koymaktadır [2, 3]. Aynı şekilde, hastanedeki mobil varlıkların zamanında bulunamaması veya geçici olarak kayıp görülmesinden kaynaklanan sorunlar tüm tıp dünyasında bilinmektedir. Bulunamayan varlıklar, kayda geçirmede karşılaşılan zorluklardan dolayı, ortaya çıkan kayıplar kesin olarak hesaplanamamaktadır. Bahse konu

kayıpların yaşanmaması için, kablosuz iletişim teknolojisi kullanılan takip uygulamaları son zamanlarda popüler yaklaşım olarak öne çıkmaktadır. Kullanılan kablosuz hastane takip sistemleri üç ana başlık altında toplanmaktadır [4]:

1. Hasta Yönetimi,
2. Personel Yönetimi,
3. Varlık Yönetimi.

Kablosuz hastane takip sistemlerini tanımlayan bir standart bulunmamaktadır. Dolayısıyla, teknolojik verinin yönetimi-güvenliği-mahremiyeti konularında yaşanan sorunlar, kullanılan yöntemlerin teknik çözümleriyle giderilmektedir. Bazı sorunlara rağmen, kablosuz uygulamalar verilen sağlık hizmetlerinde verimlilik, kalite ve yönetim kolaylığı konularında faydalar sağlamaktadır. Akademik olarak da, 2012 yılına varmadan yaygınlaşan kablosuz uygulamalarla ilgili çok sayıda bilimsel yayın bulunmaktadır [5].

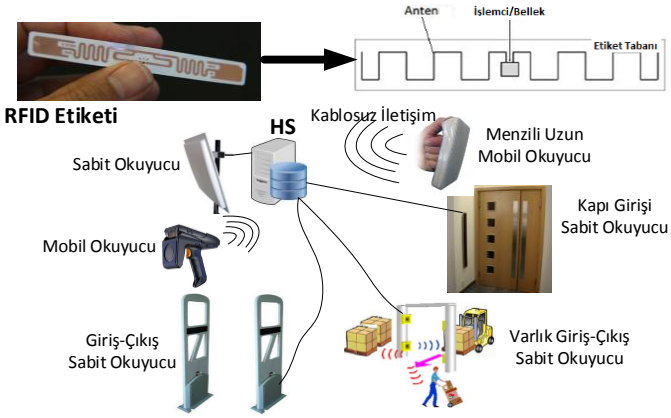
Kablosuz hastane uygulamalarında kullanılan başlıca teknolojiler ise şunlardır:

1. Bluetooh,
2. WiFi,
3. Zigbee,
4. Aktif cihazlı Radyo Frekanslı Kimlik Tanıma (RFID),
5. Pasif cihazlı RFID,
6. Ultrason,
7. Kızıl ötesi.

Kullanılan kablosuz yöntemler arasında RFID dışındaki teknolojiler, bilgisayarlar arası ve bilgisayarlar ile çevre birimleri arasındaki iletişimler için tasarlanmışlardır. Sadece RFID, takip edilmesi istenilen cisimler için biçimlendirilmiş teknolojidir. En ucuz yöntem ise sadece bir elektronik etiketin (tag) kullanıldığı pasif RFID olarak bilinmektedir. RFID kullanılarak yapılan hasta, ilaç, varlık ve tıbbi malzeme takibinde karşılaşılan sorunlar, yapılan strateji/taktik hataları ve bunlara karşı alınması gereken teknik ve idari önlemler belirlenmiştir [5].

Diğer bir bağımsız çalışmada, hastanelerde kullanılan kablosuz uygulamaların uygulama alanları, kullanım seviyeleri göz önüne alınarak değerlendirilmiştir [6]. Uygulamaların kullanım seviyeleri düşük, orta, yüksek derecelerle sınıflandırılmış ve en başarılı uygulamaların en yüksek kullanım seviyesine sahip olanlar olduğu belirlenmiştir. Başarılı olarak değerlendirilen uygulamaların en fazla RTLS varlık takibi alanında olduğu sonucuna varılmıştır [6].

Kablosuz hastane RTLS'lerinde kullanılan teknolojilerin arasında en popüler olanlardan bir tanesi de en ucuza mal olan pasif RFID teknolojisidir. Bu teknolojide takip edilmek istenen şahıs veya varlığın üzerine elektronik bir etiket tutturulmakta veya yapıştırılmaktadır [4]. Etiket, kullanılan frekansa göre uzak veya yakın mesafeden okunmaktadır. Etiketin içerisinde etikete özel çok uzun bir kimlik numarası (ID) bulunmakta ve etiketin üzerinde bulunduğu varlığın yegâne kimliğini ortaya koymaktadır. Okuyucunun konumu bilindiği takdirde, elektronik etiketin, dolayısıyla üzerine tutturulmuş varlığın yeri ortaya çıkmaktadır. HS'ne okuyucu vasıtasıyla düşülen kayıt varlığın en son görüldüğü yerin yaklaşık birkaç metre hatayla tespit edilmesine sebep olmaktadır. Bu teknolojide kullanılan en yaygın iki yöntemden birincisi Şekil 1'de görülmektedir. Etiket, HS'ne genellikle kabloyla bağlı yüksek frekanslı (Ultra High Frequency UHF) farklı tip ve menzile sahip okuyucularla birkaç metre uzaktan okunabilmektedir.



Şekil 1: UHF yöntemli RFID uygulama örnekleri.

İkinci yöntem ise Şekil 2'de görülmektedir. Bu yöntemde etikete hafifçe dokunmak suretiyle etiket çok yakın mesafeden (NFC: Near Field Communication) okunmaktadır. Bu tür etiketlerin okuyucuları, günümüzde yaygın olarak kullanılan mobil telefon ve tablet bilgisayarlarında bütünleşik şekilde gelmektedir. UHF okuyuculara göre NFC okuyucuları çok ucuza satılmaktadır. Ancak, etiketlerde durum farklıdır. UHF etiketleri ucuz, fakat bilgi güvenliği açısından fakir, NFC etiketleri ise UHF etiketlerinden daha pahalı ancak daha çok donanımlıdırlar. NFC etiketler, plastik kartlar (kütüphane, kimlik kartı v.b.) şekline de getirilerek üstün güvenlik algoritmalarına sahip birer gömülü sistem haline de gelebilmektedirler. İki yöntem arasındaki en önemli fark, okuyucular ile HS arasındaki bağlantıdır. UHF okuyucuları genellikle kablo ile bağlanırken NFC okuyucuları kablosuz olarak HS'ne bağlanmaktadırlar. Her iki okuyucu da yüksek bellek ve işlemci gücü kaynağına sahip olduğundan, HS ile olan bağlantılarını güvence altına almakta ispatlanmış güvenlik protokollerini kullanabilmektedirler.

Şekil 2: NFC teknolojisiyle RFID uygulaması.

Havadan iletilen bilgilerin dinlenebileceği düşünüldüğü zaman, etiketlerin okunma yöntemi bakımından UHF'in daha emniyetsiz olduğu görülmektedir. Etiket okuma mesafesinin

uzunluğu ve UHF etiketlerinin kısıtlı kaynaklarından ötürü daha fazla güvenlik açığı ortaya çıkmaktadır. NFC etiketleri ise hem daha üstün kaynaklara sahip, hem de iletişim hafifçe dokunmakla gerçekleştiğinden çok yakınında kötü niyetli biri olsa da, iletişim esnasında iletilen bilgiler dinlenememektedir.

Bu çalışmanın geri kalan bölümlerinde, ilgili çalışmalara 2. bölümde yer verilmektedir. 3. bölümde hastane varlıklarının yer tespiti ve takibi konusundaki önerimiz bulunmaktadır. 4. bölümde önerinin performansı, maliyeti ve güvenlik özellikleri değerlendirilmiştir. 5. bölümde ise sonuç yer almaktadır.

II. İLGİLİ BİLİMSEL ÇALIŞMALAR

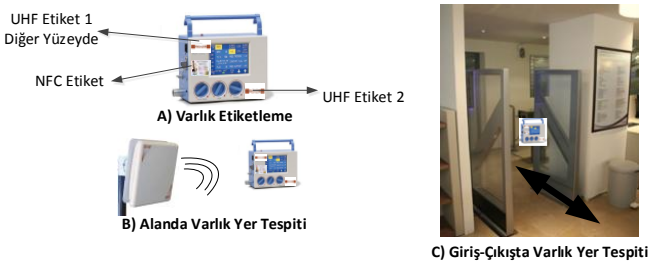
Hastanelerde kablosuz uygulamalar öneren çalışmaların özetlendiği yayınlar, konuya olan ilgiyi ortaya koymaktadır [4, 6]. Listelenen hastane uygulama önerilerindeki birçok kablosuz çözüm arasında en fazla RFID alanında çalışma bulunmaktadır [6, 7]. Hastanelerde kullanılan RTLS'ler de birçok araştırmaya konu olmuştur [6]. RTLS'ler, yer tespiti yapılması istenen cisme ve kullanılan kablosuz yönteme göre farklı gibi görünseler de, neticede öncelikle yer tespiti için düşünülmüştürler. Sistemlerin kullanım seviyeleri, personelin sistemi kullanmaya karşı yaklaşımının etkisi, incelemeye dâhil edilmiştir. Netice olarak, varlık takibi amacıyla kurulan RTLS'lerin, yer tespit uygulamalarının hastanelerdeki en başarılı RFID uygulamaları olduğu sonucuna varılmıştır [6].

RFID'nin önerildiği çalışmalarda ön plana çıkan akademik tartışma konusunu, okuyucu ile etiketin birbirlerini karşılıklı kimlik onayı (mutual authentication) oluşturmaktadır. Çünkü kimlik onayı protokolleri zayıf olduğu zaman, etiketlerin içerdiği gizli bilgiler ele geçirilerek ciddi güvenlik zaafları ortaya çıkarılmaktadır. RFID etiketlerinin çok sınırlı bellek ve işlemci kaynaklarından, güçlü birer gömülü sistem sayılabilecek kaynaklara kadar yelpaze oluşturmasından dolayı, zayıf kimlik onayı protokolleri önerilebilmektedir. Takibi yapılacak cisimlerin sayısı çok olduğundan, maliyeti ucuz etiketler tercih edilmekte, kaynakları çok kısıtlı bu etiketler ise güvenlik açığı olan protokollere davetiye çıkarmaktadır. RFID etiket kullanımına örnek olarak, Walmart'ın 2005 yılından beri ticari ürünlerinde ucuz RFID etiketleri kullanması gösterilebilir [8].

UHF etiketlerde yaygın olarak EPC Global Class-1 Generation-2 standardı (Gen-2) kabul edilmektedir [9]. Gen-2 uyumlu etiketlerin sayısız üründe kullanılabilmesi için fiyatlarının barkod kâğıdına rekabet edebilmesi gerekmektedir. Fiyat rekabeti, Gen-2 etiketlerin güvenlik özelliklerinin 16 bitlik rasgele sayı üreteci (PRNG: Pseudo random number generator), XOR ($\oplus$) ve dönüşsel artıklık denetimi (CRC: Cyclic Redundancy Check) fonksiyonları gibi veri güvenliğini sağlamakta zayıf fonksiyonlara dayandırılmasına sebep olmaktadır [10]. Kimlik onayı üç zayıf fonksiyona dayandırılan etiketlerdeki zafiyetler ve yapılan düzeltme önerileri birçok yayında yer almaktadır [10, 11]. Ancak, yapılan önerilerde takibi yapılan cisimlerin (İnsan veya eşya) hasta güvenliği kurallarına göre kötü niyetli kullanıcıların insafına bırakılmaması gerekmektedir. Bu prensibi başlangıç noktası kabul ederek, hastane varlıklarının yer tespiti ve takibi için tek tip etiket kullanan önerilerin aksine daha güvenli bileşik (combo) bir pasif RFID çözüm önerisi sunmaktayız.

Güvenlik açısından zafiyetleri bilinen Gen-2 etiketlere karşın NFC teknolojisinde kullanılan etiketler, uluslararası alanda onaylanmış güvenlik algoritmalarını bünyesinde barındırabilmektedir [11]. Etiket fiyatının nispeten yüksek olmasına rağmen NFC okuyucularının fiyatları ucuzdur. Dolayısıyla, Gen-2 ve NFC uygulamalarının toplam sahiplenme maliyetleri birbirinden çok yüksek çıkmamaktadır. NFC etiket ve okuyucuları ile ilgili daha detaylı teknik ve ilave referans bilgileri [11] çalışmasından elde edilebilir.

Gen-2 ve NFC etiketlerinin özellik bilgileri ışığında, yer tespiti ve varlık takibi için iki kademeli bir uygulama düşünülebilir. Birkaç metre uzaktan okunabilen Gen-2 etiketi vasıtasıyla varlığın yeri, yakın temasla da yüksek güvenlik önlemleriyle bilgi alış verişi yapılabilir. Üzerine hem Gen-2, hem de NFC etiketi takılan veya ikisinin de mevcut olduğu bileşik bir etiketle iki kademeli uygulama gerçekleştirilebilir.



Şekil 3: Varlık etiketleme ve varlık yer tespiti.

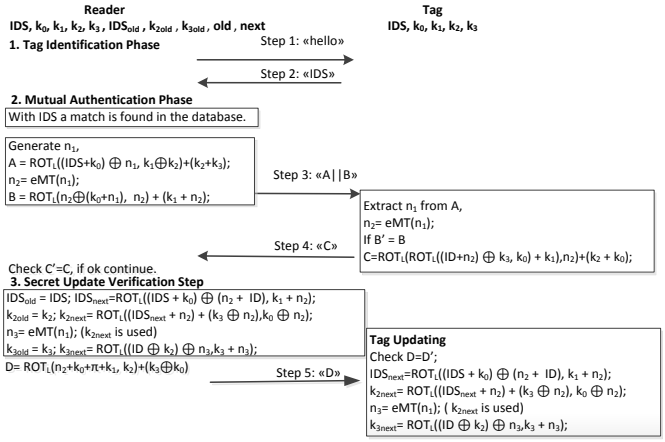
III. ÇÖZÜM ÖNERİSİ

Çözüm önerimizin konusu, ucuzluğu ve pratikliği sebebiyle popüler olan pasif RFID'ye dayalı hastane varlık tespit ve takip uygulamasıdır. Çalışmamızın diğer çalışmalardan farklılığı, tek bir teknoloji yerine iki teknolojiyi bir arada kullanmasıdır. Çözüm önerimizin adı Gen-2 – NFC Bileşik RFID Teknolojili Hastane Varlıkları Yer Tespiti ve Takibi olarak düşünülmüştür. Önerimiz iki aşamadan oluşmaktadır. Şekil 3'te görülen önerinin, aşamaları aşağıda açıklanmaktadır:

A. *Varlık Yer Tespiti Aşaması*

Varlıklar, kullanım açısından acil ve öncelik sırası ile fiyat hassasiyetine göre sınıflandırıldıktan sonra Şekil 3A'da görüldüğü gibi etiketlenmektedir. Bu durumda varlık, iki yandan da birkaç metre uzaklıktan etiketi okunarak tespit edilebilecek özelliğe kavuşturulmaktadır (Şekil 3B). Varlığın depolandığı alandan çıkış bölgesindeki dar bir geçiş bölgesine (alış veriş merkezlerinde konumlandırıldığı gibi) sabit ayaklı okuyucular yerleştirilmektedir (Şekil 3C). Aynı şekilde, diğer bina ve bölüm girişlerine de görünür olmasına gerek duyulmadan okuyucular yerleştirilmektedir. Böylece varlığın çıkışı ve giriş yaptığı bölüm tespit edilebilmektedir. Kayıp varlığın en son görüldüğü bölüme varıldığında mobil bir okuyucunun menzili azamiye ayarlanarak varlığın yeri tespit

edilmektedir. Gen-2 etiketi ile gerçekleştirilecek karşılıklı kimlik onayı protokolü ULERAP Şekil 4'te görülmektedir. Protokol kabul edilen önceki bir çalışmamızda önerilmiştir [12], dolayısıyla anlatım burada tekrarlanmamıştır. Birinci aşamada, ikinci aşamada beklenen güvenlik derecesi beklenmemekte, sadece yer bilgisi elde edilmektedir.

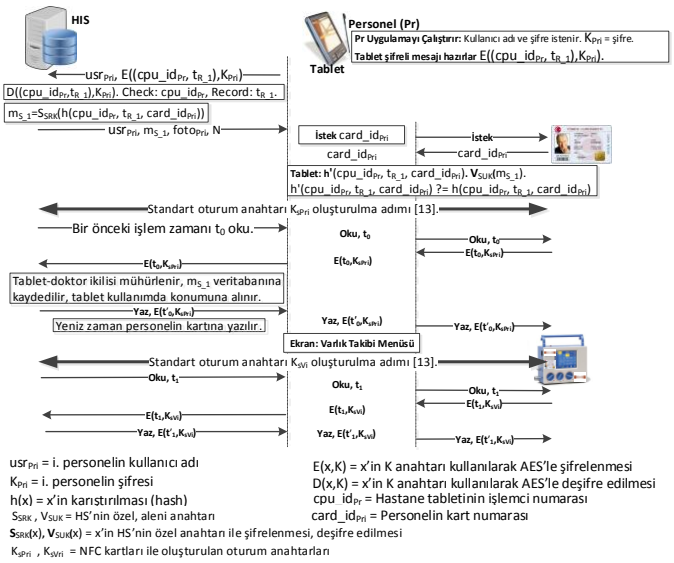


Şekil 4: Yer tespitinde kullanılan ULERAP protokolü [12].

B. *Varlık Takip Aşaması*

Varlığın depoda, kullanımda veya bulunduğu yerde güvenli bir şekilde kimliğinin onaylanması gerekmektedir. Elektronik saldırı veya hatalı kullanıma maruz kalan, özellikle pahalı hastane varlıklarının, bilgi gizliliği (confidentiality) çerçevesinde takibi, bir NFC etiketi ile sağlanmaktadır (Şekil 3). İleri Şifreleme Sistemi (AES: Advanced Encryption System) algoritması kullanarak kimlik onayı yapan ticari bir NFC etiketinin karşılıklı kimlik onayı protokolü 5 adımdan oluşmaktadır [13]. Önceden paylaşılmış gizli bir anahtarla okuyucu ve NFC etiketi arasında gerçekleşen kimlik onayı sonucunda, sadece etiketin okuyucuya dokunduğu esnada geçerli bir oturum anahtarı elde edilmektedir. Kimlik onayı sonrasında okunan ve etikete yazılan bilgiler, oturum anahtarı kullanılarak AES'le şifrelenip takas edilmektedir. AES şifreleme algoritmasını çözdüğünü ortaya atan bir yayın henüz bulunmamaktadır. Dolayısıyla, Şekil 5'te önerdiğimiz varlık takibi uygulama protokolünde, bahse konu NFC etiketi ile gerçekleştirilen iletişimde, bilgilerin deşifre edilmesi mümkün değildir. Oturum anahtarı oluşturulan karşılıklı kimlik onayı protokolündeki standart adımlar, Şekil 5'te "standart oturum anahtar oluşturma adımı" olarak kısaltılmıştır. Uygulamanın NFC okuyucuya yüklenen yazılımında yer bilgisi girişi istenerek, Gen-2 etiketi ile elde edilen yer bilgisi teyit edilmiş olmaktadır. Protokol kısaca şöyledir:

Öncelikle hastaneye ait bir tablet bilgisayara NFC etiketli kimlik kartına sahip görevli personel, Gen-2 – NFC Bileşik RFID Teknolojili Hastane Varlıkları Yer Tespiti ve Takibi yazılımına kullanıcı adını ve parolasını girmektedir. Yazılım tabletin işlemci numarası ve sistem zamanını kullanarak bilgileri personelin gizli anahtarı (kullanıcının parolası kullanılarak sistem yöneticisi tarafından oluşturulur) ile şifreleyerek HS'ne gönderir. HS, kullanıcı adından personelin bilgilerine ulaşır. Mesajı veri tabanında kayıtlı personelin gizli anahtarı ile açar ve bilgilere personelin kimlik kartı numarasını da ekleyerek kendi özel anahtarı (private key) ile şifreleyip, personelin fotoğraf sıra numarası $foto_{Pri}$ ve kimlik kartı ile oturum anahtarı oluşturma esnasında kullanılmasını istediği anahtarın sıra numarası (N) ile birlikte tablete gönderir. Tablet yazılımı, HS'nin açık anahtarını (public key) kullanarak m_{S_1} mesajını açar ve karıştırılmış (hash) sonucu alır. Personelden, kimlik kartını tablete dokundurmasını ister. Personelin kart numarasını alır ve kendisi de bir hash hesaplar. HS'den gelen veri ile kendi hesapladığı doğru ise, personel kartına HS'nin verdiği N'yi iletir. Bu aşamadan sonra personelin fotoğrafı yazılım penceresinde belirir ve yazılım oturum anahtarının oluşturulması için kart ile HS'ne aracılık eder. Oluşturulan oturum anahtarı ile HS kart içinde gizlenen son okuma zamanını kontrol eder ve personelin kartına yeni zamanı yazar. Yazılım, personelden yer bilgisini girmesini ve sonunda kartını almasını ister. Bu işlem sonucunda HS, personel ile hastaneye ait tableti birbirine eşler ve tableti kullanımda olan tabletler listesine alır. Yazılım önceden paylaşılmış farklı bir gizli anahtarın numarasını varlığın NFC kartına vererek, HS ile varlık üzerindeki NFC etiketi arasında oturum anahtarı oluşturulmasına yardımcı olur. Varlık kartındaki zaman okunup kontrol edilir ve yeni zaman yazılır.



Şekil 5: Önerilen şifreli varlık bilgisi okuma protokolü.

Her iki aşamada da okuyucular, HS'ne bağlı olduğundan bilgiler anlık izlenip güncellenebilmektedir. Böylece, merkezi varlık yönetimi karar mekanizması oluşturulmaktadır. Burada tek tehlike, Gen-2 etiketlerinin varlık üzerinden düşmesi veya kasten sökülmesidir. Dolayısı ile varlıklar teslim alınırken Şekil 5'teki adım gerçekleştirilmelidir. Sistem "sorumluluk en son teslim alanda" şeklinde çalışmaktadır.

IV. Performans, Maliyet ve Güvenlik Analizleri

A. Performans

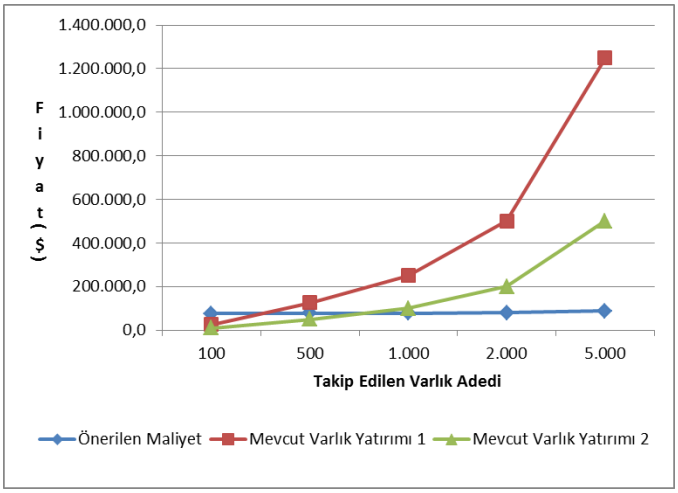
Gen-2 ve NFC etiketlerinin performansları ile ilgili teknik karşılaştırması Tablo 1'de yer almaktadır. Tablodan da görüleceği gibi teknolojiler arasındaki farklardan dolayı etkin varlık konum tespit ve takibi uygulaması için hiçbir etiket tipi tek başına istenilenleri karşılamamaktadır. Her iki etiketin de cismin üzerindeki mevcudiyeti zorunlu görülmektedir.

Tablo 1: Gen-2 ve NFC etiket özellikleri.

Özellik	**Gen-2 (UHF) Etiketi**	**NFC DesFire EV1 Etiketi**
Standart	ISO 18000-6	ISO/IEC 14443A
Kapsam	Temassız entegre	Temassız entegre
Enerjilendirme	Pilsiz (pasif)	Pilsiz (pasif)
Kullanım alanları	Ürün etiketi	Kimlik kartları
Kullanım yerleri	Alış-veriş zincirleri	Ödeme, kütüphane, kimlik
Menzil	7m'ye kadar	0-100 mm
Okuma sayısı	1000 etiket/s	1 etiket/s
Çalışma Frekansı	860-960 MHz	13.56 Mhz
Bellek kapasitesi	512 bit	2, 4, 8 kB NV-bellek
Kimlik Onayı	⊕	AES
Veri Doğrulama	16 bit CRC	16/32 bit CRC; MAC, CMAC
Mobil Okuyucusu	Sınırlı	Yaygın, ucuz

B. Maliyet

Gen-2 etiketleri barkotların yerini almaya en yakın teknoloji olarak lanse edilmekte; bellek, işlem gücü, menzil gibi özellikleri sabit tutularak milyonlarca ürünün üzerine takılmaları hedeflenmektedir. Tablo 2'de Gen-2 ve NFC etiketleriyle okuyucularının ortalama birim fiyatları verilmektedir. Gen-2 etiketlerin fiyatları Tablo 2'den de görüleceği gibi NFC etiketlerinden düşüktür. Ancak, Gen-2 etiketlerinin okuyucuları NFC okuyuculardan çok daha pahalıdır. Bir hastane için gerekli olan etiket ve okuyucu sayısı hizmet veren hastanenin kabul ettiği hasta, klinik sayısı ve kullanılan mobil teçhizat, cihaz ve araçların sayılarına bağlıdır. Örnek olarak 1000 varlığın takibi için gerekli yatırım hesaplanabilir. Yatırımda 2000 Gen-2 etiket, 1000 NFC etiket, 50 sabit Gen-2, 5 mobil Gen-2 ve 10 NFC okuyuculu tablet kullanılacağını dikkate alarak; ayrıca yılda %10 işletim masrafı düşünülerek, 3 yıllık toplam sahiplenme maliyeti Amerikan Doları cinsinden şöyle bulunabilir: {Gen2- etiketler [(2000×0,5) + NFC etiketler (1000×0,623) + Gen-2 okuyucular (55×1027) + NFC okuyucular (10×199)] + üç yıllık ilave işletim masrafı}. 100 ve 1000 adet varlık için toplam maliyetler Tablo 2'de verilmiştir. UHF ve NFC okuyucu sayısı sabit tutularak (maliyeti 58.475$) 100, 500, 1000, 2000 ve 5000 varlık takibi için 3 yıllık toplam maliyetler ayrı ayrı hesaplanarak grafik halinde Şekil 6'da verilmiştir (Önerilen Maliyet). Aynı grafikte, mevcut bir varlığın ortalama değeri 100$ (Mevcut Varlık Yatırımı 1) ve 250$ (Mevcut Varlık Yatırımı 2) kabul edilerek, 100, 500, 1000, 2000 ve 5000 varlığın toplam bedelleri gösterilmektedir. Şekil 6'dan da anlaşılacağı gibi varlık sayısının veya ortalama varlık bedelinin artması ile Gen-2 – NFC Bileşik RFID Teknolojili Hastane Varlıkları Yer Tespiti ve Takibi'nin maliyeti, varlıkların maliyetine oranla ihmal edilebilir bir yatırım haline gelmektedir. Sürekli düşen RFID fiyatları ve yüksek bedelli mobil varlıklar arasındaki fark, RFID yatırımını destekler yönde gelişmektedir.



Şekil 6: Önerilen maliyetler ile mevcut yatırımın karşılaştırması.

C. Güvenlik

HS ile okuyucular arasındaki kablolu veya kablosuz kanalın, her hastanede tam korunduğunu iddia etmek yanlış bir sav olacaktır. Ayrıca, UHF okuyucu ile etiketler arasındaki havadan iletişim de rahatlıkla dinlenerek saldırı gerçekleştirilebilir. Dolayısıyla, gerçekçi bir senaryo olarak çalışmamızda her iki kanala da saldırı yapılabileceği düşünülerek ayrı ayrı güvenlik önlemleri alınmıştır. Ancak, okuyucu ve etiketler üzerine yapılan fiziksel saldırılarla merkezi HS'ne erişimi olan çalışanların içeriden yapabileceği saldırılar bu çalışmada ele alınmamıştır.

Tablo 2: Önerinin okuyucu, etiket ve işletim maliyetleri

Etiket Tipi	**Fiyat/Ürün ($)**		**İlk Yatırım ($)**	**İşletim ($)/Yıl**	**100 Varlık ($)/3 yıl**	**1000 Varlık ($)/3 yıl**
	Etiket	Okuyucu			Genel Toplam	Genel Toplam
Gen-2	0,50	1027	57.485	5.748,5	76.228,5	78.127,4
NFC	0,623	199	2.613	261,3		

HS ile okuyucular arasındaki iletişimin güvenliği özellikle karşılıklı kimlik onayı yapılan Şekil 5'te gösterilmektedir. Burada RSA kripto sistemindeki özellik kullanılarak, kritik bilgiler HS'nin özel anahtarı ile şifrelenmektedir. Bilgileri ancak HS'nin açık anahtarı yüklü hastaneye ait okuyucular açabilmektedir. Şekil 4'teki ULERAP protokolünde de, okuyucuların HS ile olan bağlantısı RSA kullanılmak suretiyle güvenlik altına alınmış ancak gösterim basit tutulmuştur.

Bunun dışında, RFID teknolojilerinde saldırıların daha çok okuyucu ile etiket arasındaki iletişime yapıldığı bilinmektedir.

Çünkü kısıtlı işlem ve hafıza gücünden dolayı etiketler gelişmiş güvenlik algoritmalarını destekleyememektedirler. RFID etiketlerine yapılan saldırılar bilgisayarlara yapılan saldırılara benzemektedir ve bilinen saldırılar (known attacks) olarak adlandırılmaktadırlar.

Şekil 4'te önerilen ULERAP protokolünün pasif ve aktif saldırılara karşı gösterdiği direnç, öneriyi yaptığımız önceki yayınımızda detaylı olarak gösterilmektedir [12]. Yapılan rotasyon kripto-analizi (rotational cryptoanalysis) ile ULERAP'ın bilgi gizliliği ve iletişim mesajlarının bütünlüğünü korumakta açıklarının bulunmadığı ispatlanmaktadır. Gen-2 etiketlerinde en önemli tehlikeyi fiziki saldırılar, etiketlerin varlıkların üzerinden sökülmesi veya yeterli sayıda sabit veya hareketli okuyucu olmaması oluşturmaktadır.

Şekil 5'te önerilen NFC etiketinin kullanıldığı protokol de bilgi gizliliği, bilgi bütünlüğü ve ileriye dönük gizlilik (forward security) sağlayarak kendisinden beklenen güvenlik hizmetlerini (security services) sunmaktadır. Çünkü AES algoritması ve mesaj doğrulama kodu (MAC: Message authentication code) algoritmaları kullanılarak aşağıdaki bilinen RFID saldırıları bertaraf edilmektedir.

Tüm bilgileri açığa çıkarma (full-disclosure): AES algoritması kullanılarak hassas bilgiler gizli anahtarlarla şifrelendiği için bu saldırı mümkün olmamaktadır. AES çözülemediği için aktarılan bilgiler gizli kalmaktadır.

Etiket kopyalama (cloning): Kopyalama için gereken etiket içerisindeki bilgiler açığa çıkartılamadığı için bu saldırı çaresiz kalmaktadır. Fiziksel kopyalama kapsamımız dışındadır.

Kimlik çalma (ID theft): Etiket kimliği çalma mümkün değildir çünkü kullanılan karşılıklı kimlik onayındaki gizli anahtarlar sadece sayılarla işaret edilmekte, asla açıkta geçmemektedir. Bilgiler de gizli anahtarlarla şifrelendiğinden, herhangi bir etiketin kimliğine bürünme mümkün olamamaktadır.

Taklit etme (impersonation): Bir etiketin gizli bilgileri veya anahtarları ele geçirilemediği için taklit etme saldırısı gerçekleştirilememektedir.

Ortadaki adam (man in the middle): Böyle bir saldırının dokunmak kadar yakın iletişim kullanan NFC teknolojisinde mümkün olmadığı kabul edilmektedir. Ortadaki adam aradaki iletişime giremeyeceği gibi hiçbir gizli bilgi veya anahtara sahip olmadığından, taraflarla herhangi bir kimlik onayı gerçekleştiremez.

Mahremiyet (privacy) ve kimlik izi sürme (identity tracing): Kartın numarası başlangıçta açıkta gitmesine rağmen, numaranın HS'den okuyucuya şifreli gönderilmesi ve kartın uzaktan okumasının fiziksel olarak mümkün olmamasından dolayı bu saldırıların başarıya ulaşması mümkün olmamaktadır. Kaldı ki önerilen ticari kart numara yerine rasgele bir sayı cevabı verme alternatifi de sunmaktadır.

Tekrarlama (replay): Önceden kaydedilen geçerli bir kimlik onayı kaydı, önerdiğimiz protokolde fayda sağlamamaktadır. Çünkü her oturumda yeni rasgele sayılar ve sistem zamanı kullanılmakta, her seferinde de yeni oturum anahtarı oluşturulmaktadır. Dolayısıyla, her oturumdaki mesajlar yeni değerlere sahip olmakta, eski bir mesajın tekrarlanması sonuç getirmemektedir.

Hizmet inkârı (denial of service): Bu saldırı, NFC etiketlerine uzaktan erişilemediği, dolayısıyla onları gereksiz uzun hesaplamalara sokarak meşgul etmek mümkün olmadığından yapılamamaktadır.

Senkronizasyon bozma (de-synchronization): Bazı adımlardaki mesajları bloklayarak karşı tarafın farklı değerlere (t_0, t_1 gibi) güncellemesi mümkün olmadığından HS ve etiket arasında farklı bilgi oluşturularak bilgi senkronizasyonu bozulamaz.

V. SONUÇ

Bu çalışmada hastanelerde kullanılan mobil teçhizat, alet ve araçların ihtiyaç duyulduğu anda hazır bulunmaları için bir sistem önerilmektedir. Sistem iki aşamadan oluşan RFID teknolojisini kullanmaktadır. Dünyada, önerilen sistemin farklı yapıda veya tek tip RFID teknolojisi ile oluşturulmuş örnekleri bulunmaktadır. Önerimiz, kolayca tedarik edilebilen somut ürünler kullanılarak gerçekleştirilebilmektedir. Çözüm önerisi, en son teknoloji güvenlik algoritmalarını kullandığı için bilinen saldırılara dirençlidir. Önerilen çözümün, çok sayıda veya bedeli yüksek varlıkların bulunduğu hastanelerde rahatlıkla kurulabileceği görülmektedir.

KAYNAKÇA

[1] Joint Commission. (2010) National Patient Safety Goals (NPSGs). [Online]. Available: http://www.allhealth.org/BriefingMaterials/JointCommission-Oct2009-2010NationalPatientSafetyGoals-1722.pdf

[2] R. Kaushal, D. W. Bates, C. Landrigan, et al "Medication Errors and Adverse Drug Events in Pediatric Inpatients," *The J. of the Am. Med. Assoc.*, vol:285, pp. 2114-2120, 2001.

[3] Eurobarometer. (2006) Survey on medical errors. [Online]. Available: http://ec.europa.eu/public_opinion/archives/ebs/ebs_241_en.pdf

[4] S. F. Wamba "RFID-Enabled Healthcare Applications, Issues and Benefits: An archival Analysis (1997-2011)," *J. of Medical Systems*, vol:36, no:6, pp. 3393-3398, 2012.

[5] W. Yao, C. H. Chu, Z. Li "The Adoption and Implementation of RFID Technologies in Healthcare: A Literature Review," *Journal of Medical Systems*, vol:36, no:6, pp. 3507-3525, 2012.

[6] J. A. Fisher, T. Monahan "Evaluation of real-time location systems in their hospital contexts," *Int. J. of Medical Informatics*, vol:81, no:10, pp. 705-712, 2012.

[7] Information Security Group. (2014) RFID Security and Privacy Lounge. [Online]. Available: http://www.avoine.net/rfid/index.php

[8] M. L. Songini (2006) Wal-Mart details its RFID journey [Online]. Available: http://www.computerworld.com/s/article/109132/Wal_Mart_details_its_RFID_journey

[9] GS1. (2013) UHF Class 1 Gen 2 Standard v. 2.0.0. [Online]. Available: http://www.gs1.org/sites/default/files/docs/uhfc1g2/uhfc1g2_2_0_0_standard_20131101.pdf

[10] M. H. Ozcanhan, G. Dalkilic "Analysis of Two Protocols Using EPC Gen-2 Tags for Safe Inpatient Medication," in *IEEE Int. Symposium on Innovations in Intelligent Systems and Applications*, pp. 1-6, 2013.

[11] M. H. Ozcanhan, G. Dalkilic, S. Utku "Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients," *Radio Frequency Identification*, pp. 19-33, 2013.

[12] M. H. Ozcanhan, G. Dalkilic, "Mersenne Twister Based RFID Authentication Protocol," *Turk. J. Elec. Eng. & Comp. Sci*, accepted to be published.

[13] T. Kasper, I von Maurich, D. Oswald, C. Paar "Chameleon: A Versatile Emulator for Contactless Smartcards," in *Information Security and Cryptology*, pp. 189-206, 2010.

Hukuk Öğretiminde Adlî Bilişim

Türkiye Örneği Bağlamında Bir Değerlendirme

Doç. Dr. Çetin Arslan [1]

[1]Hacettepe University, Ankara/Turkey, cetinarslan68@gmail.com

***Abstract*— Computer forensics is an area of law which is developing and becoming important. However, the education on the computer forensics is not provided in law faculties. The non-thesis master's programs and the certification programs are far from the quality to provide the required proficiency. The solution to remedy this deficiency is to educate the law faculty students on the computer forensics which is now the most important branch of evidence law. In this study, we will mention the importance of computer forensics, the general situation of Turkish legal education and the present and required positions of computer forensics in the legal education. In so doing, we aim to attract attention on the place of computer forensics which is one of the developing areas of law in legal education.**

***Keywords*— Computer/digital forensics, law school, education, information technology law**

I. GİRİŞ

Bilgi Çağı olarak nitelenen 21. yüzyılda "bilişim"den etkilenmeyen kişi, kurum, meslek veya bilim dalı neredeyse yok gibidir. Bu bağlamda bizatihi hukuk sistemi yanında, hukukun muhatabı ve uygulayıcıları da kaçınılmaz bir şekilde bu etkinin kapsamında kalmaktadırlar. Gerçekten bir taraftan yeni nesil kanun, tüzük veya yönetmelik vb. mevzuatta elektronik ve bilişimle ilgili birçok hüküm (ör. e- fatura, e-defter, e-imza, e-ödeme, bilişim suçları) birer hukuk normu olarak mevzuattaki yerini alırken, diğer taraftan Türk yargı sisteminin alt yapısı tamamen "Ulusal Yargı Ağı Bilişim Sitemi (UYAP)" olarak isimlendirilen elektronik ortamda sağlanmaktadır. Ayrıca gerek ceza, gerekse hukuk yargılamasında elektronik veya dijital delilin doğrudan veya dolaylı şekilde kullanılmadığı hemen hiçbir uyuşmazlık bulunmamaktadır.

Bilişimin hukukla etkileşime girdiği veya temas ettiği noktalarda ise yorumlanması, değerlendirilmesi ve çözülmesi gereken birçok durum veya sorun ortaya çıkmaktadır. Bu durumda ister teorik, isterse pratik alanda yer alsın hukukçunun, söz konusu kesişme noktalarında uzmanlık veya en azından temel düzeyde bilgi gereksinimi ortaya çıkmaktadır. İyi bir hukukçu için vazgeçilmez bir ihtiyaç olarak ortaya çıkan bu donanım kuşkusuz özel gayretlerle edinilebilirse de, bir öğretim politikası olarak hukuk fakültelerinin müfredatlarında yer alması kaçınılmaz gözükmektedir. İşte bu çalışmada biz, hukuk eğitiminde adli bilişimin yeri ve önemini ortaya koymaya çalışacağız. Bunu yaparken sistematik olarak, önce genel olarak hukuk eğitiminin bulunduğu yeri, ardından adli bilişim ile hukukun bağlantısını, sonra hukuk eğitiminde adli bilişimin mevcut konumunu ve olması gereken yerini netleştirmeye çalışacağız.

II. GENEL OLARAK HUKUK EĞİTIMI

Hukukun siyasetle iç içe geçtiği ve gerek ulusal gerek uluslararası gelişmelerle güncel bir tartışma konusu niteliğini sürekli olarak koruduğu ülkemizde hukuk eğitimine olan talep son yıllarda giderek artmaktadır. Bunda, şüphesiz ülkemizde uyuşmazlıkların genelde sulh yoluyla çözülmeyip yargıya intikal etmesinin ve hukukun artık hemen herkesin günlük hayatının bir parçası haline gelmesinin de etkisi büyüktür.

Artan talebin de etkisiyle ülkemizde 2009'da 55 hukuk fakültesi bulunmakta iken bu sayı 2013 yılı itibariyle 32'si devlet, 44'ü vakıf üniversitesi olmak üzere toplam 76'ya yükselmiştir **[1]**. Bu yetmiş bir hukuk fakültesine 2013 yılında on beş bin dört yüz yirmi öğrenci alınmış ve böylelikle hukuk fakültelerinde öğrenim gören toplam öğrenci sayısı kırk bini aşmıştır. Giderek ivme kazanan bu artışa karşılık, bu fakültelerde yalnızca 354 profesör, 164 doçent ve 537 yardımcı doçent ders vermektedir **[2]**. Bir araştırma görevlisinin yardımcı doçent olarak öğretim kadrosuna girmesi en azından 6–8 sene sürebilmekte iken her yıl bir yeni hukuk fakültesi açılabilmektedir. Bunun sonucunda, öğrenim elemanı sayısı / öğrenci sayısı oranı giderek küçülmektedir. Öğrenci sayısının artmaya devam etmesi durumunda öğretim elemanı sayısındaki yetersizliğin büyüyeceği açıktır.

Fakültelerin müfredatlarına bakıldığında, ders saati, kredi sayısı, tamamlanması gereken asgarî ders yükü ve derslerin içeriklerinin büyük farklılıklar gösterdiği göze çarpmaktadır. Örneğin, bir üniversitede dönemde beş zorunlu ders alınırken diğerinde ikisi seçmeli on ders alınabilmektedir. Bu farklı sistemlerden mezun olan öğrencilerin nitelikleri de

farklılaşmaktadır. Hukukî anlamda yetkinlik düzeyi farklı olan bu öğrencilere denk diplomalar verilmekte ve bu kişiler, uygulamada aynı pozisyonlara talip olabilmektedir. Örneğin, sosyal güvenlik hukuku pek çok üniversitede senelik zorunlu ders iken bazı üniversitelerde **[3]** seçmeli ders olarak dahi okutulmamaktadır.

Bunun yanı sıra, hukuk eğitimi bazı fakültelerde yalnızca mevzuatın öğretilmesine indirgenmiş ve öğrenciler hukuk fakültesinden hukuk nosyonu, analitik ve eleştirel düşünce yapısı ve adalet duygusu oturmadan mezun olmaya başlamıştır. Sadece olan hukuk öğretilmekte, olması gereken hukuk üzerine düşünülme olgusu teşvik edilmemektedir. Bunun neticesinde, sosyal hayatın yeni gelişen kavram ve kurumları ile hukuk arasındaki bağ zayıflamakta ve hukuk bu yeni kurumların ihtiyaçlarına cevap veremez hâle gelmektedir.

III. ADLÎ BILIŞIM VE HUKUKLA ILIŞKISI

"Adlî bilişim" teriminin kökeni İngilizcede "computer forensics"tir. Bilgisayar anlamına gelen "computer" ile "mahkemeye ait, adlî" anlamlarına gelen "forensics" kelimelerinin bir araya gelmesinden türetilen bu terim Türkçeye birebir çevrildiğinde "adlî bilgisayar" anlamı ortaya çıksa da kavramsal olarak genellikle 'adlî bilişim' ifadesi kullanılmaktadır. Doktrinde "bilgisayar kriminalistiği" olarak da adlandırılabilmektedir. Biz kavram olarak "adli bilişim" ifadesini kullanmayı tercih etmekteyiz.

Adlî bilişim, "elektronik ortamlardan elde edilen bulguların, bilişim teknik ve teknolojileri kullanılarak hukukî delillere dönüştürülme süreci" olarak tanımlanabilir **[4].** Adlî bilişim, adlî olayların aydınlatılması amacıyla, olay yerinden, dijital veri saklama ve iletme özelliğine sahip araçların toplanması, içerisindeki dijital delillerin tespit edilmesi ve adlî organlara raporlanması süreci içerisinde yapılan çalışmaların bütünüdür **[5]**. Adlî bilişimin amacı suçla ilgili dijital delilleri elde etmektir. Bu konuda araç olarak bilgisayar teknolojilerinden faydalanılmaktadır. Dijital deliller, fiziksel deliller gibi doğrudan elde edilip değerlendirilemediğinden, bunun için birtakım teknik donanım ve yazılımlara ihtiyaç duyulmaktadır. İşte dijital delillerin özelliği nedeneiyle ortaya çıkan ihtiyaç ve sıkıntılar, adlî bilişim konusundaki gelişmeleri teşvik etmektedir.

Günümüz toplumu, bilgisayar ve internet toplumu haline gelmiştir. Bireyler günlük hayatlarının birçok ihtiyacını internet üzerinden karşılamakta, aktif olarak sosyal medya ve internet kullanmakta ve çıkan uyuşmazlıklar da genellikle elektronik ortamda vücut bulmaktadır. Sorunun kaynağı bilişim olunca çözümü de bilişim yöntemleriyle sağlamak gerekmektedir. Zira uyuşmazlığı ortaya koymaya yarayacak deliller de çoğu zaman elektronik araçlar üzerinde yer almakta veya teknolojik yöntemler kullanılarak elde edilmektedir. Bu sebeple günümüzde bilişim, adlî olayların çözümünde kullanılmakta ve "adli bilişim" gün geçtikçe önem kazanan bir alan hâline gelmektedir. Doktrinde "yeni suç mecrası" **[6]** olarak da anılan bu alanda suçlulukla mücadele edilebilmesi ve delillerin hukuka uygun bir şekilde toplanıp değerlendirilebilmesi için adlî bilişim konusunda hukukî düzenlemelerin detaylandırılması ve hukukçulara bu konuda eğitim verilmesi şarttır.

Yargılamada amaç gereçeğe ulaşmaktir. Maddî gerçeğin ortaya çıkarılmasında ise delil serbestîsi ilkesi geçerli olup bu ilke, hukuka uygun olmak kaydıyla her türlü şeyin delil olarak kullanılabileceği anlamına gelmektedir. Adlî bilişim de bir ispat vasıtası olması sebebiyle muhakeme hukukunun bir parçasını oluşturur. Son yıllarda etkinliği artan bilişim hukuku konularına yardımcı bir disiplin olarak ortaya çıkan adlî bilişimin hukukla ilişkisi daha çok delil hukukuna ilişkin konularda görülmektedir. Dijital, diğer bir ifade ile elektronik deliller bu iki alanın ortak paydasını oluşturmaktadır. Elektronik delil, elektronik bir araç üzerinde saklanan ya da elektronik bir araç vasıtası ile iletilen muhakeme aracıdır. Video görüntüleri, dosya ve klasörler, silinen dosyalar, gizli ve şifreli dosyalar, indirilen öğeler, internet geçmişi, iletişim kayıtları, çeşitli bilgisayar programları elektronik delil olarak kullanılabilen öğelerdir. Bu deliller, bilgisayarlarda, internet ortamında, cep telefonlarında, hafıza kartlarında, taşınır belleklerde, CD ve DVD'lerde, MP3 çalarlarda, kamera ve fotoğraf makinelerinde, yazıcı, faks ve fotokopi makinelerinde, modemlerde, GPS'lerde ve hatta oyun konsollarında bulunabilir **[7]**. Adli bilişimin amacı, suç ile ilgili olabilecek dijital delilleri elde etmektir. Bu amaca ulaşmak için kullanılacak yöntemler ise bilgisayar inceleme ve analiz tekniklerdir. İşte hukuk, bu delillerin uygun şekilde nasıl toplanacağı, saklanacağı, aktarılacağı, kullanılacağı ve inceleneceği ile ilgilenmektedir.

Ceza muhakemesi açısından bakıldığında adlî bilişim yalnızca bilişim suçlarında delil elde edilmesi amacıyla kullanılmakla kalmayıp aynı zamanda klâsik suçların da çeşitli aşamalarını ortaya koymakta yardımcı olmaktadır. Örneğin, bir hırsızlık suçunda, yapılan plânlar, çizilen krokiler, telefon görüşmeleri, mailler incelenerek dijital deliller de elde edilebilir ve maddî gerçeğin ortaya çıkarılmasında kullanılabilir.

Bunun yanı sıra, adlî bilişim, ceza muhakemesi işlemlerini internet ortamında veya internet aracılığıyla yapılabilir hâle getirmiştir. Bunun sonucu olarak, yargılama sürecinin hızlanması ve bireylerin makûl sürede yargılanma hakkının ihlal edilmemesi ve bazı insan hakları ihlâllerinin önüne geçilmesi beklenmektedir.

IV. HUKUK EĞITIMINDE ADLÎ BILIŞIM

Muhakeme sürecinde, iddia ve savunma makamlarınca ileri sürülen tez ve anti-tez niteliğindeki argümanlar sentezlenerek gerçeğe ulaşılmaya çalışılmaktadır. Hâkimin vicdanında somut olaya ilişkin bir kanaât oluşturmak maksadıyla yaratılan bu çelişmenin çözümü ise ancak süreçte elde edilen deliller sayesinde mümkün olabilmektedir. Bu çerçevede, kısaca "sayısal ortamda delil elde etme faâliyeti" **[8]** olarak tanımlanabilecek olan adlî bilişimin, esas itibarı ile usûl/yargılama hukukunun, ceza ve ceza muhakemesi hukuku özelinde ise ceza muhakemesi hukukunun çalışma sahasına girdiğini söylemek yanlış olmayacaktır.

Adlî bilişim, yukarıda da ifade edildiği üzere, kişilerin bilişim teknolojilerinden istifade etmek suretiyle işledikleri suçlara ilişkin verilerin toplanıp incelenmesine ve elde edilen sonuçların bir rapor hâlinde adlî makamlara sunulmasına yönelik olarak yürütülen faaliyetler bütünüdür. Bir kimsenin bu alanda yetkin sayılabilmesi için ise, takdir edileceği üzere, kapsamlı ve derinlikli bir eğitimden geçirilmesi, yetkinliğinin profesyonel yöntemlerle sınanması ve nihayet eriştiği yetkinliğin belgelendirilmesi şarttır.

V. MEVCUT DURUM

Uygulamaya bakıldığında, idare hukukundan icra ve iflâs hukukuna, aile hukukundan ceza hukukuna hukukun hemen her dalında bilişim hukukunu ilgilendiren birtakım uyuşmazlıklarla karşılaşıldığı ve bu alanlarda artık dijital delil yoğun şekilde kullanıldığı hâlde sadece bir kaç hukuk fakültesinde, lisans müfredatlarında bilişim hukukuna ilişkin derslere yer verdiği görülmektedir.

Örneğin, İstanbul, Çankaya, Başkent, Akdeniz ve Dokuz Eylül üniversiteleri hukuk fakültelerinde hemen her yıl, farklı adlar altında, bilişim hukukuna dair seçmeli dersler açılmaktadır. Hatta Koç Üniversitesi Hukuk Fakültesi müfredatına bakıldığında, burada "Bilişim Teknolojileri Hukuku" dersinin öğrencilere zorunlu ders olarak okutulduğu görülmektedir.

Buna karşılık, yetmiş altı fakültenin tamamı incelendiğinde, bu üniversitelerin bu açıdan müstesna olduğunu söylemek mümkündür. Zira Galatasaray, Bilkent, Ankara, Gazi, Yeditepe ve Atatürk üniversiteleri başta olmak üzere, isim yapmış pek çok üniversitede, hukuk fakültelerinin bilişim hukuku derslerine müfredatlarında yer vermediği/ veremediği görülmektedir. Bunda, lisans programlarının dört yıla (sekiz döneme) sıkıştırılmaya çalışılmasının payı, şüphesiz büyüktür.

Bu nedenle, gerek nitelikli öğretim görevlisi/ üyesi sayısının azlığı ve gerek lisans düzeyinde –haftalık iki ya da üç saatten- dönemlik verilecek bir ders ile uygulamadaki açığı kapatmanın imkânsızlığı dolayısıyla, bazı üniversiteler bu alana yönelik olarak tezli-tezsiz yüksek lisans programları açmak yoluna gitmişlerdir. Bilişim teknolojisini kullanan mesleklerde işgücü kalitesini yükseltmek ve bilişim hukukuna vâkıf deneyimli hukukçular yetiştirmek yönünde atılan ilk adım Gazi Üniversitesi Bilişim Enstitüsü'nün kurulması olmuştur **[9]**. Enstitü bünyesinde açılan adlî bilişim tezli yüksek lisans programı ile bu alanda diğer üniversitelere öncülük eden Gazi Üniversitesi'ni Bilişim & Teknoloji Hukuku Enstitüsü **[10]** ile İstanbul Bilgi Üniversitesi ve Bilişim Enstitüsü bünyesinde açılan bilişim hukuku tezsiz yüksek lisans programı ile Hacettepe Üniversitesi **[11]** izlemiştir. Bilişim suçlarından güvenli yazılımlara, adlî bilişimde bilirkişilik müessesesinden siber güvenliğe pek çok farklı konu başlığını kapsayan bu programlar sayesinde kişilere –uzman olmayan kişi ve/veya kuruluşlarca görece niteliksiz sertifika programlarına kıyasla- akademik bir altyapı kazandırılmakta ve böylelikle uygulamadaki yetkin personel açığı belli ölçüde kapatılabilmektedir.

VI. ÖNEMI VE OLMASI GEREKEN DURUM

Lisans öğretiminde verilen ceza muhakemesi derslerinde, ceza muhakemesinin süjeleri, muhakeme şart ve işlemleri, koruma tedbirleri, görev, yetki, delil ve bilirkişilik gibi konu ve müesseseler ana hatları ile anlatılıyor ise de günümüzde hukukun ayrılmaz bir parçası olan adlî bilişime ilişkin olarak öğrencilere –ne yazık ki- yeterli altyapı sağlan(a)mamaktadır. Program müfredatlarının güncel gelişmelerin gerisinde kalması dolayısıyla geleceğin avukatları, hâkimleri ve akademisyenleri adlî bilişimden bîhaber mezun olmaktadırlar. Bunun neticesinde de avukat ve savcılar bilişim hukukuna ait delillerin nasıl elde edilip saklanacağını ya da ne şekilde kullanılacağını bilememekte; hâkimler ise bu delillerin değerlendirilmesi noktasında sıkıntılar yaşamaktadır. Bu durumun önlenmesinin tek yolu ise adlî bilişime ilişkin derslere hukuk fakültelerinde ve lisansüstü programlarında yer verilmesidir.

Nasıl ki hukuk tarihi ya da Roma hukuku dersleri hukukun temellerinin ve gelişim aşamalarının anlaşılması açısından faydalı bulunuyor ve müfredatlarda yer alıyorsa, hukukun yeni gelişen dalları da ders olarak fakültelerde okutulmalıdır. Nitekim bu anlayış kapsamında rekabet hukuku, anayasa şikâyeti, ekonomik suçlar gibi dersler seçmeli ders olarak müfredatlara eklenmektedir. Adlî bilişim de aynı şekilde, ya ilgili derslerde (ceza muhakemesi veya medeni usûl) ayrı bir başlık altında okutulmalı ya da müfredatta seçmeli ders olarak yer almalıdır. Dijital delillerin artık ceza ve hukuk muhakemesinin ayrılmaz bir parçası olduğu düşünüldüğünde,

adlî bilişimin ayrı bir ders olarak okutulması, kanaâtimizce, daha uygun olacaktır.

Hukuk fakültelerinde özel hukuk ve kamu hukuku ayrımı yapılmaksızın bir hukuk öğrencisinin mezun olduktan sonra ihtiyaç duyacağı tüm bilgiler öğrencilere verilmektedir. Verilen dersler değişen mevzuata göre güncellenmekte, mevzuatla birlikte değişen ihtiyaçlara cevap vermektedir. İşte, bu çerçevede, ceza muhakemesi derslerinin içeriğinin de günümüzde kullanılan kurum ve araçlara daha geniş yer ayıracak şekilde değiştirilmesi gerekmektedir. Bu kurumların başında da adlî bilişim gelmektedir. Zira günümüzde deliller fiziksel olmaktan çok dijital şekilde görülmektedir ve bu husus, delil hukukunun güncel gelişmelere uygun anlatılmasını gerekli kılmaktadır. Kamu hukuku yüksek lisans programlarında ise, ceza ve ceza muhakemesi alanında uzmanlaşmak isteyen hukukçular için adlî bilişim seçmeli dersleri yer almalıdır.

VII. SONUÇ

Türk hukuk eğitiminde adlî bilişim konusuna yeterince yer verilmediğini görmekteyiz. Gelişen kavramların zamanla hukuk öğretiminde bir yer edinmesine karşılık adlî bilişim henüz tüm lisans programlarında yer almamaktadır. Bunun neticesinde ise, hukuk fakültesi mezunları günümüzün en etkin hukuk dallarından biri olan bilişim hukuku ve adlî bilişim alanında bilgi sahibi olmadan lisans eğitimlerini tamamlamaktadırlar. Oysaki uygulamada en sık karşılaşılan sorunlar artık çoğunlukla bilişimle ilgili olmaktadır. Bunun neticesinde, yeni mezun avukatlar ve genel olarak hukukçular yetkin olmadıkları bir alanda çözüm üretmeye çalışmakta ve bunda da –ne yazık ki- pek başarılı olamamaktadırlar.

Yüksek lisans programlarında ya da sertifika programlarında **[12-13]** adlî bilişim konusuna yer verilse de bunun lisans programında alınacak eğitimle eşdeğer olmadığı açıktır. Öncelikle her mezun lisansüstü eğitime devam etmemektedir. Öte yandan, sertifika programları zahmetli ve masraflı olabilmektedir. Ayrıca, lisans eğitiminde öğrencilerin her konuda sağlam bir temele sahip olması hedeflenirken adlî bilişimin bu alanlardan biri olmaması günümüz teknolojisinin geldiği nokta ile tezat teşkil etmektedir. Hukuk fakültesi öğrencilerinin özel hukuk ve kamu hukukunun çeşitli alanlarında aldıkları temel eğitimlerinin bir parçası da adlî bilişim olmalıdır. Bu sayede, çağın ihtiyaçlarına cevap verebilen hukukçuların yetişmesi sağlanacaktır.

Köklü hukuk fakülteleri yerleşmiş usûller nedeniyle ders programlarında ya da ders içeriklerinde pek fazla değişikliğe gitmemektedirler. Ancak, yeni kurulan fakülteler için adlî bilişim derslerinin en başından ders programlarında yer edinmesi faydalı olacaktır. Yeni fakülteler eskilerini taklit etmek yerine yeni bir vizyon ve misyon edinmeli **[14]**, güncel ihtiyaçlara cevap veren konulara ders programlarında yer vermelidirler. Bu sayede, hukuk güncelliğini korumuş olacak, güncel sorunlar hukuksal çözümlere kavuşacak ve hukukun üstünlüğü ilkesi sarsılmadan etkinliğini korumaya devam edecektir.

REFERENCES

[1] Muharrem Kılıç'ın "Türk Yükseköğretiminde Hukuk Fakültelerine İlişkin Durum Tespit Raporu" başlıklı çalışmasından aktaran Ankara Barosu Başkanlığı, http://www.ankarabarosu.org.tr/Detay.aspx?SYF=8457, erişim tarihi: 25.03.2014.

[2] Taha, Akyol, "Bilimde Kalite", http://www.hurriyet.com.tr/yazarlar/24507932.asp, erişim tarihi: 25.03.2014.

[3] http://www.hukuk.bilkent.edu.tr/program.html, erişim tarihi: 25.03.2014.

[4] http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/, erişim tarihi: 26.03.2014.

[5] http://www.adlibilisim.org.tr/index.php/hakkimizda/2013-04-25-04-43-07/adli-bilisimin-tan-m, erişim tarihi: 26.03.2014.

[6] Muharrem, Özen, İhsan, Baştürk, Bilişim-İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara 2011, s. 87-89.

[7] http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/, erişim tarihi: 26.03.2014.

[8] Ayrıca bkz. M. Özen, İ. Baştürk , s. 140..

[9] Bu konuda ekteki tabloya bakınız.

[10] http://be.gazi.edu.tr/ erişim tarihi: 27.03.2014.

[11] http://cyberlaw.bilgi.edu.tr/, erişim tarihi: 27.03.2014.

[12] http://www.bilisim.hacettepe.edu.tr/, erişim tarihi: 27.03.2014.

[13] http://yusem.yasar.edu.tr/egitim-programlari/adli-bilisim-egitimi-sertifika-programi/, erişim tarihi: 27.03.2014.

[14] http://sem.aydin.edu.tr/index.asp?id=415&islem=program, erişim tarihi: 27.03.2014.

[15] Kemal Gözler, "Küreselleşme Sürecinde Hukuk Eğitimi", *Legal Hukuk Dergisi,* Yıl 6, Sayı 69, Eylül 2008, s.3021-3030.

Implementing Secure Communication on Short Text Messaging

Avinash Chandragiri, Peter A. Cooper, Yanxin Liu and Qingzhong Liu

Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, USA
Emails: akc021@shsu.edu; cooper@shsu.edu; yanxin@shsu.edu; liu@shsu.edu

***Abstract*—On-line Short Text (OLST) in social networking tools such as micro blogs, instant messaging platforms, and short message service (SMS) via smart phones has become a routine in daily life. OLST is appealing for personal covert communication because it can hide information in a very short carrier text, and this concealment is hard to detect due to the diversity of normal traffics. However, designing appropriate schemes confronts several challenges: they need to be provably secure, and their performance needs to maintain high efficiency and handy usability due to the short length of OLST messages. In this paper, we implement a family of customized Cryptographic schemes known as HSym, HCod, HNum, and HPhs and Steganographic schemes HMea, HAbr, and HEmt for text hiding in OLST. These schemes are evaluated in terms of their security and their performance with regard to metric that address the particular characteristics of OLST: hiding rate. All implemented schemes are proved to be at least computationally secure, and their performance in terms of hiding rate justifies their applicability in social networking tools that utilize OLST.**

***Keywords*— Steganography, secure communication, short text, text messaging.**

I. Introduction

Steganography is the art or practice of concealing information within another digital cover file, which is currently dominated by multimedia files such as image, video, and audio data [4, 5] and most literatures in steganography and the detection have been focused on multimedia-based steganography and steganalysis [15,16,17,18,19,20,21,22, 23]. Recently, text steganography, where information is hidden in carrier (or cover) texts, has attracted considerable interest from researchers [6]. Text cover files are very different from image, video and audio multimedia data files, since multimedia data files generally have good room of redundancy to accommodate the hidden data, and human eyes/ears cannot perceive the changes.

In text steganography, a cover text is usually of ordinary length, such as a Microsoft Word document [6, 7]. While text steganography is different from multimedia-based steganography, On-Line-Short-Text (OLST) [1] is even quite different from cover texts in terms of information hiding. It has a limited word or symbol count, and it is usually input by hand. The text may include some personal touches such as shorthand acronyms, special phrases, emotion symbols ("emoticons"), and preferred formats or styles. Currently, several special information hiding methods exist for specific languages [10], and some methods for text hiding have been proposed [11]. However, most existing schemes for text hiding have not yet been strictly justified in a formal framework for provable security. More importantly, because OLST has its own special characteristics, new methods that can address these particular features are needed. Compared to hiding methods for cover texts, those for OLST require more subtle justification. Moreover, the performance of text hiding for OLST is different from other types of text steganography. For example, the concealing rate needs to be very high because the text is short, and the ease of use for users must be maximized because OLST is usually input manually. OLST usually has a client tool that provides graphic user interface to facilitate text input. People using OLST platforms communicate with each other by typing characters and punctuation. Most client tools also support shortcut input of emotion symbols ("emoticons") for "angry", "sad", "happy", "frustrated", etc. (there are dozens of such symbols), and the character size and font can also be set as a customized option by users. Usually, chatting occurs between two peers; however, chatting can also occur between a peer and a group, where all members of a group can receive one peer's input. In this case, the intended recipient in the group is the information reveler, and the others are observers).

II. Problem formulation

Generally speaking, there are three entities in OLST:

(1) An information hider [1]: A person or a program that hides hidden information in OLST;

(2) A hidden information reveler [1]: A person or a program that recovers hidden information in OLST; and

(3) An observer [1]: A person or a program that fully accesses the OLST and may be aware of the existence of hidden information in the observed OLST.

The formal definitions used are as follows.

Definition 1 Information hider is a Polynomial Time Turing Machine (PTTM) that can hide hidden information in carrier information.

Definition 2 Hidden information reveler is a PTTM that can recover hidden information from carrier information.

Definition 3 Observer is a PTTM that observes carrier

information that hides hidden information.

Definition 4 Hidden information [1] is hidden by information hider. Usually, Hidden information belongs to {a, b, c…….z, A, B, C….Z, Symbols}.

Definition 5 Carrier information [1] is transferred from information hider to hidden information revealer and hides hidden information.

III. Existing Systems

A. Word Shifting

Word Shifting [12] method is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This method is identified less, because change of distance between words to fill a line is quite common. But if somebody was aware of the algorithm of distances, they can compare the present text with the algorithm and extract the hidden information by using the difference. Although this method is very time consuming, there is a high probability of finding information hidden in the text.

B. Hiding using whitespaces

This concept is very straightforward. A message to hide is first converted into a binary format. Then, every bit whose value is 1 is represented by an extra whitespace between a particular set of two words in the carrier text; whereas, every bit whose value is 0 leaves the original single whitespace between the next particular set of two words. For example, “the boy went to school today” can be deciphered as “101001”. In fact, two spaces exist between “the” and “boy”, between “went” and “to”, and between “today” and the end of the sentence. This results in a bit of value 1 in positions 0, 2, and 5 respectively. In contrast, only a single space exists between “boy” and “went”, between “to” and “school”, and between “school” and “today”. This results in a bit of value 0 in positions 1, 3, and 4 respectively. Basically, the whitespace technique is very suspicious as a normal reader would right away notice the existence of some extra whitespaces in the text. Additionally, this method cannot encode too much information especially in small text.

IV. Proposed methods

In this section we implement new text hiding methods for Online Short Text (OLST).

1. Cryptographic Methods

A. Hiding by Symbols: HSym

In this method the text is hidden by mixing some character to original text. The resultant hiding text will be send to others.

Input: Text (what)

Output: Hidden Text (dfefe}{dd)

Algorithm:

1: Read input Text T

2: Get each Character C

3. for each Character in C
   a. Get ASCII Value of Character C
   b. Add Random integer Value
   c. Convert to equivalent character.
   d. Add to array
4. Do steps a, b, c, d until you reach end of the input.

B. Hiding by Coding: HCod

In this method the text is hidden by some code. Here we are using Huffman code algorithm for hiding the text in the form binary form.

Huffman coding [1] is a form of statistical coding, not all characters occur with the same frequency, yet all characters are allocated the same amount of space. Code word lengths are no longer fixed like ASCII. Code word lengths vary and will be shorter for the more frequently used characters.

Input: Text (what)

Output: 00011010111001111011

Algorithm:

1. Scan text to be compressed and tally occurrence of all characters.
2. Sort or prioritize characters based on number of occurrences in text.
3. Build Huffman code tree based on prioritized list.
   a. Count up the occurrences of all characters in the text.
   b. What characters are present?
   c. What is the frequency of each character in the text?
   d. Create binary tree nodes with character and frequency of each character
   e. Place nodes in a priority queue– The lower the occurrence, the higher the priority in the queue.
   f. While priority queue contains two or more nodes

- Create new node
- Dequeue node and make it left sub tree
- Dequeue next node and make it right sub tree
- Frequency of new node frequency of left and equals sum of right children
- Enqueue new node back into queue
- Dequeue the single node left in the queue.
- This tree contains the new code words for each character.
- Frequency of root node should equal number of characters in text.

4. Perform a traversal of tree to determine all code words.
5. Scan text again and create new file using the Huffman codes.

C. Hiding by Number: HNum

In this method the text is hidden by mixing numeric values to original text. The resultant text will be in the form of number.

Input: Text (what)

Output: Number (436)

Algorithm:

1: Read input Text T

2: Split the text into words where space occurs and store them in an array.
3: Get the element in the array and store it as a string.
4. Until you reach the end of the string do the following:
A. Get each character in the string.
B. convert the character into integer and add random number to it.
5. Add the values of each character in the string.
6. Add it to a string.
7. Do steps 3, 4, 5 until you reach end of the text.

D. Hiding by Phrase: HPhs

As many phrases are involved in chatting, we therefore propose HPhs, a method that uses phases to represent hidden information. HPhs can easily generate carrier text actually, it can hide any hidden information independent from carrier information. The content of carrier information has no relation to hidden information, so perfectly secure hiding is guaranteed. We select the most frequently used phrases[1] and create a file that includes interjections ("ah","well", "haha", "oh"," hey", and "yeah"), remarks ("wait", "OMG", and "gosh"), modal particles ("hmm" and "ok"), emotion symbols (":-)" or ":-("); punctuation ("?", "!"), and phrases ("BTW" (by the way),"FYI" (for your information), "IC" (I see), "TY" (thank you), "great", "neat", and "cool").

Input: Text (what)
Output: FYI (For Your Information)
Algorithm:
1. Store list of phrase words
2. Get each Sentence S
3. for each Sentence in Text
A. select phrase
B. hide the original S with selected Phrase
4. Display hide info

2. Steganographic Methods

A. Hiding by Meaning: HMea

In this method the information hider and the revealer share the table which contains the information about the words in American English which mean the same as in British English, but spelled differently.

Check list
0 → British English
1 → American English
Example:
Embedding: movie in my flat ("secret 10")
movie in my flat
Extracting: movie in my flat
"secret 10"

B. Hiding by Abbreviations: HAbr

In this method we make two lists of abbreviated forms one with usual abbreviations and other with chat abbreviations. Information hider and revealer share the usual abbreviation list, chat abbreviation list and check list.

Check list
0 → full form, 1 → abbreviated form
Information hider and revealer share the usual abbreviation list , chat abbreviation list and check list.
Example:
Embedding :
"I am dng mastersofscience at SHSU."
secret "101"
"I am dng mastersofscience at SHSU."
Extracting :
"I am dng mastersofscience at SHSU."
secret "101"

C. Hiding by Emoticons: HEmt

In this method we hide the information in Emoticons symbols that are being used most frequently in chat. The information reveler and hider share certain set of emoticons list. Based on the position and appearance of the emoticons its meaning changes.

Check list:
Emoticon Sentence=0
Sentence Emoticon=1
-Emoticon =00
+Emoticon =01
Emoticon-=10
Emoticon+=11
Emoticon'= Equivalent number assigned to emoticon
(Emoticon)2 = First letter of name of emoticon
Other emoticon symbols = Do nothing.

V. Analysis

A. Security analysis

In all our methods we have used random generator which has high security properties:

Pseudo randomness: The generator's output looks random to an outside observer.

Forward security: The third party which learns the internal state of the generator at a specific time cannot learn anything about previous outputs of the generator.

Break-in recovery / backward security. The third party which learns the state of the generator at a specific time does not learn anything about future outputs of the generator, provided that sufficient entropy is used to refresh the generator's state.

Even if the third part know the algorithm and the reverse engineering is performed in knowing the original text it will consume a lot of time (days/years).

B. Performance analysis

Using cryptographic methods we hide all the symbols as we are demolishing the original text into a disguised text which can provide almost an unbreakable security which proves that its hiding rate is 100%, but it gives a suspicious look. Using steganographic methods the number of symbols hiding will be less but it will be high secured as no one knows the meaning. The message will not be in a suspicious form. For HMea let there be two sentences' in which we are hiding 3 symbols for every sentence and every sentence contains 5 words and each word is of 5 characters. Therefore hiding rate is 6/25. For HAbr and HEmt, use of abbreviations and emoticons in chat or SMS is high, usually more than half of the text will be either in emoticons or abbreviations, therefore the hiding rate will be more than 50%.

VI. CONCLUSION

The implemented family of text hiding schemes in OLST known as HSym, HCod, HNum, and HPhs, HMea, HAbr, and HEmt. Their security and their performance in terms of hiding rate were examined. Analysis shows that all the implemented schemes have at least computationally secure hiding. Moreover, the schemes hiding rate guarantees their applicability in social networking tools that utilize OLST.

REFERENCES

[1] W. Ren, Y. Liu and J. Zhao, "Provably Secure Information Hiding via Short Text in Social Networking Tools", TSINGHUA SCIENCE AND TECHNOLOGY ISSNll1007-0214ll01/18llpp225-231, Volume 17, Number 3, pages 225-231, June 2012.

[2] M. Shirali-Shahreza, "Steganography in MMs". In: IEEE International Multitopic Conference (INMIC'07). Lahore, Pakistan, 2007: 1-4.

[3] Z. H. Wang, C.C. Chang, T.D, Kieu et al. "Emoticon based text steganography in chat". In: Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA'09). Wuhan, China, 2009, 2: 457-460.

[4] H. Wang and S. Wang. "Cyber warfare: Steganography vs. steganalysis". Communications of the ACM, 2004, 47(10): 76-82.

[5] Y. Wang and P. Moulin. "Perfectly secure steganography: Capacity, error exponents, and code constructions". IEEE Transactions on Information Theory, 2008, 54(6): 2706-2722.

[6] V. Chand and C. O. Orgun. "Exploiting linguistic features in lexical steganography: Design and proof-of-concept implementation". In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). New York, USA, 2006, 6: 126b.

[7] T. Y. Liu and W.H. Tsai. "A new steganographic method for data hiding in Microsoft word documents by a change tracking technique". IEEE Transactions on Information Forensics and Security, 2010, 2(1): 24-30.

[8] M. Khairullah. "A novel text steganography system using font color of the invisible characters in Microsoft word documents". In: Second International Conference on Computer and Electrical Engineering (ICCEE'09). Dubai, 2009, 1: 482-484.

[9] Y. L. Liu, X. M. Sun, C. Gan, et al. "An efficient linguistic steganography for Chinese text". In: IEEE International Conference on Multimedia and Expo. Beijing, China, 2007: 2094-2097.

[10] M. H. Shirali-Shahreza and M. Shirali-Shahreza. "A new synonym text steganography". In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'08). Harbin, China, 2008: 1524-1526.

[11] J. Langford, N. Hopper, L. von Ahn. "Provably secure steganography, extended abstract". In: Advances in Cryptology (CRYPTO'02). California, USA, 2002, 2442: 119-123.

[12] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O. Gorman, "Document marking and identification using both line and word shifting," INFOCOM'95 Proceedings of the Fourteenth Annual Joint Conf. of the IEEE Computer and Communication Societies, 1995, pp. 853-860.

[13] H. Kabetta, B. Y. Dwiandiyanta, and Suyoto, "Information hiding in CSS: a secure scheme text steganography using public key cryptosystem," Int. Journal on Cryptography and Information Security, vol.1, pp. 13-22, 2011.

[14] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol.35, pp. 313-336, 1996.

[15] Q. Liu., Sung, A.H. and Qiao, M. "Neighboring joint density-based JPEG steganalysis". *ACM Transactions on Intelligent Systems and Technology*, 2(2): article 16, 2011.

[16] Q. Liu. "Steganalysis of DCT-embedding based adaptive steganography and YASS". In *Proc. The Thirteenth ACM workshop on Multimedia and Security*, pp. 77-86. 2011.

[17] Q. Liu. "Detection of misaligned cropping and recompression with the same quantization matrix and relevant forgery". In *Proc. 3rd International ACM workshop on Multimedia in Forensics and Intelligence*, pages 25-30. 2011.

[18] Q. Liu., and Chen, Z. "Improved approaches with calibrated neighboring joint density to steganalysis and seam-carved forgery detection in JPEG images". *ACM Transactions on Intelligent Systems and Technology*. 2014. http://tist.acm.org/papers/TIST-2012-11-0181.R2.pdf

[19] Fridrich J. and Kodovsky J. "Rich models for steganalysis of digital images". IEEE Transactions on Information Forensics and Security, 7(3): 868-882, 2012

[20] Q. Liu, A.H. Sung, Z. Chen and X. Huang, "A JPEG-based statistically invisible steganography", Proceedings of the Third International Conference on Internet Multimedia Computing and Service, pages 78-81, 2011.

[21] Q. Liu, A.H. Sung, Z. Chen and J. Xu, "Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images", Pattern Recognition, vol. 41, Issue 1, pages 56-66..

[22] Q. Liu., Sung, A.H. and Qiao, M. "Derivative-based audio steganalysis". *ACM Transactions on Multimedia Computing, Communications and Applications*, 7(3): article 18, 2011.

[23] M. Qiao, A. H. Sung and Q. Liu, "MP3 audio steganalysis", Information Sciences, volume 231, pages 123-134, May 10, 2013.

Legal Concerns and Challenges in Cloud Computing

Sundar Krishnan [1] and Lei Chen [2]

[1] Department of Computer Science, Sam Houston State University, Huntsville, Texas, USA, sxk030@shsu.edu
[2] Department of Computer Science, Sam Houston State University, Huntsville, Texas, USA, chen@shsu.edu

***Abstract*— Legal issues have risen with the changing landscape of computing, especially when the service, data and infrastructure is not owned by the user. With the Cloud, the question arises as to who is in the "possession" of the data. The Cloud provider can be considered as a legal custodian, owner or possessor of the data thereby causing complexities in legal matters around trademark infringement, privacy of users and their data, abuse and security. By introducing Cloud design focusing on privacy, legal as a service on a Cloud and service provider accountability, users can expect the service providers to be accountable for privacy and data in addition to their regular SLAs.**

Keywords—Terms of Service (ToS), Cloud, Privacy, Legal challenges of Cloud, LaaS (Legal as a Service), Risk, Service Level Agreement SLA, Privacy Impact Assessment (PIA), Cloud Service Provider (CSP)

I. INTRODUCTION

Cloud computing in layman's terms can be defined as a network of virtual computers hosted outside our firewalls. Cloud computing caters to the demands of Information Technology in terms of increasing capacity and features with decreasing costs. Thus, accessing the Cloud comes with a cost known as the subscription fee per service, also known as service models. Users (post authentication) can access the Cloud using browsers on their tablets, desktops and laptops.

This paper begins with discussing the two most popular issues of user-privacy and data-privacy challenges on the Cloud. The paper also discusses a few solutions to these issues. It concludes with a discussion on Cloud designs, Accountability and LaaS (Legal as a Service) as options that can be provided by the Service Providers to the data users via the SLAs.

A. *User privacy in the Cloud*

Privacy is a very important consideration in the Cloud computing world since actual or perceived privacy weaknesses will impact compliance, data security and user trust thereby giving rise to legal complications [1][5]. Unfortunately, legal rights and regulatory authority for the protection of the user privacy in the Cloud computing world is not well defined [9].

Access and storage of user's movements and behavioral information while on the Cloud has a huge market for the data mining and advertising companies. Information such as viewing habits within the Cloud generates huge statistics that has a market. As user's movement on the Cloud is tracked and stored, this data is of very high interest to many companies. They study the movements to in turn spam the user with products that they may want in the near future. For example, a user looking for a mobile phone may also need a service plan. Thus, smart programs working in the background pop-up messages prompting the user with various service plans from different cell phone carriers.

Companies would like to know the patterns of user movement within the Cloud thereby better enabling them to setup their products so that the user can be attracted to them. Data-mining companies also take interest in how we search and apply for jobs and where we get our news, to how we find friends. Often the service providers do not let the user know that their presence on the Cloud could lead to collection and marketing of such statistics. Also, many users do not feel the importance of such risks until it's too late.

In summary, since Cloud computing is still evolving, service providers often change their policies, SLAs and Operating *ToS* and are not obligated to inform the users. In many cases, they do notify the users on their websites, but, user ignorance steers them to ignore such information updates. Despite user ignorance of the challenges of using the Cloud, users are embracing the Cloud and taking advantage of its benefits like low costs, reliability, security and simplicity. Due to its sudden surge in popularity, Cloud computing may find itself a prey to security, privacy and legal issues.

II. BACKGROUND

A. *Data Privacy - Laws and Acts*

When users place their data and applications on the Cloud servers, they lose the ability to maintain complete control of that information. The critical and sometimes sensitive information that was once safely stored on personal computers now resides on the servers of online companies. Such data security concerns prevent companies and users from taking advantage of the Cloud. Security concerns can be of 3 types: Traditional Security, Availability, and Third-party data control [7].

Traditional security concerns involve Virtual Machine level attacks, cross-site scripting, and phishing of a Cloud provider, computer and network intrusions, attacks or hacking. Availability concerns center on critical applications up-time, single point of failure and assurance of computational integrity. Third-party control of data concerns are about legal

implications of data location, loss, data-audit, contractual obligations, data lock-ins etc.

1) Electronic Communications Privacy Act*:* Under this Act, data stored in the Cloud may be subject to a lesser standard for law enforcement to gain access to it than if the data were stored on a personal computer. Moreover, the ToS and SLAs for Cloud services often makes it clear that they will preserve and disclose information to law enforcement when served with a legal process. Thus, data privacy issues exist such as appropriate collection of data, appropriate data use, data disclosure, safe data storage, retention of data, data access and ways of keeping the user informed about how these issues are handled and impact them.

2) Stored Communications Act: Cloud computing allows users to store and access their files and data away from their personal machines. The Cloud is seen as a single application or a device that can be accessed from various computing devices. Although users might expect that their data stored on the Cloud is private, in reality they do not enjoy a lot of privacy. By passing the Stored Communications Act (SCA) [19], Congress hoped to encourage development and use of new and emerging methods of communications by protecting citizen's privacy rights. The SCA limits the government's ability to compel Internet service providers to disclose information stored with them. The Act defines service providers as Electronic Communications Services (ECS) and Remote computing Services (RCS). The level of privacy protection afforded by a stored communication differs based on which category the service provider falls in and sometimes, for how long the communication was stored.

In summary, as the current Stored Communications Act is outdated and complicated, the courts have interpreted it in an inconsistent and unclear manner [14]. The extent to which protections under the SCA apply is an open question and depends on the courts applying the reasoning of *Theofel (Theofel v. Farey-Jones* 359 F.3d 1066 (9th Cir. 2004) [18]).

3) Federal Information Security Management Act (FISMA): This Act was enacted in 2002 to recognize the importance of information security to the economic and national security interests of the United States. It provides a uniform regime to address levels of risk that may arise from domestic and international sources. It requires federal agencies to create and implement programs to review information security and report the results to the Office of management and Budget (OMB).

With the Federal agencies taking to the Cloud to reduce costs, security and data privacy concerns are primary reasons for not migrating their systems into the Cloud. Also, they are concerned about losing control and thus want visibility into the Cloud's security incidents and risk management.

The General Services Administration (GSA) and Office of Management and Budget (OMB) have focused on security and data privacy as top priorities to facilitate Cloud adoption through the Federal Cloud Computing Initiative, GSA's Blanket Purchase Agreement (BPA) for Cloud Infrastructure as a Service (IaaS) and the Federal Risk and Authorization Management Program (FedRAMP), the government-wide program providing a standardized approach to security assessment, authorization and continuous monitoring for Cloud products and services [15].

4) Fourth Amendment issues: The Fourth Amendment [14] provides that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" [15]. The architecture of the Internet and Cloud is such that the courts are unlikely to apply the Fourth Amendment protections for users.

Since the information is inherently handled and processed by third parties, it may be difficult to separate coding information from protected content. Also, it is unclear as to which machine or set of machines on the Cloud would be considered as the "container" in the warrant.

5) The USA PATRIOT ACT: This Act gives FBI access to any business record as long as a court order is issued. This privilege can be used to obtain data from the Cloud without the knowledge of the user. This can increase the mistrust between the users and the governmental agencies and could deter users from using the Cloud services.

6) Jurisdictional Issues: In the Cloud design, users can access their data from any location as the data can be stored on distributed virtual servers in data centers spread across many countries. Cloud service providers consider the location of the data centers for purposes like costs, laws, infrastructure and labor. Thus, the question arise "Which country's laws to apply"? User data is stored across many data centers in the world and is dependent on the service provider's agreements with the operators of the data-centers. Legal experts are wary of cases involving a Cloud. Also, if software development is conducted on a Cloud, Copyright issues could arise from country to country depending on which machine was used for which developer [17]. Such scenarios are further complicated when developers are scattered around the world. Thus, the locations of the data centers affect the legal rights of the users.

7) HIPPA: Health information service providers who *store* user medical information may not be subject to the privacy protections of the Health Insurance Portability Protection Act. Even when it is clear that user data is protected, Cloud service providers often limit their liability to the user as a condition of providing the Cloud service leaving users with limited recourse should their data be exposed or lost [10].

III. SOLUTIONS TO LEGAL CHALLENGES

A. *Privacy Impact Assessment (PIA)*

A Privacy Impact Assessment (PIA) is a predictive and proactive systematic business process to evaluate possible future effects that a particular activity or task that may have on user's privacy. It focuses on understanding the system thereby identifying and mitigating any adverse privacy impacts. It

informs decision makers who must decide whether the task should proceed into the next step and if so; in what form.

Although reactive processes such as privacy issue analysis, privacy audits and privacy law compliance checking can be applied to existing systems, a proactive measure can be well managed if planned well.

Privacy Impact Assessment (PIA) was initially launched by the Information Commissioners Office (ICO) of UK to help organizations access the impact of their Cloud operations on personal privacy. This process was primarily intended for use in the public sector risk management but has been a value to private sector businesses that process personal data. The role of a PIA within the Cloud is to ensure that the risks to personal privacy are mitigated and should be initiated early in the design phase and needs to be revisited in every phase. The output of this process needs to undergo corrective action and the fed back into the next stage in the design process in an iterative manner.

In conclusion, many PIA tools have now been designed and have been well embraced by organizations when dealing with the Cloud. A typical PIA tool contains a set of questions and answers with calibrated weightage [10]. A drawback of this tool is that the organizations or users need to drive its implementation rather than the service provider. PIA tools are one of the many layers that will eventually be needed to protect user privacy.

B. *Assessment of Cloud design*

Privacy designs need to be assessed at different phases of the design like in the initiation, planning, execution, closure and decommission phases [4]. The ignition phase should deal with the setting of high level privacy requirement recommendations, strategy and goals.

The Planning phase would elaborate on these requirements and goals and detail their inputs and outputs. The execution phase would be identifying the problems relating to the solutions which have been proposed and considering any alternative approaches if needed. Documenting issues and privacy exposures also are a part of this phase. In the closure phase, audits, change management processes, business continuity, disaster recovery are considered. Finally the decommission phase is to properly dispose the private and sensitive information obtained during the product's lifecycle. J.C. Cannon [11], [12] describes the processes and methodologies on how to integrate privacy considerations during development process. Auditing existing systems to identify privacy problem areas and protecting them against privacy intrusions is a competitive advantage for the product and the organization. At all phases, privacy experts need to be involved with adequate training.

C. *Use of PETs*

Privacy Enhancing Technologies (PET) can be any technology that exists to protect or enhance an individual's privacy including facilitating individuals to their rights under various Acts and Laws [4]. Examples of such technologies include privacy management tools that enable inspection of server-side policies, secure access mechanisms for users to check and update their personal data, pseudonymization tools that allow users to withhold their true identity.

The Privacy Enhancing Technologies Symposium [13] addresses the aspects of privacy technologies, the design and realization of privacy services for the Internet, data systems and networks. This symposium brings together anonymity and privacy experts from around the world to discuss advances and new perspectives around the privacy of user's personally identifiable information.

In conclusion, since the benefits of PETs is huge to organizations, many technologies are being developed and debated such as Wallets of multiple virtual identities, anonymous credentials, Negotiation and enforcement of data handling, etc.

D. *PccP Model*

The PccP model as described by Rahman [8], prescribes a three layered architecture. The layers include the Consumer Layer, the address mapping Layer and the Privacy Preserving Layer. The Consumer layer consists of the users while the address mapping layer helps in mapping the user and an IP address from a pool such that the user's actual IP address is made obscure. The transformed IP address is then used while navigating in the Cloud. The Privacy Preserved Layer has a unique user Cloud Identity Generator to generate a unique user Identity thereby ensuring the privacy of the user. Rahman proposes algorithms to generate the Unique Service Dependent Identity and Privacy preserver Match Logic.

To conclude, Rahman's Model attempts to enhance the privacy of sensitive user information such as IP addresses based on IP masking and unique identity generation until the user is present on the Cloud. However, this model needs further evaluation as to the extent of anonymity needed for the user.

E. *Accountability for Cloud Services- A4Cloud.*

Cloud service providers lack accountability frameworks making it difficult for users to understand, influence and determine how their SLAs will be honored. Cloud services allow enterprises to outsource their business to third parties. The complexity of the services provider's eco-system may not be visible to the data user or enterprise. The A4Cloud project helps to create solutions to support users in deciding and tracking how their data will be used by the Cloud service providers by combating risk analysis, policy enforcement, monitoring and compliance auditing for security, assurance and redress.

The A4Cloud [2], [16] project is an Integrating project (IP) launched in 2012 in the EU's 7th Framework Program (FP7) led by HP Labs with many European countries as partners. The A4Cloud aims to enable the Cloud service providers to give the data users appropriate control and transparency over how their data is used and allow them to make choices about how the Cloud service providers protect their data in the Cloud. A4Cloud also aims to monitor and check compliance against user’s expectations, business

policies and regulations and lastly implement accountability ethically and effectively. An interdisciplinary co-design approach is the cote to the A4Cloud by combining legal, regulatory, polices, business processes and technical measure into a framework for accountability.

A4Cloud aims to [4]:

- Enable Cloud service providers to give their users appropriate control and transparency over how their data is used.
- Enable users to make choices about how Cloud service providers may use and will protect data in the Cloud.
- Monitor and Check compliance with user expectations, business policies and regulations.

Implement accountability ethically and effectively.

(Fig 1. A4Cloud interlocking Objectives [4])

A4Cloud Objectives: A4Cloud has four interlocking objectives to bring users, providers and regulators together in chains of accountability for data in the Cloud, clarifying liability and providing greater transparency overall.

Objective 1 [4]: Develop tools that enable Cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the Cloud, delivering increased levels of accountability to their customers.

Objective 2 [4]: Create tools that enable Cloud end users to make choices about how Cloud service providers may use and will protect data in the Cloud, and be better informed about the risks, consequences, and implementation of those choices.

Objective 3 [4]: Develop tools to monitor and check compliance with users' expectations, business policies and regulations. The A4Cloud provides a comprehensive accountability monitoring solution that would address the issue of preserving privacy and protecting confidential information.

Objective 4 [4]: Develop recommendations and guidelines for how to achieve accountability for the use of data by Cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

In conclusion, A4Cloud Solution is a promising project that promises to address major barriers to trustworthy Cloud-based services. It helps to support service providers by using audited policy enforcement techniques, assessing and detecting policy violations, managing incidents and obtaining redress.

F. *Legal as a Service (LaaS)*

Security, privacy and law-awareness are some of the biggest challenges faced by the Cloud service providers (CSP) to implement. Thus, Law-as-a-Service (LaaS) has been suggested for CSPs as a law-aware semantic Cloud policy infrastructure. The semantic legal policies in compliance with the laws are enforced automatically at the super-peer levels to enable LaaS. This allows CSPs to deploy their Cloud resources and services without worrying about law violations. Afterward, users could query data from the law-aware super-peer within a super-peer domain. Each query is also compliant with the laws. The law-aware super-peer is a unique guardian, who provides data integration and protection services for its peers within a super-peer domain. Each super-peer enforces the legal policies to enable data integration and protection services.

A privacy protection policy is a combination of ontologies and rules, where Description Logic (DL) based ontologies provide data integration, while Logic Program (LP)-based rules provide data query and protection services after data integration. Policies are shown as a combination of OWL-DL ontologies and stratified Datalog rules with negation for a policy's exceptions handling through defeasible reasoning. Law-as-a-Service (LaaS) enhances self-managed SaaS (System as a Service) on the automated security and privacy policy in the virtual data centers. Structure data is modeled as ontologies and used for data integration. Furthermore, the stratified Datalog rules with exceptions handling capabilities extend ontologies to enhance data protection and query services.

In summary, the concept of Law-as-a-Service (LaaS) [6] has been suggested by Hu, Wu and Cheng for CSPs as a law-aware semantic Cloud policy infrastructure. This seems as an exciting approach where a super-peer (unique law-aware guardian and trusted proxy) provides LaaS for its peers. The Super-peer also specifies how law compliant legal Cloud policies are enforced and unifies in the super-peer domain. This approach seems to be further developed and explored.

IV. CONCLUSION

A search on online databases yielded very few published papers and articles on Legal challenges around Cloud Computing. This shows that this area of concern is not yet fully explored or discussed. A probable cause is due to the fact that Cloud boundaries are spread across geographies and each country has their own legal frameworks to deal with the Cyber world thereby complicating industry understanding of the Cloud and its legal complexities.

Cloud fears arise due to the perception of loss of control over sensitive data. The current control measures do not adequately address user's fears. Increased trust in the Cloud coupled with cryptographic techniques can help implement reliable controls thereby provide demonstrable business intelligence advantages to the Cloud stakeholders.

Cloud Providers are still fine-tuning their Service Level Agreements (SLAs) and Terms of Service (ToS) as the Cloud concept is yet in its infancy and unless users know the legal impact of Cloud Computing, the SLAs will not have the needed teeth to deal with legal issues arising out of the Cloud.

Additionally, laws need to be further enacted to deal with the Cloud designs. A broad international legal framework in cyberspace is the need of the hour as each country increases it's footprint in the Internet world. This kind of framework may best implemented by the United Nations to its member countries given its international reach.

V. FUTURE WORK

The main issues related to cloud computing implementation are data-security, privacy, and law-awareness. By coupling legal compliance into CSP services, law-awareness can be incorporated into the cloud infrastructure. The concept of Law-as-a-Service (LaaS) [6] as suggested for CSPs is a law-aware semantic Cloud policy infrastructure. In this infrastructure framework, a super-peer (unique law-aware guardian and trusted proxy) provides LaaS for its peers. The Super-peer also specifies how law compliant legal Cloud policies are enforced and unifies in the super-peer domain. This approach seems to need further exploration and pilot-implementation.

(1) References

[1] Tom Kirkham, Django Armstrong, Karim Djemame, Marcelo Corrales, Mariam Kiran, Iheanyi Nwankwo, Ming Jiang, Nikolaus Forgo, "Assuring Data Privacy in Cloud Transformations," trustcom, pp.1063-1069, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, http://origin-www.computer.org.ezproxy.shsu.edu/csdl/proceedings/trustcom/2012/4745/00/4745b063.pdf.

[2] Siani Pearson, Vasilis Tountopoulos, Daniele Catteddu, Mario Sudholt, Refik Molva, Christoph Reich, Simone Fischer-Hubner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, Ronald Leenes, Chunming Rong, Javier Lopez, "Accountability for cloud and other future Internet services," cloudcom, pp.629-632, 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, 2012, http://origin-www.computer.org.ezproxy.shsu.edu/csdl/proceedings/cloudcom/2012/4511/00/06427512.pdf.

[3] George Kousiouris, George Vafiadis, Theodora Varvarigou, "A Front-end, Hadoop-based Data Management Service for Efficient Federated Clouds," cloudcom, pp.511-516, 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 2011, http://origin-www.computer.org.ezproxy.shsu.edu/csdl/proceedings/cloudcom/2011/4622/00/4622a511.pdf.

[4] Siani Pearson, "Taking account of privacy when designing cloud computing services," icse-cloud, pp.44-52, 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009, http://origin-www.computer.org.ezproxy.shsu.edu/csdl/proceedings/icse-cloud/2009/3713/00/05071532.pdf.

[5] Masooda N. Bashir, Jay P. Kesan, Carol M Hayes, and Robert Zielinski. 2011. Privacy in the cloud: going beyond the contractarian paradigm. In *Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies* (GTIP '11). ACM, New York, NY, USA, 21-27.DOI=10.1145/2076496.2076499 http://doi.acm.org/10.1145/2076496.2076499.

[6] Yuh-Jong Hu, Win-Nan Wu, and Di-Rong Cheng. 2012. Towards law-aware semantic cloud policies with exceptions for data integration and protection. In *Proceedings of the 2nd International Conference on Web Intelligence, Mining and Semantics* (WIMS '12). ACM, New York, NY, USA, , Article 26 , 12 pages. DOI=10.1145/2254129.2254162 http://doi.acm.org/10.1145/2254129.2254162.

[7] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (CCSW '09). ACM, New York, NY, USA, 85-90. DOI=10.1145/1655008.1655020 http://doi.acm.org/10.1145/1655008.1655020.

[8] Syed Mujib Rahaman and Mohammad Farhatullah. 2012. A framework for preserving privacy in cloud computing with user service dependent identity. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (ICACCI '12). ACM, New York, NY, USA, 133-136. DOI=10.1145/2345396.2345419 http://doi.acm.org/10.1145/2345396.2345419.

[9] Electronic Privacy Information Center, "Cloud Computing", http://epic.org/privacy/cloudcomputing/.

[10] David Tancock, Siani Pearson, Andrew Charlsworth, University of Bristol, "A Privacy Impact Assessment tool for Cloud Computing", 2010, http://salsahpc.indiana.edu/CloudCom2010/slides/PDF/A%20Privacy%20Impact%20Assessment%20Tool%20For%20Cloud%20Computing.pdf.

[11] J.C. Cannon, "Review of Privacy: What Developers and IT Professionals Should Know", Addison Wesley, 2004, http://dl.acm.org.ezproxy.shsu.edu/citation.cfm?id=1071713.1071733&coll=DL&dl=ACM&CFID=326091868&CFTOKEN=96522449.

[12] Privacy Enhancing Technologies Symposium , "PETS 2013", http://petsymposium.org/2013/.

[13] Hein Timothy M Nguyen, Notre Dame Law School, 2012, "Cloud cover: Privacy protections and the stored communications Act in the age of cloud computing, http://www3.nd.edu/~ndlrev/archive_public/86ndlr5/Nguyen.pdf.

[14] Official Bill of Rights in the National Archives, "Bill of Rights", http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

[15] CGI, "Cloud Security for federal Agencies", 2012, http://www.cgi.com/files/white-papers/Cloud-Security-Federal_Agencies.pdf.

[16] Cloud Accountability Project (A4Cloud), http://www.a4cloud.eu/.

[17] C Ian Kyer, Gabriel M.A. Stern, Where in the World is My Data, "Jurisdictional issues with Cloud Computing", http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf.

[18] Lauren Gelman , The Center for Internet and Society, Ninth Circuit Court of Appeals: Stored Communications Act and Computer Fraud and Abuse Act Provide Cause of Action for Plaintiff, 2003, http://cyberlaw.stanford.edu/packets001500.shtml.

[19] From Title 18—CRIMES AND CRIMINAL PROCEDURE, 18 USC Ch. 121: STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, [Online], http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim

Mobile Biometric Security Systems for Today and Future

N. Yıldırım[1] and A.Varol[2]

[1]Fırat University, Elazig/Turkey, nilyildirim87@gmail.com
[2]Fırat University, Elazig/Turkey, varol.asaf@gmail.com

***Abstract*— Mobile devices are providing facility to human life in many areas such as online shopping, mobile banking and online messaging etc. therefore it has become an essential part of daily life. This scenario has directed people and institutions to seek more new ways regarding the security of mobile because all of the major transactions get done on mobile devices. Passwords (one-time passwords, complex character passwords, etc.) and login screen drawings of devices cannot ensure the safety of mobile devices, their applications and users therefore the hacking is becoming common. Biometric identification which is specific and distinguishing feature it is considered more secure than passwords because it is difficult to copy and alter. Biometric security systems are new as application for mobile systems and they need advancement and development in hardware and application fields. In this paper, we will discuss existing biometric systems for mobile device, operating systems and applications developed for biometrics security.**

***Keywords*—Mobile, Security, Biometric Systems, Mobile Biometric Security. HCI**

I. Introduction

Mobile devices have become a part of human life with the privilege of portability and the daily life is not complete without these devices. Hardware manufacturers, operating system and application developers take a variety of security measures due to personal, private and sensitive information in mobile devices. To ensure the security passwords, PINs or patterns are used to unlock the screen. Processing with password, unlocking mobile phone screens with PIN or pattern drawing, entering the card information for payment every time it is both time-consuming and challenging for users. However, the distinguishing human biometric features can be used as distinctive instead of all these passwords. This can offer a more secure and practical solution for the user. It is under consideration nowadays to use biometric as solution for security protection of mobile devices.

Face, fingerprint, palm, vein, voice and signature recognition features are often used as biometric identification. New generation smart phones and mobile operating systems allows developers to create biometric recognition and security applications using the camera, sound and touching features. Recently, mobile devices with biometric fingerprint sensor have given a different dimension to biometric identifications. In this paper, biometric security, the importance of biometric security for mobile devices, developed biometric applications for mobile, future of biometrics in mobile and applications in terms of human-computer interaction (HCI) are discussed.

II. Biometric Security Systems

Biometric technologies are described as automated authentication and verifying the identity of a living person based on the physiological and behavioral characteristic [1]. In all of biometric systems, the samples (fingerprint, voice, retina, etc.) taken from people are stored in a storage device after translated into a numerical expression and encryption, afterwards, when users want to log in to the system again, compatibility of records is checked via matching previously existing reference points with the stored reference point [2].

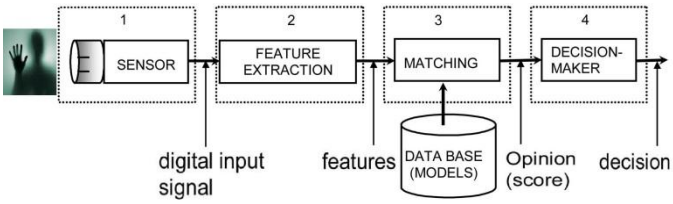


Figure 1: Operating mode of biometric security systems [3].

Biometric recognition systems can be listed as iris, retina, face, fingerprint, vein, palm for physiological biometrics and voice, signature, keystroke for behavioral biometrics. Physiological biometrics is based on the measurements of a part of the living human body and behavioural biometrics means measurements that are provided from an action implemented by the user [3].

In a survey of 188 people about the use of biometrics, it is measured that 71.8 percent of users use fingerprint recognition it is a big majority and 6 percent of users use hand geometry and signature recognition while face recognition is measured as only 1 percent [4]. So it is clear that the most applied biometric method is fingerprint. A fingerprint consists of the ridges on a person's finger and a fingerprint distinguishes from others by the unique pattern of those ridges [5]. Face recognition is the simplest and natural way to identify biometric authentication of living human and also face recognition has three types; single image, multiple image and frame by frame video [3]. According to Javelin Strategy & Research [6], 35 percent of consumers use fingerprint matching method as biometric as seen in Figure 2.

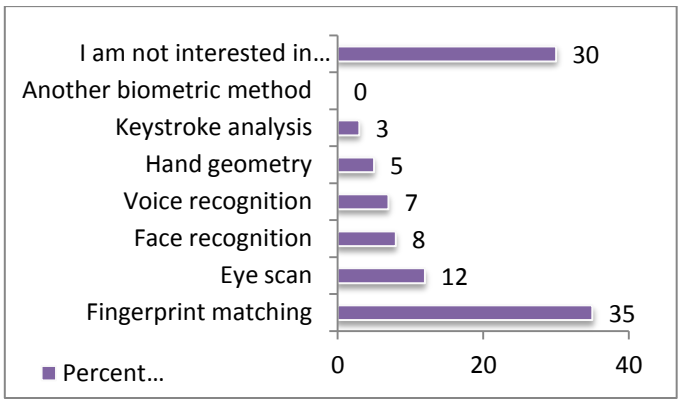


Figure 2: Biometric usage by consumers [6].

While collecting data with biometric devices, data accuracy, and detecting that the data which is gathered from living user are important [7]. Liveness detection is important for biometric systems because spoof biometric data can be gathered from a living user and can be used in illegal operations [7]. Nowadays, motion pictures, determination of a person's vein structure and use with fingerprint or palm recognition (with infrared rays), heartbeat and telling desired sentence with person's own voice are used for liveness detection due to biometric identification copying such as fingerprint, face is also possible. Two methods are applied together is defined as bi-modal authentication as described. Bi-modal authentication is important to identify the real person. Using only one way authentication is less secure than bi-modal authentication due to the risk of copying and capturing biometric information.

III. Mobile Biometric Security systems

Considering the security measures on mobile devices, followed security measures emerge;

- SIM card security with the PIN code
- Drawing shapes on the screen or pin number input for security of access to smart mobile phones.
- E - mail and password authentication for accessing some applications.
- Various applications for ensuring the safety and validity of mobile phones.

All of these security measures are not sufficient for the case of stolen or illegally access. It is likely to be stolen PIN number of mobile SIM card and screen pattern password or screen PIN number by shoulder surfers or to be seized e-mails and passwords by malicious people. When the credit card is saved to Google Play Store or Apple App Store, a person who knows the phone password can shop from markets. Considering all this negativity, biometric features of user have been starting to use to protect the mobile device and therefore user.

In Karnan and Krishnaraj's study [1], durations, times, typing errors and force of keystrokes have been used as behavioral biometric characteristic for accessing to mobile devices. But it is understood that to evaluate the keystrokes as biometric characteristic and compare results too hard.

In Tsai et al.'s study [8], they have proposed the use of biometric identification with one-time password (OTP) for mobile banking transactions. With the increase of the techniques for seizing one-time passwords, this has been a threat to mobile users. In the proposed system, it is recommended for banks to store the user's fingerprint, iris and face captured records to avoid this situation and to improve the security of mobile banking. When the user enters the correct OTP, biometric verification is required via real-time biometric capture from user. Thus the user will be able to enter the mobile banking system [8].

In the study [9] about mobile payment system via fingerprint, at first, user enters credit card and fingerprint templates and templates are saved. After obtaining a public key with an SSL connection, hash template of the fingerprint are created. The verification process is done after fingerprint hash and credit card information are sent to the server by public key.

In Omri et al.'s paper [10] , a handwriting authentication system has been proposed and covered. User's handwriting templates are saved to the database. The biometric recognition system runs on a server which is on the cloud virtual machine. The password that is entered by handwriting to mobile device with touch screen is compared with the password which is in the database and provided to enter to system.

A. Biometric Security Applications for Smart Mobile Devices

Mobile Smart Phones enable the user to develop applications by using some telephone features as camera, microphone, and stylus (in some smart mobile devices like iPad and Galaxy Note). By the advantages of these features, users develop applications about biometric security systems for mobile devices. Face, fingerprint and iris recognition applications being developed using the camera of mobile device also the applications have been developed for voice recognition using a microphone and signature recognition using a stylus. In addition to all of these hardware features, Google has developed "face unlocks" for Android 4.0 (Ice Cream Sandwich) [11]. *Camera.Face* class on Android helps developer to identify a face. When face detection is used with a camera, the *Camera.FaceDetectionListener* lists the face objects (left eye, right eye, mouth, and cheekbone) to use in focusing and measurement [12].

As well as Android, iOS has brought *AVCaptureStillImageOutput* class with *SquareCam* [13] for camera settings and has created *CIFaceFeature* class for face recognition. The following features are defined by the facial recognition objects of iOS; left eye, right eye, mouth, smiling, left and right eye closed positions [14]. Android and iOS systems also include speech recognizer classes as well as face recognition classes.

Some of known Android applications about biometric recognition and biometric security systems and its area of use have been described in Table 1.

Table 1. Biometric applications and their functions.

Application Name and Platform	Biometrics	How it works
FastAccess [15] Android	Face Recognition	It is used for accessing Android devices, applications, GooglePlay etc. by facial recognition.
Visidon AppLock [16] Android	Face Recognition	It protects any application (i.e. SMS, Gallery, E-Mail, Facebook, etc.) on the user's phone using face recognition
Mobbeel [17] Android and iOS	Face,Iris, Voice, Signature Recognition	This API uses these biometric for recognitions. Signature recognition needs iPads and it comes with digital certificate. User can use multi biometrics for security.
RecognizeMe [18] iOS	Facial Detection	It locks iPhone using face detection with front camera
FaceLock [18] iOS	Facial Detection	It scans user's face and user accesses the iPhone and it only detects the real user's face.
FaceVault [18] iOS	Facial Detection	It uses facial Recognition and if it fails, it passes to pattern-based unlocking. It detects user's face even if wearing glasses or make up.
Signedoc [19] Android and iOS	Signature Recognition	With this API user signs documents with legal validity on mobile or tablet. It recognizes user's signature
XyzmoSIGNificant [20] Android and iOS	Signature Recognition	This app processes signing documents, mailing of paper originals, and long-term storage of documents. User can sign documents electronically with a tablet or smartphone.
Start Voice Recognition [21] Android	Voice Recognition	This application uses voice recognition system on Android and is used for to lock the screen of user's phone. It is only used on devices which support the Quick Start.
BioLock v1.0 [22] Android	Face and Iris and PIN Combined Recognition	It uses two forms of biometrics (face or iris) with a PIN and creates a encrypted key and it is used to lock or open the phone or user data.
SESTEK Voice Signature (Vocal passphrase) [23]	Voice Recognition	It is a biometric voice recognition application which verifies the identity of the person who calls.
HoyosID [24] Android and iOS	Face Recognition	This application performs face recognition with the front camera of the mobile device and all accounts, user names and passwords are required to save in this application. When the application recognizes the face, it enters the passwords instead of the user. In addition, the passwords are stored in telephone, not on the internet.

Besides these applications, mobile smart phone manufacturers create face recognition applications for user to open unlocked phone screen as well as Samsung Galaxy Nexus *[25]*.

B. Biometric Security Solutions as Hardware for Smart Mobile Devices in Today

The use of biometric recognition on mobile devices has started with cameras and microphones as hardware features and the operating systems which allow using them with programming. According to Gartner's report, 30 percent of organizations will use biometric authentication on mobile devices by 2016 and this usage may be facial, voice, iris recognition and user password [26]. Goode Intelligence predicts that 3.4 billion users will use biometric systems on their mobile devices by 2018 and mobile device producers will earn 8.3 billion dollars [27].

Mobile device manufacturers have started to carry different biometric sensors on mobile devices due to practical and safer methods of biometric authentication for users. Now fingerprint sensors are able on the latest smart mobile devices. Apple's Touch ID creates a strong biometric platform on consumer mobile devices by 2018 and fingerprint sensors will be standard on mobile devices until 2015 [27].

In Goode's mobile biometric market report 2013-2018, the factors in realization of mobile biometric market growth are discussed in the following [27]:

- Biometrics is presented to end-users and consumers like Apple iPhone 5s and Touch ID technology.
- Biometrics that can be used easily brings practical mobile device protection due to mobile device authentication methods (PIN or password) are cumbersome and unpractical.
- The use of biometric authentication system for mobile commerce is a convenient and safe way for payment methods.
- Many authentication companies as FIDO Alliance are making plans to support biometrics and this support will also be provided on mobile devices.
- Fingerprint templates are kept in a secure area called "secure vault" by Apple's Touch ID fingerprint solution and all the security measures makes mobile devices safer for biometrics. .

a. iPhone 5s as iOS Device and Touch ID

Touch ID for iPhone was developed as a fingerprint identification technology. Fingerprint sensor is located under the main screen button as seen in Figure 3.

Figure 3: iPhone fingerprint sensor [28].

When touching (without pressing) the home button of iPhone 5s, Touch ID sensor reads fingerprints and unlocks the phone's lock automatically [28]. One of the features in this system, as users use fingerprint sensor, the system learns the types of the fingerprint. The system allows five fingers identification and 50,000 different fingers should be tested for random matching of fingerprints [29]. Also Touch ID has reading fingerprint in 360 degrees feature, which means the system can read fingerprints in any direction of phone. Also fingerprint data is encrypted and protected with the safe containment within the A7 chip and none of applications can access fingerprint information [29].

Touch ID is used for;

- Shopping from Tunes Store, App Store and iBooks Store,
- Unlocking iPhone.

iOS does not allow to use Touch ID features for developers in terms of security. This hampers developing applications using fingerprint sensor.

b. HTC One Max and Samsung Galaxy S5 as Android Device

HTC One Max is the first Android mobile device which includes fingerprint sensor. Fingerprint scanner is located below the camera lens at the back of the phone. The system allows identification of three fingers and fingerprint identification is used for unlocking phone (Figure 4) [30]. It also has A7 chip security as iPhone.

Figure 4: Fingerprint recognition of HTC One Max [30].

Fingerprint sensor that is integrated into Galaxy S5 home button is used for unlock device and pay. Samsung Galaxy S5 differs from other fingerprint features because it allows third party application developers to create applications using fingerprint sensor API (Pass API) [31]. It is associated with PayPall and Samsung Galaxy S5 users can shop via Paypall using fingerprint biometric.

C. HCI for Biometric Systems on Smart Mobile Devices

Human Computer Interaction can be explained as interaction between users of computer and technology and computer hardware and software. Human Computer Interaction (HCI) has become more important in human lives because technology and technological devices have become a part of human life.

Blanco-Gonzalo et al. [32] have investigated the usability evaluation of biometrics in mobile devices. Handwriting signature recognition is used for usability evaluation. IPad is used as a mobile device. The effects of usability of biometric signature with different styluses were measured with different parameters. The results have been different with each stylus [32]. This illustrates the importance of mobile device usability of biometric recognition. It can be interpreted that the errors arise from usability can cause not confirmed entries in the biometric recognition process.

When biometric technologies on mobile devices are analyzed by usability branch of HCI, some points are discovered that may prevent safety and practicality for users.

- Using the rear camera for face recognition on mobile devices affect the usability. Because the user cannot take his/her picture accurately from back camera.
- When using the styluses for signature recognition, signature pairings may not be accurate [32] due to the type of styluses or touch screen. Appropriate hardware affects usability.
- The location of the fingerprint sensor on a mobile device is very important for usability. While HTC places the fingerprint sensor below the rear camera, Samsung and iPhone have positioned it under home screen button. Be present of the sensor on the display side of the mobile phone can positively affect usability. When iPhone reads fingerprint from 360 degrees by touching, Samsung and HTC needs to scroll up and down of the finger in one direction. This may not be very practical and may not be easy to find the correct position of the finger for the user.
- Biometric identification applications should not exhibit an inverse approach to the user's habits. Speed and simplicity of applications affect the usability.

IV. CONCLUSION

Today with technology advent, information security has become more important. It is seen that passwords or PINs are insufficient for ensuring and protecting the security of information. The importance of mobile device technologies in human life and all kinds of personal information carried on these devices was also necessary to take different security measures. Unique biometric features of human are used as the password with existing technology. Image, voice and signature of the person have been used as biometrics with the help of camera, microphone and touchscreen features of the mobile device. Phone protection, application access, e-signature transactions are provided via these characteristics.

Mobile device manufacturers install the fingerprint sensor in the devices for identification of fingerprint which is frequently used biometrics. In this way user security is protected and operations which require password can be performed only by one touch. In addition, usability of biometric recognition systems for HCl will increase use of mobile biometric systems by everyday users.

It is concluded that with the popularization of mobile devices which include fingerprint sensor, mobile biometric recognition will be used in the following ways:

- Biometric recognition, especially fingerprint, for mobile payment transactions will bring mobile payments in a safer and easier position.
- Using the fingerprint as the screen lock of device will be easier and safer for users.
- Mobile banking will provide fingerprint along with one-time-password and mobile applications will be updated in this way.
- Through allowing developers of using fingerprint sensor for creating applications, different ideas will be born for mobile biometrics and a new page will be opened in mobile security.

REFERENCES

[1] M. Karnan and N. Krishnaraj, «Bio Password - Keystroke dynamic Approach to Secure Mobile Devices,» inside *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*, Coimbatore, 2010.

[2] A. Varol and B. Cebe, «Yüz Tanıma Algoritmaları,» inside *5th International Computer & Instructional Technologies Symposium (ICITS'11)*, Elazig/Turkey, 2011.

[3] M. Faundez-Zanuy, «Biometric Security Technology,» *Aerospace and Electronic Systems Magazine, IEEE* , vol 21, no. 6, pp. 15-26, 2006.

[4] L. S. Nelson, America Identified: Biometric Technology and Society, Cambridge MA: The MIT Press, November 12, 2010, p. 272.

[5] K. K. A.Ghany, H. A. Hefny, A. E. Hassanien and N. I. Ghali, «A Hybrid approach for biometric template security,» inside *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, İstanbul, 2012.

[6] T. Caldwell, «Voice and facial recognition will drive mobile finance,» *Biometric Technology Today*, vol 2012, no. 10, pp. 2-3, 2012.

[7] P. Matthew, «Autonomous synergy with biometric security and liveness detection,» inside *Science and Information Conference (SAI), 2013*, London, 2013.

[8] C.-L. Tsai, C.-J. Chen and D.-J. Zhuang, «Secure OTP and Biometric Verification Scheme for Mobile Banking,» inside *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, Vancouver, BC, 2012.

[9] M. Gordon and S. Sankaranarayanan, «Biometric Security Mechanism In Mobile Payments,» inside *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On*, Colombo, 2010.

[10] F. Omri, S. Foufou, R. Hamila and M. Jarraya, «Cloud-based mobile system for biometrics authentication,» inside *ITS Telecommunications (ITST), 2013 13th International Conference on*, Tampere, 2013.

[11] T. Caldwell, «Goode Intelligence predicts £130m growth in mobile phone biometrics,» *Biometric Technology Today*, vol 2012, no. 3, p. 2, 2012.

[12] Android Inc., «Camera.Face,» Android Inc., 10 March 2014. [Online]. Available: http://developer.android.com/reference/android/hardware/Camera.Face.html. [have accessed 12 March 2014].

[13] Apple Inc., «SquareCam,» Apple Inc., 4 April 2013. [Online]. Available: https://developer.apple.com/library/ios/samplecode/SquareCam/Introduction/Intro.html. [have accessed 5 March 2014].

[14] A. Inc., «CIFaceFeature Class Reference,» Apple Inc., 18 September 2013. [Online]. Available: https://developer.apple.com/library/mac/documentation/CoreImage/Reference/CIFaceFeature/Reference/Reference.html. [have accessed 5 March 2014].

[15] Sensible Vision, Inc, «Face Recognition-FastAccess,» Sensible Vision, Inc, 13 February 2014. [Online]. Available: https://play.google.com/store/apps/details?id=com.sensiblevision.android.fassoapplock&hl=tr. [have accessed 10 March 2014].

[16] Visidon, «Visidon AppLock,» Visidon, 30 October 2012. [Online]. Available: https://play.google.com/store/apps/details?id=visidon.AppLock. [have accessed 10 March 2014].

[17] Mobbeel, «MobbID , the multi biometric solutions for mobile applications,» Mobbeel.com, 2012. [Online]. Available: http://www.mobbeel.com/wp-content/uploads/downloads/2012/02/MobbID.pdf. [have accessed 8 March 2014].

[18] Techfat.com, «Top 5 Face Recognition Apps For iPhone

In 2013,» techfat.com, January 2014. [Online]. Available: http://techfat.com/2013/09/15/top-5-face-recognition-apps-iphone-2013/. [have accessed 4 March 2014].

[19] Mobbeel, «We release Signedoc and draw a tablet to celebrate it!,» Mobbeel.com, 26 February 2014. [Online]. Available: http://www.mobbeel.com/we-release-signedoc-and-draw-a-tablet-to-celebrate-it/. [have accessed 7 March 2014].

[20] Xyzmo, «Signature Capture for iPad and Android - Sign on the Dotted Screen,» Xyzmo Significant Signature Solutions, 2013. [Online]. Available: http://www.xyzmo.com/en/products/Pages/digital-signature-ipad-android.aspx. [have accessed 10 March 2014].

[21] R. Pizzoni, «Start Voice Recognition,» 26 December 2013. [Online]. Available: https://play.google.com/store/apps/details?id=it.RiccardoP.VoiceSearchStart. [have accessed 10 March 2014].

[22] L. Zipson, «Biometric access to mobiles in pipeline,» *Biometric Technology Today,* vol 2010, no. 8, p. 2, 2010.

[23] SESTEK, «Sesli İmza,» sestek.com, 2012. [Online]. Available: http://www.sestek.com/tr/sesli-imza. [have accessed 10 March 2014].

[24] HoyosLabs, «HoyosID™ How it Works,» HoyosLabs, 2014. [Online]. Available: http://www.hoyoslabs.com/innovation. [have accessed 13 March 2014].

[25] J. Cipriani, «How to use face unlock on the Galaxy Nexus,» cnet.com, 6 January 2012. [Online]. Available: http://howto.cnet.com/8301-11310_39-57353793-285/how-to-use-face-unlock-on-the-galaxy-nexus/. [have accessed 11 March 2014].

[26] C. Stamford, «Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016,» Gartner.com, 4 February 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2661115. [have accessed 18 March 2014].

[27] Goodeintelligence.com, «Goode Intelligence forecasts that the market for mobile biometric security products and services is set to grow and will generate over $8.3 billion revenue by 2018,» Goodeintelligence.com, 28 September 2013. [Online]. Available: http://www.goodeintelligence.com/media-centre/view/goode-intelligence-forecasts-that-the-market-for-mobile-biometric-security-products-and-services-is-set-to-grow-and-will-generate-over-83-billion-revenue-by-2018. [have accessed 18 March 2014].

[28] Apple Inc., «iPhone 5s: Touch ID'yi kullanma,» Apple Inc., 31 January 2014. [Online]. Available: http://support.apple.com/kb/HT5883?viewlocale=tr_TR&locale=tr_TR. [have accessed 8 March 2014].

[29] Apple Inc., «iPhone 5s: Touch ID güvenliği hakkında,» Apple Inc., 06 November 2013. [Online]. Available: http://support.apple.com/kb/HT5949?viewlocale=tr_TR. [have accessed 10 March 2014].

[30] HTC Corporation, «About Fingrprint Scanner,» HTC Corporation, 2014. [Online]. Available: http://www.htc.com/tr/support/htc-one-max/howto/434515.html. [have accessed 13 March 2014].

[31] Chip.com.tr, «Galaxy S5, iPhone'a "hodri meydan" dedi!,» Chip.com.tr, 1 March 2014. [Online]. Available: http://www.chip.com.tr/haber/galaxy-s5-iphone-a-hodri-meydan-dedi_45711.html. [have accessed 13 March 2014].

[32] R. Blanco-Gonzalo, L. Diaz-Fernande, O. Miguel-Hurtado and R. Sanchez-Reillo, «Usability Evaluation of Biometrics in Mobile Environments,» inside *Human System Interaction (HSI), 2013 The 6th International Conference on*, Sopot, 2013.

New Method for Automatic Fingerprint Recognition System: Entropy and Energy – Adaptive Network Based Fuzzy Inference System (EEANFIS)

A. Varol and E. Avci

Firat University Department of Software Engineering, 23119, Elazig, TURKEY

***Abstract* - Today, in the light of innovations in the field of biometrics, biometric images and the processing of biomedical images have gained importance. With the development of technology, the high rate of failure due to old techniques, such as the location of automatic fingerprint recognition methods have been overcome. The margin of error in fingerprint identification work carried out in order to minimize the number of automatic fingerprint identification operations can be found in the literature. In this study, a method is developed for automatic fingerprint recognition based Entropy-Energy and Adaptive Network Based Fuzzy Inference System (EEANFIS). For this purpose, first a fingerprint image database was developed. In preprocessing phase, the center-edge changing method was obtained using the method of variation in distance vector images. On the feature extraction and classification phases, the pre-processing steps for each of the images obtained from the energy, norm entropy, the logarithmic energy entropy and threshold entropy values were calculated for feature vector. Thus, a feature vector is obtained to which classification stage ANFIS classifier inputs are given. Finally, the ANFIS classifier in the testing phase of the correct classification performance is provided, and the success rate is calculated to be an average of 85.71 %. This EEANFIS method correct recognition performance was compared with the Artificial Neural Network (ANN) classifier correct recognition performance by using same feature vector and ANN classifier correct recognition performance was obtained as 85.06%.**

***Keyword*: Automatic people recognition system; automatic fingerprint recognition system; fingerprint images; adaptive network based fuzzy inference system classifier; center-edge changing method.**

I. INTRODUCTION

Fingerprint indexing and the manual approach have used in today's research to improve the efficiency of manual fingerprint identification, although the clever methods are used to match a growing demand. Manual fingerprint indexing has a very asymmetric distribution which has led to divisions. It can read many more than one finger for a few species, which does not contribute to the effectiveness of the research. The fingerprinting procedure has taken too much time and processes of the phases have had very slow [1–4].

These works have resulted in the development of automated fingerprint identification systems in the past few decades. Law enforcement agencies led the development of fingerprint identification systems. Recently, however, many illegal practices have increased identity fraud, and therefore the use of biometric technology to identify individuals is needed [2–7].

Biometric identification of the people can be fixed by using different biometric features such as physical (fingerprints, face, retina, iris) and behavioral (signature) biometrics. For example, fingerprints are physical in nature, but depends on the behavior of individuals. Therefore, some biometric features are tools, which identify the physical and behavioral characteristics [6–8].

Similarly, speech is also partly determined by biological structure. These individual biological structures together with the person's speaking style generate speech. Often similarities are noted between parents, children and siblings in their sound, shape and even the signature. The same argument can also be applied to the face. Faces may be very similar for twins at birth, but during their development the faces will change, depending on the person's behavior [10–13].

Are individuals requiring privileged access to particular information at this location authorized? Is the service only available for registered users? Answers to these questions are important to businesses and government agencies. Because biometric identifiers are easily misused for fraud, sharing will not be allowed. Parties in identifying the type of chips used in traditional tools and the knowledge-based methods are considered more reliable. Biometric identification is useful for the target user (to withdraw money without a pin number), improved safety (difficulty of access to pirates), or for enhanced activity as may be specified. In law enforcement applications, fingerprint-based identification has achieved tremendous success. The fingerprint detection tools are decreasing costs, offer inexpensive programming power and presence of increasing fraud / theft activities, commercial, civil and financial areas [10–13].

Fingerprint identification was necessary due to the increasing number of commercial systems based on appropriate assessment protocols. The first fingerprint verification competition was a good start in terms of the establishment of protocols. Fingerprints (biometrics) rapidly joined various sites (e.g. mobile phones), the biometric system's overall accuracy of impact as well as security and

privacy issues have social acceptance, and its analysis is also essential [1–15].

In this study, a method is developed for automatic fingerprint recognition based Energy - Entropy and Adaptive Network Based Fuzzy Inference System (EEANFIS) for this purpose, first a fingerprint image database was developed. In preprocessing phase, the center – edge changing method were obtained using variation in distance vector images. On the feature extraction and classification phases, energy, norm entropy, logarithmic energy entropy and threshold entropy values were calculated for each of the images obtained from the pre-processing step. A feature vector is thus obtained and it is given to ANFIS classifier inputs in classification stage. Finally, in the testing phase of the correct classification performance of the ANFIS classifier, the success rate is provided about average of 85.71%.

II. BIOMETRIC SYSTEMS

In biometric systems, the person in question has no specific physical or behavioral characteristics to decide which reality is the pattern identification system. Construction of a biometric system usable at the point of how important an issue is defined by the individual to decide. Depending on the application state, biometric authentication system is called authentication [1–5].

In verification systems, the biometric characteristics obtained and previously stored in the system. They are compared with data stored in patterns to determine the individual's true identity. Whether the person is alleged to have decided it does not make one to one comparison. Verification system is not whether you accept or reject people [2–8].

To establish the identity of individuals from among multiple options a comparison is made individual by individual. The application of these terms is often used in the biometric field, sometimes with the same meaning as that used in verification.

III. ADAPTIVE NETWORK BASED FUZZY INFERENCE SYSTEMS CLASSIFIER

In Adaptive Network Based Fuzzy Inference System (ANFIS), both artificial neural network and fuzzy logic are used. ANFIS is consisted of if-then rules and couples of input-output, for ANFIS training is used learning algorithms of neural network [16-18]. The structure of ANFIS used for texture image classification in this study is given in Figure 1.

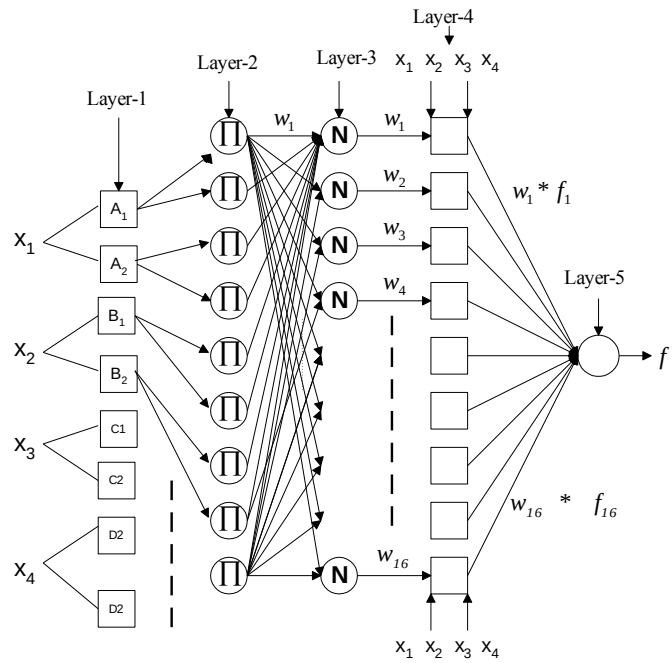


Figure 1. The structure of ANFIS used for texture image classification in this study.

In this study, it is assumed the fuzzy inference system under consideration has 4 inputs (x1, x2, x3, x4) that are wavelet energies of sub-images, which are A, H, D, and V. A typical rule set with base fuzzy if-then rules can be expressed as

If x1 A1 x2 B1 x3 C1 x4 D1 then

$$f_1 = px_1 + rx_2 + qx_3 + sx_4 + u \tag{1}$$

Where, p, r, q, s, u are linear output parameters. This ANFIS is structured by using 5 layers, which are composing the input memberships, calculating the firing strength of rules, normalization, set the consequent parameters and calculating the overall output of ANFIS. In addition to this ANFIS has 16 (24) if-then rules.

IV. ARTIFICIAL NEURAL NETWORKS CLASSIFIER

Artificial Neural Networks (ANNs) have been used to model the human vision system [12], [19]. They are biologically inspired and contain a large number of simple processing elements that operate in a manner analogous to the most elementary functions of neurons. NNs learn by experience, generalize from previous experiences to form new ones, and can make decisions. Neural elements of a human brain have a computing speed of a few milliseconds, whereas the computing speed of electronic circuits is of the order of microseconds. The ANNs are parallel process elements which have the following characteristics [19–23]:

- ANN is a mathematical model of a biological neuron.
- ANN has process elements which are related to one another.

- ANN keeps knowledge with connection weights.

Neural network models provide an alternative approach to implementing enhanced techniques. A simple process element of ANNs is given in Figure 2(a). A three-layer ANN structure is given in Figure 2(b). Here, symbols "ψ" and " / " represent Log-sigmoid and linear activation functions respectively.

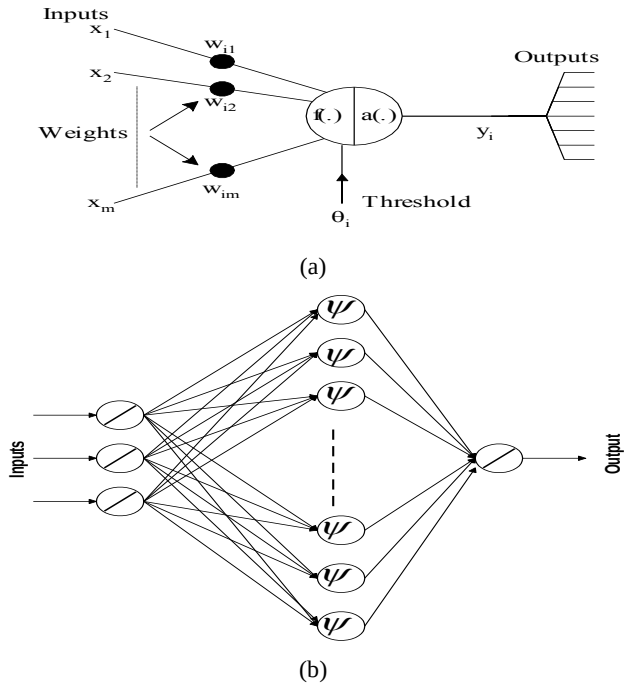


Figure 2(a). A simple process element of ANNs, **(b)** A three-layer ANN structure.

Output of ith process element in this simple model is given Equation 2:

$$y(t+1) = a\left(\sum_{j=1}^{m} w_{ij}\, x_j(t) - \theta_i\right) \tag{2}$$

Where, a(.) is an activation function, and θi is the threshold value of ith process element. The knowledge processes of the process element are formed from two parts: input and output. The output of the ith process element is calculated with Equation 3 [19].

$$f_i \triangleq net_i = \sum_{j=1}^{m} w_{ij}\, x_j - \theta_i \tag{3}$$

V. DIGITAL IMAGE PROCESSING STAGES

In the literature, there is information on a large amount of digital image processing hardware and software. In Figure 3, the basic steps for image processing are given [8–13].

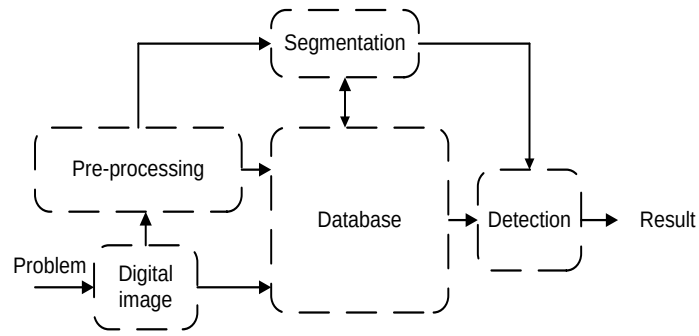


Figure 3. Basic steps for image processing.

The first step is to obtain the digital image for image processing. To do this, a sensor input and output must be digitized in the mark. The image sensor can be determined according to the application. In next step, the digital image obtained after the pre-stage process is the next step. The pre-production stage of the process follows in order to obtain better results from the image. This pre-production stage contains the contrast, expansion and noise elimination processes. A partitioning operation is performed in the third stage. Segmentation is used to dissect an image within its structure. Autonomous segmentation of digital image processing is one of the most difficult processes. After segmentation, the output is the raw data. The computer must be able to process this data. At this point, the decision must be made on the outer limits of the data in the image of an object with regard to whether you are within the inside of the line [12–14].

This section is also called pre-processing, and features the extraction stage. At this stage, basic morphological operations are introduced in the following order.

- Gray-Level Screening: To process the image color the images are converted to black and white images of 0 and 1s. Here, 0 and 1 represent black and white colors respectively.
- Histogram Indication: A histogram is used to show the gray-level distribution in the image.
- Image Thresholding: Thresholding is one of the most important approaches for the purposes of image segmentation [10]. In the thresholding process, the image objects within the image are separated from the background.

The distribution of gray-level (image histogram) is used for thresholding images. According to this histogram, the objects and background pixels belonging to the image can be divided into two main groups. In this case, the easiest way to distinguish the object from the background is through a histogram. The threshold value T is determined by using a histogram. A threshold value T will be used to compare the pixel values in the image. Accordingly for any (i, j), if the f (i, j) pixel value is larger than the T (i, j) pixel, this f (i, j) pixel will belong to a point object, otherwise this f (i, j) pixel belongs to the plan, which will be a point in the image.

- Canny Edge Extraction Method: Edge extraction is one of the basic issues in image processing. The edges of an image change against drops, brightness, color, texture and shows. Canny edge extraction method is a multi-step extraction technique for edges.

The main purpose of this method is to obtain a good image from the edges of unearthed objects. The canny edge extraction algorithm contains the items listed below:

Unwanted details in the structure are reduced by passing (m, n) size images f (m, n) through a Gaussian filter noise. This process is also expressed in Equation (4) below:

$$g(m,n) = G_\sigma(m,n).f(m,n) \tag{4}$$

Here, $G_\sigma = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{m^2+n^2}{2\sigma^2}\right)$ is in the form of a Gaussian filter function.

- The Center-Edge Changing Method: The center-edge changing method is one-dimensional representation of the two-dimensional border. The center-edge changing method can be defined as a drawing. The r in the function represents a shape and this shape has a center of gravity located on the border between any points representing the Euclidean distance. The calculation of the Euclidean distance is also expressed in Equation (5) below [13–17]:

$$r = \sqrt{(x - x_m)^2 + (y - y_m)^2} \tag{5}$$

Where x is the horizontal component of the border of the point, xm is the horizontal center of gravity of the point, y is the vertical component on the border of the point, and ym is the vertical center of gravity of the point. Figure 4 is at any point on the boundary. In addition to this point, the horizontal position represents the reference angle. The graphic in Figure 4 shows the sequence of the Euclidean distance, which is between center point of square and each points of edges of square [12].

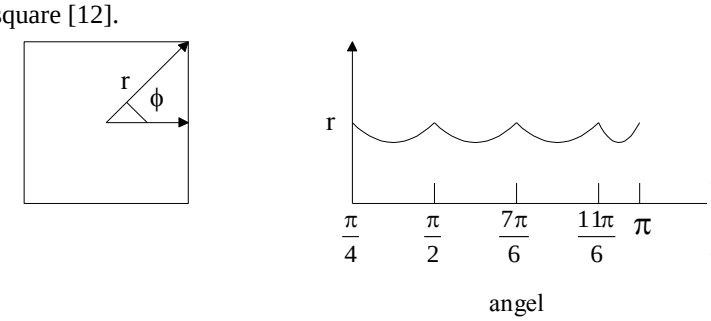


Figure 4. Application of the center-edge changing method for a square.

- Energy: The energy is the integral of powers [18]. In signal and image processing, the energy is total power of data.

$$E = \frac{1}{N}\sum_{i,j=1}^{N}(s_i)^2 \tag{6}$$

In here, E is energy. N is size.

- *Entropy:* The concept of entropy was first used in signal processing and in particular in the field of communication by Shannon [13–16]. Entropy-based features give information about signal definitions. The concept of entropy may be a system with the aim of measuring the regularity of thermodynamics. It is a well-known concept in physics. The entropy measurement method measures the degree of the disorder of any sign [14].

In recent years, entropy has been widely used in the field of signal processing and become a concept. Equations for different types of entropy widely used in signal processing are given below [3–7]:

Norm Entropy:

$$E(s) = \sum_i |s_i|^p \quad and \quad 1 \le p < 2 \tag{7}$$

Logarithmic Energy Entropy:

$$E(s) = \sum_i \log_2(s_i^2) \quad and \quad \log(0) = 0 \tag{8}$$

Entropy Threshold:

$$E(s) = \sum_i E(s_i) \tag{9}$$

where ε is a positive threshold value

$$|s_i| > \varepsilon \Rightarrow E(s_i) = 1 \quad and \quad |s_i| \le \varepsilon \Rightarrow E(s_i) = 0$$

VI. APPLICATION OF AUTOMATIC FINGERPRINT RECOGNITION SYSTEM BASED ENERGY-ENTROPY AND ADAPTIVE NETWORK BASED FUZZY INFERENCE SYSTEM (EEANFIS)

This automatic fingerprint recognition based Entropy-Energy and Adaptive Network Based Fuzzy Inference System (EEANFIS) method is mainly composed of four stages: pre-processing, feature extraction, classification and testing. During these stages are given below with:

1. Pre-Processing Stage: In this stage, firstly a fingerprint images database was created. Then the pre-processing steps described in Chapter 4 are used. The above-mentioned fingerprint images in the first part of this stage have been translated from color to gray images. The fingerprint images are converted into gray-level images. Then, gray-level image histograms of these gray-level images are obtained. The threshold value is determined by utilizing the image histogram of each of these fingerprint images. This value is determined according to the value above the threshold value for the

pixels in the image, and for the output values in the bottom a value of 1 has been assigned a value of 0. Thus the picture is separated from the background. Once separated from the background image, we apply the Canny edge extraction algorithm, thus the edges of the objects in these images can be determined. Finally, the center-edge changing method is applied to these fingerprint images.

Morphological and Logical Operations: These are structural processes. Sometimes, an image of an object and the background it is to be distinguished from determine that the appropriate threshold values may not be sufficient. In this case, we need to carry out additional processing. The object can be separated from the background. These techniques are performed using some morphological and logical operators. The morphological and logical operators used in this study are gray-level screening, histogram indication, image thresholding, Canny edge extraction, and center-edge changing. The results of these morphological and logical operations for fingerprint images are given in Figures 5–7 respectively.

Figure 5. Some of fingerprint images used in this study.

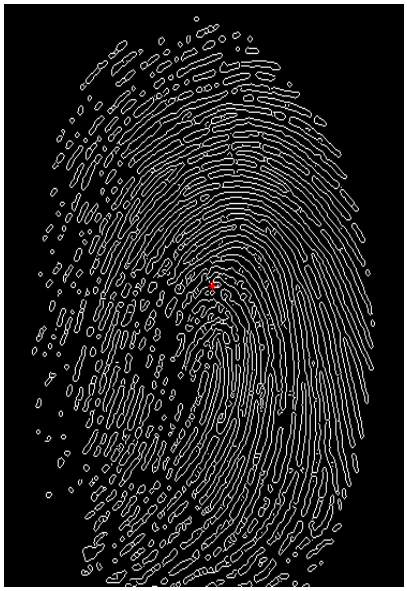


Figure 6. A fingerprint image obtained after the application of the Canny edge detection process and center-edge changing methods.

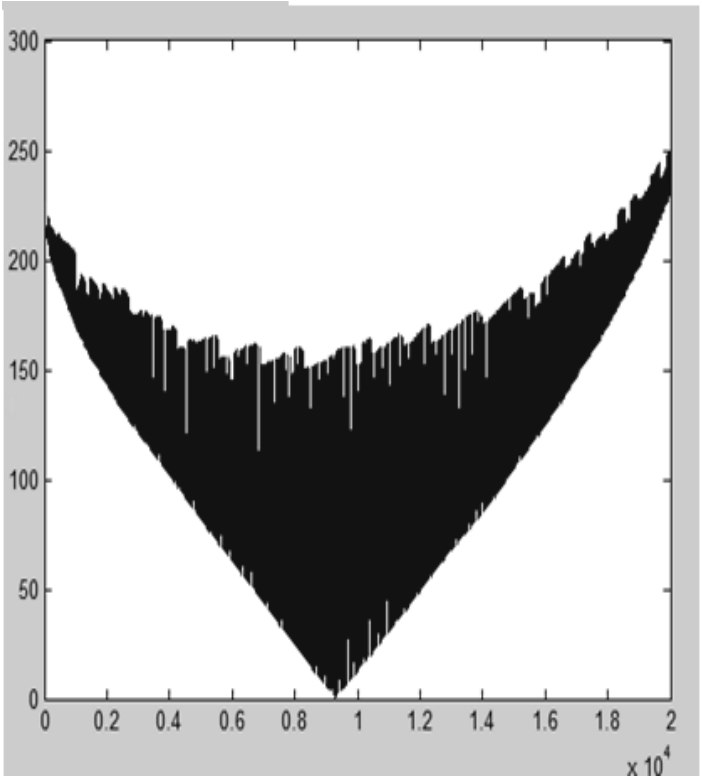


Figure 7. Fingerprint image distance vector found by applying the center-edge changing procedure.

2. Feature Extraction Stage: In this stage, the fingerprint images pre-processed in Stage 1 (Pre-Processing Stage) are used. In this feature extraction stage, energy and the three different entropy values which are the norm, logarithmic energy and entropy threshold values, are calculated for each of these 40 x 80 = 3200 fingerprint images. Thus, the size of the obtained feature vector at the end of the feature extraction stage is 3200 x 4. Half of this 3200 x 4 size feature vector is used in the classification stage. Namely, a 1600 x 4 (40 x 40 x 4) feature vector is given as input to the ANFIS classifier. The rest of this 1600 x 4 size feature vector is used in the testing stage of the correct classification performance of the EEANFIS method used in this study.

3. Classification using Adaptive Network Based Fuzzy Inference System Classifier: This stage is the classification stage. Here, half of the 3200 x 4 (40 x 80 x 4) feature vector obtained in the feature extraction stage is used for classification. This feature vector is given as input to the ANFIS classifier. The rest of this 3200 x 4 (40 x 80 x 4) feature vector obtained in the feature extraction stage is used for testing the correct recognition ratio of the EEANFIS algorithm for fingerprint images in the testing stage. The training parameters of the ANFIS classifier used in this study are given in Table 1. This EEANFIS method correct recognition performance was compared with the Artificial Neural Network (ANN) classifier correct recognition performance by using same feature vector and ANN classifier correct recognition performance was given on Table 2.

Table 1. ANFIS structure and training parameters.

The number of layers
5 (Input: 4, Rules number: 16, Output: 1)
Type of Input Membership Functions
Bell-shaped
Training parameters
inear parameters (a_i, c_i) and Least squre errors for linear parameters (p_i, q_i, r_i, s_i, u_i))
Reaching epochs number to sum-squared error
0.000001

Table 2. Multi-layer neural network structure and training parameters.

Number of layers	3
Number of Layer Neurons	Input: 3, Hidden Layer: 10, Output: 1
Initiate weights and biases	The Nguyen-Widrow method
Activation functions	Log-sigmoid
Training parameters	Back propagation
Learning rule	
Mean square error	0.00000001

From among these values, for example, the number of hidden layers, the number of cells in the hidden layers, the learning rate and the value of the activation function, can after several tries be selected to provide the best performance. The EEANFIS method is developed for automatic people recognition from their fingerprint images. The structure of this EANFIS algorithm is provided in Figure8.

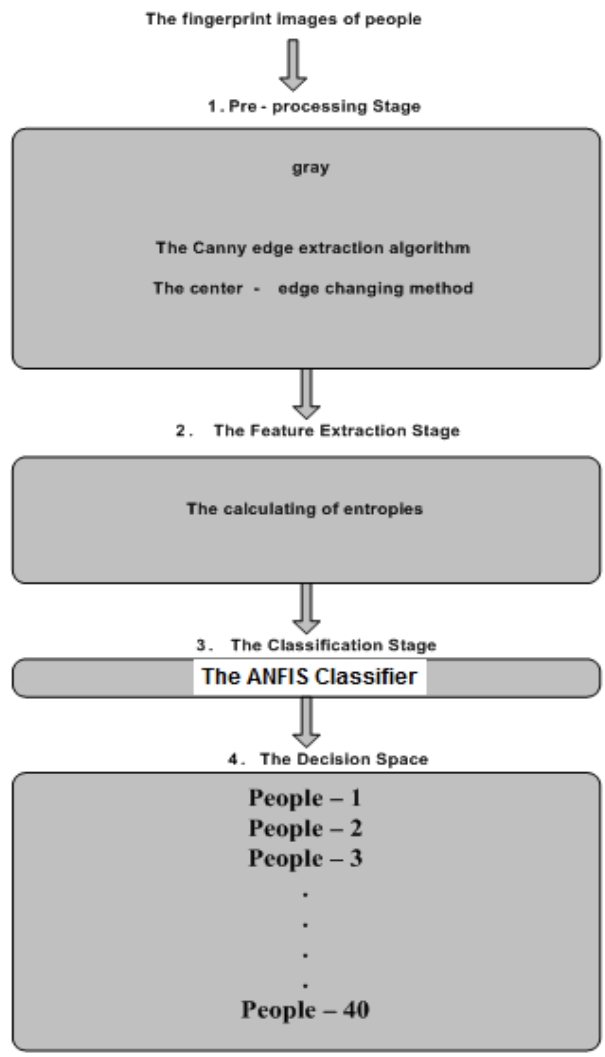


Figure 8. Structure of EEANFIS algorithm used in this study.

4. Testing Stage of Correct People Recognition Performance of EEANFIS: This is the 4th stage accomplished by using the EEANFIS algorithm to test the accuracy of the recognition results. For this purpose, the remainder of the 3200 x 4 (40 x 80 x 4) feature vector obtained in the feature extraction stage is used for testing the correct people recognition ratio of the EEANFIS algorithm for fingerprint images in the testing stage. So, a 1600 x 4 (40 x 40 x 4) feature vector is used in this stage. The detection accuracy of the proposed EEANFIS algorithm obtained is given in Table 3.

Table 3. Correct people recognition rates for the proposed EEANFIS approach.

People	**Number of the correct recognition fingerprint images**	**Number of incorrect recognition fingerprint images**	**Correct recognition rate (%)**
People-1	37	3	91.5
People-2	36	4	91
People-3	33	7	88
People-4	33	7	81.5
People-5	30	10	82
People-6	32	8	81
People-7	39	1	95.5
People-8	33	7	81.5
People-9	34	6	86
People-10	36	4	92
People-11	33	7	84.5
People-12	30	10	75
People-13	32	8	82
People-14	35	5	85.5
People-15	38	2	95
People-16	33	7	83.5
People-17	32	8	82
People-18	35	5	88.5
People-19	39	1	98.5
People-20	33	7	82.5
People-21	34	6	86
People-22	38	2	95
People-23	31	9	75.5
People-24	33	7	88
People-25	34	6	86

People-26	29	11	71.5
People-27	33	7	82.5
People-28	31	9	77.5
People-29	32	8	85
People-30	36	4	90
People-31	34	6	85
People-32	30	10	72
People-33	38	2	93
People-34	39	1	97.5
People-35	33	7	82.5
People-36	32	8	80
People-37	35	5	87.5
People-38	34	6	86
People-39	38	2	95
People-40	34	6	86
Total	**1361**	**239**	**85.18**

A demonstration of the effectiveness of the proposed invariant features of the automatic fingerprint recognition system based EEANFIS algorithm is given in Table 3. As can be seen from Table 3, the overall correct recognition rate was about 85.71%. This EEANFIS method correct recognition performance was compared with the Artificial Neural Network (ANN) classifier correct recognition performance by using same feature vector and ANN classifier correct recognition performance was obtained as 85.06 %.

As shown that these results, the correct recognition performance of this EEANFIS method is more superior to the correct recognition performance of this ANN classifier.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

In the literature there are many pattern recognition studies [19–24]. In these studies, many different feature extraction methods are used. In this study, the center-edge changing and entropy calculation methods are used for feature extraction. There are some advantages to these methods, such as invariance under rotation and scaling operations.

In this study, a method is developed for automatic fingerprint recognition based Entropy-Energy and Adaptive Network Based Fuzzy Inference System (EEANFIS) method. For this purpose, first a fingerprint image database was developed. In preprocessing phase, the center and the edges were obtained using the method of variation in distance vector images. On the feature extraction and classification phases, energy, norm entropy, the logarithmic energy entropy and threshold entropy values were calculated for each of the images obtained from the pre-processing step. A feature vector is thus obtained and it is given to ANFIS classifier inputs in classification stage. Finally, in the testing phase of the correct classification performance of the ANFIS classifier, the success rate is provided about average of 85.71 %.

The main reason for the incorrect classification of fingerprint images concerns similar shapes. A few of the fingerprint images are unreliably identified due to their similar shape. As shown in these results, the pre-processing stage is the most important part of this EEANFIS method for the correct recognition of fingerprint images.

REFERENCES

[1] Gonzalez RC and Woods RE. Digital Image Processing. New York, NY, USA: Addison-Wesley Press, 1993.

[2] Kulkarni AD. Computer Vision and Fuzzy–Neural Systems. New York, NY, USA: Prentice Hall Press, 2001.

[3] Shannon CE. A mathematical theory of communication. Bell System Technology Journal 1948; 27: 379–423.

[4] Tonga S Bezerianosa A Paula J Zhub Y and Thakora N. Nonextensive entropy measure of EEG following brain injury from cardiac arrest. Elsevier Physica A, 2002; 305: 619–628.

[5] Principe JC, Euliano NR and Lefebvre WC. Neural and adaptive systems. New York, NY, USA: John Wiley & Sons, 2000.

[6] Overwijk MHF and Reefman D. Maximum-entropy deconvolution applied to electron energy-loss spectroscopy. New York, NY, USA: Pergamon Micron, 2000.

[7] Li X. Edge directed statistical inference with applications to image processing. PhD Thesis, Princeton University, 2000. pp. 131.

[8] Forsyth DA and Ponce J. Computer Vision: A Modern Approach. New York, NY, USA: Prentice-Hall, Englewood Cliffs, NJ., 19-34, 2002.

[9] Parker J. Algorithms for Image Processing and Computer Vision. New York, NY, USA: John Wiley, 1996.

[10] Shapiro LG and Stockman G. Computer Vision. New York, NY, USA: Prentice Hall Press, Englewood Cliffs, NJ, 45-67, 2001.

[11] Shannon CE. A mathematical theory of communication. Bell System Technology Journal 1948; 27: 379-423.

[12] Principe JC Euliano NR and Lefebvre WC. Neural and Adaptive Systems. New York, NY, USA: John Wiley, 2000.

[13] Overwijk MHF and Reefman D. Maximum-entropy deconvolution applied to electron energy-loss spectroscopy. New York, NY, USA: Pergamon Micron, 2000.

[14] Coifman RR and Wickerhauser MV. Entropy-based algorithms for best basis selection. IEEE Transaction on Information Theory 1992; 38: 713–718.

[15] Diaz E. Microbial Biodegradation: Genomics and Molecular Biology. Poole, UK: Caister Academic Press. 2008.

[16] Tannock GW. Probiotics and Prebiotics: Scientific Aspects. Poole, UK: Caister Academic Press. 2005.

[17] Mengesha et al. Clostridia in anti-tumor therapy. Clostridia: Molecular Biology in the Post-genomic Era, UK: Caister Academic Press. 2009.

[18] Rong L and Li D. A web based expert system for milk cow disease diagnosis system in China, Computer and Computing Technologies in Agriculture 2008; 2: 1441–1445.

[19] Avci E. A new optimum feature extraction and classification method for speaker recognition: GWPNN. Expert Systems with Applications 2007; 32: 485–498.

[20] Avci E. An expert system based on wavelet neural network-adaptive norm entropy for scale invariant texture classification. Expert Systems with Applications 2007; 32: 919–926.

[21] Avci E. Comparison of wavelet families for texture classification by using wavelet packet entropy adaptive network based fuzzy inference system. Applied Soft Computing 2008; 8: 225–231.

[22] Avci E. An automatic system for Turkish word recognition using discrete wavelet neural network based on adaptive entropy. Arabian Journal for Science and Engineering 2007; 32: 239–249.

[23] Dogantekin E Avci E Erkus O. Automatic RNA virus classification using the Entropy-ANFIS method. Digital Signal Processing 2013; 23: 1209-1215.

Providing Patient Rights with Consent Management

E. Olca[1] and O. Can[2]

[1]Izmir University, Department of Software Engineering 35350 Uckuyular-Izmir Turkey, emreatlier@gmail.com
[2]Ege University, Department of Computer Engineering 35100 Bornova-Izmir Turkey, ozgu.can@ege.edu.tr

***Abstract*—Electronic Health Record (EHR) is a secure, confidential and point-of-care information resource for health care institutions. EHR provides obtainment to health information where ever and whenever it is needed by authorized users, and gives support to clinical workers by closing loops in communication and accessing to the correct information. However, privacy and security risks have emerged for personal health information. Thus, effective policy rules are required to ensure personal privacy and to manage access to personal health records. This paper examines base terms such as personal data, personal health information and electronic health record under security and privacy concepts, and also mentions legal definitions of these terms. In addition, this work outlines the electronic consent management model to protect personal health information by considering patients' preferences for how their medical data will be used in the future.**

***Keywords*—Consent management, privacy, health care, electronic health record.**

I. Introduction

In health care domain, patient records and treatment data are required as a significant resource for scientifical and statistical evaluations. In addition to these evaluations, this information yields patient's medical history in form of systematic documentation by recording observations and administration of drugs and therapies, and so on. The continuity of the treatment can be provided through obtaining a variety of types of notes saved over time by health care professionals. Further, in legal cases this medical information has an important role as a juristic document.

The healthcare industry is constantly evolving. This provides many advantages and a remarkable quality in patient care. As the patient records and treatment data are kept in digital environment, they can be easily accessed at any time and from anywhere. In this manner, electronic health records can be accessed by health care workers as an essential prerequisite [1] and patient data can be seen by the whole clinical team involved in health care. Eventually, more clinical workers through the electronic health care environment can obtain patient information. Although these broaden access to medical records yields convenience, it also brings personal privacy risks like using patient's medical data without her consent [2].

Thus, security preventions should be taken against threats to personal privacy and health care organizations should secure patient's sensitive data. The lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish and possible social stigma [3]. Health care employees can be given the access to patient records, but at the same time protective mechanism should be deployed to satisfy patient's privacy needs. As a consequence of increasing risks, some juristic arrangements have been performed in Constitutional of the Republic of the Turkey. In this paper, some Articles related to privacy are given from this constitution [4]. Under the title of "Privacy and Protection of Private Life", in Article 20 [4] - Privacy of Individual Life, personal data is protected with a distinct expression. In recent years, new regulations were made in this article. For example, with additional paragraphs to Article 20, "the explicit consent of the person" term was emphasized and personal data which involve medical information that can be only used with the consent of the individual.

This paper outlines the potential privacy risks in health care domain and the importance of patient's right to her privacy. The paper is organized as follows: Section 2 clarifies personal data and personal health data definitions. Electronic health records are described in Section 3. Section 4 presents security and privacy concerns of electronic health records and examines the related work. Finally, Section 5 concludes and proposes an electronic consent management to satisfy patient's privacy needs.

II. PERSONAL DATA AND PERSONAL HEALTH DATA

It is important to clarify the "personal data" and "personal health data" terms before examining electronic health records and to mention if they are protected by law. This section explains these terms respectively.

A. Personal Data

In Article 2a EU Data Protection Directive (also known as Directive 95/46/EC) [5], personal data definition is as follows: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

Personal data is an information that determines anyone individually through of itself. As this may be single information, it may also be a large number of interrelated information. For example, person's name, date of birth,

photograph, address, bank statements, credit card numbers, IP address, fingerprint, medical report and etc.

Another essential term associated with personal data is "processing of personal data". Processing personal data means performing any operation or a set of operations on personal data such as retrieval, collection, recording, storage, modification, manipulation, use, transmission, dissemination or publication, and even blocking, erasure or destruction of personal data [5].

According to Article 20 [4] in Turkish Constitutions, "*Everyone has the right to demand respect for his or her private and family life. Privacy of private or family life shall not be violated.*" In 20/3, "*Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law*". Thus, if processing of personal data is being asked, person's explicit consent or regulation based on laws is obligatory.

In Article 8 [6], the privacy of family life is mentioned as follows "*Everyone has the right to respect for his private and family life, his home and his correspondence*". Interference by a public authority with the exercise of this right can only be discussed in some cases like national security, for the protection of health or morals, public safety and so on. The terms of *private life* and *correspondence* comprise "personal data" and the right to respect for private life poses the right to respect for personal data. As a principle, this issue is untouchable and under the protection of both European Convention on Human Rights and Constitutional of the Republic of Turkey.

B. Personal Health Data

The World Medical Association [7] in Washington defined personal health information as follows: "*Personal health information is all information recorded with regard to the physical or mental health of an identifiable individual.*"

In Health Insurance Portability and Accountability Act of 1996 (HIPAA) [8], health information is mentioned as any information which is generated or obtained by a health care service, public health authority, life insurer, health care professional and is associated with physical or mental health for the entire period of life. Also, it relates to the past, present, or future payment for the provision of health care to an individual. In terms of security of health information, some HIPAA Rules are assigned. For example, the HIPAA Privacy Rule protects the privacy of individually identifiable health information. The HIPAA Security Rule enforces national standards for the security of electronic protected health information or identifiable health information in electronic form.

Personal health information refers to patient's medical conditions, medical history, interactions with the doctor, diagnosis, medicines, treatments, body specifications, laboratory tests and radiology results. Hence in worldwide standards, personal health information takes part in personal data category as "*sensitive*" and "*special quality*".

III. ELECTRONIC HEALTH RECORD

Health Care Information and Management System Society (HIMSS) defined electronic health record as [9]: "*The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.*"

This health record is longitudinal as it involves whole term of care, from birth to death. It is also patient-centered. Because one EHR relates to only one individual, not to a set of subject of care. EHR involves past and present events recorded, and also involves future instructions and prospective information. Thus, EHR is prospective. The Electronic Health Record is a secure, confidential, complete, real-time, point-of-care information resource for health care institutions. Thereof, EHR can be defined as repository of data concerning the health of a subject of care in electronic form, recorded and conveyed securely and accessible by different health and community services. The potential subjects of electronic health records (EHRs) should be aware of the existence of any system or program that accesses, collects, processes and/or transmits data about them [10].

In terms of policy ownership of an EHR, the subject of the EHR has her personal health information, not professional or institutional stakeholders. Because, a person gets health service with her individual payment or her tax. Health record is created by health care service as a result of the patient's request. As mentioned before, health information is personal data and involved by a right of protecting private life. In addition, institutional rights never go ahead of individual rights. Conversely, individuals or professionals of health organizations are responsible for protecting patients' rights.

Translating existing patients' health records to electronic health records has caused the following affirmative developments:

- Quick access to patient information in an emergency
- Better documentation and advanced audit ability
- Enhancement of patient treatment and health care
- Increasing quality and effectiveness provides an automatization of the workflow
- Better planning of health services
- Avoiding duplication of laboratory tests which results by gaining time and money
- Ease in creating legal information and documentation
- Interference that results in delays or gaps in healthcare
- Collection of data for quality management, reporting, resource management, and public health disease surveillance

Besides these advances, the following negations have arisen:

- The poverty in patient privacy
- Economic, moral and social damages of people
- Trading over the collected patient data
- Unintended usage of the collected patient data
- Unfair distinctions on patients' medical history

EHR ensures that clinical workers can access timely to the complete information and gains money for the patient, for the health care institutional and even for the country. The USA could potentially save $81 Billion annually by getting into a universal Electronic Health Record (EHR) system [3].

IV. Electronic health record as a Security concern

In addition to the advances in electronic health records, the negativity has an inevitable importance. EHR increases efficiency of health care, but also introduces new critical risks such as the ones that are mentioned above. These risks have rigidly importance and constitute the electronic version of assault, battery and voyeurism. Because, the manipulation of an EHR without an appropriate right or permission may be linked to non-consensual interference with the body of the subject of the EHR [10]. For example in the USA, 75% of patients worry about health websites that share information without their permission [11]. Unfortunately patients believe that medical data disclosures are the second highest reported privacy breach [12].

On the other hand, patients do not know their legal rights over their medical data or how to manage these rights. A recent survey in England [13], about 28–35% of patients don't care about their privacy and they are indifferent to their health information such as age, gender, diagnosis, reason for treatment, medical history used by professionals for other purpose or unintended usage. Only about 5–21% of patients, however, expected to be asked for consent to get and manipulate their health information by their health professionals or general practitioner. And only about 10% of the patients expected to be asked for consent to scientifical and statistical works for a wide variety of purposes such as providing better information to future patients and research articles on diseases and treatments.

There are some other overarching conclusions on patients' thoughts [14]. Firstly, patients strongly believe that their health context should be shared only with health care workers. Secondly, patients provide a general consent for the need of information sharing to health care professional but in some cases expressly preclude the disclosure of information such as a sexually transmitted disease (STD) condition. Thirdly, patients deny all access to her health information to third parties and family members, except for circumstances that agree to share information among physicians. Lastly, patients reject the notion of releasing information to be used in present and future circumstances such as treatments like drug rehabilitation, STD and psychiatric treatment.

Information security research has an increasing impact within the information systems. While much is known about growing stream of research in information security, very little work has existed to study information security risks in the health care domain.

To handle various information risks, privacy and security form paramount part of any electronic environment for EHR [15] and researches have been achieved to ensure privacy and security and to manage data access control. Algorithms and frameworks have been developed. Role-based information access, contextual access control, attributable roles and permissions can be given as examples to recent researches. This progress is being made in some various fronts such as the use of autonomous agents, authorization policy framework for peer-to-peer distributed healthcare systems, encrypted bar code frameworks for electronic transfer of prescription, electronic consent models that allow patients to give or withhold consent to clinicians who wish to access their medical record [3]. An e-consent model is a crucial security and privacy mechanism to protect EHRs and to increase patients' awareness on their legal rights over their medical data.

Besides security and privacy, the electronic healthcare system must be connected to the rules in legal ground. For example, The American Recovery and Reinvestment Act of 2009 (ARRA) signed into law by President Barack Obama on February 17, 2009 clearly calls for the accelerated creation and exchange of electronic health records (EHRs) for all Americans [16]. Also, for increasing risks in medical health records, some standards or regulations have been proposed at both the state and the federal level in the USA such as Health Insurance Portability and Accountability Act (HIPAA) [3] and IMIA Code of Ethics for Health Information Professionals (HIPs) [17].

V. E-CONSENT MANAGEMENT

The term of consent is defined as restricting the disclosure of sensitive information according to the wishes of the patient. Electronic consent systems allow the subject of electronic health record to permit or deny the disclosure of the medical information to particular people [15].

Subject of electronic health records should be able to give or withhold consent to those who wish to access their electronic health information for the purpose of using, transmitting, manipulating and so on [2]. Patients' health information is critical information in order to improve quality of healthcare. But, disclosure of health information causes privacy violations. For example, institutions such as HIPAA [8] allow healthcare organizations to disclosure personal health information to researchers only if they have obtained consent from subjects of electronic health record [3].

Consent management is a process that enables consumers to constitute privacy preferences and/or policies to those who shall have access to their electronic personal health information, for what purpose and under what circumstances [18].

Besides of patients' explicit consent, they may grant someone to give or withhold consent on the basis of a

contractual relationship or on the basis of a relationship. Whether individual consent or patient' s duly empowered representatives, still, in each instance the principle of privacy of personal information entails that any such access must always be on the basis of informed consent [10].

On the other hand, it was reported [19] that the complexity of consent and privacy protection works are time-consuming and cost-amplifying progresses. To be more practicable to accomplish electronic consent mechanism, simplifying the language of privacy and consent forms to facilitate comprehension by patients is recommended [3].

VI. Conclusion

This paper outlines personal data, personal health data, electronic health records and consent management. In order to understand EHR and the security of EHR, personal data and personal health data should be examined. Also, legal aspects of these terms should be realized. Although EHR improves the effectiveness of information exchange, coordination, and communication between different health and community institutions, it also raises the critical issue of patient privacy. E-consent deals with patients' privacy concerns. Patients must be able to give or withhold consent to health care professionals who want to access their medical records. Patients, who are the subjects of EHRs, should have the right to inform their consent over their personal and medical data; herewith, the health care services and professionals have to ensure that this right is satisfied and medical information will not be misused[10]. However, there exist different consent behaviors and their expectation varies with the needs of health care domain and patient's preference. Electronic consent is not a one-size-fits-all system. When choosing consent model, patient trust and anticipations, legal requirements, complexity of implementations and time and cost should be considered attentively [20]. Subjects of EHR have different choices for the electronic access of health information. Thus, it is important to define patient's consent policy. Most consent models develop a mechanism for capturing specific inclusion and exclusion criteria that defines patient's preferences [2]. It is also critical that the healthcare institutions focus time, money and energy into defining and implementing electronic consent model. Balancing between protecting patients' rights to privacy and civil liberties while ensuring that health care providers have access to confidential patient health information as well as they need is actually a very delicate process. Thus, future research is needed to examine distinct frameworks and/or algorithms for capturing patient's consent and to implement patient's consent to e-health system. While developing new algorithms, the complexity of clinical work and patient's needs should be studied deeply. Probably there will no obvious design mechanism but anyhow, it is important to develop e-consent model which can be applicable to the different health domains with considering patient's privacy policies and care organization's requirements.

References

[1] R.S. Dick, E.B. Steen, and D.E. Detmer, "The Computer-Based Patient Record—An Essential Technology for Health Care," *in National Academy Press*, Washington DC, 1997.

[2] E. Coiera, R. Clarke, "e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment," *J Am Med Inform Assoc*., vol. 11, pp.129–140, 2004.

[3] A. Appari, M.E. Johnson, "Information security and privacy in healthcare: current state of research," *Int. J. Internet and Enterprise Management*, vol. 6, no. 4, pp.279–314, 2010.

[4] Constitution of the Republic of Turkey [Online]. pp. 25-26. Available: http://global.tbmm.gov.tr/docs/constitution_en.pdf

[5] D. Elgesem, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data," *Ethics and Information Technology*, vol. 1, no. 4, pp. 283-293, 1999.

[6] U. Kilkelly, "A guide to the implementation of Article 8 of the European Convention on Human Rights," *Human rights handbooks*, no. 1.

[7] *WMA General Assembly*, Washington, DC, USA, October 2002.

[8] Protected Health Information: What Does PHI Include?, *HIPAA* [Online]. Available: http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include/

[9] Health Care Information and Management System Society (HIMSS) [Online]. Available: http://www.himss.org/library/ehr/?navItemNumber=13261

[10] E.-H. W. Kluge, "Informed consent and the security of the electronic health record (EHR): some policy considerations," 2003.

[11] A. Raman, "Enforcing privacy through security in remote patient monitoring ecosystems*," in 6th International Special Topic Conference on Information Technology Applications in Biomedicine*, Tokyo, Japan, pp.298–301, 2007.

[12] R. Hasan, W. Yurcik, "A statistical analysis of disclosed storage security breaches," *Proceedings of 2nd ACM Workshop on Storage Security and Survivability*, Alexandria, VA, pp.1–8, 2006.

[13] B. Campbell, H. Thomson, J. Slater, C. Coward, K. Wyatt, and K. Sweeney, "Extracting information from hospital records: What patients think about consent," *Quality and Safety in Healthcare*, vol. 16, no. 6, pp.404–408, 2007.

[14] P. Sankar, S. Moran, J.F. Merz, and N.L. Jones, "Patient perspectives on medical confidentiality: a review of the literature," *Journal of General Internal Medicine*, vol. 18, pp.659–669, 2003.

[15] N.P. Sheppard, R. Safavi-Naini, and M. Jafari, "A digital rights management model for healthcare," *IEEE International Symposium*, pp. 106-109, July 2009.

[16] *American Recovery and Reinvestment Act of 2009*, Superintendent of Documents, United States Government Printing Office.

[17] IMIA Code of Ethics for Health Information Professionals [Online], 2002. Available: http//:www.imia.org

[18] *Implementing Consumer Privacy Preferences in Health Information Exchange (HIE) using Service-oriented Architecture (SOA)*, HIPPAAT CONSENT MANAGEMENT, March 2009.

[19] J.J. Shen, L.F. Samson, E.L. Washington, P. Johnson, C. Edwards, and A. Malone, "Barriers of HIPAA regulation to implementation of health services research," *Journal of Medical Systems*, vol. 30, no. 1, p.65, 2006.

[20] *Consent management for health information exchanges*, OPTUM. White Paper, 2012.

Risk Management Methods in Small Scale Companies

F. Mastjik[1] and C. Varol[2]

[1] Department of Computer Science, Sam Houston State University, Huntsville, TX ,USA, fxm010@shsu.edu
[2] Department of Computer Science, Sam Houston State University, Huntsville, TX, USA, cvarol@shsu.edu

***Abstract*— Information system risk management is an important part of a company process to maintain business practices. This paper first analyzes three risk management methods: EBIOS, NIST 800-39, and IT-Grundschutz. Although these methods have been widely adopted and recognized, these methods fit for large scale businesses. Therefore, with analyzing the advantages and disadvantages of these methods, we proposed a new risk management method that is focused for smaller businesses and organizations. The advantages gained are simplified method that can potentially reduce the cost for risk management and foster collaboration between small businesses due to the nature of the method.**

***Index Terms*—Ebios, IT-Grundshutz, NIST 800-39, Risk Management**

I. Introduction

Ever since the conception of business, humans have always tried to establish methods on managing the risk posed to businesses. D.Hubbard [1] defines risk management as "identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events". As humans advance in the technology field, the importance of risk management roles in relation to business continuity have grown . Standards and guidelines have been produced by international organizations to provide methods on information system risk management [2], [3], and [4]. ISO 27001 [2] specifies that "a risk assessment has to be carried out before any controls can be selected and implemented, making risk assessment the core competence of information security management." While NIST 800-37 [3] acknowledges that there are various threats to information security from predicted and unpredicted vectors, which needs to be understood by the people who are responsible for the management of information security in an organization, especially its leaders.

Even though there have been international standards implemented for the information system risk management, there have been at least two common issues that are faced by all information risk planners. For example in [4], NATO acknowledges that the various existing methodologies differs in methods for classification even if conceptually similar. From this statement we know that the first issue is the need to establish common risk analysis method or devise a process as guideline for interoperability between different methods. The second issue is smaller organizations or businesses sometimes are not considered in these methods since they are commonly made for large organizations and enterprises. Further analysis/approach is needed to custom-modify the methods to be able to cater to smaller organization needs which can be done either by introducing a support tool or by partially modifying the method itself. After thorough analysis, it is decided that a modification needs to be made by proposing a new method which improves upon the three methods discussed in this. The results gained are hybrid approach of combining specific parts of the three methods which is based on simplicity and efficiency yet still maintain a level of robustness.

II. Overview of Risk Management Methods

In order to manage a risk, set of guidelines that provides a way to arrange the process in a logical order is needed. According to S.K Katsicas [5], methodology is the principles and rules that motivates action. Figure 1 [4] describes the classic steps in a risk management process:

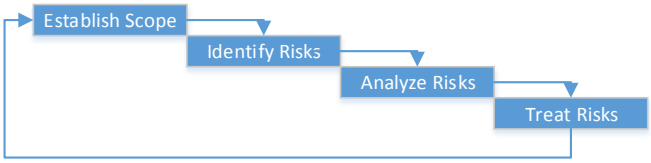


Fig.1 Classic Risk Management Process

NIST 800-39

Concerned over the rise of cyber security threats in the recent years, NIST worked on re-developing the stance and viewpoints for IT risk management system guideline described in SP 800-30. The focus of the guideline is then shifted to managing risk on enterprise level instead of only managing the risk on information system level. This is done by creating a superset of special publication; the NIST SP 800-39 which was released on March 2011 with its aim is the integration of organization-wide risk management.

SP 800-39 was written for federal information systems and organizations, but the guideline can be applied to other organizations. The main advantage of this method is its structured yet flexible approach for managing the risk related to information systems on enterprise level. Its main disadvantage is as described and confirmed by [6] is that its

process are tailored for enterprise level and would pose a level of complexity if implemented on smaller organization. The main process involved is shown on Figure 2 [6].

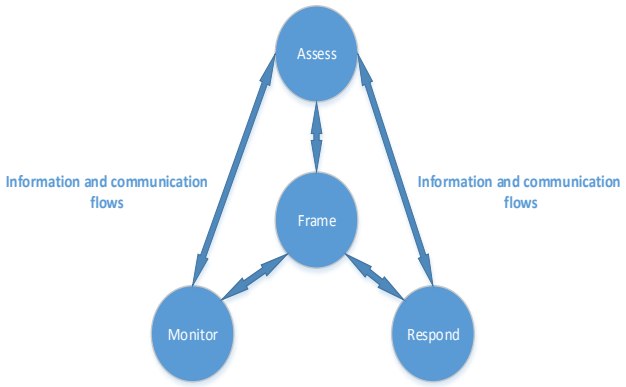


Fig.2 NIST 800-39 Risk Management Process

To explain further, the arrows represent the flow of the process where risk framing provides information to all the sequential step by step activities that moves from risk assessment, to risk response, and to risk monitoring. For example, risk framing produces an output in the form of information related to the threat which is the primary input to the risk assessment component. Risk assessment produces yet another output that is the primary input for the risk response.

The flow of the information and communication to all components are considered to be flexible in order for the process to respond in as quick, and as dynamically as possible. For example as stated by [6] an immediate change or directive in policy might require implementing additional risk response measures. This directive can be communicated directly from risk framing component to risk response component.

EBIOS

EBIOS methodology was created in 1995 by the French national security agency[7]. It is one of the main methods used in France and French speaking countries due to its open-source nature both in the guideline documentation, and the development of the tools to support the method. In 2010, French National Security Agency Information System division, also known as Agence Nationale de la Sécurité des Systèmes Information (ANSSI) released an update of the methodology to better accommodate the development in IT risk transformation. This update was collaboration between ANSSI and EBIOS club which is an independent non-profit group. Figure 3 , depicts the modules in the risk management process [7].

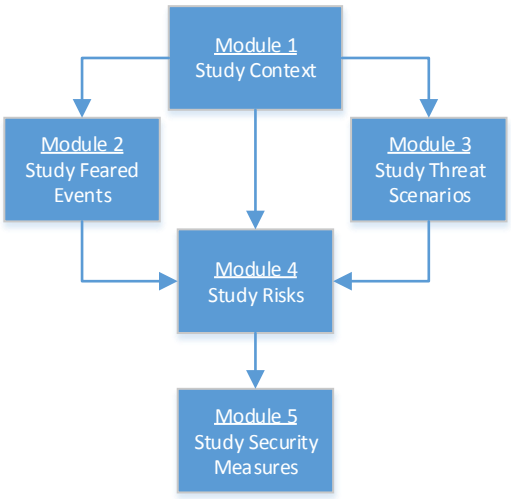


Fig.3 EBIOS Risk Management Process

From the figure above we understand that EBIOS consists of five modules. The first module establishes context as part of the management risk metrics. It also creates the critical assets along with their support assets. The second module contributes to risk assessment by identifying and assessing the security needs (availability, confidentiality, integrity) and all impacts in case of violations to the security requirements. It will also produce the source of threats (human, environmental, etc.). The third module is closely related to the second module where it will identify scenarios where threat exploits vulnerabilities. The fourth module further evaluates the risks and identifies security objectives. Finally, the fifth module will be responsible for risk treatment and selection of controls.

EBIOS's main advantage is it is one of the two methods available for free in Europe besides IT-Grundschutz, and it is the only one with open-source tool to support. Its disadvantage is the lack of updated documentation in English, particularly for the latest updates that was released in 2010. EBIOS also claims to be made for private and public sector but made no claims on the size of organization it supports.

IT-Grundschutz

In 2005, Bundesamts für Sicherheit in der Informationstechnik (BSI) as the authority for Federation of Germany in Information security consolidate its collection of over 4000 pages to produce a standard for information security risk management which is known as BSI-Standard 100-2: IT-Grundschutz methodology. According to [8], this methodology provides a detailed description of how to produce a practical security concept, how to select appropriate security safeguard, and how to implement the security concept. It conforms to the ISO 27001 and subsequently, ISO 27005 as with EBIOS. Figure 4further illustrates the management process [8].

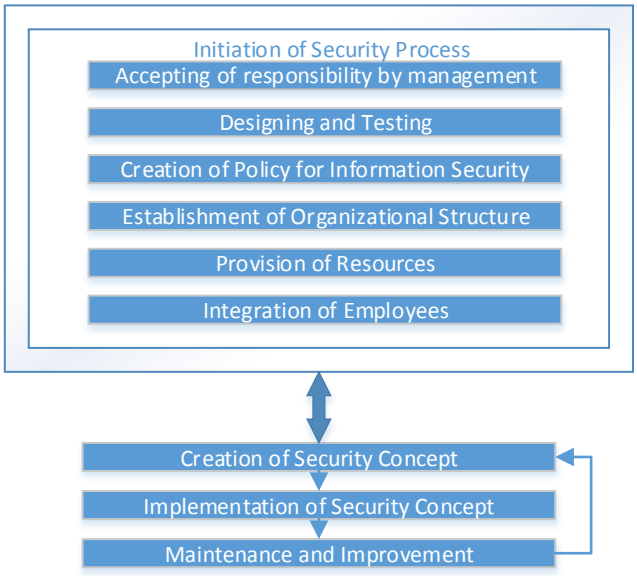


Fig.4 IT Grundschutz Risk Management Process

IT Grundschutz method starts with the initiation of security process where management must initiate, control, and monitor the security process. Some of the self-explainable phase inside the frame can be done in parallel. For example the design and planning phase can be done at the same time. The next phase which is the creation of security concept consists of structure analysis, determination of protection requirements, selection and adaptation of safeguards, basic security checks, and supplementary security analysis. The step continues with implementation of security concept, from there maintenance and constant improvement are to be done for security purposes. Finally, a certification of ISO 27001 may be based on the successful implementation of IT Grundschutz.

IT Grundschutz's main advantage is its uniqueness where the method [8] possess a catalogue containing common standard threats and its solution for common business process and IT system which will reduce expense of risk management process by cutting time and resources needed. Another advantage is the catalogue can hold information of organization on various size. The cataloguing method also pose as its disadvantage as full analysis of new problems not existing in the catalogue needs to be done with the emerging of new technologies which partially beat its purpose in expense and process reduction.

III. Risk Management Method for Small Organization

As mentioned in the introduction, one of the issues found in common risk management methods such as but not limited to the three methods discussed before, is they are aimed generally to a larger enterprise. While implementation of the methods to smaller organizations is possible, it will introduce greater cost and a potential of information redundancy if viewed from "information-as-needed" point of view. By studying these methods, we can derive that their processes are widely different and the quantity of sub-process/sub-steps may vary which adds to the complexity and cost to perform these steps for smaller organizations. Also some of them possess useful processes that can be useful for smaller businesses or organizations while they may be also lack in other processes. For example, while EBIOS does not possess the concrete post-implementation monitoring strategy and evaluation as showcased by NIST 800-39, it does however do initial study of existing security measures which is not included in NIST 800-39.

The processes from the three methods can be generalized as: context definition, risk assessment, monitoring/evaluation. Also for EBIOS/IT-Grundschutz implementation of a security certification is an option.

Based on the analysis, a proposed combination method of Context Study from EBIOS, Knowledge catalogue concept from IT Grundchutz and Continuous Risk monitoring and evaluation from NIST-800-39 can be combined into the following diagram:

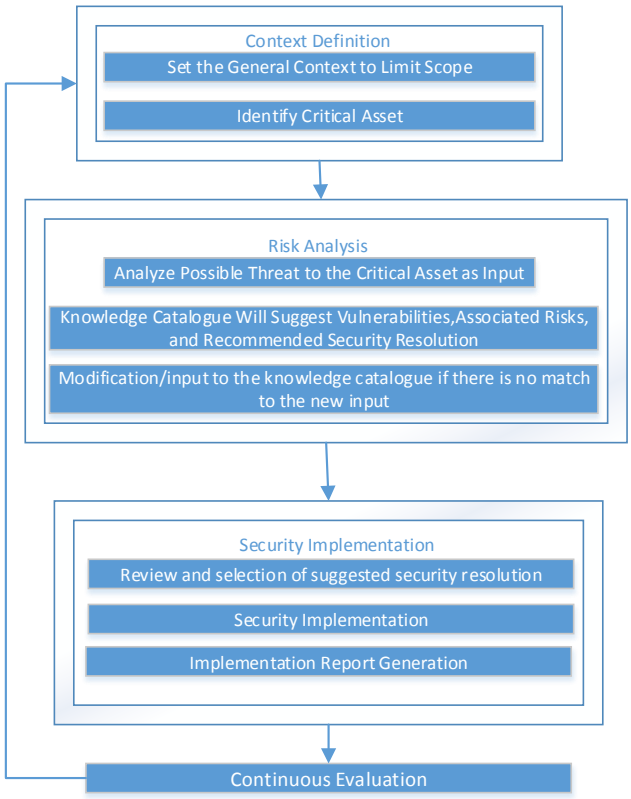


Fig.5 Proposed Management Method Process

Context Definition

First stage is the context definition. In this stage the person/team will define the context of the plan to limit the scope of the plan and avoid scope creeping; the main activity will be identification of critical asset of the business.

Risk Analysis

Once context definition is done, analysis of any possible threats that can affect the critical assets then is listed as a list of inputs. These inputs are then compared to the knowledge catalogue to see if there are any existing similar threats from which can be derived its vulnerabilities, associated risks, and

recommended security resolution/controls. If there are no matches of the inputs in the knowledge catalogue, further risk assessment will be done to define vulnerabilities, associated risks, and recommended security resolution/controls. This can become a basis for future risk analysis.

Security Implementation

From the risk analysis, the risk assessment report will provide the list of risks and recommended security resolutions/controls. At this stage, the stakeholder (usually business owner) can then decide which controls he wants to be implemented and a report documenting the implementation is generated along with the list of any risks that are not controlled due to acceptance from the stakeholder.

Continuous Evaluation

A continuous evaluation of current risks and controls effectiveness can be done to determine if there are any changes to the plans or the controls needs to be made.

These three steps and the continuous evaluation is derived from the three methods explained, however it differs in a sense where the steps are simplified, the time taken can be potentially reduced and involves minimum personnel to perform instead of a full team. This can potentially be done within the organization itself instead of hiring professional services.

IV. Benchmark and Comparisons

In order to analyze if the method will provide cost reduction efficiency while still providing comprehensive risk management to smaller organization three test cases are conducted. Specifically, company A is a small IT consultancy with 20 staff employed, the entire company management process is handled by the owner himself. Due to business demand and client regulations, the company needs to implement a risk management plan as a part of its compulsory disaster recovery plan.

The owner hires a consultant team who charges $200/hour to plan and implement the entire risk management control. Considering EBIOS method is used and each steps/sub-stages of the main stages takes an average of 1 hour to perform due to small scale complexity of the company, here is the estimated cost:

EBIOS Cost estimation

Stages	Total Hour(s)	Results
Study Context	13	Study scopes and critical assets list
Review Of Undesirable Events	3	Threat scenarios lists
Study Threat Scenarios	2	Threat scenarios evaluation report
Risk Study	6	Risk Assessment Report
Study of Security Measures	8	Security measures implementation report
Security Accreditation	1	ISO certification/security certification

To complete the entire planning and implementation it takes at least a minimum of $6600 (33*$200) not including the cost for security accreditation which can easily cost thousands of dollars. Even though the accreditation is removed it will still cost a minimum of $6500 for one full cycle of implementation. However, when we apply the same scenario with the new proposed method we obtained the results that are reflected in Table II.

PROPOSED METHOD COST ESTIMATION

Stages	Total Hour(s)	Results
Context Definition	2	Study scopes and critical assets list
Risk Analysis	3	Risk Assessment Report
Security Implementation	3	Security Measures Implementation report
Continuous Evaluation	1	Evaluation Report

To complete the entire planning and implementation it takes at least a minimum of $1800 (9*$200), not including the cost for the constant evaluation. This cost can be adjusted as a monthly cost of $200 for 1 hour evaluation each month (if necessary) which yields an additional annual cost of $2400. One full cycle implementation with monthly evaluation will cost $4200 per year.

In the second test case NIST 800-39 method is used for comparison. While the method is specifically aimed as a part of ERM (Enterprise Risk Management) according to [4], we will perform the same scenario above:

NIST 800-39 cost estimation

Stages	Total Hour(s)	Results
Risk Framing	4	Risk Framing (assumptions, constraints, risk tolerances, and priorities/trade-offs) Report
Risk Assessment	3	Risk Assessment Report
Risk Response	3	Risk Response Report
Risk Monitoring	2	Monitoring Report

As shown in Table III, to complete the entire planning will cost $2400 (12x200) considering the extra sub-step taken to define the monitoring strategy and the actual monitoring we can assume that there is an additional cost of $2400 if the monitoring is done 1 hour/month. One full cycle implementation with monthly evaluation will cost $4800 per year.

Considering another case where company B is a large enterprise of 500+ employees and are conducting its risk management planning due to requirements from its clients for the company to be ISO 27001 certified. They hire a large auditing firm to perform the entire planning and implementation for a rate of $2000/hour. Considering the complexity and large quantity of assets of the company, it might take them a few weeks to a month to complete each steps and the cost can be in thousands of dollars. Also considering the case above is related to enterprise and certification in which a well-known international standardized methods are needed, we can disregard the comparison analysis since the proposed method does not have the security accreditation steps needed which is the reason why methods such as EBIOS and IT Grundschutz are made for larger enterprise due to the nature of the completeness of its analysis. That is also the reason why the focus of this paper aims at smaller organizations.

V. Challenges to proposed method

Several challenges to the proposed method are available:

Knowledge Catalogue Security

In order for the proposed method to be adopted widely, the key lies in the knowledge catalogue which contains information regarding known threat, vulnerabilities, and commonly proposed solutions (i.e. fire as threat, fire alarm not installed as vulnerability, and fire alarm installation as solution). However, in order to fully maximize the potential of the catalogue it needs to be publicly available for business and organization to access. This means that the contributor to this repository needs to come from the actual business which performs its risk management using the proposed method. These companies might be hesitant to do this as that means they are divulging at least a part of their risk management assets. Therefore complete contributor anonymity and an independent regulator are needed to be able to regulate the knowledge catalogue.

Limitation to Smaller Business

The proposed method is aimed mainly for smaller business which does not require international certification or at least not at the level where they are considering using this method. The information may lack the complexity and completeness of information a standardized method such as EBIOS or IT Grundschutz can offer.

VI. CONCLUSIONS

Several various methods exist for Risk Management and most of them are widely adopted by Enterprise across the globe. According to SBA [9] almost 25 percent of business does not reopen after a major disaster", this is no doubt due to the lack of risk management and disaster recovery plan. The proposed risk management method holds a potential to be adopted by smaller organization to assist in their implementation of a cost-effective and information-scalable risk management plan.

Future area of study in this field and topic aims especially at analysis on improving the management process to cater to larger business without sacrificing its simplicity and cost efficiency, perhaps by implementing a CBA for further cost saving. Integration with security accreditation can be done with further development of the component. Finally, more knowledge-base model as an alternative to the IT-Grundschutz needs to be created and made publicly accessible which can become alternative to smaller businesses with different traits than their European counterparts. The development of software or spreadsheet/document based on these can prove fortuitous and immensely helpful to the effort.

References

[1] D.Hubbard.The Failure of Risk Management: Why It's Broken and How to Fix It,NY:John Wiley & Sons,2009.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Information technology – Security techniques – Information security management systems – Requirements, ISO Standard 27001:2005.

[3] Guide for Applying the Risk Management Framework to Federal Information Systems,NIST Special Publication 800-37:2010.

[4] W.Mees,J.Savoie,M.Vanecek,P.Jenket,R.Stalker,F.Jordan, and F.Rousset, "Improving Common Security Risk Analysis" NATO:Paris,France,Rep.RTO-TR-IST-049,2008.

[5] S.Katsicas. Computer and Information Security Handbook, MA: Morgan Kaufmann,2009.

[6] N.Hunstad, "The Application of NIST Special Publication 800-39 for Small Businesses and Organizations"M.Sc.Thesis,UMN,MA,2011.

[7] ANSSI, "Expression of Needs and Identification of Security Objectives : EBIOS Method of RIsk Management",ANSSI:Paris,France,2010.

[8] IT Grundschutz Methodology, BSI - Standard 100-2:200.

[9] IBHS.Open For Business,USA,2007

SQL Injection: Hardening MYSQL

Noe Nevarez, and Bing Zhou

Department of Computer Science, Sam Houston State University Huntsville, Texas 77340
{nxn008,zhou}@shsu.edu

***Abstract* – SQL Injection (SQLI) is still ranked 1st among all the different types of vulnerabilities in the Open Web Application Security Projects report for 2013** [1]. **There have been many tools which parse applications which check the syntax of commands before they are eventually sent to the Database Management System (DBMS). I propose a number of different techniques used to harden DBMS running MYSQL/PHP. The combination of MySQL and PHP is chosen for testing since it is freely accessible, a very popular platform for developing applications on.**

Keywords – SQLI, MySQL, application security, DBMS

I. INTRODUCTION/BACKGROUND

SQLI has been around for a little over 10 years now. Every year the exploitation becomes worst and in increasing devastation [2]. One of the main reasons for this is the development of applications without a sound security policy to enforce standards. It also depends on how the infrastructure used during the communication process. For example, a client accesses access a web page which then sends SQL commands to the DBMS. If the DBMS is external facing, there is usually a firewall which has rules set to allow the SQL destination port only. There should also be rules for the web application which accesses the DBMS. The standard ports for web applications are usually TCP 80/443. Since these ports are usually golden ports, which are ports allowed through most firewalls, they will enable an attacker exploit imperfections in the source code and redirect malicious SQL injected code through port 80/443.

There are many examples of SQL Injection attacks sited by organizations across the internet. For example, InfoWorld reports a surge in SQL attacks year-by-year [3]. The attacks are usually originating from Russia, China, Brazil, Hungary, and Korea. Many of these attacks are some of the simplest to check and are usually created by script kiddies. An Intrusion detection system (IDS) and Intrusion Prevention System (IPS) can identify and prevent many of these forms of attacks. However, once these types of systems are identified (IDS/IPIS), it is offend very easy for a hacker to evade detection. There should be a security team of some sort at every organization to prevent these types of occurrences at all hours of the day.

SQL Administrators primarily detected SQL injection attacks through the use of pattern matching against signatures and keywords known to be malicious. This form of attack was known as a Trojan horse form of SQLI. This form is of attack fit a certain pattern as it went through application firewalls and IPSs. As such these devices usually dropped the packet before it even came through the application Instrastructure. Hackers since developed a new SQLI attack technique called Trojan Zebra [4]. This form looks very similar to the typical Trojan horse, but has a different pattern that isn't easily detected by most Intrusion detection systems. Even if the pattern of the Trojan Zebra is known, every Trojan Zebra can be different. This is why it's called Trojan Zebra, since the pattern (strips) can be easily changed.

The queries that are typically used for SQL injection are broken down into the following [5]:

- Tautologies
- Logically Incorrect Queries
- Union Query
- Piggy-Backend Queries
- Stored Procedures

The SQL Tautology attack is an attack that works by inserting an "always true" fragment into a WHERE clause of an SQL command statement. A logically incorrect query attack is used to determine what type of error message gets outputted back. The attacker can then find out the vulnerable parameter in the application or database schema. A Union Query attack exploits a vulnerable parameter and injects the union keyword to retrieve information. The user can use the information again to run other queries. In a Piggy-Backed query attack, an attacker inserts or adds additional queries onto the original query. These types of queries are extremely harmful as you can imagine. A stored procedure attack allows an attacker to execute procedures present on the DBMS. The reason why stored procedures are vulnerability is because they are constructed using scripting languages that can be susceptible to exploits like buffer overflows.

II. RELATED WORK

Injection attacks have dominated the top of web application vulnerability lists for much of the past decade. SQL Injection (SQLI) is the most exploited vulnerability [6]. The root cause is in the concatenation of characters together to create a string, a database command. Various techniques and method approaches attempt to prevent attacks. However, not any one method can prevent all occurrences and could involve manage changes to the application environment [7].

Preventing SQLI has been approached by a query optimization process which gets the output back in a timely matter [8]. It converts the query into something the query processing engine understands. If the query conforms to language rules, it then gets translated into an algebra expression to represent it as a data structure tree.

The heuristic approach uses a pattern matching for error message that are produced by the application under test [9]. This approach gathers information, identifies input parameters, generates attacks and reports results. Utilizing V1p3R approach, it was found that it spotted all injection vulnerabilities with less consumption of resources [9]. This definitely speeds up the process and provides the best balance between speed and productivity.

The Specification-based approach creates a specification list for the application [7]. It includes phases before a command occurs. This approach involves the creation of a specification list which contains a set of rules that describes the expected structure of the desired SQL statement within the code of application. Analyzing and determining the syntactic units will determine its validity. After various tests, the proposed methodology detected and prevented all of SQL Injections before they could be executed. This new method showed promising results [7]. The key to a successful tool that not only detects and prevents vulnerabilities is people working and sharing together in an effort to secure information (data).

III. MYSQL/PHP HARDING TECHNIQUES

MySQL has been among the most popular DBMS since its initial release in 1995. PHP has also been the web application of choice for many programmers learning how to implement ecommerce based applications. Below you can see an example of the PHP code used to implement an SQL Tautology attack based attack.

- **Normal:** where password = “x”
- **Injected:** WHERE password = “x” OR “x”=”x”

As you can see in the injected attack, the statement (OR ‘x’=’x’) has been appended to the original statement. This allows the query to behave differently than the developer intended. This statement will always be true can could allow an attacker to display much more information from tables. Not only can these injection techniques be used to access more information, they can also be used to delete entries in important tables.

It turns out that PHP and MySQL has developed code to prevent this Tautology SQLI technique. There is a function called **“mysql_real_escape_string()”** that once enabled it will parse the SQL statement string and replace those quotes with an escape quote. Once you put the bad SQL query into the parentheses “()” of the “mysql_real_escape_string()”, it will automatically escape the added code and prevent the extra statements from being executed.

IV. EXPERIMENT/RESULTS

The experiment will consist of a PHP application running on a webserver running Apache 2.2.17 and MySQL 5.1.54 on Ubuntu. We have setup a simple application which grabs information from a database depending on the input of the web form. The query can be seen in FIGURE 1 below.

```
$item= ""; DELETE FROM lbci WHERE 1 or username = "";

$lbcitable_SQLselect = "SELECT ";
$lbcitable_SQLselect .= "IP,CI,coalesce(NETWORK,'N/A')NETWORK,co
,LOCATION,TYPE ";
$lbcitable_SQLselect .= "FROM ";
$lbcitable_SQLselect .= "lbci ";
$lbcitable_SQLselect .= "WHERE NETWORK like '$item%'limit 2";
```

This query’s end goal is to grab the IP, CI, and network information from the “lbci” table, where the network matches a specific subnet which the user inputs in the web form. What we can do is inject another command (ex. $item) which actually deletes information located within the table. This can cause major problems for people who actually use this application for information important to the organization as a whole.

As talked about in the section III, we can use the “mysql_real_escape_string()” to sanitize the query before it is actually sent to the DBMS. It would be as simple as adding the statement below to mitigate such an attack.

SANITIZE MYSQL STATEMENT

$item = mysql_real_escape_string($item);

This statement will escape all the quotes so that the extra statement is effectively disabled and doesn’t delete important data from the table.

V. CONCLUSION AND FUTURE WORK

The Tautology attack method is a very basic form of attack that is still prevalent in many Application/DBMS systems.

Using the security functions like “mysql_real_escape_string” can help to eliminate these common attack methods. Functions like are also utilized in other programming languages like Java, Python, and C#. It is very important to keep your software distribution updated so new security enhancements can be taken fully advantage of. There are many SQL Injection scanners out the web for free that can help even a notice web developer secure their environment. In the future I would like to demonstrate how one can prevent many of the other forms of attacks like Union and Piggyback attacks. It would also be beneficial to test many of the enterprise level DBMS like Oracle and MSSQL. Since the sheer amount of SQLI based attacks seems to rise every year, it seems that we need a revolutionary new way to detect and prevent this. We need to educate students of the future to properly have a work force whose sole purpose is to prevent these types of attacks. It’s clear that the security professional workforce must increase and expanded.

VI. REFERENCES

[1] OWASP, " Category:OWASP Top Ten Project," 12 June 2013. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[2] HackerTarget.com, "10 years of SQL Injection," 2013. [Online]. Available: http://hackertarget.com/10-years-of-sql-injection/.

[3] R. Chandran, "SQL Injection attacks sky rocketing," PLYNT, 26 July 2006. [Online]. Available: http://www.plynt.com/blog/2006/07/sql-injection-attacks-sky-rock/.

[4] L. M. Vittle, "SQL Injection Evasion Detection," September 2007. [Online]. Available: http://www.f5.com/pdf/white-papers/sql-injection-detection-wp.pdf.

[5] DBNetworks, "SQL Injection Attacks: Detection in a Web Application Environment," 2013. [Online]. Available: http://www.dbnetworks.com/pdf/sql-injection-detection-web-environment.pdf.

[6] E. Couture, "Web Application Injection Vulnerabilities," 20 May 2013. [Online]. Available: http://www.sans.org/reading_room/whitepapers/application/web-application-injection-vulnerabilities-web-app-039-s-security-nemesis_34247.

[7] K. Kemalis and T. Tzouramanis, "SQL-IDS: a specification-based approach for SQL-injection detection," *SAC '08 Proceedings of the 2008 ACM symposium on Applied computing*, pp. pages -- 2153 -- 2158, 2008.

[8] E. Al-Khashab, F. S. Al-Anzi and A. A. Salam, "PSIAQOP: preventing SQL injection attacks based on query optimization process," *KCESS '11 Proceedings of the Second Kuwait Conference on e-Services and e-Systems* , no. 10, 2011.

[9] A. Ciampa, C. A. Visaggio and D. M. Penta, "A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications," *SESS '10 Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems* , pp. 43-49, 2010.

Steganalysis of Quality Pair JPEG Steganography

Kasim Tasdemir, Fatih Kurugollu, Sakir Sezer

The Institute of Electronics, Communications and Information Technology (ECIT),
Queen's University Belfast, Belfast/UK,
{ktasdemir01, f.kurugollu, s.sezer}@qub.ac.uk

***Abstract*— The number of steganography methods in the literature is increasing and every novel steganography idea attracts new steganalysis studies. One of the most recent image steganography algorithm is Quality Pair JPEG Steganography (QPJ). It embeds the message by manipulating JPEG quantization tables and it is capable of evading steganalysers Stegdetect and Farid's schema. Yet, there is not any steganalysis study targets the QPJ. In this paper, we propose a targeted steganalysis of QPJ algorithm which successfully detects the stego images. We investigate its security through the effects on DC coefficients between the image blocks imposed by the embedding method. First, we discover the statistical dependencies of DCT coefficients of adjacent 8x8 image blocks which are highly corrupted by the QPJ algorithm. Then, based on this corruption, we developed a targeted steganalysis algorithm that reveals the images carrying the secret message with a high accuracy.**

***Keywords*— Steganalysis, JPEG, Steganography, Quality Pair, Quantization Factor, Quantization Table.**

I. Introduction

STEGANOGRAPHY is a term for covert communication. The purpose of this secret communication technique is to send messages to the recipient without rising any suspicious sign that may attract attention of a warden. It uses inconspicuous objects as a carrier of the secret message. The steganography algorithm is decided to be failed when a warden notices that the carrier object is not innocent [1].

On the warden's behalf, steganalysis is an art of determining the objects carrying secret message [2]. For digital media, steganography algorithms try to not to disturb the statistics of the cover media. However, embedding a secret message without altering these statistics is not a trivial task. Steganalysis algorithms relies on this fact to reveal the hidden message in an image [3].

Steganalysis algorithms are categorized into two main groups: blind and targeted steganalysis. Blind steganalysis algorithms are developed for defeating multiple steganography algorithms and they can also be adopted to attack to a new steganography algorithm. The steganalysis that attacks to a specific steganography algorithm goes into targeted steganalysis category. The proposed steganalysis algorithm is a targeted steganalytic algorithm against a steganography method using JPEG images as medium.

JPEG is the most popular image format used in Internet which makes it a good cover candidate in point of view of image steganography. One of the recently proposed JPEG based secure steganography methods is the Quality Pair JPEG steganography (QPJ) algorithm [4]. Basically, it alters the quality factors of a JPEG file to embed the secret message. The image blocks are quantized with different quality factors depending on the message bits. If the message bit is 1, the corresponding image block is quantized with high resolution. Otherwise, it is quantized with lower quality factor. The blocks with low resolution does not introduce any human perceivable distortions in the image. To the best knowledge of authors, there is no steganalysis study targeting [4] and it is reported in [4] that the method successfully evades recent steganalysis attacks. However, in this study we exhibit that the correlation of adjacent blocks are highly disturbed by QPJ steganography and we exploit the resulting statistical corruption.

Steganalysis of QPJ algorithm should not be confused with double-compressed JPEG steganalysis methods, which is one of the subsection of JPEG steganalysis subject [5]. In double-compression detection algorithms, it is assumed that the image is partially or completely compressed with another quality factor [6, 7]. As it is explained in Section 2, QPJ algorithm is not an exactly double compression algorithm because it uses two different quality factors for each image block depending on the message bit. Hence, instead of assuming it a double JPEG compression and analyzing for secondary quantization matrix over whole image, a block by block analyze approach should be used.

The rest of the paper is organized as follows. Firstly, a brief overview of the QPJ steganography algorithm is introduced in Section II. The proposed steganalysis method for QPJ is presented in Section III. The high detection rate of the proposed method is shown in Section IV through experimental results.

II. Brief Overview of the QPJ Algorithm

The QPJ steganography algorithm depends on the fact that if

an image region I_1 has the quantization factor Q_1, and re-quantized with Q_2 to obtain I_2 then $I_1 - I_2$ has a local minimum value when $Q_1 = Q_2$ [8]. In the secret message embedding stage, the 8×8 image block is quantized with Q_1 if the corresponding message bit is 1. Otherwise, Q_2 is used as the quality factor for this block. Finally, the whole image is saved as a JPEG image with 100% or 95% quality.

The embedding stage is as follows. Let M be the binary secret message matrix of size $M \times N$. The cover image I is of size $P \times Q$ where $P/Q = M/N$. The message embedding stage has two steps as follows.

Step I The host image I is divided into blocks of size $P/M \times Q/N$.

Step II If $\begin{cases} M(m,n) = 0, & compress\ I(i,j)\ with\ Q_2 \\ M(m,n) = 1, & compress\ I(i,j)\ with\ Q_1, \end{cases}$

for all i, j satisfy $\lceil i/(P/M) \rceil = m; \lceil j/(Q/N) \rceil = n$. Then the image is saved in JPEG format with a high quality such as 100 or 95.

In the message reconstruction stage, the stego image $S_{Q1,2}$ is re-quantized with Q_2, where Q_2 has lower resolution than Q_1 to obtain the re-quantized image, S_r. Then, $S_{Q1,2}$ is subtracted from S_r. In the difference matrix, the 8×8 blocks close to zero are considered to be carrying message bit 1 while the other blocks correspond to 0. QPJ embeds all blocks without regarding different embedding rates because of the limited capacity provided by the algorithm.

III. Steganalysis of the QPJ Algorithm

Adjacent pixels in natural images are highly correlated [9]. This correlation is reflected to the DC coefficients in the block base DCT applications. In natural images, DC coefficients of neighboring blocks are similar. After quantization stage in JPEG compression, they have certain values such as integer multiples of quantization scale factor. Hence, in JPEG images the difference between the DC coefficients of adjacent image blocks can have multiples of quantization factor. However, if adjacent blocks of the image are quantized with different quantization matrixes, the difference array shows an unnatural behavior. The QPJ steganography method corrupts these dependencies between neighboring 8×8 blocks because it quantizes each block with a different quantization matrix, either Q_1 or Q_2. This type of quantization process causes different rounding errors as well as it weakens the dependencies between low frequency values of DCT of neighboring blocks. This provides a crucial clue resulting in a successful detection which will be explained in the following sections.

A. Extracting the Feature

Using different quantization tables for different 8×8 image blocks in JPEG compression causes unnatural variations among these blocks. In order to reveal the unnatural variations we examined the difference array, $\mathbf{D}$, in horizontal direction which is defined as

$$D[(i-1)n + j] = C_{i,j} - C_{i,j+1} \quad i = 1,\ldots,m,\ j = 1,\ldots,n-1 \quad (1)$$

where $C_{i,j}$ is the DC coefficient of DCT block at position (i, j) and where $m = M/8$ and $n = N/8$ corresponds the number of blocks in the horizontal and vertical directions. The difference vector $\mathbf{D}$ is calculated over horizontal direction. It can be calculated for vertical and diagonal directions as well to increase the detection accuracy. However, we observed that differentiating only over horizontal direction is good enough for a successful detection.

Embedding the secret message using QPJ algorithm introduces ripples in the histogram of $\mathbf{D}$ vector as shown in Fig. 1. The source of the peaks are investigated in Section III-B. This unnatural ripples on the $\mathbf{D}$ histogram of stego image are the main sources of the features extracted in the proposed steganalysis algorithm.

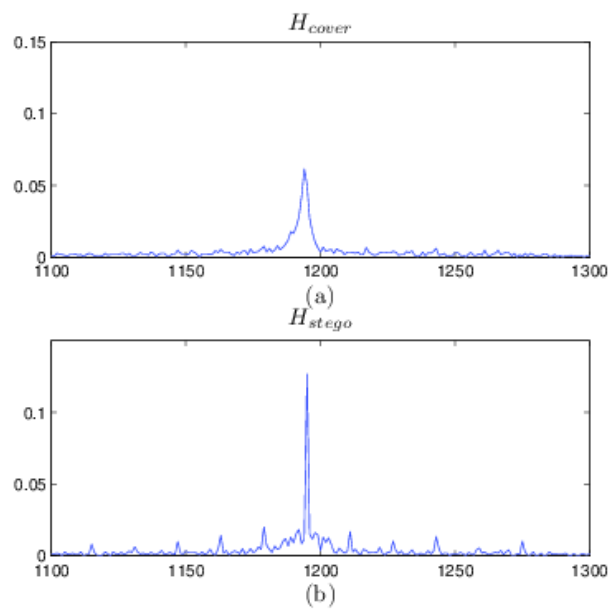


Figure 1: Histograms of $\mathbf{D}$ of stego and original image. H of a cover image is shown in (a) and H of its stego is shown in (b), which has significant distortions.

The ripples are more obvious and easier to distinguish in frequency domain as it is shown in Fig. 2. Let $\mathbf{H}$ be the normalized histogram of $\mathbf{D}$. F is defined as follows:

$$F = FFT(\mathbf{H}) \quad (2)$$

where FFT is Fast Fourier Transform. The stego and the cover images have obviously different F. The Fig. 2 shows the difference between F_{stego} and F_{cover}, which corresponds to the different F of stego image and the cover image.

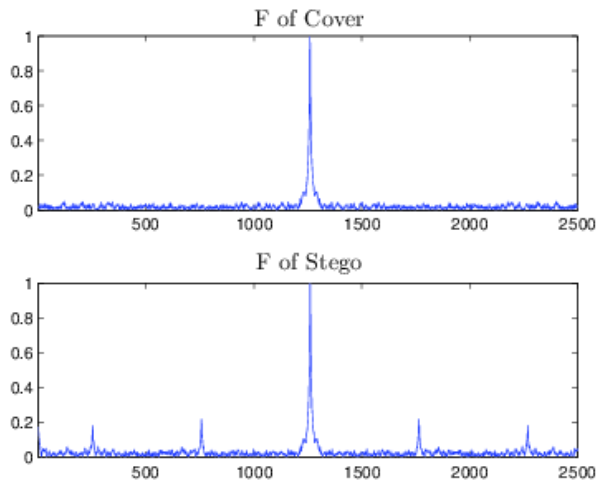


Figure 2: The FFT of normalized histograms of $\mathbf{D}$. The first one shows F of a cover image. The second part shows the F of a stego one, which has significant peaks at specific frequencies.

While significant peak values appear at F_{stego}, F_{cover} has a more precise Laplacian look and does not have any significant peaks except the one at the DC frequency.

B. *Investigation of the Source of the Peaks*

The difference array $\mathbf{D}$ corresponding to a QPJ stego image has an unnatural histogram because the probability distribution of the DC coefficients are not as similar as the natural images anymore. For instance, if an image is saved as a JPEG with 95% quality, its DC value is quantized with the first element of the quantization matrix, q, which is 2 for 95% quality JPEG images. If the blocks of the image quantized and dequantized with either $q=2$ or $q=5$, the DC values can only be multiples of 2 or 5. This causes a periodic $\mathbf{H}$. In order to show the periodicity in $\mathbf{H}$, we can extract a generalized expression for $\mathbf{H}$ is the normalized histogram of $\mathbf{D}$ considering 8 bit grey scale images.

Let q_1 and q_2 be the two quantization pair used in the QPJ algorithm. The probability density function, PDF, of the DC values f_q, is defined in (3).

$$f_q(k) = \begin{cases} \lceil q/256 \rceil & if\ k = 0, q, 2q \ldots, nq \\ 0 & otherwise \end{cases} \tag{3}$$

where $nq \le 256$ and $0 \le C < 256$. Similarly, PDF of the DC values quantized with q_1, f_{q_1}, is q_1 periodic in [0,255] discrete interval as shown in Fig. 3.

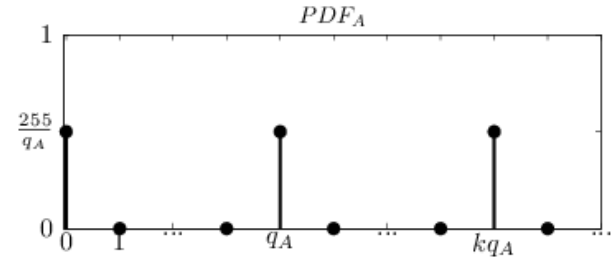


Figure 3: The PDF of the DC values of image blocks, f_{q_1}, when $q = q_1$.

Here, in order to model the corruptions on stego image we made an assumption that a DC value an image block, $C_{i,j}$, is an iid random variable, $\psi_{i,j}$ $\forall i, j$. Thus, the difference array $\mathbf{D}$ is another random variable, ζ, which depends on $\psi_{i,j}$ and $\psi_{i,j+1}$. Then the normalized histogram of $\mathbf{D}$, can be modeled as PDF of ζ, f_ζ. By the definition of $\mathbf{D}$ in (1), f_ζ depends on PDF of adjacent DC values $\psi_{i,j}$ and $\psi_{i,j+1}$. The PDF of ψ, f_ψ, can be defined as in (4) since each block is quantized with either q_1 or q_2 with equal probability.

$$f_\psi = 0.5(f_{q_1} + f_{q_2}) \tag{4}$$

By the definition of $\mathbf{D}$ in (1), $f_\zeta(k)$ of an image block is the probability of having k amount of greater DC value than the image block at its left hand side as defined in,

$$f_\zeta(k) = \sum_{n=0}^{255} f_{\psi_{i,j+1}}(n+k \mid \psi_{i,j} = n) f_{\psi_{i,j}}(n) \tag{5}$$

where $k = 0, \ldots, 255$. Since $\psi_{i,j}$ and $\psi_{i,j+1}$ are assumed to be iid, (5) can be rewritten and evaluated using (4) as follows:

$$f_\zeta(k) = \sum_{n=0}^{255-k} f_\psi(n) f_\psi(n+k) \tag{6}$$

$$= \sum_{n=0}^{255-k} 0.5(f_{q_1}(n) + f_{q_2}(n))\ 0.5(f_{q_1}(n+k) + f_{q_2}(n+k))$$

$$= 0.25 \sum_{n=0}^{255-k} \{ f_{q_1}(n) f_{q_1}(n+k) + f_{q_2}(n) f_{q_2}(n+k)$$

$$+ f_{q_1}(n) f_{q_2}(n+k) + f_{q_2}(n) f_{q_1}(n+k) \} \tag{7}$$

Actually Eq. (6) is a convolution. It was expected because f_ζ is the PDF of sum of two random variables $\psi_{i,j}$ and $-\psi_{i,j+1}$.

A statistical model for $\mathbf{H}$ is obtained in (7). Thus, $F = FFT(\mathbf{H})$ can be estimated as $\hat{F} = FFT(f_\zeta)$. A graph of $\hat{F}$ for quantization pair $q_1 = 16$ and $q_2 = 3$ is shown in Fig. 4. In Fig. 4 it is obvious that the realization of statistical model for estimated F, $\hat{F}$, is very similar to the F of a stego image. And this explains why the peaks appear as a result of QPJ steganography algorithm.

After modeling the F of a stego image, several approaches can be used to detect stego images. One of the approaches is to measure the distance between $\hat{F}$ and F. Then, a decision system can be trained with the distance measurements. However, it is observed that peaks appear after message embedding with considerable heights. In stead of use a computationally expensive algorithm for feature extraction, these peaks can be used as features. In order to optimize the ratio of cost of the algorithm versus the detection rate, it is shown that heights of local pitches are good descriptors for stego images.

The rest of the algorithm deals with extracting the major local peak value, which is the highest peak value except the peak at the lowest frequency, from the F and deciding the image as a stego or a cover.

C. Finding the Major Local Peak Value

In stead of using F for feature extraction, the energy of the signal F, E, is used because of two reasons. The first reason is the energy of the signal at peak frequencies are more emphasized than in F. Another reason is carrying the calculations on real numbers is computationally lighter than using complex numbers. The energy spectral density of F is calculated as follows:

$$E = \frac{F^{*}F}{2\pi} \tag{8}$$

The peak at the lowest frequencies which corresponds to the DC frequency exists in both cover and stego images. Hence, it can not be an descriptive feature. It needs to be excluded. We observed that the DC peak fades out after $\pi/24$ frequency. Thus, we only take the $(\pi/24, \pi)$ frequency region into consideration:

$$\overline{\mathbf{E}} = E(\omega) \tag{9}$$

where $\omega \in (\pi/24, \pi)$. We can use a simple outliers detection method known as the three sigma rule to find the peaks [10]. Instead of using the mean of the signal, using a median filter gives better results because in this way peak values do not affect the mean as much as in averaging. Let $\mathbf{P}$ be the peaks vector defined in (10) as the following:

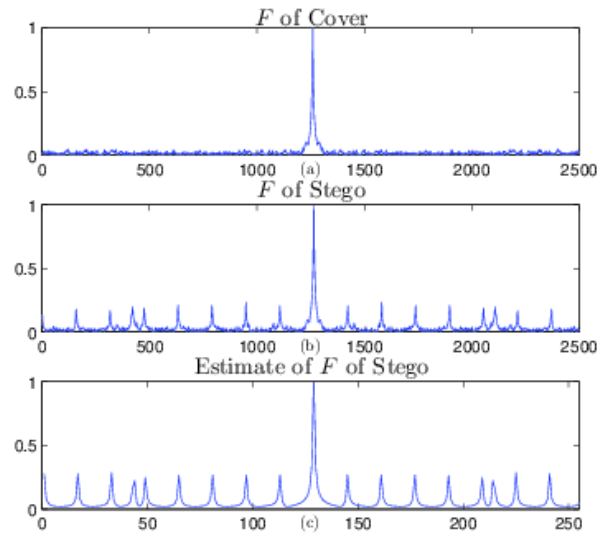


Figure 4: The stego image is obtained by QPJ algorithm using quality pair q_3 and q_{16}. (a) is the F of an original cover image and (b) is the F of the corresponding stego image. (c) is estimated as FFT of (7) for the same quality pair.

$$\mathbf{P} = \overline{\mathbf{E}} - (Median(\overline{\mathbf{E}}) + 3\sigma_{\overline{E}}) \tag{10}$$

$$P_{max} = max(\mathbf{P}) \tag{11}$$

where $Median(\overline{\mathbf{E}})$ is the median filtered $\overline{\mathbf{E}}$ vector and $\sigma_{\overline{E}}$ is the standard deviation of the $\overline{\mathbf{E}}$ vector. Peaks are significantly remains above the $Median(\overline{\mathbf{E}}) + 3\sigma_{\overline{E}}$ line for a stego image as shown in Fig. 5.

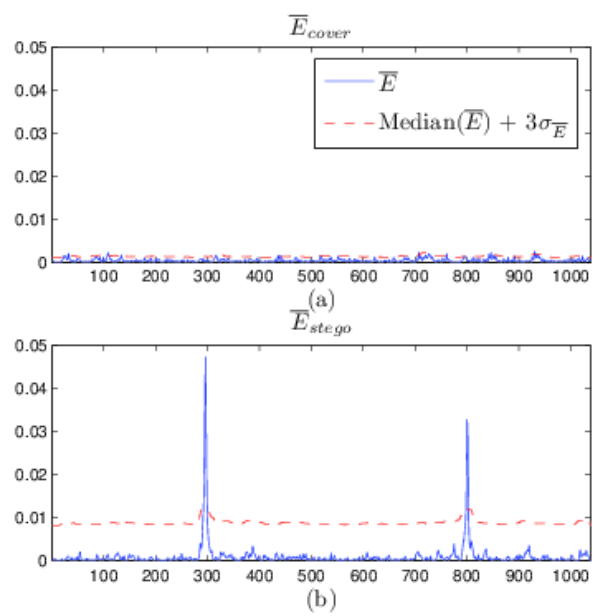


Figure 5: Cropped energy spectral density $\overline{\mathbf{E}}$ of F and $Median(\overline{\mathbf{E}}) + 3\sigma_{\overline{E}}$ line. The parts of $\overline{\mathbf{E}}$ above the red line are considered as peaks. Peak analyze graph of a cover image is shown in (a) and the Peak analysze graph of corresponding to a stego image is shown in (b).

The height of the biggest peak that remains above the $Median(\overline{\mathbf{E}})+3\sigma_{\overline{E}}$ line, P_{max}, is the only feature that is used in the proposed decision algorithm.

D. Detecting the Stego Images

Stego and cover images have significantly different P_{max} values. The Fig. 5 shows that the images which have embedded secret messages using the QPJ algorithm have significant peak amplitudes. Fig. 6 shows the comparison of the P_{max} values of the first 500 stego images and 500 cover images in test data set. Stego images are obtained using $Q_{1,2}=\{95,85\}$ quality factor pair and the corresponding cover images saved with quality factor $Q=100$. As it is seen in Fig. 6 stego images have higher P_{max} values than corresponding cover images. A simple decision method that depends on a predefined threshold successfully reveals which images are the manipulated images by the QPJ algorithm. The image is considered as *Stego* if $P_{max}>\tau$. The threshold value, τ, is decided as the threshold which minimizes the false positive and false negative rates for training image set. In the experiments, first 4000 image is taken as training image set.

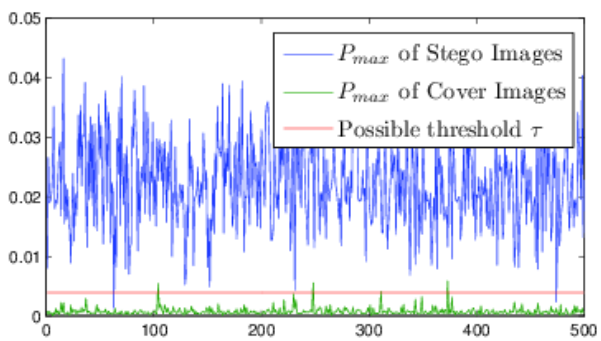


Figure 6: Comparison of P_{max} of 500 stego and 500 cover images. Red line is the possible threshold, τ, to be selected.

IV. Experimental Results

Three different image databases, BOWS [11], BOSSbase [12] and UCID [13] containing 10000, 9073 and 1338 images, respectively, are used in the test stage. Colored images are converted to gray scale images. The experiment is performed for original images and their three different QPJ stego versions. The QPJ steganography applied to the original image sets for 72 different quantization pairs $Q_{1,2}$. In total, 73x20411 images used in the experiments.

We used the first 4000 images of BOSSbase image set to choose a threshold τ that minimizes the equal error rate using both the false positive (FP) and the false negative (FN) rates. FP is defined as incorrectly deciding an image as a cover while the image is actually a stego. FN is defined as deciding an image as a stego while the image is actually a cover. The selected images are embedded with three quality pairs, $Q_{1,2}$. Then the threshold, τ, is calculated as 39×10^{-4} experimentally using this training set containing 4000 images.

The rest of the image data set was used for evaluating the performance of the proposed steganalysis algorithm. The images with $P_{max}\geq\tau$ were considered as stego images while the images have $P_{max}<\tau$ were considered as cover images. It is worth to mention that we only consider cover JPEG images compressed with 100% quality factor in the tests since this is the requirement of the QPJ algorithm to recover the message. As is seen in Fig. 7, the ROC curve of the test stage shows that the detection accuracy of the proposed method is over 99% at equal error rate. The detection accuracy in terms of each quality pair and each data sets is given in Table 1. The detection accuracy rate (DAR) is given in terms of the average value of FN and FP ($DAR=1-\frac{1}{2}(FP+FN)$). Table 1 shows that the proposed targeted steganalysis algorithm successfully defeats the QPJ method over 99% detection accuracy most of the time. The lowest detection accuracy is 95.63% at 95-90 quality pair. There are two reasons for it. The first reason is the image is not corrupted so much because the quality is high. As the authors stated in [4], the highest PNSR value is obtained at 95-90% quality pair which means the message data loss is the highest. And the correct decoding rate is low for this quality pair. The second reason is at this much high quality, quantization value for DC coefficient is close to 1. Or, more precisely $Q_1=2$, $Q_2=3$ for quality pair of 95-90%. Hence, f_ζ has high frequency ripples where the noise has a high frequency as well. The maximum value of the peak is not as obvious as in other quality pairs such as $Q_{1,2}<90$.

In QPJ steganography method, the authors introduce a term Correct Decoding Rate (CDR) which is defined as the ratio of the number of pixels decoded correctly to the total number of pixels in the secret image. Some images having partly absolutely black or have dark pixels, are not good cover images in terms of CDR. So, the QPJ steganography algorithm can not embed the secret with a high CDR for some cover images. In this case, the cover and stego images would be similar since stego images do not contain much information. The proposed steganalysis algorithm failed to detect such problematic stego images which their usage in a steganographic communication is questionable.

Some of the image steganography algorithms allow the user to choose the embedding rate in order to adjust the trade-off between robustness and the amount of information. Nevertheless, the QPJ algorithm does not give such opportunities in practice. Altering the quality factors of JPEG files affects the quality of 8×8 image blocks. In the decoding stage, the image can be examined only block wise to see if the block carries 1 or 0. Thus, in the QPJ algorithm each 8×8 image block can contain only 1 bit of information in practice. So, it is not possible to compare the performance of the

proposed steganalysis algorithm with respect to different embedding rates.

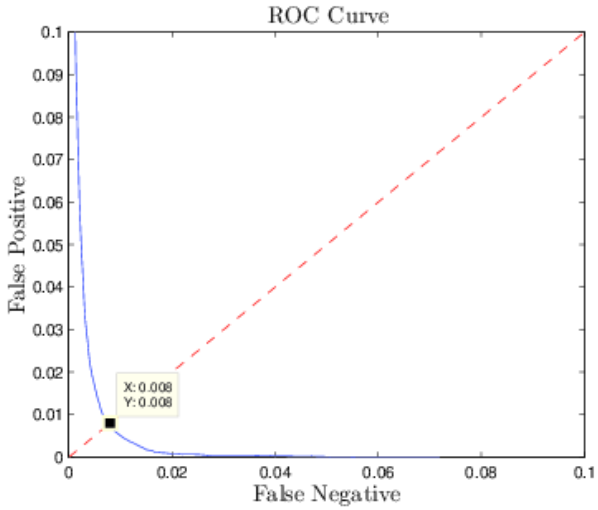


Figure 7: The ROC curve shows that the detection accuracy of the proposed steganalysis algorithm is over 99% at equal error rate.

Table 1: Detection rate (%) for various Q1 and Q2 pairs.

Q2 \ Q1	95	90	85	80	75	70	65	60	55
90	95.63								
85	99.31	98.99							
80	97.53	99.64	99.23						
75	99.73	99.90	99.98	99.72					
70	96.68	99.74	99.48	99.86	99.98				
65	96.85	98.73	99.81	99.97	99.98	99.74			
60	98.43	98.95	99.48	99.91	99.98	99.98	99.62		
55	99.24	99.47	99.58	99.61	100.0	99.80	99.94	99.74	
50	99.74	99.49	99.59	99.34	99.95	99.94	99.78	99.94	99.76
45	98.99	99.77	99.98	99.65	99.97	99.45	99.97	99.83	99.98
40	99.12	99.93	99.92	99.59	99.97	99.69	99.68	99.94	98.77
35	98.53	99.45	99.39	99.94	99.95	99.72	99.30	99.61	99.95

V. Conclusion

In this paper, a targeted steganalysis algorithm which is successfully detecting the QPJ steganography has been proposed. The algorithm reveals the corruption in the dependency of the DC values residing in neighbouring blocks in the DCT domain. It basically shows that unnatural significant peaks appear on the FFT of histogram of the difference array calculated over neighbouring DC coefficients. This scheme is simple because only one feature is extracted for each image. It does not require any neural network or SVM training which are common in many targeted and blind steganalysis algorithms. The detection accuracy rate of the proposed algorithm is over 99%, which is sufficiently high for a targeted steganalysis algorithm. Thus, the stego images generated by QPJ steganography are successfully detected by the proposed steganalysis algorithm.

Acknowledgment

This study was supported by an EPSRC grant to the project Centre for Secure Information Technologies (CSIT) (EP/G034303/1).

References

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st ed. New York, NY, USA: Cambridge University Press, 2009.

[2] C. Cachin, "An information-theoretic model for steganography," in *Information Hiding*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 1525, pp. 306–318.

[3] B. Li, J. Huang, and Y. Q. Shi, "Steganalysis of yass," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 3, pp. 369–382, Sept 2009.

[4] J. M. Guo and T. N. Le, "Secret communication using jpeg double compression" *Signal Processing Letters, IEEE*, vol. 17, no. 10, pp. 879–882, Oct 2010.

[5] T. Pevny and J. Fridrich, "Detection of double-compression in jpeg images for applications in steganography," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 247 –258, June 2008

[6] J. Luk and J. Fridrich, "Estimation of primary quantization matrix in double compressed jpeg images," in *Proc. of DFRWS*, 2003.

[7] A. Popescu and H. Farid, "Statistical tools for digital forensics," in *Information Hiding*, ser. Lecture Notes in Computer Science, J. Fridrich, Ed. Springer Berlin / Heidelberg, 2005, vol. 3200, pp. 395–407.

[8] H. Farid, "Exposing digital forgeries from jpeg ghosts," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 1, pp. 154–160, March 2009

[9] T. Pevn ´ y, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," in *Proceedings of the 11th ACM workshop on Multimedia and security*. New York, NY, USA: ACM, 2009, pp. 75–84.

[10] D. Ruan, G. Chen, E. E. Kerre, and G. Wets, Eds., *Intelligent Data Mining: Techniques and Applications*, ser. Studies in Computational Intelligence. Springer, 2005, vol. 5.

[11] Bows2 original database. [Online]. Available: http://bows2.gipsalab.inpg.fr

[12] Raw image dataset from the boss contest. [Online]. Available: http://boss.gipsa-lab.grenoble-inp.fr

[13] G. Schaefer and M. Stich, "Ucid - an uncompressed colour image database," in *In Storage and Retrieval Methods and Applications for Multimedia 2004, volume 5307 of Proceedings of SPIE*, 2004, pp. 472–480.

The Importance of Keeping Network Devices under Control in Big Networks for Network Forensics

F. Ertam[1], T. Tuncer[2] and E. Avci[3]

[1]Fırat University, Elazig/Turkey, fatih.ertam@firat.edu.tr
[2]Fırat University, Elazig/Turkey, turkertuncer@firat.edu.tr
[3]Fırat University, Elazig/Turkey, enginavci@firat.edu.tr

***Abstract*— Network forensics is to capture, record and analyze security attacks and other problems, which might occur on the network. Network forensics is accepted as a sub-branch of digital forensics. Also, it is possible to consider network device forensics as a sub-branch of network forensics.**

In order to determine whether there is a crime or not, it is not enough to take and scrutinize entire information in the personal computer of suspicious users. The data traffic on the network is significant to be on record before and after the case.

It is extremely important to take necessary security measures on network devices so that those records are not damaged. For the purpose of satisfying the necessities which might arise, the network should always be kept under control of the network administrator –before and after the case of digital forensics-. In addition, any activity without the administrator's knowledge should be prohibited.

Especially, following information is crucial to be recorded in order to keep the network under control:

- **Usage frequency of ports existing in the network devices which are used as switches**
- **The information about whether different devices are in action on the same port at different times or not**
- **Which ports are not used for a long time**
- **Which ports are uplink ports**
- **How many Mac addresses are seen behind the port**
- **The information about vLan (Virtual Local Area Network) numbers on the port.**

Devices connected on the network should be automatically and periodically detected and reported. Besides, being able to show location of connected devices is another issue that facilitates the network management.

Together with so many open-source codes which are practicable for network management, netdisco software is used in order to carry out the processes mentioned above. Tests are executed on a university campus which has 150 manageable switch devices.

***Keywords*— network forensics, network device forensics, network security, open source software, netdisco**

I. Introduction

Digital forensics is accepted as a discipline which is trying to establish standards for collecting, recording, classifying and analyzing the evidence obtained in the form of data. In other words, digital forensics is the data processing technic applied in legal issues [1].

The sub-branches of digital forensics might be listed like that: computer forensics, network forensics, network device forensics, GSM (Global System for Mobile Communications) forensics, social media forensics, GPS (Global Positioning System) forensics [1][2].

Given the rapidly increasing amount of digital crimes, network forensics plays a significant role in the process of analyzing evidence [3].

Network forensics analysis is the process of extracting intrusion patterns and investigating malicious activities conducted over the network[4]

Network Forensics can be considered as tracking, recording and analyzing the local networks, wide area networks or internet network traffic; and accordingly giving necessary information to judicial authorities [5].

The network forensics tools always combine the ability to passively monitor, capture all network traffic, analyze traffic, track down security violations and protect against future violations and attacks. The essential functions of network forensics analysis tool is to capture network traffic, to analyze the traffic according to the user's needs, to discover useful and interesting things about the analyzed traffic [6,7,8].

It is more appropriate to think Network Device Forensics as a sub-branch of network forensics, than thinking it as a sub-branch of digital forensics. Devices like Switch, Hub, Router, Repeater, Bridge, Firewall and even the network card of users, which are existing in the network system, can be thought as network devices.

Those devices are necessary to be configured properly so that information saved on those devices is retrieved correctly.

It is obligatory to for people without permission to accessing network devices. Attempts to fall under the network by connecting different devices without the knowledge of administrator should be blocked [9].

There are many toolkits for building network traffic analysis and statistical event records [10, 11, 12, 13].

Among the available open-source codes, netdisco is frequently used for university campus networks [14][15]. Followings can be detected, scrutinized and reported by

netdisco:

- Port usage information,
- Switches existing in the network,
- vLan and MAC addresses on switching ports,
- which ports on the switch are actively used,
- which ports are used at most,
- which ports are always inactive.

Reporting are done daily, weekly, monthly and annually.

II. Methods and Techniques

A. *The Edge Switch Configuration:*

Before information is gathered by using netdisco software, certain configuration settings are carried out on the edge switches located behind the backbone switch.

Maclocking, Spanningtree and DHCPSNOOPING can be considered to be included in the configuration settings which are to be made before network reporting is conducted [2, 16].

B. *Maclocking:*

Locking the MAC address is made on the switching device so that users do not use multiple devices by linking a seperate switching device or network device to the cable from the switching device of the network system without the knowledge of the system administrator. By this way, only one active device can be connected to each port of the switching device. This situation is shown in Figure 1.

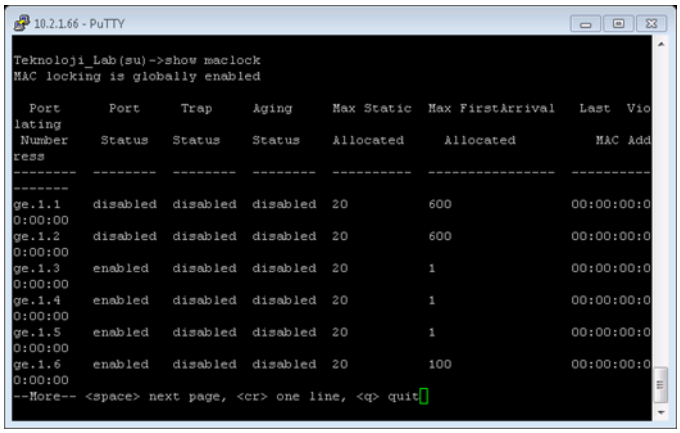


Fig. 1 Maclocking

C. *Spanningtree:*

Spanningtree is activated in order to avoid loops which may occur in the switching device. Therefore, even linking a cable from switching device to the same switching device again doesn't affect the operation of the device.

Otherwise, the switching device goes round in circles and creates an unnecessary network traffic and interfere with the proper operation of the network. The Spantree version which is set for the switching device is shown in figure 2 and RSTP (Rapid Spanning Tree Protocol) version is selected for Spanningtree.

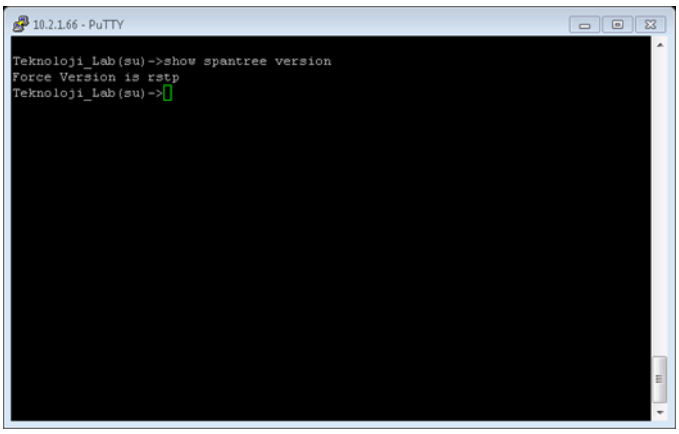


Fig. 2 Spanningtree version

D. *DHCPSNOOPING:*

DHCP is a protocol that allows clients to automatically obtain information, such as IP (Internet Protocol) address, subnet mask, default gateway and DNS address [17]. Thanks to the DHCP, the necessity for defining static IP addresses is eliminated.

To assign a static IP to each user has certain disadvantages. Firstly, as wide networks have thousands of users and assigned IP addresses mustn't conflict with each other, the work should be done very carefully. Considering just this process, it becomes clearly appear that system administrators would have so much trouble, if DHCP was not used.

Another big problem that might occur is the necessity for fixing subnet masks carefully. Users on the same subnet mask must have the same subnet mask. So, a separate IP block must be defined for virtual LAN (vLAN), which is used for system management in wide networks.

Another difficulty of static IP assignment is the requirement for the information about IP block and which local virtual networks are assigned to switching devices that users are connected. For the internet output outside the network, when a static IP address is to be assigned to the existing local virtual network, the gateway IP address must be registered.

In order not to occur problems mentioned above, DHCP servers help users' computers which are linked to the ports of switching devices.

For the purpose of preventing unwanted DHCP servers from working, "DHCPSNOOPING configuration settings" are applied to edge switches where clients are linked to the network. By this way, unwanted situations will be avoided.

Backbone switches and edge switches can be connected each other via the fiber optic cable or the copper cable. The UPLINK port is used for transporting the transmission line by this way and the distribution of transmission on edge switches. Only in UPLINK ports which are assigned with vLAN, DHCPSNOOPING is operated reliably. In all other ports, although a fake DHCP server can be founded on a machine, it is prevented from working via DHCPSNOOPING [4].

Clients in the edge switching device are shown in figure 3. Those clients retrieve IP and Mac address and indicate which vLan ID and port they are associated with.

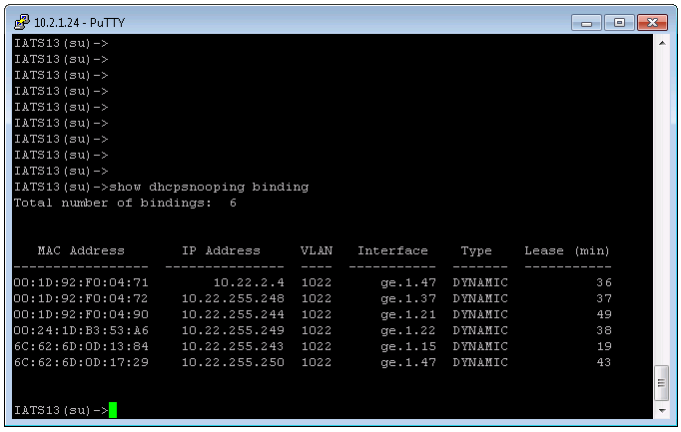


Fig. 3 Dhcpsnooping binding

E. *Open Source Network Management Software:*

Netdisco software is a web-based, open-source network management tool that has been developed since 2003[9]. This software is preferred because it has been developed for a long time and it is suitable for university campuses.

Firstly, the automatic installation script is downloaded from the software's official website. It is installed on a computer whose OS is UBUNTU. After the installation, the required command is entered so that netdisco can discover the network.

The discovery process and its result report are seen in figure 4 and 5. Information about network devices is gathered via SNMP (Simple Network Management Protocol). Accordingly, SNMP settings of devices on the network must be active. Another protocol that may be used is CDP (Cisco Discovery Protocol). The collected data is stored in a database so that it can be supervised via a web-based interface.

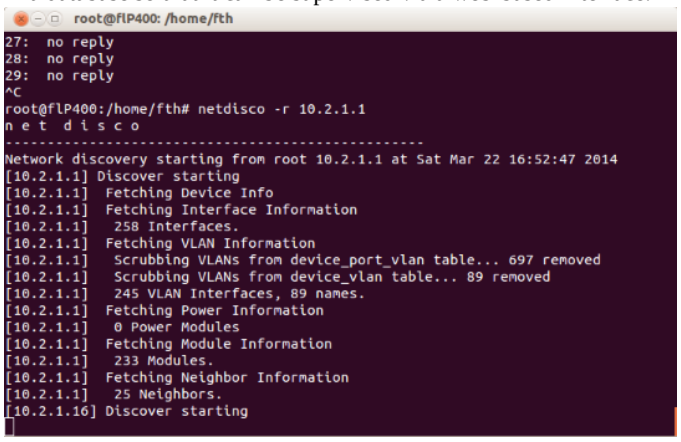


Fig.4 Netdisco discovery

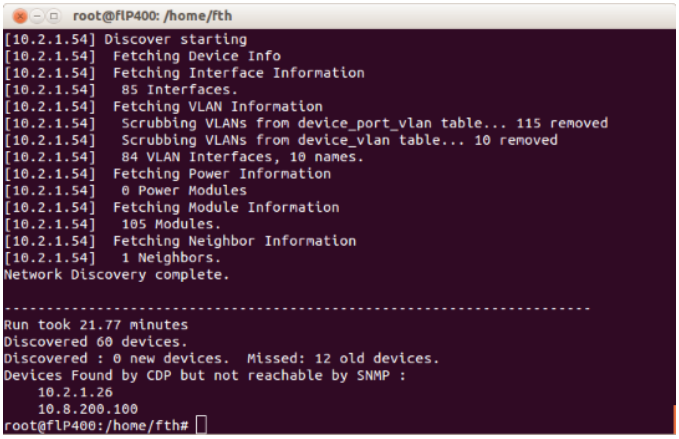


Fig.5 Netdisco, after the discovery of the report

Netdisco software has a web-based interface. Together with its interface, it is possible to list discovered network devices according to their name, firmware version, location and vLan id. This interface is shown in the figure 6.

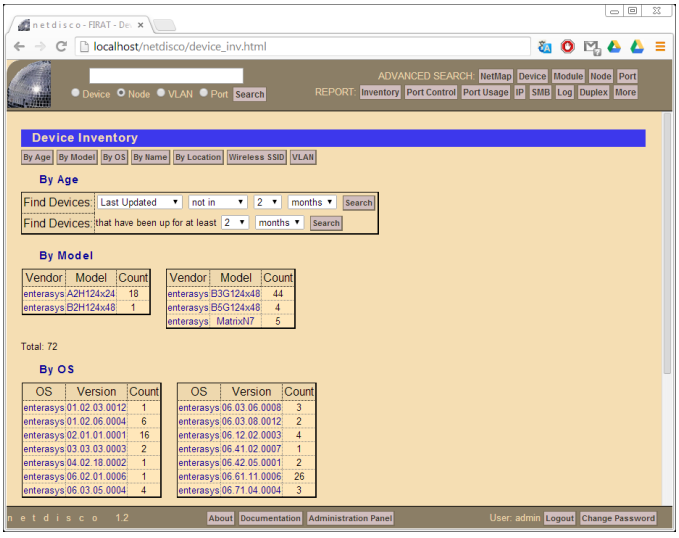


Fig.6 Netdisco Web Interface

According to the data in figure 6, it is seen that 72 pcs Enterasys branded switching devices of different models are discovered. As switching devices bounded as stack have just one IP address, they are seen as one device and they are listed in the module form. Also, switching devices which are connected to the network without the permission of network administrators are detected and reported.

As seen before, one can reach the port's name, speed and vLan information by clicking the link of one of the discovered switches. Also, it is possible to see the MAC address, which is active at that moment or was active before.

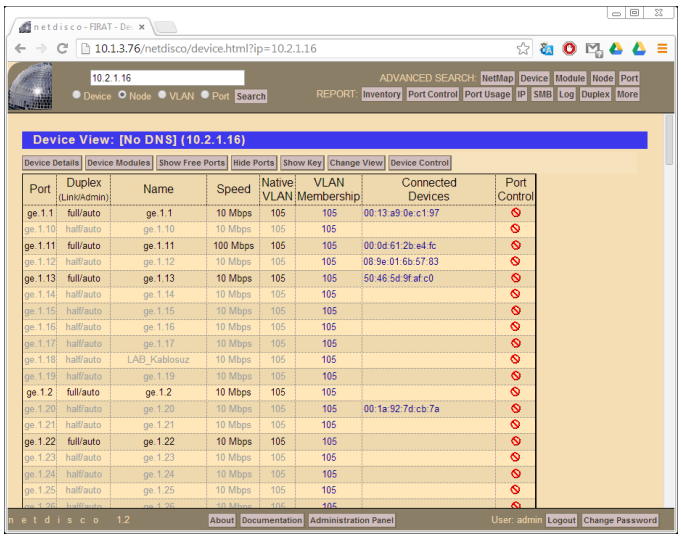


Fig.7 Netdisco Switch Web Interface

When one click on and enter the title "device details", it is possible to list information about the switch's location, MAC address, brand, model and when it was discovered. Also, one can see the modules on the switch.

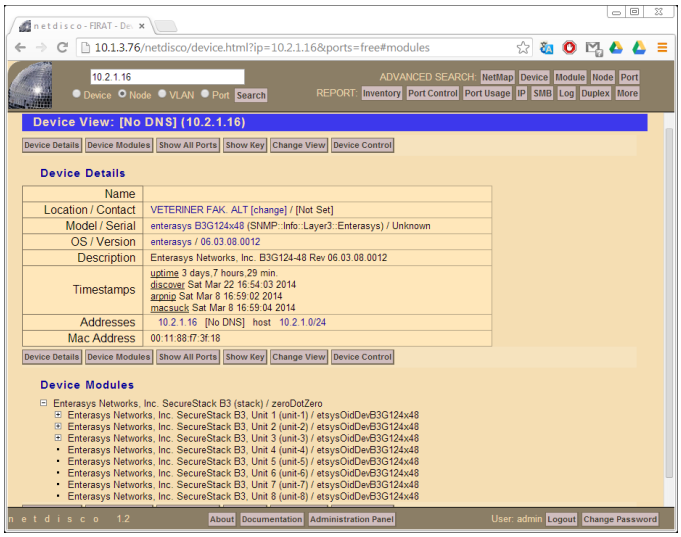


Fig.8 Netdisco Switch Device Details

In addition to current data, it is also possible to report a daily, weekly, monthly or annually information about active devices, how many ports are used, how many ports have recently been used and how many ports have not been used in any switching device within any specific time.

The number of active ports having been used in the last 3 days is shown in figure 9. Similarly, it is possible to obtain information about which switch has the largest number of free port within a desired period of time.

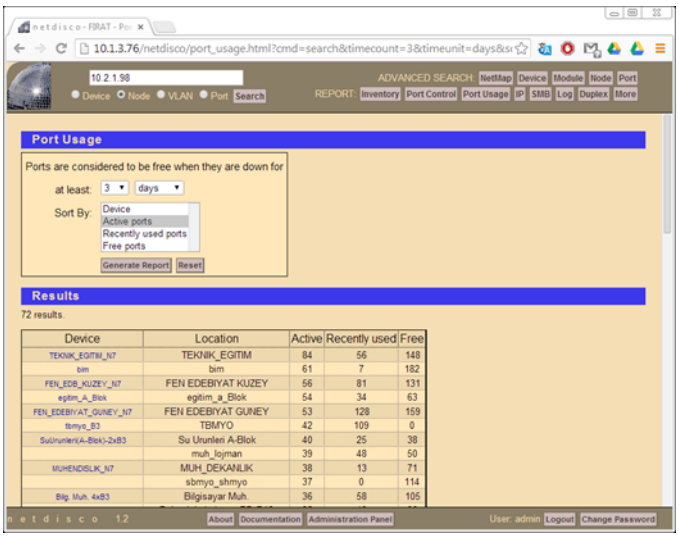


Fig.9 Netdisco Switch Active Ports

In order to automatically and periodically execute the switch discovery and the database update, netdisco commands are provided to work every morning at 8.00. This automatization is done by entering a crontab entry to UBUNTU, which is the OS netdisco is operated on.

It is also possible to create a topology graph based on relative positions of discovered switches by using the netmap option. At the same time, it is possible to search a MAC address and see which ports it was connected to before.

III. Results

In this study, for the purpose of managing and reporting wide networks like universities, an open source network management software is installed on UBUNTU OS and run in a university which has approximately 150 pcs switching devices.

Firstly, DHCPSNOOPING, MACKLOCKING and SPANNINGTREE configurations are applied. Manageable switching devices with IP address located on the university network are discovered with netdisco software.

After the discovery, information, such as which MAC addresses are active, how long they are active, how many ports are not used, is obtained. Although netdisco software by itself is not enough for the network management, it is possible to be used together with log records received from firewall device.

To create a visual network topology by using netdisco software makes network management easier. Network optimization is provided with the supervision of the usage number of ports on the switch.

Knowing which MAC addresses are on ports has a big importance for gathering evidence related to network forensics. As the following conditions creates suspicion, it is possible to have necessary measurements before a legal case happen:

- When there is the same MAC address continuously,
- When a port which has not been used for a long time is connected to the network with a different MAC address,
- Or when a free port is started to be used.

REFERENCES

[1] Daniel L., Daniel L., "Digital Forensic : The Subdisciplines", Digital Forensic for Legal Professions, S17-23, 2011

[2] Fatih Ertam; Türker Tuncer; Engin Avci, Importance of Network Devices and Their Secure Configurations at Digital Forensics, E-Journal of New World Sciences Academy, DOI: 10.12739/NWSA.2013.8.3.1A0349 8 / 3 / 171-181 , 2013

[3] Mohammad Rasmi, Aman Jantan, A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics, Procedia Technology, Volume 11, Pages 540-547, 2013

[4] Saad, S. ; Traore, I., Method ontology for intelligent network forensics analysis, Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on Digital Object Identifier: 10.1109/PST.2010 , Page(s): 7 - 14, 2010

[5] Emmanuel S. Pilli; R.C. Joshi, Rajdeep Niyogi, Network forensic frameworks: Survey and research challenges, Digital Investigation, Volume 7, Issues 1–2, Pages 14-27, 2010

[6] Corey, V.; Peterman, C.; Shearin, S.; Greenberg, M.S.; Van Bokkelen, J.; "Network forensics analysis", Internet Computing, IEEE, Volume: 6 Issue: 6, Page(s): 60 –66 , 2002

[7] Mark Reith, Clint Carr, Gregg Gunsch, "An Examination of Digital Forensic Models", International Journal of Digital Evidence, Volume 1, Issue 3 , 2002

[8] Yanet Manzano and Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", The 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, at the United States Military Academy, June 2001

[9] S.D Jeon, Digital forensic technology tendency and expectation, information policy 13/4, 2006.

[10] S. Ioannidis, K. G. Anagnostakis, J. Ioannidis, and A. D. Keromytis. "xPF: packet filtering for lowcost network monitoring". In Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR), pages 121--126, May 2002.

[11] 10.S. McCanne and V. Jacobson. The BSD packet filter: A new architecture for user-level packet capture. In Proc. of the USENIX Technical Conf., 1993

[12] K. G. Anagnostakis, S. Ioannidis, S. Miltchev, and J. M. Smith. Practical network applications on a lightweight active management environment. In Proceedings of the 3rd International Working Conference on Active Networks (IWAN), pages 101-- 115, October 2001.

[13] Fulvio Risso, Loris Degioanni, An Architecture for High Performance Network Analysis, Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC 2001), Hamm met, Tunisia, July 2001.

[14] https://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html (online 24.03.2014)

[15] http://www.netdisco.org (online 24.03.2014)

[16] Fatih Ertam; Haluk Dilmen; Engin Avci, Investigation The Effect Of Using DHCPSNOOPING In Big Networks, 7th International Advanced Technologies Symposium(IATS'13), 2013

[17] J-H. Wang ; T.L Lee, Enhanced intranet management in a DHCP-enabled environment, Computer Software and Applications Conference, 2002. COMPSAC 2002. Proceedings. 26th Annual International Digital Object Identifier: 10.1109/CMPSAC.2002.1045119, S 893 - 898 , 2002

The Road Map for Digital Forensic Law of Turkey

İ. Baştürk

Prosecutor of Supreme Court, Ankara/Turkey, ihsanbasturk@hotmail.com

***Abstract*— There is no doubt utilization of information technologies in criminal procedure can be an effective tool to protect right to a fair trial which is guaranteed under the European Convention on Human Rights and the Constitution of the Republic of Turkey. In terms of criminal law, digital forensic is a field of the criminal procedure law. In this article I will recommend a roadmap for Turkey in the field of digital forensic which examination of present situation.**

***Keywords*— Digital forensic in Turkey, criminal procedure law, information technologies on criminal procedure, digital evidence, fundamental rights and digital forensic.**

I. GİRİŞ

Bilişim teknolojileri sayesinde ceza muhakemesi hukuku birçok kolaylıklara kavuşmuş; muhakeme işlemleri ağ ortamında veya ağ vasıtasıyla yapılabilir hâle gelmiştir. Ceza muhakemesinde bilişim teknolojilerinden yararlanılmasının Avrupa İnsan Hakları Sözleşmesi'nde ve Türkiye Cumhuriyeti Anayasası'nda da güvence altına alınmış olan "adil yargılanma hakkına" erişilmesinde etkin bir araç olabileceği kuşkusuzdur. Bilişim teknolojilerinden yararlanılarak ceza muhakemesi sürecinin yürütülmesine ilişkin tüm faaliyetler "adli bilişim" olarak adlandırılmaktadır. Bu anlamda, adli bilişim -ceza hukuku yönünden bakıldığında- ceza muhakemesi hukukuna ait bir alandır.[2] Bu itibarla, adli bilişim alanını *Türk Ceza Muhakemesi Hukuku yönünden değerlendirerek* mevcut durumun tespiti ile ihtiyaç duyulan noktalar ortaya konularak Türkiye için bir yol haritası çıkarılacaktır.

II. ADLİ BİLİŞİM

Bilişim teknolojilerinden yararlanılarak ceza muhakemesinin yürütülmesine ilişkin faaliyetler bütünü olan *adli bilişim*, hukuk ile bilişimin kesiştiği çok disiplinli bir alan olarak karşımıza çıkmaktadır. Ceza muhakemesi hukukuyla doğrudan bağlantılı olan adli bilişim alanındaki normların da ceza muhakemesi hukukunda olduğu üzere *demokratik hukuk devletini ve insan haklarını korumaya, bu anlamda adil yargılanma hakkını, delillerin doğrudan doğruyalığını gerçekleştirmeye elverişli, muhakemede sadelik, ucuzluk ve etkinliği sağlayabilecek nitelikte* olması gereklidir.

A. Adli Bilişimin Konusu

Adli bilişimin konusunu *hukuka uygun yollardan elde edilmiş sayısal veriler* oluşturmaktadır. Hangi durumlarda kimlere ait bilgisayar sistemlerinde arama yapılabileceği, bunlara hangi usullerle el konulabileceği, elde edilen verilerden ispat aracı olarak nasıl yararlanılabileceği hususlarının ayrı bir çalışma konusu olduğu kuşkusuzdur.[3]

Bilgisayar sistemlerinde yürütülen faaliyetlerin niteliği gereği, her aşamada gerek bilgisayarlar, gerekse servis sağlayıcıların sistemlerinde çok sayıda iz bırakılmaktadır. İşte suç oluşturan fiillerin delillerinin yani *bilişim aygıtlarından verilerin ortaya çıkartılıp muhakeme süjelerinin müşterek değerlendirilmesine sunulması*, adli bilişimin temel konusunu oluşturmaktadır.

B. Adli Bilişimin Amacı

Ağ ortamının suç işlemek için adeta gizli, gizemli bir yönünün varlığı, bu yolla işlenen suçları giderek arttırmaktadır. "Yeni suç mecrası" olarak da adlandırılabilecek bu ortamdaki suçlulukla etkin mücadele gereği ve delillerini ortaya koyma zorunluluğu, adli bilişimin gelişimini zorunlu kılmaktadır. Sayısal delillerin fiziki olarak elle tutulamadığı ve görülemediği kuşkusuzdur. İşte bu verileri görünür hale getirebilmek ve muhakeme süjelerinin müşterek tartışmalarına açabilmek için bazı bilişim araçları ile yazılımlara ve ayrı bir uzmanlığa ihtiyaç duyulmaktadır. Tam bu noktada adli bilişim karşımıza çıkmaktadır. Adli bilişim prosedürünün amacı, suç ile ilgili olabilecek sayısal delilleri elde etmektir. Bu amaca ulaşmak için kullanılacak yöntemler ise bilgisayar inceleme ve analiz tekniklerdir.

C. Ceza Muhakemesinde Adli Bilişim

1. İşlevi

Ceza muhakemesi süjeleri, *kollektif bir hüküm* ile çözdükleri uyuşmazlığın maddi ve hukuki iki kısmından birincisi olan maddi meseleyi çözebilmek için, gerçeği araştıracaklardır.[4] İşte yargıcın muhakeme sonucunda maddi olayı çözmesine ve böylece bunu sabit görmesine veya görmemesine hizmet eden araçlara "delil" denir.[5] Ceza muhakemesinde maddi hakikat ve serbest kanaat arandığından, mahkemeyi gerçeğe ulaştırabilecek her şey delil olabilir.[6] Ceza muhakemesi hukukunda deliller, ceza uyuşmazlığını oluşturan olayın bir parçasını ispat edebilecek nitelikte ve beş duyu organımızla algılanabilecek maddi bir yapıya sahip olmalıdır.[7] Bu bağlamda, sayısal ortamda bulunan delillerden de ispat faaliyetinde yararlanılabileceği kuşkusuzdur.[8]

Günümüzde adli bilişim, ceza muhakemesinin maddi gerçeğe ulaşma amacının gerçekleştirilmesinde önemli bir

araç durumuna gelmiştir. Bilgisayar sistemleri ile adli bilişim araçlarının sağladığı olanaklardan soruşturmaları hızlandırmak ve arama usullerini otomatikleştirmek için kanun yapıcılar şimdi giderek artan bir şekilde yararlanmaktadırlar.[9] Örneğin, çocuk pornografisi içeren görüntü dosyaları adli bilişim yazılımlarıyla otomatik olarak bulunarak şüphelinin bilinen görüntüleriyle karşılaştırılabilmektedir.[10] Bu itibarla, günümüzde suçlulukla mücadelede adli bilişim tartışmasız bir öneme sahiptir.

Adli bilişim bir prosedür, faaliyet olup; bizatihi bir "delil" değildir. Adli bilişim, delil içeriğinin öğrenilmesi ve değerlendirilmesi sürecidir. Delil olan şey ise, ispat faaliyetinde kullanılacak olan ve adli bilişim teknikleriyle toplanarak öğrenilmek istenen sayısal verilerdir.

2. Veri Kavramı

Sayısal verilerin ayırt edici niteliği bir bilgisayar tarafından işlenmiş ve/veya saklanmış olmalarıdır. Adli bilişim sürecinin konusunu oluşturan bu sayısal verileri ifade etmek için "elektronik delil,[11] elektronik olarak işlenmiş ve saklanmış veri,[12] sayısal delil, elektronik olarak saklanmış veri, bilgisayar verisi" gibi çeşitli kavramlar kullanılmaktadır. Çalışmamızda Avrupa Konseyi Siber Suç Sözleşmesi'nde (SSS-Sözleşme)[13] yer verilen ve bilgisayar programlarını da kapsayan *"bilgisayar verisi (computer data)"* terimini tercih ettiğimizi belirtmek isteriz.

Bilgisayar verisi, ceza muhakemesinde ispat faaliyetinde yararlanılacak ve sayısal ortamda bulunan, bir bilgisayar tarafından işlenmiş veya saklanmış her türlü bilgi olarak ifade edilebilir.

3. Sayısal Delillerin Hukuki Niteliği

Ceza muhakemesi hukukunda uyuşmazlığı oluşturan olayın bir parçasını ispat ederek muhakeme sürecinde maddi hakikate ulaşılmasının aracı delillerdir. Ceza muhakemesi hukukunda *delil serbestisi ilkesi* geçerli olup, bu ilke her şeyin delil olabileceği ve her şeyin her şeyle ispatlanabileceği anlamını taşımaktadır.[14] Belirtilen serbestinin varlığı yanında, delillerin taşıması gereken bazı özellikler vardır. İspat aracı olabilecek deliller, hukuka aykırı olmamak kaydıyla; gerçekçi, akılcı, olayı temsil edici ve ortak (müşterek) algılanabilecek nitelikte olmalıdır.[15]

Delil olabilme özelliklerini taşıyan ve elektronik ortamda bulunan verilerin de maddi gerçeğe ulaşmak anlamında bir delil aracı olabilecekleri şüphesizdir. Ancak bilgisayar verileri tanık, sanık, tanık ve sanıktan başka kişilerin açıklamaları, belgeler gibi -tek başına- bir olguyu ispatlayabilecek güce sahip değildir.[16] Bilgisayar verilerinin ceza muhakemesi hukukunda "belirti" niteliğinde kabul edilmeleri gerekmekte olup, bu yönüyle keşif konusu oluşturacakları açıktır.[17] Klasik anlamda keşfe nazaran bazı özellikler göstermekle birlikte adli bilişim; *konusunu bilgisayar verilerinin oluşturduğu bir keşif türü* olarak nitelendirilebilir.[18] Adli bilişim ile elektronik keşif birbirinin ayrılmaz parçası olup, elektronik keşif, dört farklı veri (data) çeşidini kapsamaktadır: Aktif, kopya (replicant), arşiv ve artık (residual) veri.[19] Keşif, var olan durumun ve suç delillerinin tespitine de yaradığından, delillerin kaybolmamasını sağlar. Bu nedenle keşif, aynı zamanda bir ceza muhakemesi tedbiri işlevini de görmektedir.[20]

Ceza muhakemesinde ispat faaliyetinde başvurulacak tüm delillerde olduğu gibi, adli bilişim prosedürü sonucu elde olunacak sayısal delillerin de tüm ceza muhakemesi süjelerinin müşterek (ortak) algılamasına sunulabilecek nitelikte olmaları gereklidir. Ceza muhakemesi hukukunda ancak duruşmaya getirilen ve duruşmada taraflarca ortak olarak algılanabilecek ve üzerinde tartışılabilecek delillerin hükme esas alınabileceği ilkesi karşısında, sayısal delillerin de bu tartışmayı mümkün kılacak şekilde bulunması zorunluluğu vardır. Bu anlamda iz, eser ve delil niteliğindeki verilerin de bulundukları yerden çıkarılarak muhakeme süjelerinin müşterek değerlendirmesine sunulmaya elverişli ortamlara aktarılması gereklidir.

4. Sayısal Delillerin Bütünlüğünün Korunması Problemi

Sayısal delillerin nitelikleri gereği en önemli problem, doğruluklarının ispatlanması sürecinde yaşanmaktadır. Gerçekten de sayısal delilin kolaylıkla değiştirilebileceği gerçeği karşısında, ceza muhakemesinde ispat aracı olabilecek sayısal delillerin doğrulukları kuşkudan uzak olmalıdır. Ceza muhakemesinde kuşkunun olduğu yerde ispattan söz edilemeyecektir. Bu amaçla ilk olarak ABD'de 1993 yılında *"sayısal delilin doğruluğu (bütünlüğü)"* bir davada tanımlanmıştır. Buna göre, *elektronik doğruluk (bütünlük)*, yetkili bir kaynak tarafından elde edilip muhafaza altına alındığı veya depolandığı zamandan beri (yetkisiz) herhangi bir tarzda değiştirilmemiş olan elektronik delili anlatır.[21] Ülkemizde yürürlükte olan yasal düzenlemelerde belirtilen şekilde bir ilke yer almamakta ise de ceza muhakemesi hukukunun genel ilkeleri çerçevesinde soruna yaklaşıldığında, ispat aracı olabilecek sayısal delilin ilk niteliğinin "doğruluğun (bütünlüğün) kuşkuya yer vermeyecek biçimde belirlenebilirliği" olduğu tartışmasızdır.

Sayısal delillerin bütünlüğünün korunmasının temyiz mahkemesi (Yargıtay) kararlarında da vurgulandığı görülmektedir.[22]

III. TÜRK CEZA ADALET SİSTEMİNDE ADLİ BİLİŞİM KURALLARI

A. Ceza Muhakemesi Hukukundaki Adli Bilişim Normlarının Değerlendirilmesi

"Bilgisayarlarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve elkoyma" başlıklı 134. madde, adli bilişim konusunda Türk Ceza Muhakemesi Kanunu'nda (CMK) yer verilen "tek kural" niteliği taşımaktadır. *"Genetik inceleme sonuçlarının gizliliği"* başlıklı CMK'nın 80. maddesi ve telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucu elde edilen iletişim içeriklerinin yok edilmesine ilişkin 37/3-4. maddesi, kişisel verilerin gizliliği ve korunmasına ilişkin bazı kurallar getirmekle birlikte, doğrudan adli bilişim alanına ilişkin değildir.

CMK'nın 134. maddesiyle bir "koruma tedbiri" olarak öngörülen, bilgisayarlarda, bilgisayar programlarında ve

bilgisayar kütüklerinde arama, kopyalama ve elkoyma tedbirinin, genel olarak SSS ile uyumlu hükümler taşıdığı söylenebilir. Mevcut norm -uygulamadan doğan sorunlar dışında- adli bilişim sürecinin uzaması nedeniyle yapılacak arama işlemlerinde elkoymaya imkân tanınmaması sebebiyle işlevsiz kaldığı; diğer taraftan savunma hakkını kısıtlayıcı yönleri bulunduğu gerekçesiyle haklı olarak eleştirilmektedir.[23] Diğer taraftan adli bilişime ilişkin bu koruma tedbirine, belirli bir ağırlık ölçüsü aranmaksızın tüm suçlar için başvurabilmek mümkündür. Halbuki, temel hak ve özgürlüklere ciddi müdahale oluşturan bu tedbire ancak belirli ağırlıktaki suçlar söz konusu olduğunda başvurulabilmelidir. Bu itibarla adli bilişim alanındaki esas norm temel hakların korunması bakımından yeterli güvenceyi taşımamaktadır.

B. Ağ ve Bulut Bilişim Ortamlarında Adli Bilişim Prosedürünün Yürütülmesi ve Hukuki Problemler

1. Ağ Ortamı ve Adli Bilişim

Bilişim ağları ortamında delil elde etmek, üzerinde veri depolayan sayısal cihazlardan delil elde etmeye nazaran bazı özellikler göstermektedir. Ağ ortamında suçlulukla mücadele etmenin en büyük güçlüklerinden birisi, faili teşhis etmek ve suç teşkil eden fiilin kapsamı ile etkilerini değerlendirmektir. Bir diğer sorun, birkaç saniyede değiştirilebilen, taşınabilen ya da silinebilen elektronik verilerin geçici niteliğidir.[24] Diğer yönden, ağ ortamı söz konusu olduğunda -kural olarak- hemen ulaşabileceğimiz, maddi olarak elde tutulabilen bir sayısal cihaz bulunmamakta, deliller ağda servis sağlayıcıların sistemlerinde bulunmaktadır. Ayrıca, bir servis sağlayıcının sunucu bilgisayarlarını yerinden alıp laboratuar ortamına götürmek de mümkün olmayacaktır. Ağ aracılığıyla işlenen suçlarda hareket ve netice Dünya'nın farklı ülkelerinde gerçekleşebilmektedir.[25] Pratikte birçok zaman kullanıcının bir ülkede bulunduğu, servis sağlayıcıların da farklı ülkelerde olduğu düşünüldüğünde, adli bilişim prosedürünün kapsamı daha iyi anlaşılabilecektir. İşte bu nedenlerle verilerin bulunduğu/elde edileceği kaynağın özellikleri itibarıyla ağ ortamından veri elde etmede adli bilişim aşamaları da farklılık göstermektedir.

Ağ ortamında *sayısal delillere ulaşmak için bazı katmanlar*dan söz edilmektedir, bunlar:

1) Saklama, biriktirme ve dökümantasyon,
2)Sınıflandırma, karşılaştırma ve ferdileştirme,
3) Yeniden kurma (inşa)
katmanlarıdır.[26]

Adli bilişimin belirtilen katmanlarının gerçekleştirilebilmesi için, İnternet servis sağlayıcılarının verileri ve kayıtları önem taşımaktadır. Ağ ortamından elde edilecek verilerin sonlanmış veya devam etmekte olan bir iletişime ait verilerden oluşacağı düşünüldüğünde, bu verilerden hangilerine ispat aracı olarak başvurulabileceğinin saptanmasında *servis sağlayıcılara yüklenen sorumluluklar* belirleyici hale gelmektedir. İnternet servis sağlayıcıların "yükümlülükleri kapsamında" tuttukları kayıtlardan adli bilişim sürecinde yararlanılabileceği şüphesizdir. Bu bağlamda, *gizlilik haklarının özüne dokunmayacak biçimde ve orantılılık ilkesi gözetilerek* kayıtların tutulabileceği ve kullanılabileceği hatırdan çıkarılmamalıdır. Bu konuda Alman Federal Anayasa Mahkemesi'nin 2 Mart 2010 tarihli kararında telefon ve İnternet ağı verilerinin yığın depolanması yönteminin Anayasaya aykırı olduğu sonucuna ulaştığı halen hafızalarımızdadır.[27]

2. Bulut Bilişim Ortamı ve Adli Bilişim

Bulut bilişim *(Cloud computing)* veya işlevsel anlamıyla çevrim içi bilgi dağıtımı; bilgisayarlar arasında temel kaynaktaki yazılım ve bilgilerin bilgisayar ağları üzerinden paylaşımının sağlanarak verilerin diğer bilgisayarlar üzerinden kullanılması imkanı sağlayan hizmetlerin genel adıdır.[28] Bu hizmetin bulut sözcüğü ile ifade edilmesinin nedeni, verilerin depolandığı konum itibariyle kullanıcının başının üstünde adeta bulut gibi durması ve ihtiyaç duyulduğunda yer, zaman ve aygıttan bağımsız olarak çağrılarak kullanılmasına imkan tanımasıdır. İlk başlarda hizmet sağlayıcılar tarafından yedekleme amaçlı olarak kullanılmış olan bulutlar zaman içinde yaygınlaşarak; kurulumu kolaylaştırmak, bakım gereksinimlerini azaltmak ve IT maliyetlerini düşürmek gibi avantajlı yönleriyle tercih edilir hale gelmiştir.[29]

Bulut bilişim hizmetinden yararlanılan durumlarda, klasik anlamdaki arama, kopyalama ve el koyma tedbirlerinin nasıl uygulanacağı tartışılmalıdır. Çünkü, bulut hizmetinden yararlanıldığı durumlarda tedbire konu oluşturan veriler kişisel bilgisayarlarda değil, bulut servis sağlayıcıların sistemlerinde saklanmakta, barındırılmaktadır. Bu anlamda bakıldığında, CMK'nın 134. maddesi, *"bilgisayar"* sözcüğüne *"computer"* sözcüğü karşılığı olarak dar anlamıyla yer vermiş iken; genel olarak bu maddeyle paralel düzenlemeler getiren Adli ve Önleme Aramaları Yönetmeliği[30] 17. maddesiyle *"bilgisayar ağları, diğer uzak bilgisayar kütükleri ve çıkarılabilir donanımları"* da kapsamına almıştır. SSS ise, belirtilen tüm aygıtları kapsayacak biçimde *"bilgisayar sistemleri"* ve *"bilgisayar verileri"* terimlerini isabetli olarak tercih etmiştir.

Bilindiği üzere, değişik biçimlerdeki uzaktan adli bilişim yazılımları ve özellikle bunların olası fonksiyonları (arama, kaydetme, kimlik belirleme, mekan izlemeye yönelik bir kamera veya mikrofonu aktif hale getirme) tartışılmaktadır.[31] Bu bağlamda Alman hukukunda, terör suçu ile ilgili inceleme ve araştırmalarda federal polise *bilgisayar içinde uzaktan arama yapma* yetkisi tanıyan normun Alman Anayasa Mahkemesi tarafından iptal edildiği hatırlanmalıdır.[32]

3. Uluslararası İşbirliği İhtiyacı

Suç teşkil eden fiile ilişkin verilerin bulut servis sağlayıcının sisteminde veya ağda tutulması durumunda ulusal sınırlar dışında da tedbir uygulanabilir mi sorusu cevaplanmalıdır. CMK, bilgisayar ağlarında arama konusunda da bir düzenleme getirmemiştir.[33] Sadece iletişim söz konusu ise, CMK'nın 135 vd. maddelerine başvurulabilir; ama iletişim yoksa bilgisayar ağlarında arama yapılabilmesi bakımından özel bir norma ihtiyaç duyulmaktadır.[34]

SSS'nin 19/1. maddesinde *"Taraflardan her biri, yetkili mercilerinin ulusal sınırları içinde aşağıdakileri arama ..."* yetkisinden söz edilerek, Sözleşme'deki *tedbirlerin sadece ulusal sınırlar içinde uygulanabileceği* açıkça ifade

edilmektedir. Verilerin hangi andan itibaren ulusal sınırlar içinde olduğunun kabul edileceği konusu ise Sözleşmeye Taraf Devletlerin kendi ulusal hukuk sistemlerine bırakılmıştır.[35] Yine SSS'nin 19. maddesinin gerekçesinde de, "b*u maddede, devletlerin olağan yasal yardımlaşma kanallarından geçmek zorunda kalmadan başka devletlerin ulusal sınırları içinde bulunan verileri aramasına ve bunlara el koymasına imkân tanıyan "sınır ötesi arama ve elkoyma" konusuna değinilmemektedir. Bu konu, aşağıda, uluslararası işbirliğiyle ilgili Bölümde ele alınmıştır"[36] ifadeleriyle* konu açıklanmıştır. Bu itibarla ulusal sınırlar dışında tedbir uygulanabilmesi *SSS, uluslararası adli yardım antlaşmaları ve Türk Ceza Kanunu'nun (TCK) ulusal yetki kuralları çerçevesinde* gerçekleştirilebilecektir. Diğer taraftan, elektronik ortamdaki ulusal yetki kurallarının belirlenerek bilgisayar ağlarında tedbir uygulanmasına yönelik hukuki dayanağın sağlanması öncelik taşımaktadır.

Sonuçta, ağ ortamında ve bulut bilişim ortamında adli bilişim prosedürünün yürütülmesine ilişkin somut normlara ve bu alanda uluslararası hukuki işbirliği kurallarına olan ihtiyaç da ortaya çıkmaktadır. Türkiye Cumhuriyeti Devleti SSS'ni imzalamış ise de usulüne uygun şekilde onaylayarak Anayasa'nın 90/son maddesi gereğince bir iç hukuk metni haline getirmesi gerektiği kuşkusuzdur.[37] Aksi durumda uluslararası yardımlaşmaya ilişkin kuralların işletilmesi güç gözükmektedir. Öte yandan, SSS'nin yürütülmesinde de ülkelerin sahip olduğu farklı hukuki ve teknik kapasiteler ile anlayışlar dolayısıyla türlü güçlüklerin yaşandığı bilinmektedir. Bu anlamda, suçun ortaya çıkmasından sonra cezalandırılmasına yönelik klasik anlayışın yetersiz kalması kaçınılmaz olup, diğer tedbirlerin dışında, devlet-özel sektör işbirliğine, bireyler ve şirketlerin kendilerini koruyucu önlemler geliştirmesine, etkili bir etik eğitime dayalı, suçun önlenmesine yönelik bir modele önem verilmesi tavsiye edilmektedir.[38]

C. Adli Bilişim ve Kişisel Verilerin Korunması

Adli bilişimin konusunu oluşturan delillerin, kişisel veri içermesi olasıdır. Bu sebeple, adli bilişim safhalarında kişisel mahremiyetin korunması gerektiği tartışmasızdır.

CMK'da "kişisel verilerin korunması amacına yönelik" bazı ilkelerin benimsendiği görülmektedir. Gerçekten, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi esnasında elde edilen verilerin yok edilmesi gereği (md.137/3); genetik inceleme sonuçlarının gizliliği (md. 80); sanığa veya mağdura ait kişisel verilerin yer aldığı belgelerin açıkça istemeleri halinde kapalı oturumda okunmasına mahkemece karar verilebilmesi (md. 209/2) CMK'nın kişisel verilerin korunmasını amaçladığı kurallardan başlıcalarıdır.

CMK'nın belirtilen normların varlığına rağmen, kişisel verilerin korunmasına dair bazı temel güvencelerden yoksun olduğu dikkat çekmektedir. Öncelikle, *şüpheliden elde edilen verilerin imha edilmesi konusunda* CMK'da hiçbir bir kural getirilmemiş olduğunu ifade etmeliyiz. Şöyle ki şüpheli hakkında kovuşturmaya yer olmadığına karar verilmesi veya davanın beraat hükmüyle sonuçlanması hâlinde, elde edilen verilerin imha edilmesi gereği konusunda CMK'da bir hüküm bulunmamaktadır. İkinci olarak, SSS'nin 19/3-d maddesindeki "verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesi tedbiri" de CMK'da yer almamaktadır.[39] Bu sebeple özellikleri gereği başlı başına suç oluşturabilen (örneğin, çocuk pornografisi içeren veriler gibi) veya bulundurulması dahi tehlike oluşturan verilerin (örneğin, virüs programları veya bomba imalatına dair veriler gibi) suç soruşturmasında elde edilmesi durumunda ne yapılacağı konusunda CMK'da bir çözüm sunulmamaktadır. Bu itibarla, verilerin imhası ile erişilemez, kullanılamaz hale getirilmesi ya da silinmesi tedbirine Türk Ceza Adalet Sisteminde acilen ihtiyaç duyulduğunu belirtmeliyiz.[40]

D. UYAP Bilişim Sisteminin Yasal Dayanağı ve Problemler

Ulusal Yargı Ağı Projesi (UYAP) bilişim sistemiyle; yargı birimlerinde entegrasyon, bağlı ve ilgili kuruluşlarda adalet hizmetlerinin daha etkin ve verimli şekilde yürütülmesi, iş süreçlerinin hızlandırılması ve elektronik arşivin oluşturulması amaçlanmıştır.[41] Günümüzde UYAP bilişim sistemi Türk yargısı için vazgeçilmez bir konumdadır. Dava dosyaları dahi elektronik ortamda "e-dosya"[42] olarak düzenlenmeye başlanmış, muhakeme tamamıyla bilişim ortamında yürütülebilir hâle gelmiştir.

CMK'nın 38/A maddesiyle her türlü ceza muhakemesi işlemlerinde UYAP sistemi kullanılacağı, bu işlemlere ilişkin her türlü veri, bilgi, belge ve kararın bu sistem vasıtasıyla işleneceği, kaydedileceği ve saklanacağı ilkesi getirilmiştir. Ancak, bu normun şu noktalarda problem doğurma potansiyeli taşıdığı düşüncesindeyiz:

1.Söz edilen normdaki "*Her türlü ceza muhakemesi işlemlerinde* Ulusal Yargı Ağı Bilişim Sistemi (UYAP) *kullanılır.* Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır" şeklindeki ifade biçimi ceza muhakemesinde UYAP bilişim sisteminin kullanımın adeta zorunlu bir unsura dönüştürmektedir. Belirtilen düzenlemenin ifade bozukluğu içermesi sebebiyle bu şekilde istenmeyen bir sonuca yol açıldığı kanaatindeyiz. Şöyle ki; bu normdaki ifade şekli UYAP sistemi dışında *fiziki ortamda hiçbir ceza muhakemesi işlemi yapılmasına* izin vermemektedir. Halbuki olması gerekenin; yargı mercilerine seçim hakkı tanıyacak şekilde veya olası teknik imkansızlık vb. durumlarda muhakemenin fiziki ortamda da yürütülebilmesi olduğu kuşkusuzdur. Bu itibarla, belirtilen normda "Her türlü ceza muhakemesi işlemlerinde Ulusal UYAP *kullanılabilir"* şeklinde bir düzenlemenin tercih edilmesi gerektiği düşüncesindeyiz.

Öte yandan CMK'nın söz edilen normunun bu emredici ifadesi karşısında, "fiziki ortamda yürütülen muhakeme işlemlerinin hukuka aykırı olacağı" sonucu akla gelebilmektedir. Gerçekten, söz edilen maddenin, "muhakemenin fiziki ortamda yürütülmesine imkan tanıyan" CMK'nın 35/1, 52 ila 60, 147 ile 148. maddeleri karşısında *özel ve sonraki norm* olduğu kuşkusuzdur. Bu itibarla, "CMK'nın 38/A maddesi lafzıyla yorumlandığında" *her türlü ceza muhakemesi işlemi* UYAP sistemi kullanılarak yürütülecek; bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar UYAP vasıtasıyla işlenecek, kaydedilecek ve saklanacaktır. Dolayısıyla *UYAP ortamında yapılmayan muhakeme işlemlerinin hukuka aykırılığı* gündeme gelecektir.

2. İkinci olarak, CMK'nın 38/A maddesindeki ceza muhakemesinde UYAP bilişim sistemi kullanılmasını zorunlu kılan normun aynı Kanunun diğer bazı ilkeleriyle de çeliştiğini belirtmeliyiz. Örneğin, CMK'nın 219/1. maddesi; "*duruşma için tutanak tutulacağı*, tutanağın mahkeme başkanı veya hâkim ile zabıt kâtibi tarafından imzalanacağı" hükmünü içermektedir. Yine CMK'da yer verilen "ifade veya sorgu bir tutanağa bağlanır. Bu tutanakta aşağıda belirtilen hususlar yer alır" (md. 147/1) kuralları *hep fiziki ortamda ceza muhakemesi işlemlerinin yürütülmesine ilişkin* ifadeler içermektedir. Anlaşıldığı üzere duruşma tutanağı düzenlenmesinden söz eden bu normların *ceza muhakemesinin fiziki ortamda yapılması varsayımı*ndan hareket ettiği kuşkusuzdur. Yine CMK'nın 219. maddesinde yer verilen "…işlemlerin teknik araçlarla kayda alınması halinde, bu kayıtlar vakit geçirilmeksizin *yazılı tutanağa dönüştürülerek* mahkeme başkanı veya hâkim ile zabıt kâtibi tarafından imzalanması gerektiği…" yolundaki kural iyice zihinleri karıştırmakta; elektronik ortamda yapılan işlemlerin dahi tutanağa bağlanması kuralını getirerek, elektronik ortamın tüm avantajlarını hiçe saymaktadır.

Kısacası, CMK'nın belirtilen fiziki ortama ilişkin normlarıyla aynı Kanun'un 38/A maddesi karşılaştırıldığında; muhakemenin birbirinden farklı biçimlerde (ilk grup normlar fiziki ortamda; 38/A maddesi ise elektronik ortamda) yürütülmesinden söz ederek bir çelişki ortaya çıkmaktadır. Her ne kadar CMK'nın 38/A maddesinin sonraki ve özel norm olduğu düşünülebilecek ise de temel amacı insan hak ve özgürlüklerini korumak olan ceza muhakemesi hukukunda böyle çelişkilere yer olamayacağı kuşkusuzdur. Bu itibarla, CMK'nın 38/A maddesindeki söz edilen "emredici" nitelikteki ifadenin yargı mercilerine "seçimlik hak tanıyıcı" biçime dönüştürülmesinde yarar bulunmaktadır. Böylelikle ceza muhakemesinde adli bilişim sürecinin uygulanmasına dair hukuki altyapıya ilişkin kuşkular ortadan kalkacaktır.

IV. SONUÇ

Suçlulukla mücadelede adli bilişim tartışmasız bir öneme sahiptir. Bu itibarla, adli bilişim alanını *Türk Ceza Muhakemesi Hukuku yönünden değerlendirerek* bulunulan durumun tespiti ile ihtiyaç duyulan eksiklikler ortaya konularak Türkiye için bir yol haritası çıkarıldığında dikkat çeken konular şöyle sıralanabilir:

1. *"Sayısal delilin doğruluğu (bütünlüğü)"* ilkesi yasal düzenlemelerde yer almamakta ise de ceza muhakemesi hukukunun genel ilkeleri çerçevesinde konuya bakıldığında, ispat aracı olabilecek sayısal delilin ilk niteliği *doğruluğun (bütünlüğün) kuşkuya yer vermeyecek biçimde belirlenebilirliğidir*. Nitekim temyiz mahkemesi (Yargıtay) uygulamalarında da sayısal delillerin doğruluğu (bütünlüğü) ilkesinin öneminin vurgulandığını görmekteyiz.

2. *"Bilgisayarlarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve elkoyma"* başlıklı 134. madde, adli bilişim konusunda CMK'da yer verilen "tek kural" niteliği taşımaktadır. Genel olarak SSS ile uyumlu hükümler taşıdığı söylenebilecek olan bu norm, adli bilişim sürecinin uzaması nedeniyle yapılacak arama işlemlerinde elkoymaya imkân tanımaması ve savunma hakkını kısıtlayıcı olduğu gerekçesiyle eleştirilmektedir.

3.CMK md. 134'deki temel hak ve özgürlüklere ciddi müdahale oluşturan tedbire ancak belirli ağırlıktaki suçlar söz konusu olduğunda başvurulabilmesi gerekli iken hafif olarak adlandırılabilecek suçlar için dahi başvurabilmesi mümkündür. Bu durum, temel hak ve özgürlükler yönünden bir güvencesizlik oluşturmaktır.

4. CMK'nın 134. maddesinde yer verilen tedbire başvurabilmek için aranacak şüphe derecesi ve bilgisayar sistemlerine el konulması durumunda şüpheliye yedeklenen verilerin bir kopyasının verilmesi zorunlu tutulması kabul edilmiştir. 2012 yılında gerçekleşen bu değişiklikle adli bilişim alanında temel hakların korunması bakımından olumlu bir adımdır.

5. Ağ ortamından delil elde ederek yürütülecek adli bilişim faaliyetinde servis sağlayıcıların "yükümlülükleri" önem taşımaktadır. Bu bağlamda, gizlilik haklarının özüne dokunmayacak biçimde ve orantılılık ilkesi gözetilerek kayıtların tutulabileceği ve kullanılabileceği hatırdan çıkarılmamalıdır.

6. Ağ ve bulut bilişim ortamında adli bilişim prosedürünün yürütülmesine ilişkin somut normlara ihtiyaç duyulmaktadır. Bu anlamda Türkiye Cumhuriyetinin bir an önce SSS'ni usulünce onaylaması gereklidir. Öte yandan, SSS'nin yürütülmesinde yaşanan güçlüklerin aşılması için, suçun ortaya çıkmasından sonra cezalandırılmasına yönelik klasik anlayış yetersiz kalmaktadır. Bu sebeple, diğer tedbirlerin dışında toplumun tüm kesimlerinin işbirliğine dayanan, koruyucu önlemler geliştirilmeli, etik eğitime dayanan suçun önlenmesine yönelik bir model benimsenmelidir.

7. CMK'da "kişisel verilerin korunması amacına yönelik" bazı ilkeler benimsendiği halde bazı temel güvencelerin bulunmadığı dikkat çekmektedir. Örneğin, şüpheliden elde edilen verilerin imha edilmesi konusunda hiçbir bir kural mevcut değildir. Yine belirli nitelikteki verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesi tedbirine de yer verilmemiştir.

8. UYAP bilişim sistemine ilişkin CMK'nın 38/A maddesinin emredici ifadesi karşısında, "fiziki ortamda yürütülen muhakeme işlemlerinin hukuka aykırı olacağı" sonucu düşünülebilecektir. Bu normun aynı Kanun'un diğer bazı ilkeleriyle de çeliştiğini belirtmeliyiz. CMK'nın 38/A maddesindeki söz edilen "emredici" nitelikteki ifadenin yargı mercilerine "seçimlik hak tanıyıcı" biçime dönüştürülmesi yararlı olacaktır. Böylelikle ceza muhakemesinde adli bilişim sürecinin uygulanmasına dair hukuki altyapıya ilişkin kuşkular ortadan kaldırılmış olacaktır.

Suçlulukla mücadele etme amacına ulaşmaya çalışırken temel hak ve özgürlüklerin güvence altına alınması gereği hiçbir zaman ihmal edilmemelidir. Ceza muhakemesi hukuku için günümüzde adli bilişimin vazgeçilmez bir yerde olduğu kuşkusuzdur. Bu itibarla, demokratik toplumların yolu; adil yargılamayı gerçekleştirmeye elverişli ceza muhakemesi normlarıyla adli bilişime ilişkin kuralları kabul etmek ve uygulamaktan geçmektedir.

REFERENCES

[2] M. Özen, İ. Baştürk, *Temel Hak Ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, Adalet Yayınevi, Ankara 2011, s. 140.

[3] Ayrıca bkz. İ. Baştürk, *Bilgisayar Sistemleri ile Verilerinde Arama Kopyalama ve Elkoyma,* Fasikül Aylık Hukuk Dergisi, Ankara Ağustos 2010, S. 9, s. 23-32.

[4] N. Kunter, F. Yenisey, A. Nuhoğlu, *Muhakeme Dalı Olarak Ceza Muhakemesi Hukuku,* 18. baskı, Beta Yayınevi, İstanbul Ekim 2010. s. 573.
N. Centel, H. Zafer, *Ceza Muhakemesi Hukuku,* 6. bası, Beta Basım A.Ş. İstanbul Kasım 2008, s. 197-198.

[5] N. Toroslu, M. Feyzioğlu, *Ceza Muhakemesi Hukuku,* Savaş Yayınevi, Ankara Eylül 2009, s. 169.

[6] N. Kunter, F. Yenisey, A. Nuhoğlu, s. 575.

[7] N. CENTEL, H. ZAFER, s. 199.

[8] Ayrıca bkz. V. Ö. Özbek, *Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi"* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, s. 181-202.

[9] M. Gercke, *Understanding Cybercrime: A Guide For Developing Countries,* September 2012, Second Edition, ITU March 2011, s. 122. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf (25.02.2014).

[10] M. Gercke, s. 122 ve Figure 22.

[11] S. Mason, Bilişim ve Hukuk Uluslararası Hukuk Kurultayı, Ankara 08-11 Ocak 2008 tarihinde sunulan tebliğ metni, Ankara 2009, Cilt II, s. 173.

[12] Bkz. V. Ö. Özbek, s. 183.

[13]http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (11.03.2014).
Avrupa Konseyi Siber Suç Sözleşmesi ve ekinde bulunan, "gerekçe" niteliğindeki *"Açıklayıcı Rapor" (Explanatory Report),* çalışmamızda, sırasıyla *"Sözleşme", "Açıklayıcı Rapor/ Explanatory Report"* olarak anılacaktır.

[14] N. Kunter, F. Yenisey, A. Nuhoğlu, s. 36. N. Toroslu, M. Feyzioğlu, s. 170.

[15] N. Kunter, F. Yenisey, A. Nuhoğlu, s. 575-579, N. Toroslu, M. Feyzioğlu, s. 171-173, N. Centel, H. Zafer, s. 199-200.

[16] V. Ö. Özbek, s. 182.

[17] V. Ö. Özbek, s. 185-188.

[18] Bu bağlamda uygulamada "elektronik keşif" veya "sayısal keşif" terimlerinin de kullanıldığı görülmektedir.

[19] L. Keser Berber, *Adli Bilişim (Computer Forensic),* Yetkin Yayınları, Ankara 2004, s. 79.

[20] N. Toroslu, M. Feyzioğlu, s. 205.

[21] A. Karagülmez, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Seçkin Yayıncılık Ankara 2005, s. 340.
Elektronik delilin kabul edilebilirliği konusunda ABD'de 1993 yılından beri uygulanan ve "Daubert Test" olarak adlandırılan süreç ile ilgili bilgi için bkz. A. Karagülmez, s. 340-341.

[22] Yargıtay bir kararında konuyu (özetle) şöyle vurgulamıştır:
"…gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; … bilgisayardaki virüslü dosya veya dosyaların orijinallerinin korunup korunmadığı, birebir yedeklerinin alınıp alınmadığı hususlarının araştırılması, e-posta veya e-postaları gönderenin IP adresinin bilirkişi raporları doğrultusunda tespiti… gerektiği…"
Bkz. Yargıtay, 11. Ceza Dairesi, 16.04.2007 tarihli, 2005/6376 - 2007/2551 No'lu kararı.

[23] Ayrıca bkz. M. Özen, İ. Baştürk, s. 164.

[24] *Explanatory Report*, No. 133.

[25] T. Demirbaş, *Ceza Hukuku Genel Hükümler,* Yeni Türk Ceza Kanunu'na Göre Gözden Geçirilmiş 5. Baskı, Seçkin Yayıncılık, Ankara Kasım 2007, s. 140.

[26] İnternette sayısal delillerin toplanması için bir "rehber yaklaşım" örneği olarak adlandırılan bu katmanlar için bkz. E. Casey, *Digital Evidence and Computer Crime, Forensic Science, Computers and The Internet,* Academic Press, Third Printing, Cambridge 2001, s. 115-118.

[27] Belirtilen karar için bkz. Ş. Kartal, *Alman Anayasa Mahkemesi'nden Bireysel Mahremiyete İlişkin Özgürlükçü Bir Karar Çıktı,* http://www.bilisimhukuk.com/2010/03/bireysel-mahremiyet-hakkinda-alman-mahkemesi-karari/ (07.03.2014).

[28] http://tr.wikipedia.org/wiki/Bulut_bili%C5%9Fim (10.03.2014).

[29] Bulut bilişim konusunda ülkemizden bir uygulama örneği için bkz. http://www.ttnetbulutu.com/index.jsp (10.03.2014).

[30] 01.06.2005 tarih ve 25382 sayılı Resmi Gazete'de yayımlanmıştır.

[31] M. Gercke, s. 444-445.

[32] Craxi v. İtalya, Başvuru No: 25337/94 için bkz. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61229#{"itemid":["001-61229"]} (12.03.2014). Alman hukukundaki düzenleme ve bilgisayarlardaki verilerle ilgili AİHM kararlarının değerlendirilmesi için ayrıca bkz. N. Kunter, F. Yenisey, A. Nuhoğlu, s. 1111-1114.

[33] M. Özen, İ. Baştürk, s. 153.

[34] Y. Ünver, H. Hakeri, *Ceza Muhakemesi Hukuku,* 4. Baskı, Adalet Yayınevi, Ankara 2011, s. 426.

[35] Bkz. *Explanatory Report*, No. 190.

[36] Bkz. *Explanatory Report*, No. 195.

[37] SSS'nin uluslararası yardımlaşma alanında nasıl sonuç vereceğini tespit etmenin zamanı gerektirdiğine dair bkz. M. Önok, *Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği,* , Marmara Üniversitesi Hukuk Fakültesi Dergisi C. 19, S. 2, İstanbul 2013 (Özel Sayı), s. 1264-1265.

[38] Ayrıca bkz. M. Önok, s. 1264.

[39] Aynı yönde bkz. M. Özen, İ. Baştürk, s. 165-166.

[40] Aynı yönde bkz. M. Özen, İ. Baştürk, s. 161-162.

[41] http://www.uyap.gov.tr/destek/yayep/genelgeler/124-1.pdf (14.03.2014).

[42] Bkz. http://www.yargitay.gov.tr/index2.php?pgid=13 (14.03.2014).

The Role of Database Forensics in Cyberspace Law Enforcement

M. S. Metzger and B. Zhou

Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, mxs054@shsu.edu
Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, zhou@shsu.edu

***Abstract*— since a computer analyst whistleblower by the name of Edward Snowden provided The Guardian (A British national daily newspaper), with top-secret National Security Agency (NSA) intelligence documents regarding the United States of America surveillance on phone and internet communication, our intelligence community is experiencing immense scrutiny regarding their constitutional interpretation of the fourth Amendment. The role of Database Forensics plays a vital part in both the intelligence and law enforcement communities in terms of their ability to collect metadata within specific databases to help solve or prevent potential crimes. The purpose of this paper is to highlight some of the benefits database forensics offers to law enforcement and the challenges that come with the collection of database metadata. Finally, additional recommendations are suggested with the hope of further research opportunities.**

***Keywords*- Database Forensics, National Security Agency (NSA), Metadata, Cyberspace, App, Relational Database Management System (RDBMS), Structured Query Language (SQL), Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) system, Foreign Intelligence Surveillance Act (FISA,)**

I. INTRODUCTION

In today's society, protecting any form of historical record of events and data is critical for a wide range of applications within any organization or government entities. There are instances where historical data are relied on to be used as recovery after system state failure, to analyze previous events after a computer network security breach, or even to review an organizations compliance with network security policies. Because the cost of high storage capacity disk has become extremely affordable, the deliberate preservation of historical data by many organizations including government entities have made it easy to capture all sort of database information for further analysis.

For many of us around the world especially Americans, the introduction of various innovative technologies such; online and mobile banking, access to various social networking platforms, or even the ability to remotely arm or disarm an alarm system via an app installed on a mobile devices are all examples of database driven technologies. By definition, database forensics is a division of digital forensic science that focuses on the forensic study of databases and their related metadata [6]. In the intelligence and law enforcement community, extracting metadata from database servers such as Oracle MySQL or a Microsoft SQL server, plays a critical part in an investigator quest to help solve a database forensics investigation.

Since the aftermath of September 11th 2001 attacks, the intelligence community within the United States government, has devoted a substantial amount of resources in ensuring that the use of information technology will not only help in identifying potential threats, but rather assist in making better decisions in handling any potential threats and improve the way intelligence information is shared between the federal, state and local governments that could potentially protect the US from terrorism and other threats. The enactment of this level of information sharing has created an enormous collection of data within the various law enforcement agencies and to make sense of these collected data, the metadata found within the various databases are used to help law enforcement close any missing gaps.

During this research, my intent is to focus on the benefits of database forensics within the various intelligence agencies and highlight some of the challenges and concerns they are confronted with. Since the leak of Edward Snowden National Security Agency (NSA) intelligence documents to a British newspaper, regarding the level of surveillance on phone and internet communication, many Americans are uncomfortable and questing the scope of the metadata collected.

This paper is organized in the following order: Sections 2 provides an overview of the research that has been performed in the field of Database forensics and Cyber-Space, Section 3 explains the Main Technical Methods used by the intelligence community to conduct database forensics investigation. Section 4 addresses the future of database Forensics and finally, Section 5 presents the conclusion to this study.

II. BACKGROUD

A. Research Awareness

There are very limited number of books and research papers available on database forensics specifically, and according to the authors of a paper titled, A Framework of Database Forensic Analysis, discusses how the lack of research is due to the inherent complexity of database that are not fully

understood in a forensic context yet [5]. A database security expert by the name of David Litchfield, did an excellent job explaining the above premise which is; There seems to be this no-man's-land where no one's doing it simply because the forensics and IR people understand very well their own technologies, whereas with databases you have to understand things like SQL. You have to understand the architecture. So they leave it to the database guys to do it," Litchfield said, "whereas the database guys are probably thinking, 'Wow, I understand databases, but the whole forensics thing is way out of my depth, so I'll leave it to the other guys [7].

On the other hand, the authors of the research paper titled Database Forensics, believes that the current forensic tools are challenged by the amount of data theses databases contains and their ability to examine the database integrity after it is preserved [3]. The authors further discusses how It is quite apparent that most database forensics tools significantly alter the database and despite the fact that it may be acceptable for the evidence to be altered in some fashion, with the ability to document and repeat this process should be kept at minimum, which is not something most of the database tools are capable of accomplishing [3].

One of the key functions of any database administrator, is ensuring that all the databases they are responsible for, are back-up on a regular basis. With that being said, a traditional database backup does not capture deleted or hidden files during the backup process. Another important fact that was discuss in the same article is that, today's databases are typically not encrypted due to the fact that query optimizers are not good at handling encryption without experiencing a significant decrease in system performance [3]. Some of the pros and cons included in this article include:

Pros

- Ability to generate logs from Intrusion Detection Systems (IDS)
- Reports from a Security Information and Event Management (SIEM) system.
- Ability to perform database audit and forensics analysis after a database is compromised.
- The utilization of data mining tools and applications can be a huge help in database forensics analysis.

Cons

- Little literature available on database forensics.
- Most forensics tools out tend to alter the database in a significant way.
- Most forensics tools have difficulties handling encrypted databases.
- The challenge of preserving and analyzing large amount of database information.

B. Database Security Weakness

Adane and Khanuja on the other hand, research focus on the violation of database security threats. Their approach highlighted some of the independent risks to confidential data stored in databases and that many organizations including government entities are extremely susceptible to compliance audit failures and database penetrations attacks. The authors went on to list several factors that could pose potential database security risks such as [4]:

- Budget Constraints
- Not having a clear understanding of the threats
- A lot of IT personnel having "root" database access
- Absence of skilled security professional
- Organization not having anyone with the appropriate database security skillsets.
- Not having a clear understanding of database security processes and procedures.
- Lack of inter-departmental cooperation

Some of the points noted above are very similar to points encored and concerns made by other authors throughout this research. The authors went on to further discuss forensic methodology by defining it as a logical and carefully planned order of operations that is executed during a digital investigation [4]. They emphasis how its sole purpose is ensuring that investigation are documented and executed in a manner that is court friendly and the collected data need to be submitted as evidence. Adane and Khanuja provided some database forensic characteristics that are worth mentioning and they included:

- Understanding the relation between the data dictionary versus the conceptual layer
- Data dictionary contains information that a forensics investigator may find of interest.
- The outside schema outlines the data to be delivered to a specific user.
- During the process of a forensics investigation, users generated views by the various schemas may become useful during an investigation.
- Take into consideration the Operating System's management files used for the physical layer.
- Pay special attention to the amount of logging that occurs in a database.
- The process of restoration or recreation of any data should be performed under a forensic captured process.
- Finally, detailed logs or metadata or even a combination of the two can be used in determining whether and authorized or unauthorized executed a specific action.

The authors also focus in the area of tampering and forensic aspects of a database and the methodologies used for tamper detection which includes:

- Database Forensic Algorithms
- Forensic Tamper Detection of an Audit Log (audit trail)
- Database Artifacts for Database Investigation (Resident and Non-Resident Artifacts).

Finally, some of the Pros and Cons discussed in this paper include:

Pros

- Provided an algorithm for protecting audit logs.
- Proposed an innovative approach in which cryptographically-strong One-way has functions prevent an intruder from getting into a database.

Cons

- Database security vulnerability
- Violation of database security threats
- Risks to confidential data that's resides in databases.
- Database security weakness leaves users vulnerable to

C. Collection of Artifact

In this section, Adane and Khanuja explained where the MySQL server artifacts reside within an operating system files and areas of memory that are unequivocally reserved for SQL server use. It is important to note that, these data facts can exist inside large, core MySQL server files, such a database data or transaction log files, or inside smaller, less visible files. These artifacts form the crucial collection of data that can be used for any database investigation. There are abundant artifacts and each plays a vital role in benefiting a MySQL server investigation in so many level [5]. Example of MySQL data facts and activities includes:

MySQL System Call

- Query Cache
- Key Cache
- Record Cache
- Table Cache
- Hostname Cache
- Heap Table Cache
- Privilege Cache
- Triggers
- Data Files
- InnoDB Tablespace

Tools and Applications

- Activity Reconstruction
- Authorization and Authentication Analysis
- Report Generation

Finally, some of the Pros and Cons the authors discuss include;

Pros

- Performs auditing to ensure data integrity and as a mechanism to detect any database tampering.
- Auditing also ensures

Cons

- Database can be altered deliberately or accidentally by authorized or unauthorized users
- Auditing systems can easily be bypass depending on the level of database knowledge by an attacker.
- Lack of awareness about importance of database forensics.
- Budgetary constraints.

D. Forensics in Cyber-Space

Unlike the previous article, this one focuses on the legal challenges nations are confronted with in terms of how Cyber-Space should be regulated. Wilson stated that, in order to identify the legal challenges which may arise in the future in the field of forensic analysis in cyber-space it is important to seek to understand the current legal framework, modern society and the workplace environment, both internationally and locally [2]. Some of the legal challenges in Cyber-Space include:

- Global liability issues
- Jurisdiction (Which nations are responsible for a global spread attack).
- Risk issues
- Response and regulatory issues
- Commercialization issues
- Regulatory and investigation issues
- Data and document retention issues
- Human rights issues
- Independence, objectivity and expertise issues (Forensic investigations and analysis).

After addressing so of the legal issues Wilson spent time discussing the risk involve in doing business in cyber space by saying; risk issues for cyber-space include viruses damaging own system and being forwarded to third parties. Third parties (hackers etc.) have the capacity to damage systems through unauthorized access, sabotage and identity theft. The protection of data such as confidential information will be vital. The uncovering of fraud and other criminal techniques will be a key concern. [2]

Some of the Pros and Cons discuss in this article by Wilson seek to find solutions in the following areas specifically:

Pros

- Encouraging innovation
- Uploading legal rights in cyber-space
- Protection of fundamental human rights
- Managing and dealing with security breaches
- Having effective and compliance protocols in place (encryption security, firewall, virus protection).
- Protection of intellectual property

Cons

- Wanting to make human rights issue a priority when someone knowingly committed a cybercrime.

III. Main Technical Section

Since a computer analyst whistleblower by the name of Edward Snowden provided The Guardian (A British national daily newspaper), with top-secret National Security Agency (NSA) intelligence documents regarding the United States of America surveillance on phone and internet communication, the NSA intelligence community is experiencing immense scrutiny regarding the full scale of the re metadata programs. Many Americans has always suspected that the government is

spying on it citizens but never knew the extent of it, until Snowden made available reviling evidence that reaffirms most Americans suspicions.

Now that U.S. phone companies and certain social networking sites like Facebook and Google admitted that they quietly send the government data about a list of who called whom and when, and the various sites we visited and how long we were there, all because of a secret order by the Foreign Intelligence Surveillance Act (FISA)Court [8].

E. Importance of Metadata

With communications technology and database forensics tools and applications readily available at the disposal of any government entities, the amount of information contained within metadata is extremely revealing than any of us can fathom. Particularly when we are dealing with metadata at the scale that we now know the NSA, FBI or any other government entities are receiving on a daily basis. To put this in prospective, an article by Matt Blaze says it best; "Metadata, on the other hand, is ideally suited to automated analysis by computer. Having more of it just makes it the analysis more accurate, easier, and better. So while the NSA quickly drowns in data with more voice content, it just builds up a clearer and more complete picture of us with more metadata [8]."

Context yields insights into who we are and the contained, concealed relationships between us. A complete set of all the calling records for an entire country is therefore a record not just of how the phone is used, but, coupled with powerful software, of our importance to each other, our interests, values, and the various roles we play [8].

F. Benefits of database Forensics in Law Enforcement

The concept of data mining within the scope of database forensics have help a lot of law enforcement agencies solve important criminal activities via cyberspace, a direct database attack or even a patrol police officer helping its department build a massive databases with license plate readers installed his or her patrol car.

The basics concept of law enforcement tracking everything we do is definitely frightening but if the information collected, will assist them in identifying or solving a known threat to our civil liberty, then I am sure most American will support such surveillance with a level of transparency and accountability.

IV. The Future of Database Forensics

I. Database Forensics is still in its developing stage considering the fact that with the currently available tools, there is still so much untapped information within the database metadata investigators are unable to comprehend. The best way to overcome such deficient is providing a path for both database administrators and forensics investigators a platform where both do not only understand the importance's of each profession but at the basic level understand the need to effectively preserve the content within a metadata. In the event that an attacker leaves behind evidence that can be collected by means of forensic tools during an investigation will definitely help the investigator solve that case or point them in the right direction to solving a case.

V. Conclusions

There is now question that the role of Database Forensics in both Cyber-Space and the Law Enforcement Intelligence Community has had a significant impact on the way we protect our liberty and prevent events such as 911 from ever occurring again. This research has truly been an eye opener for me in terms of the amount of information that's contained within a database metadata and with the right Forensics investigative training and techniques our intelligence community will continue to uncover information that once were thought to be impossible.

REFERENCES

[1] Erocka Chickowski. (2011, August) Database Forensics Still In Dark Ages. [Online]. HYPERLINK "http://www.darkreading.com/attacks-breaches/database-forensics-still-in-dark-ages/231300307" http://www.darkreading.com/attacks-breaches/database-forensics-still-in-dark-ages/231300307

[2] Harmeet k. Khanuja and D.D Adane, "A Framework For Database Forensic Analysis," Computer Science & Engineering: An international Journal (CSEIJ, vol. II, no. 3, pp. 27-41, 2012.

[3] Wikipedia. (2013, February) Database Forensics. [Online]. HYPERLINK "http://en.wikipedia.org/wiki/Database_forensics" http://en.wikipedia.org/wiki/Database_forensics

[4] Matt Blaze. (2013, July) Phew, NSA Is Just Collecting Metadata. (You Should Still Worry). [Online]. HYPERLINK "http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/ " http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/

[5] Nigel Wilson, "Forensics in Cyber-Space- The Legal Challenges," eForensics, pp. 21-23, 2008.

[6] Harmeet K Khanuja, "Database Security Threats and Challenges in Database Forensic: A Survey," in International Conference on Advancements in Information Technology, Singapore, 2011, pp. 170-175.

[7] Miller Ron, "The Truth is in There," pp. 38-43, March 2007.

[8] Mario A.M. Guimaraes, Richard Austin, and Huwida Said, "Database Forensics," in ACM, Kennesaw, 2010, pp. 62-65.

Üniversitelere Yapılan Siber Saldırılar ve Üniversite Yönetimi Tarafından Yapılması Gerekenler

S. Karabatak[1], F. Özmen[2] and M. Karabatak[3]

[1] Fırat Üniversitesi, Eğitim Fakültesi, Elazığ /Turkey, s_halici@hotmail.com
[3]Trakya Üniversitesi, Eğitim Fakültesi, Edirne/Turkey, fatmaozmen@trakya.edu.tr
[3] Fırat Üniversitesi, Teknoloji Fakültesi, Elazığ /Turkey, muratkar@hotmail.com

***Özet*— Bu çalışmada, bilgi üreten ve yayan eğitim kurumlarından üniversitelerin maruz kaldıkları siber saldırılar, bu saldırılara maruz kalma nedenleri, saldırılara karşı kullanılan güvenlik önlemleri ve yapılabilecekler incelenmiştir. Nitel bir çalışma olan bu araştırmada, verilerin toplanması için görüşme tekniği kullanılmıştır. Türkiye çapında, ulaşılabilen üniversitelerdeki ağ güvenliğinden sorumlu uzmanlar, araştırmanın çalışma grubunu oluşturmaktadır. Araştırma kapsamında hazırlanmış olan sorulara verilen yanıtlardan elde edilen veriler, belirlenen temalar eşliğinde kodlanmış ve temaların tekrarlanma sıklığına göre çözümlenmiştir.**

Araştırmada elde edilen bulgular, siber saldırıların en çok 5651 sayılı kanun kapsamında erişimi engellenen sitelere yönelik olduğunu; ve üniversitelerin de bu kapsamda saldırılara maruz kaldıkları görülmüştür. Bilgi güvenliği yönetim sisteminin olmaması, LOG adı verilen günlük kayıt dosyalarının analizinin gerçekleştirilememesi ve port tarama saldırılarının algılanmaması ve benzeri nedenler siber saldırıları maruz kalmayı kolaylaştırmaktadır. Bu saldırılara karşı antivirüs yazılımlarının etkin olarak kullanıldığı, üniversiteye ait güvenlik duvarının bulunduğu ve hizmet kesintilerin asgari düzeye indirilmesi için gerekli tedbirlerin alındığı belirtilmiştir. Ayrıca alınamayan bazı önlemlerin de maddi sıkıntılardan veya problemin tam anlaşılamamasından kaynaklandığı belirtilmiştir.

Üniversitelerin bilgi güvenliği için profesyonel bir ekip oluşturulması, sistem yöneticilerinin ve ekip elemanlarının, sorumlu oldukları sistemler ve bilgi güvenliği ile ilgili tekrarlayan dönemlerde eğitim almaları ve sertifikasyon sisteminin oluşturulması gibi çeşitli önerilerde bulunulmuştur.

I. GİRİŞ

Sanayi toplumundan bilgi toplumuna dönüşen hem gelişmiş hem de gelişmekte olan ülkeler için vazgeçilmez devasa iletişim ağları oluşturulmaya başlandıktan sonra birbirlerinden uzakta olan insanlar ve organizasyonlar aralarında bilgi alışverişi iletişim teknolojileri ile gerçekleştirilmektedir. Özellikle iletişim ve bilgi alışverişi için yaygın olarak kullanılan internet, günümüzde ulaşımdan bankacılığa, sağlıktan eğitime, enerjiden turizme kadar nerdeyse bütün kamu ve özel sektörlerin ihtiyaç duyduğu bir elektronik haberleşme ortamı olarak kendini göstermektedir.

Bilgi ve iletişim teknolojilerinin hızlı gelişmesine paralel olarak da örgütsel bilgi arşivleri yerini elektronik arşivlere bırakmakta ve bu arşivler de sunucu (server) ortamlarda saklanmaktadır. Böylece örgütlerin en önemli ve vazgeçilmez hazineleri olan bilgiler elektronik ortamlarda özellikle de sanal ortamlarda depolanmaktadır. Bu nedenle de sektörü veya büyüklüğü ne olursa olsun bütün organizasyonlar daha çok internete bağımlı bir hale gelmektedir.

Kamu yararı için internet ve teknolojiyi yaygın olarak kullanmaya başlayan sektörler, günümüzde internet ve teknolojinin kamu zararı için kullanılmasıyla da siber tehdit veya siber terör denilen siber saldırılara maruz kalmaktadırlar [1-5]. Siber suçlar kapsamına da giren bu saldırılar için kullanılan yöntemler ve araçlar klasik suçlara göre önemli farklılıklar göstermektedir. Siber saldırılar özellikle cep telefonu, sosyal medya ve iletişim ortamları, web siteleri, online oyunlar, elektronik posta aracılığıyla bir kişi veya bir grup tarafından yapılan ve başka bir bireyi karalayıcı, küçük düşürücü yayın ve duyurulardır. Siber saldırılar veya suçlar ileri teknoloji ve bilgiyi kullanarak yeni bir vizyon ortaya koymaktadır. Siber suçları klasik suçlardan ayıran özellikler Tablo 1 incelendiğinde daha iyi anlaşılmaktadır [6]

Tablo 1. Klasik suçlar ile siber tehdit ve suçlar arasındaki farklar

	Klasik Suçlar	**Siber Saldırılar veya Suçlar**
Amaç	Siyasal rejime ve topluma mesaj vermek için kullanılan bir araçtır	Yapılan eylemler ile toplumu, devleti veya hedef alınan örgüte zarar verme, maddi kayba uğratmak için kullanılan bir amaçtır.
Risk	Eylemi gerçekleştiren kişi ya da grup yaşamsal risk taşır	Herhangi bir yaşam riski yoktur.
Etki Alanı	Saldırının yapıldığı yer ile sınırlı	Ulusal veya uluslararası boyutlarda etkili olabilecek saldırılar olabilir.
Propaganda	Verilen mesaj bölgesel	Verilen mesaj küresel
Denetim	Suçları kontrol etmek, izlemek ve yok etmek kısmen mümkün	Siber saldırıları belirlemek, saldırganları tespit etmek veya yok etmek nerdeyse imkânsız.

Kullanılan araç	Fiziksel araçlar	Yazılım, virüs, e-bomba, radyo frekansları gibi araçlar
Uygulanacak Ceza	Suçun niteliğine göre uygulanacak ceza belli	Suçun niteliğindeki hukuki boşluklar

Çeşitli kuruluşlara yapılan siber tehditlerle ilgili yapılan araştırmalarda özellikle de Bilgi Teknolojileri ve İletişim Kurumu ile Tübitak tarafından yapılan çalışma sonucunda en çok karşılaşılan saldırı çeşitleri şöyle sıralanmıştır [9-14]: Kurumun bilişim sistemlerine girilmesi, sistemin engellenmesi, bozulması, verilerin yok edilmesi ve değiştirilmesi; kötü yazılım bulaşması; korsan yazılım dağılımı; kurumların resmi sitelerine bilgisayar sistemi üzerinde yetkisiz kontrol/erisim veya tahrifatı; bir kurumun IP adresinden başka bir kuruma veya kuruluşa yapılan DDoS saldırıları veya istek dışı elektronik posta mesajların gönderilmesi; kuruma dışarıdan DDoS saldırısı yapılması; kurumdan ayrılan kötü niyetli bir çalışanın veritabanına zarar vermesi; kurumun sistemlerine internet aracılığıyla yayılan solucanın bulaşması; telefon veya elektronik posta yoluyla yetkisiz bilgi sahibi olmaya çalışma veya kuruma ait laptop veya mobil cihazların çalınması veya kaybolması; kurum çalışanlarının 5651 sayılı kanun kapsamında erişimi engellenen sitelere giriş yapıldığının tespit edilmesi; kurumu temsil eden sahte bir web sitesinden elektronik posta mesajları gönderildiğinin tespit edilmesi; izinsiz yapılan bir çalışmalar (kazı gibi) sırasında kuruma ait fiber hattının devre dışı kalması; sistem odasında bulunan soğutma sisteminin mesai saati dışında bir saatte arızalanması; kurumun bulunduğu bölgede elektrik kesintisi yaşanmasına rağmen jeneratör sisteminin devreye girmemesi; kurum içinde kullanılan kablosuz ağların istismarı veya ele geçirilmesi veya şifre koklama (Password sniffing); Kurum içindekilerin yetkisiz erişimi veya ayrıcalık yükseltmesi; DNS Sunucularının istismarı.

Sanal ortamda gerçekleşen bu tehditler bütün kurumları olduğu gibi eğitim kurumlarını da etkisi altına almıştır. İnternet, eğitim kurumlarından üniversiteler söz konusu olduğunda küresel olarak çok geniş bir platformda, bilgilerin anında taratıldığı, erişildiği, paylaşıldığı elektronik bir ortam olmasından ve ayrıca akademisyen ve öğrencilere hız ve rekabet üstünlüğü kazandırırken, bilgi varlıkları üzerinde yetkisiz erişme, değiştirme, engelleme, çalma gibi risk ve tehditleri de beraberinde getirmektedir [15].

Üniversitelerin siber tehditlere ve saldırılara maruz kalmalarının nedeni yukarıda belirtilen nedenlerden en az birinden kaynaklanmaktadır. Özellikle üniversitelerin laboratuvarlarında kullandıkları yazılımlar her zaman güvenli kaynaklardan sağlanmamaktadır. Özellikle de öğrencilerin deneme, öğrenme, analiz etme ve merak etme gibi nedenlerle çeşitli yazılımların kurulumlarını internet üzerinden gerçekleştirmektedirler. Bu tür kurulumların sürekli denetim altında tutulması mümkün değildir. Benzer şekilde hem öğrencilerin hem akademisyenlerin hem de üniversitedeki diğer çalışanlarının girdikleri internet siteleri özellikle de günümüzde yaygın olarak kullanılan sosyal medya sitelerinden yayılan riskler web güvenlik şirketi olan Sophos'un en son yayınlanan raporundaki elektronik tehlike listesinin başında geldiği belirtilmektedir [15]. Bu siteler özellikle malware, trojan, worm, spyware, adware ve rootkit gibi zararlı yazılımları ve daha birçok virüs eklentileri taşıyabilmektedir. Sistem bazı zararlı yazılımlara uyarı vermeyebilir veya verilen uyarıları her zaman kullanıcılar tarafından dikkate alamayabilir. Uzaktan dizin ve dosya paylaşımları, açılmış portlar, hedefe saldırı aracı haline gelmiş, spam ileti kaynağı, virüs yayan bir makine şekline dönüşebilir.

Kısaca bir üniversite ağı internetten gelebilecek her türlü zararlı zararsız yazılım ve uygulamalarla karşı karşıyadır [15]. Bu araştırmada, üniversitelerde Bilgi İşlem Dairesinde görev yapan ağ ve bilgi iletişim teknolojisi uzmanlarının görüşleri doğrultusunda, üniversitelerin elektronik bilgi kaynaklarına yapılan siber saldırılar, bu saldırılara yönelik güvenlik tedbirleri ve başka neler yapılabileceği sorgulanmıştır. Bu genel amaç doğrultusunda aşağıdaki sorulara yanıt aranmıştır:

1- Üniversiteniz siber saldırıya hiç uğradı mı? Uğradı ise hangi tür saldırılara maruz kaldı?

2- Saldırıya maruz kalma nedenleri nelerdir?

3- Bu saldırılara karşı üniversite yönetimi tarafından alınan güvenlik önlemleri nelerdir ve başka alınabilecek önlemler nelerdir?

II. YÖNTEM

Araştırma nitel bir çalışma olup, veri toplama aracı olarak görüşme tekniği kullanılmıştır. Veri toplama amacı ile hazırlanan görüşme soruları araştırmacılar tarafından alan taraması yapıldıktan sonra hazırlanmış ve bu sorular iki uzman görüşünün önerileri ve düzeltmeleri ile son halini almıştır. Hazırlanan görüşme sorularına yönelik uzman görüşleri, yüz yüze veya telefon görüşmeleri aracılığıyla Türkiye'deki üniversitelerin Bilgi İşlem Dairesi'nde görev yapan ağ ve bilgi işlem uzmanlarına yöneltilen sorularla, bazılarının görüşleri ise zamanlarının yeterli olmaması nedeni ile elektronik posta aracılığıyla alınmıştır. Araştırmaya görüş bildirmeleri için üniversitelerin bilgi işlemlerinde çalışan ağ uzmanlarına mail atılmış fakat çoğundan olumlu veya olumsuz herhangi bir dönüt alınamamıştır. Araştırma için 2 özel üniversitede ve 15 devlet üniversitesinde görev yapan 17 ağ sorumlusu görüşlerini bildirmişlerdir. Fakat görüş bildiren üniversitelerin ağ sorumlularının üniversite isminin açıklanmamasını istemelerinden dolayı görüş bildiren üniversitelerin isimlerinin gizli tutulması uygun görülmüştür.

Verilerin analizi aşamasında, elektronik posta ile sorulara verilen yanıtlar, belirlenen temalar eşliğinde kodlanmış ve temaların tekrarlanma sıklığına göre çözümlenmiştir. Katılımcıların görüşlerinin analizi yapılırken AS1, AS2…AS17 şeklinde kodlanmıştır. Katılımcılar birden fazla temayı içeren görüş bildirdikleri için, temaların toplam frekans sayısı *(f)* ile sorulara cevap veren sayısı (n=17) birbirine eşit çıkmamıştır. Üniversitelerin elektronik ortamdaki bilgilerinin maruz kaldığı siber saldırılar, bu saldırıların nedenleri ve saldırılara karşı alınan güvenlik önlemlerine ilişkin görüşlerden dikkat çekici olanlar özüne sadık kalınarak sunulmuştur.

III. BULGULAR

Tablo 2 Üniversitelerin bugüne kadar maruz kaldıkları saldırıları türleri

Maruz kalınan saldırı türleri	Frekans(f)
5651 sayılı kanun kapsamında erişimi engellenen bir siteye giriş yapıldığının tespit edilmesi	*17*
Kurumun resmi web sayfasının içeriğinin yetkisiz kişilerce değiştirilmesi	*15*
Kurum içinde ismi kolaylıkla tahmin edilerek bağlanılabilen bir kablosuz ağ erişim noktasının tespit edilmesi	*12*
Elektrik kesintisi ile ilgili yaşanan sıkıntılar	*11*
SQL injection	*10*
Kurumda çalışan personelden bilgi çalma (özellikle telefon aracılığıyla) girişimi	*9*
Kuruma ait sistemlere İnternet üzerinden yayılan bir solucanın bulaşması	*9*
Kuruma başka bir kaynaktan DDoS saldırısı yapılması	*8*
Kurumdan ayrılan kötü niyetli bir personelin ayrılmadan önce veritabanına zarar vermesi	*8*
Kuruma aitmiş gibi görünen sahte bir web sitesinden istek dışı elektronik posta mesajları gönderildiğinin tespit edilmesi	*8*
Sistem odasında bulunan soğutma sisteminin mesai saati dışında bir saatte arızalanması	*8*
Kuruma ait bir IP adresinden başka bir kurum/kuruluşa DDoS saldırısı yapıldığının tespit edilmesi	*6*
Kuruma ait bir IP adresinden başka bir kurum/kuruluşa istek dışı elektronik posta mesajları gönderildiğinin tespit edilmesi	*6*
Elektronik posta yoluyla kurumda çalışan personelden bilgi çalma girişimi	*6*
Kurum içi saldırılar	*6*
İzinsiz yapılan bir kazı neticesinde kurumun İnternet bağlantısını sağlayan fiber hattının kopartılması	*4*
Spam mailler tarafından kullanıcılardan şifre talep edilmesi	*4*
Sunuculara uzaktan erişen pclerde keylogger çalıştırılmaya çalışılması	*3*
Öğrenciler veya bilgiye yeni hakim olan kişiler tarafından yapılan saldırılar	*3*
Otomasyonların işleyişini bozma	*3*
Kablosuz ağlarda eternet kartı numarası (MAC) adresine göre ip dağıtma	*2*
Ağ cihazlarına Arp piosoning saldırıları	*2*

Tablo 2'de üniversitelerin bugüne kadar en çok maruz kaldıkları saldırı türleri görülmektedir. Bu saldırı türlerinnden en fazla kurum çalışanlarından birinin 5651 sayılı kanun kapsamında erişimi engellenen bir siteye giriş yapıldığının tespit edilmesi (f=17), kurumun resmi web sayfasının içeriğinin yetkisiz kişilerce değiştirilmesi (f=15), kurum içinde ismi kolaylıkla tahmin edilerek bağlanılabilen bir kablosuz ağ erişim noktasının tespit edilmesi (f=12) ve elektrik kesintileri sırasında jeneratörün devreye girememesi (f=11) gibi sorunlar olarak belirtilmiştir.

Üniversitelerin bugüne kadar en çok maruz kaldıkları saldırı türleri ile ilgili üniversitelerin ağ güvenliğinden sorumlu olan kişilerin bireysel olarak dile getirdikleri ifadelerden bazıları şöyledir:

"O kadar çok ağ saldırısına maruz kalıyoruz ki ilk aklıma gelen üniversitenin web sayfasına yapılan saldırılar. Bunun yanında hem akademik personelden hem de çalışanlardan yasaklanan sitelere giriş yapmaya çalışanlar çok oluyor. Ayrıca otomasyonlarımızın işleyişini bozmak ve veri çalmak için de saldırılar yapılmıştır." (AS3)

"Çok fazla geçmişi olmayan bir üniversiteyiz ve en çok kurum içi saldırılara maruz kalıyoruz diyebilirim. Bunun yanında üniversitenin web mail serverından gönderilmiş gibi gönderilen emailler var. Sunuculara uzaktan erişen bilgisayarlarda keylogger çalıştırılmaya çalışılmıştır. En çok spam mailler tarafından kullanıcılardan şifre talep edilmektedir. Bir de SQL injection" (AS7)

"Kablosuz ağlarda mac adresine göre ip dağıtma, girilmemesi gereken sitelere girme, hem kurum içinden hem kurum dışından yapılan DDOS saldırıları ilk aklıma gelenler" (AS13)

Tablo 3- Üniversitelerin saldırıya maruz kalma nedenleri

Saldırıya maruz kalma nedenleri	Frekans (f)
Erişim kontrol politikasının bulunmaması	*14*
Kayıt dosyalarının(LOC) analizinin gerçekleştirilememesi	*13*
Port tarama saldırılarının algılanmaması	*11*
Sistem yöneticileri teknik olarak yetersizdir.	*10*
Güncel olmayan antivirüs sistemleri	*10*
İş sürekliliği planlarının bulunmaması	*10*
Yasal mevzuata ilişkin bilgi eksikliği	*10*
Şifrelerin yanlış kişilerle paylaşılması	*10*
Sosyal mühendislik saldırılarına ilişkin bilinç yetersizliği	*9*
Sistem tasarımı aşamasında güvenliğin göz ardı edilmesi	*9*
Kablosuz ağlardan kaynaklanan riskler	*9*

Dağıtık servis dışı bırakma saldırılarının olumsuz sonuçları	***9***
Bilgi güvenliği yönetim sistemi yoktur.	***8***
Web uygulamalarında bulunan açıklıklar	***8***
Saldırı tespit sistemi ve süreçleri yetersizdir.	***7***
Sistem yöneticilerinin güvenlik boyutunda yetersizliği	***7***
Kurum içi koordinasyonun yetersizliği	***7***
Bilgi işlem birimlerine gerekli önemin verilmemesi	***5***
Yetersiz bütçe	***4***
Yetersiz güvenlik personeli sayısı	***4***
Bazı çalışanların kendilerini ispat etmeye çalışması	***3***

Tablo 3'de üniversitelerin saldırıya maruz kalma nedenleri görülmektedir. Ağ sorumluları tarafından en fazla saldırı türlerine maruz kalma nedenleri erişim kontrol politikasının bulunmayışı (f=14), kayıt dosyalarının(LOC) analizinin gerçekleştirilememesi (f=13), port saldırılarının algılanamaması (f=11) şeklinde söylenebilir.

Üniversitelerin bugüne kadar siber saldırılara maruz kalma nedenleri ile ilgili üniversitelerin ağdan sorumlu olan kişilerin bireysel olarak dile getirdikleri ifadelerden bazıları şöyledir:

"Ağ güvenliği için yeni personeller hatta mühendis alınmıştır. Fakat bilgilerinin yetersiz olduğu görülmüştür. Eğitimlerinin çok iyi yapılması gerektiğini düşünüyorum. Alınan personelin gerçekten işten anlayan birisinin olmasına gerek vardır. Sonrada o kişi veya kişilerin eğitimleri her zaman sağlanmalıdır" (AS1)

"Bilgi güvenliği alanında yeteli altyapınının olmaması, kendisini yetkin gören ve bilgiye yeni hakim olan insanların bir nevi becerisini ortaya koyma, kendisini ispat etme girişimleri, sürekli bilgi işlem personelinin değişmesi ve yeni gelen personelin ya tecrübesizliği ya da işi anlamadığı için eski personeli bilgisizlikle suçlama" (AS4)

"Günü kurtaran çözümler alınıyor. Bilgi güvenlik sistemimiz var gibi görünse de yetersizdir. Ayrıca kayıt dosyaları analizleri tam olarak gerçekleştiremiyor. Port tarama saldırıları da tam olarak algılanamıyor" (AS8)

"Ağdaki tüm bilgisayarların merkezi bir sistemle ağa dahil edilebildikleri ve güncellenebildikleri bir altyapı oluşturulmalı ancak hem çok pahalı bir yatırım hem de takibini ve bakımını yapacak personel yoktur" (AS10)

"Yöneticiler veya çalışanlar bilgi ve tecrübe olarak yetersizler. Network sorumlularının sık sık değişmesi. Evrak işleriyle uğraşmaktan asıl işten uzaklaşma, yönetici pozisyonundaki personelin yazıcı problemleri, toner problemleri, çıktı alma vs. gibi basit işlerinin tüm zamanımızı alması yüzünden sisteme gereken önemin verilememesi" (AS13)

"Bilgi İşlem Personelinin "kendini yeterli sanması" ama aslında bu işi tam bilmemesi ve "daha fazla tedbir ve dikkati" gereksiz görmeleri... Yeterli nitelikli personelin bulunmaması" (AS16)

"Personel yetersizliği ve mali problemler, özellikle devlet üniversitelerinde bilgi işlem birimlerine yeterince önem verilmemesi ve gerekli bütçelerin ayrılmaması sonucu yeterli önlem alınması her zaman zorlaşmıştır. Teknik personelin gerekli olan eğitimi alamaması" (AS17)

Tablo 4- Üniversitelerin siber saldırılara karşı aldıkları güvenlik önlemleri

Güvenlik Türleri	**Frekans**
Kurumun güvenlik duvarı mevcuttur	***13***
Hizmet kesintileri asgari düzeye indirilmesi için gerekli tedbirler alınmıştır	***12***
Antivirüs yazılımlarının etkin olarak kullanılması sağlanır.	***11***
Tüm bilgisayarlar merkezi bir antivirus sunucu üzerinden korunur.	***10***
Üniversiteye ait Bilgi Güvenliği Yönetim Sistemleri mevcuttur	***9***
Kablosuz erişimlerin sağlandığı noktalar denetim altındadır	***8***
Kurumda periyodik olarak denetimler yapılır ve belirlenen açıklıkların giderilmesi için gerekli işlemler yapılır	***7***
Bilgi işlem, hukuk ve halkla ilişkilerden sorumlu birimler birbirleri ile koordineli çalışır.	***7***
Ddos saldırıları için gerekli önlemler alınmıştır.	***7***
5651 nolu kanuna gore gerekli kayıtlar alınır.	***7***
Kurum çalışanlarına bilgi güvenliği ile ilgili bilinçlendirme eğitimleri; çalıştaylar, konferanslar ve toplantılar düzenli olarak yapılır.	***6***
IP adreslerinin dağılımı, bilgisayar isimlendirme, kullanıcı hesaplarının oluşturulması, ortak hesapların kullanımdan kaldırılması gibi işlemler sık sık gözden geçirilir.	***6***
Saldırı Tespit Sistemi doğru yapılandırılmıştır	***6***
Port Tarama saldırısının algılanması için teknolojik altyapı oluşturulmuştur.	***6***
Bilgi güvenliği birimleri oluşturulmuştur.	***5***
Spam maillere karşı engellemeler yapılır (Mail Gateway)	***5***
Saldırı tespit sistemi kurulmuştur ve sistemin yaptığı kayıtlar düzenli olarak incelenir	***4***

Kurumlarda tüm kullanıcıların erişim hakları bellidir	***3***
İç ağda olabilecek saldırılar için ise IPS (intrusion prevention system),	***3***
Sistem yöneticileri bilgi güvenliği ilgili gerekli eğitimlerin alması sağlanır.	***1***
Düzenli penetrasyon testleri uygulanmaktadır.	**-**

"Etkin bir güvenlik duvarı sisteminin kurulması personelin bilgilendirilmesi gereklidir. Ne yazık ki bu yok. Düzenli olarak penetrasyon testleri yapılmalıdır fakat bunun da hiçbir üniversitede yapıldığını sanıyorum." (AS1)

"Gerçekten çok güzel bir konu ve soru. Tabii ki saldırılara çeşitli önlemler almaya çalışıyoruz fakat bunlar yeterli değil. Her zaman sistemde bir açık meydana geliyor. Hizmet kesintileri asgari düzeye indirilmesi için gerekli tedbirler alınmaya çalışılıyor. Kurumun güvenlik duvarı ve gerekli antivirüs programları temin edilmiş." (AS9)

"Sunucular DMOZ, arındırılmış alan içerisine taşınmıştır. Sistemimizi update yaparak güncel tutmaya çalışma, mümkün olduğu kadar az kişiyle sistem şifrelerini paylaşma. Bölge olarak sık elektrik kesintisi yaşandığından jeneratörün önüne iki adet UPS konmuş ve sistemlerin sürekli ayakta kalması sağlanmıştır. Ağ trafiğini yönetebilmek ve gereksiz trafiği önleyip, ağa bulaşacak virüsleri engellemek için bazı sitelere erişim" (AS11)

"Ağ güvenliği için yeni personel alımına gidilmiştir ama bu kişilerin sistemi tam anlayamaması ve deneyimsiz olmaları problemi çözememiştir. Yasak sitelere girişlerin kayıtları alınmaya çalışılır. Ddos saldırılarına önlemler alınmaya çalışılır. Fakat düzenli olarak penetrasyon testleri uygulanmamaktadır. " (AS12)

"Herzaman bütün personelin internetten hizmet alması esastır. Güvenlik duvarı ve antivirüs programları tamam. Ağ güvenliğinden sorumlu personelimiz var. Spamlara karşı önlemler alınmaya çalışılmıştır. IP'ler ve kullanıcı hesaplarının kontrolleri düzenli yapılır." (AS15)

IV. SONUÇ VE TARTIŞMA

Araştırma sonucunda üniversitelerin ağ sorumlularından alınan görüşler doğrultusunda diğer kurum ve kuruluşlara yapılan siber saldırıların üniversitelere de yapıldığı görülmüştür. Üniversiteler çoğunlukla bu saldırılardan, kurumun bilişim sistemlerine girilmesi, sistemin engellenmesi, bozulması, verilerin yok edilmesi ve değiştirilmesi; kötü yazılım bulaşması; korsan yazılım dağılımı; kurumların resmi sitelerine bilgisayar sistemi üzerinde yetkisiz kontrol/erisim veya tahrifatı; DDoS saldırıları veya istek dışı elektronik posta mesajların gönderilmesi; kötü niyetli bir çalışanların veritabanına zarar vermesi; kurumun sistemlerine internet aracılığıyla yayılan solucanın bulaşması; telefon veya elektronik posta yoluyla yetkisiz bilgi sahibi olmaya çalışma; kurum çalışanlarının erişimi engellenen sitelere giriş yapmaya çalışmaları; sistem odasında bulunan soğutma sisteminin arızalanması veya elektrik kesintisi yaşandığında jeneratör sisteminin devreye girmemesi; kurum içinde kullanılan kablosuz ağların istismarı veya ele geçirilmesi gibi saldırılarla daha çok karşılaştıkları ortaya çıkmıştır.

Ağ uzmanlarının görüşlerine göre üniversitelerin elektronik ve sanal ortamlarına yapılan bu saldırılara maruz kalma ve etkilenme nedenleri ise kurumlarda bilgi güvenliği yönetim sisteminin olmaması; sistem yöneticilerinin teknik olarak yetersiz olmaları; saldırı tespit sisteminin ve süreçlerinin yetersizliği; sosyal mühendislik saldırılarına ilişkin bilinç yetersizliği; antivirüs sistemlerinin güncel olmaması; sistem yöneticilerinin güvenlik ile ilgili yetersizliği; kurum içi eşgüdüm yetersizliği; erişim kontrol politikasının bulunmaması; sistem tasarımı aşamasında güvenliğin göz ardı edilmesi; kablosuz ağlardan kaynaklanan riskler; iş sürekliliği planlarının bulunmaması; port tarama saldırılarının algılanmaması; dağıtık servis dışı bırakma saldırılarının olumsuz sonuçları; web uygulamalarında bulunan açıklıklar; kayıt dosyalarının analizinin gerçekleştirilememesi; yasal mevzuata ilişkin bilgi eksikliği şeklinde belirtilmiştir.

Ağ ve bilgi güvenliğinden sorumlu olan kişilerin görüşleri doğrultusunda yapılan bu çalışma ile bilgi üreten ve yayan kurumların başında gelen üniversitelerin ciddi siber tehditler altında olduğunu ortaya çıkmıştır. Kamu veya özel kurum ve kuruluşlara yapılan saldırı türleri ile nedenleri ile ilgili yapılan çalışmalarda belirtilen saldırı türleri ve nedenleri yapılan çalışmanın bulguları ile örtüşmektedir. [10,11,16-18].

V. ÖNERİLER

Siber saldırılara maruz kalan üniversiteler için özellikle üniversite yönetimleri durumun ciddiyetinin farkına varmaları ve gerekli tedbirleri almaları gerekmektedir. Özellikle üniversite yönetiminin kurumsal düzeyde almaları gereken siber güvenlik tedbirleri aşağıdaki gibi sıralanmıştır:

- Kurumlarda bilgi güvenliği için profesyonel bir ekip oluşturulmalı ve sistem kurulmalıdır.
- Kurulan ekip ile özellikle sistem yöneticilerinin sorumlu oldukları sistemler ve bilgi güvenliği ilgili gerekli eğitimlerin alınması sağlanmalı ve yaygın kabul gören güvenlik sertifikasyonlarının alınması sağlanmalıdır.
- Üniversitelerin ağ yapıları ve sistemleri periyodik olarak denetimler yapılmalı ve belirlenen açıklıkların giderilmesi için gerekli faaliyetler gerçekleştirilmelidir.
- Saldırı tespit sistemleri kurulmalı; sistemin yaptığı kayıtlar düzenli olarak incelenmeli ve gerekli işlemler yapılmalıdır.
- Üniversite çalışanlarının tanımadıkları kişilerden gelen isteklere karşı temkinli davranmaları için tüm personele düzenli aralıklarla sosyal mühendislik ve bilgi güvenliği bilinçlendirme eğitimleri verilmeli ve çalıştaylar, konferanslar ve toplantılar yapılmalıdır.

- Antivirüs yazılımının kurumda etkin olarak kullanılması sağlanmalıdır ve bunun için tüm bilgisayarlar merkezi bir antivirüs sunucu üzerinden güncellenmelidir.
- Bilgi işlem, bilgi güvenliği, hukuk ve halkla ilişkilerden sorumlu kurum içi birimler koordineli çalışmalıdır.
- Kurumlarda tüm kullanıcıların erişim hakları belirlenmelidir.
- IP adreslerinin dağılımı, bilgisayar isimlendirme, kullanıcı hesaplarının oluşturulması, ortak hesapların kullanımdan kaldırılması ve görevler ayrılığı prensibinin uygulanması sık sık gözden geçirilmelidir.
- Kablosuz erişimlerin sağlandığı noktalar sürekli gözetim altında tutulması için gerekli önlemler alınmalıdır.
- Kurumlarda yaşanabilecek hizmet kesintilerinden asgari düzeyde etkilenmek için gerekli önlemler alınmalıdır.
- Kurumlardaki Güvenlik Duvarı ve Saldırı Tespit Sistemi doğru yapılandırılmalıdır.
- Port Tarama saldırısının kurum tarafından algılanması için teknolojik altyapı oluşturulmalıdır.
- Dağıtık Servis Dışı Bırakma gibi güncel saldırıların bertaraf edilmesi ile ilgili gerekli eğitimler alınmalı ve gerekli politikalar uygulanmalıdır. Düzenli aralıklarla penetrasyon testleri uygulanmalıdır.

Siber güvenliğin en üst düzeyde sağlanabilmesi için üniversitelerin kurumsal düzeyde yapacaklarının yanında ulusal düzeyde de yapması gereken pek çok şey vardır. Üniversiteler bilgi üretiminin ve yayılımının en önemli etken kurumları olarak, ulusal düzeyde siber güvenlik politikalarının oluşturulması bunun için gerekli bilimsel ve teknolojik araştırma ve geliştirme programlarının ve projelerinin yapılması için öğretim elemanlarına ve öğrencilere destek olması; devletin çatısı altında siber güvenlik uygulayıcı kurumların oluşturulmasını ve bölgesel ve uluslararası taraf, kurum ve kuruluşlarla işbirliği yaparak siber güvenlik ordularının bir parçası olarak görev alması; en önemlisi de siber güvenlik uzmanlarının yetiştirilmesi için üniversitelerde ilgili lisansüstü programları geliştirmesi; siber güvenlik alanında yapılacak araştırmalar için kurulacak merkezlerin kurulmasını sağlaması ve bu merkeze destek olması ve bunlara ek olarak yazılı ve görsel medyanın da bu konuda toplumun ve kurumların farkındalığın arttırılması için gerekenleri yapması gerekir.

REFERENCES

[1] Yen, S., Chen, S., (2006). The Study on Planning and Building a Cyber Forensic Laboratory in MJIB, Taiwan, IEEE

[2] Çiçek, İ., & Okatan, A.(2008) Ülkemizde adli bilişim laboratuarı kurulumu ve bilişim suçlarıyla mücadeleye katkıları. *II. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu.* http://www.emo.org.tr/etkinlikler/agbilgiguvenlik/etkinlik_metin.php?etkinlikkod=82&metin_kod=397

[3] Maltais, C. F. (2005). *Managing Cyber Crime: an Assessment of Canadian Law Enforcement Responses* (Doctoral dissertation, Charles Sturt University, Australia).

[4] Cheang, S. (2009, November). Conceptual Model for Cybersecurity Readiness Assessement for Public Institutions in Developing Country: Cambodia. In Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on (pp. 1411-1418). IEEE.

[5] Paklacı, Y. (tarih yok). *Siber Saldırı Nedir?* Mart 10, 2013 tarihinde Bilgi Ustam: http://www.bilgiustam.com/siber-saldiri-nedir/ adresinden alındı

[6] Udoeyop, Akaninyene Walter, "Cyber Profiling for Insider Threat Detection. " Master's Thesis, University of Tennessee, 2010. http://trace.tennessee.edu/utk_gradthes/756

[7] Kara, O., Aydın, Ü., & Oğuz, A. (2006). Ağ ekonomisinin karanlık yüzü: Siber terör. 5. Bilgi, Ekonomi ve Yönetim Kongresi, Kocaeli, Kasım 2006, 5. *Bilgi, Ekonomi ve Yönetim Kongresi,* Cilt II,ss.156-170, Uluslararası organizasyon

[8] Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D., & Pabian, S. (2012). Police actions with regard to cyberbullying: The Belgian case. *Psicothema*, *24*(4), 646-652.

[9] Bass, T., Freyre, A., Gruber, D., & Watt, G. (1998). E-mail bombs and countermeasures: cyber attacks on availability and brand integrity. *Network, IEEE*, 12(2), 10-17.

[10] Bilgi Teknolojileri ve İletişim Kurumu & Tübitak. (2011). *Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu.* Ankara.

[11] Cavelty, M. D. (2012). *Cyber-threats*. Handbook of Security Studies, 180.

[12] Dijle, H. & Doğan N., (2011). Türkiye'de bilişim suçlarına eğitimli insanların bakışı. *Bilişim Teknolojileri Dergisi*, 4(2), 2011.

[13] Harris, S. (2008). China's Cyber Militia. *National Journal Magazine*, 31.

[14] Koike, H., Ohno, K., & Koizumi, K. (2005, October). Visualizing cyber attacks using IP matrix. In *Visualization for Computer Security, 2005.(VizSEC 05). IEEE Workshop on* (pp. 91-98). IEEE.

[15] Şahinaslan, Ö., Şahinaslan, E., & Razbonyalı, M. (2013). *Eğitim Kurumlarına Yönelik Sızma Test Metodolojisi.* http://ab2013.akdeniz.edu.tr adresinden alınmıştır

[16] Brykczynski, B., & Small, R. A. (2003). Reducing internet-based intrusions: Effective security patch management. Software, IEEE, 20(1), 50-57.

[17] Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*, 18(1), 28-34.

[18] Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248.

INDEX

Adela Beres, 37
Ahmet Akbaş, 17
Ahmet Burak Gökalp, 51
Allisher Kholmatov, 21
Alper Özbilen, 1
Asaf Varol, 6,86,92
Avinash Chandragari, 77
Bela Genge, 37
Bing Zhou, 110130
Büşra Çağlar, 1
Çetin Arslan, 73
Ceydacan Seyrek, 1
Christhopher Hale, 43
Cihan Varol, 105
Emre Olca, 101
Engin Avcı, 92119
Erkan Tanyıldızı, 32
Fatih Kurugöllü, 113
Fatih Ertam, 119
Fatma Özmen, 139
Ferdiansyah Mastjik, 105
Fikret Hacizade, 21
Gökhan Bektaş, 21
Gökhan Dalkılıc, 58,67
İhsan Baştürk, 124
J. Lang, 26
Kasım Taşdemir, 113
Lei Chen, 43,81
Medine Çolak, 51
Mehmet Karaman, 51,63
Mehmet Hilal Özcanhan, 58,67
Michael Samson Metzger, 130
Murat Karabatak, 139
Muaz Gültekin, 17
Mustafa Uğur Eren, 51
N. Shashidhar , 26
Necati Türkay, 47
Neo Nevarez, 110
Nilay Yıldırım, 6,86
Oğuz Yarımtepe, 58
Özgu Can, 101
Özlem Milletsever, 1
Peter Cooper, 67
Piroska Haller, 37
Qingzhong Liu, 77
Resul Daş, 6
Şakir Sezer, 113
Semih Utku, 67
Semra Çakır, 51
Şeref Sağıroğlu, 1,63
Songül Karabatak, 139
Sundar Krishnan, 81
Türker Tuncer, 119
Ümit Kaş, 32
Uraz Yavanoğlu, 1
Yanxin Liu, 77