Veritabanı Sistem Güvenliği: Bir Vaka Çalışması

Database System Security: A Case Study

Rasty Shakhawan Majid
Department of Software Engineering
Firat University
Erbil, Iraq
rastyshaxawan@yahoo.com

Asaf Varol
Department of Software Engineering
Firat University
23119 Elazig / Turkey
Varol.asaf@gmail.com

ÖZET

Veri güvenliği pek çok sistemin kalbidir, bir çok kullanıcı koruma sağlaması ve kontrolü için veritabanı sistem güvenliğine bel bağlamaktadır. Bu yazı tamamıyla veritabanı sistem güvenliğine ilişkin tehditleri ve bu tehditlere karşı korunma yollarını konu almaktadır. Veritabanı sistemleri neredeyse tüm devlet sektörlerinde, kuruluş ve işletmelerde kullanıldığından pek çok saldırı için popüler hedeflerdir ve güncel tehditlere karşı güvenlikleri sağlanmalıdır. Bu yazıda başlıca tehditler ve bu tehditlerden korunma yollarının açıklanması amaçlanmıştır.

Anahtar Kelimeler: Veritabanı Güvenliği, Veritabanı Tehdidi, Tehditleri Önleme, Güvenlik Sistemini Geliştirme.

ABSTRACT

The security of data it is the heart of many systems, many clients rely on database system security to manage and control the protection. This paper is all about the threats that inflect database system and the protection of database system from threats, to improve the security of database system from threats and outside attacks, now a day database is wildly used in many governments, organization and business. Therefore, database Systems are a favorite target for threats and attacks. This paper will provide an overview of the top threats and the way for securing database System.

Keywords: Database Security, Database Threats, Threats Prevention, Improve Security System.

1. INTRODUCTION

The database system security is a subject to a massive framework of attacks and threats. This paper is meant to help the system of the database and deal with the most serious of threats by preparing a list of the top database system threats. As defined by Imperva's Application Defense Center. The strategy course for general risks and Imperva's database security system protection is supported for each threat, protecting information is at the core of numerous secure systems, and numerous users depend on a database management system to deal with the protection. Databases are fundamental to numerous business and government associations, holding information that re-designed to make them more viable and more suitable for new and modified goals. Database security is a troublesome activity that any association should upgrade in a request to run its activities easily. The different threats posture a challenge to the association as far as the integrity of the information and access, the threats can affect either by an outside unlawful program activity or by an outside power..

2. WHAT IS DATABASE SYSTEM AND THREATS

A. Database system

A database is a collection of organized information and set of data that can be easily managed, accessed and updated. It is a data structure used for organizing data and information. The database contains fields which called tables that include different fields which organized to (row, column). The index inside each row and column will help to organize the information easily. The collected data and information can be expanded, update, delete and add new information. The process of database workload will query the data automatically to organizing collected information and data [1].

B. Database System Threats

Threats are dangerous to every organization which inflect a big damage and great loss of data in every system. Now in our day t he usage of database increased also the frequency of attacks and threats increased day by days, the reason of increasing attacks because of increasing in access to data collected and saved in databases which the attackers can control this information and dominance it to gain money by selling critical information or some

attackers they use this information for personal purpose [2].

3. TOP DATABASE SYSTEM THREATS

A. Denial of Service

Denial of Service (DoS) is a common threat that can access data or database functions which denied to contagious users, (DoS) used to shut down the database network or machine which making the database system out of reach , its intended user that perfect this steps by overwhelming the objective with traffic or publishing the information which triggers a disintegration in both cases.

(DoS)can be created by many techniques that connected to the system. For example, it can be created by an occupant of the database platform allergy to shatter the server. (DoS) attacks main point is to targeting Web servers which have a big database such as banking, media companies, commerce or trade organization and government which they will use techniques not to crush information or other property but to make a great deal of to get many which they want to handle.

There is two common type of (DoS) attacks: (Flooding Services and Crashing Services). Flooding attacks work when the system extradites much traffic at the time which makes the server to buffer, infect them to slow down the system and at last stopping it. Common Flooding attacks are (buffer overflow attacks, SYN flood, and ICMP flood). Crashing services attack targeting server or system to crush it, therefore, the input will try to gather advantage of errors in the target that posteriorly crush the database system or server so that the system cannot be used or accessed [3].

B. Excessive Privilege Abuse

Excessive privilege abuse is the threat that infects the particulate user account which they are used fraudulently and/or inappropriately, either accidentally, maliciously or out of purposed unawareness of policies. According to Verizon's 2017 Data Breach Investigation Report, Excessive privilege abuse in security incidents it is the second common cause and in breaches, it is the third most common cause.

Privilege abuse it will directly infect the system with poor access control that makes the organization fails to monitor and control the activity of privileged accounts. The user of the database ends up with undue concession, the administrator of the database does not have time to give access or define new users. As a result, the large groups of users are granted with default access which they are privileges that far exceed particular requirements. [4].

C. SQL Injection

The attack of SQL injection or typically injects ("inserts) the statements which they are recognized to the database and had a vulnerable SQL channel of data. Objective data that include Web application input parameters and stored procedures. These inserted functions will be pass to the system of the database and they will be executed. By using SQL attack injection, the hackers and attackers gain full access to control the entire database injection. Hackers may be able to get unlimited access to a whole database [3].

D. Database Communications Protocol Vulnerabilities

A creation of security systems which they are being recognized in the database correspondence protocols of all database firewall system. Security functions settle in two parts (IBM, DB2). Thus, 11 out of 23 database vulnerabilities settled in the latest Oracle system which they identify with protocols. Unrecognized attacks focusing on these weak points and they can extend from unapproved information access to data corruption to crush the access of administration. The SQL Slammer worm, for instance, developed firewall in Microsoft SQL Server protocol which compels denial of service. To control the situation, no record of these fraud functions will exist in the local system trail since protocol activities are not secured by local database administrator systems [5].

E. Weak Audit Trail

All unusual database or all sensitive transactions will be recorded automatically which they should be an index of the institution underlying of any database deployment. A database with weak audit policy performs a dangerous organizational peril on many levels [4].

- Regulatory Risk

any institute or organization with weak database audit technique will find that they are at different requirements of government regulatory. The Healthcare Information Portability and Sarbanes-Oxley (SOX) the financial services section are two examples that had a clear database audit requirement for government regulation [4].

- Detection and Recovery

The last line of database defense will be represented by audit mechanisms, if the hackers control the embrace of other defenses, the data can recognize after the fact of the existence of a violation. The data can be used to connect the violation to a special user or/and repair the system [4].

4. DATABASE THREAT PREVENTION

Threat protection point to the way of security solution that used against hacking-based attacks or advanced malware which targeting the collected data in a database system, can be available as managed services or software [6].

A. Denial of Service attack prevention

Denial of service (DoS) attacks cannot be decided, however, you cannot make yourself a prey for DoS attack. You can decrease the probability to be a portion of such attack, for increased security against DoS attack can rely on the bellow points which help to odds in your favor:

1) Securing the firewall and installing antivirus program into the used network is not already done. Which helps intercept the frequency range used for authenticated users only [7].
2) For third-party services which used for protection and guidance against DoS attack, they will be effective against DoS attack but they can be expensive [7].
3) To reduce the average of attacking server configuration can help, which make the network firewall more security and increase firewall policies to block out apocryphal users from addressing the resources of the server [7].

B. Excessive Privilege Abuse prevention

Privilege Abuse comes in two property:

Abuse of legitimate privileges and Abuse of excessive privileges. Abuse of legitimate privileges it's one of the attacks that defending it, it is so hard to make your database system safe from it actually nobody can prevent his/her system from it. In each organization which work database after inflecting the system with this attack only he/she can do is to make sure that the audit trail and the information of all account and review the audit log on regular basis, because there is no way to protect the system from Abuse of legitimate privileges [8].

The second one is Abuse of excessive privileges it can easily prevent because the database does do not grant unnecessary privileges to the user and every time at the start of running database user always follow the principles of the last privilege, but at the beginning, it needs to plan the prevent way during the development process. The developer will use different account user for different application function which makes it sure that the security architecture is part of all the application architecture [8].

C. Prevent SQL Injection Attacks

The good news is that actually there is an alloy of website owners can work to prevent SQL injection but the best way is to follow the bellow point to prevent your system from any SQL injection:

1) Employ thorough data sanitization: all user input should be filtered by the website and user data need to be filtered for more context. For example, email address and phone number need to be filtered which allow only the characters of email and phone numbers.
2) Limit database privileges by context: make different database user accounts with the base levels of benefit for their use condition. For instance, the code behind a login page should query the database utilizing an account restricted just to the important qualifications table. Along these lines, a break through this channel can't be utilized to trade off the whole database.
3) Firewall of a web application: using web application firewall is a good way to prevent your data safe, the firewall will install rules that filter and block dangerous web requests. Also, SQL injection defenses can catch and prevent most attempts to go through SQL web channels.
4) Repress message errors: these messages are an essential surveillance instrument for attackers, so keep them local if conceivable. If external messages are fundamental, keep them non-specific.
5) Bypass constructing SQL queries by user input: any data that sensitization can be flawed, using SQL variables and stored procedures or preparing statements it will be safer than constructing full queries.
6) Regularly apply software patches: SQL injection vulnerabilities are frequently distinguished in business programming, it is important to remain exceptional on fixing.

7) Continuously monitor SQL statements from database-connected applications: monitoring tools that utilize machine learning and/or behavioral analysis can be especially useful. This will help identify rogue SQL statements and vulnerabilities [9].
8) Remove and delete unnecessary database capabilities: principally those that spawn command shells and those that escalate database privileges.

D. Protection of Database Communications Protocol Vulnerabilities

Database correspondence convention assaults can be vanquished with innovation ordinarily alluded to as convention approval. Convention approval innovation basically parses (dismantles) database movement and thinks about it so desires. In the occasion that live activity does not coordinate desires, alarms or blocking moves might be made.

Secure sphere's database communication protocol validation reviews and ensures against convention dangers by contrasting live database communications protocol with expected protocol structures. No other database security or review arrangement gives this ability. It is gotten from the Imperva Application Defense Center's (ADC) progressing research into exclusive database correspondence conventions and vulnerabilities. Database and application vendors including Oracle, Microsoft, and IBM have acknowledged the ADC for the revelation of genuine vulnerabilities.

Moderation methods that have prompted expanded security in their items. In view of this examination, Imperva can fuse unmatched convention learning into Secure Sphere [8].

E. Protect from Weak Audit Trail

Organizations use native audit tools supported by database vendors or depend on manual solutions and ad-hoc, unfortunately. This process does not save the necessary details to support auditing, forensics and attack detection native database audit mechanisms are extremely notorious for consuming high CPU throughput and disk resources forcing many organizations to stop auditing [9].

Most native audit mechanisms are unique to a database server platform. associations with heterogeneous database situations, this forces a noteworthy hindrance to actualize uniform, versatile review forms. At the point when clients get to the database by means of big business web applications, (for example, SAP, Oracle E-Business Suite, or PeopleSoft) it can be trying to comprehend which database get to movement identifies with a particular client [10].

It is seen that review instrument have no familiarity with who the end client is on the grounds that exclusive record name is related to the web applications. Besides, native database auditing can be turn off by the users with administrative privilege to shroud any sorts of false movement. To guarantee solid partition of obligations arrangements, the Audit abilities, and duties must be isolated from both database executives and the database server stage [10].

5. PROTECTING DATA IN DATABASE SYSTEM

Every system or applications if their security is crashed or hacked they can be reinstalled but data which is unique and important in each database system before crashing or attacking the administrator need to protect and keep it safe from any outside threats, when the developer or the user think about it. The worthiest thing on your database system is the created data, because sometime the created or saved data when it's lost may be indispensable. Some data are secret not only you want to lose them also you don't want others to see it without approval [11]. The bellow points are the main points to protect data in general:

a) Daily Data Back up: back up is one of the most serious and important steps to protect data from threats or loss. By using Wizard Mode to extend the way of creating and recovering backups or by configuring the set of backups manually then stream backup jobs to be completed regularly. Using third-party backup software which gives more sophistical choices [11].
b) Share-Level or File-Level Security: to secure your data and keep it away from others the administrator needs to give the permissions to the collected or saved data and folders. In the database, if the administrator had a shared data he/she can set permissions for the shared data to control the user account to access or not to the file that shared across the network [12].
c) Document with Password-Protection: many software or applications will give the user and developer to set passwords on individual data for open and working with the data. To keep the data readable or make a

change to it. The user needs to know the password to get the access to the data [12].

d) EFS encryption: Encrypting File System (EFS): is the combination of symmetric and asymmetric encryption which use the Built-in certificate to work with encryption method for both performance and security that protect different data and files that stored on NTFS type partitions [11].

e) Disk Encryption: For Disk Encryption: there are many software and applications (Third-Party) which used to encrypt the entire disk which the backup file or the data of the database stored in. The Third-Party products lock the whole disk and encrypt it that make the stored data inside the partition automatically encrypted. Some of these products have the ability to create invisible containers that hide the stored data inside the partition [12].

f) Steganography to Hide Data: hide data inside other data is called steganography. For example, the user can hide text or small data inside MP3 music file or (.JPEG) graphics file even sometimes can hide it inside another text file. Steganography does not encrypt the message. Some steganographic methods require the trading of the secret key and others utilize private/public key cryptography. A mainstream case of steganography programming is StegoMagic. A freeware download that will encrypt messages and shroud them in (.TXT, WAV) or (.BMP) files [11].

g) IP Security at Transferring Data: the shared data or transferred data can be captured while traveling through the network by sniffer software or hacking also called protocol analysis or network monitoring software).

h) By using Protocol Security (IPsec) the sender can protect his/her data in transit but both systems (sender system and receiver system). Encapsulating Security Payload (ESP) is the convention IPsec uses to encrypt information and data for privacy. It can work in burrow mode, for gateway-to-gateway insurance or in transport mode for end-to-end assurance [11].

6. IMPROVE DATABASE SECURITY

1) Encryption of your database is one of the important ways to improve your database security. Encryption means converting the stored data in your database to format such that which has to be intercepted, that shown itself like numbers and strings of letters with no meaning. The converted data will be readable by database easily [1].

2) Another way to keep your database safe and protected you need to leave it out of sight which means don't link it to directly and hiding it from a search engine. While you need employees to approach database data, you might not have any desire to put the sign in directly on the site. On the off chance that you have an online database, help yourself and keep it on a need-to-know premise. All things considered, the initial move toward hacking a database is discovering it in any case [1].

3) To protect database breaches the developer or the user need to keep an eye on the database. Behaviors and monitoring access of database user the make sure that no wanted behavior is displayed which maybe be a leak, what's more, general reviews of your database help find inactive accounts, helping out issues that may emerge with somebody getting old employee information perform normal reviews, and your organization can take care of security before issues emerge [13].

4) The most sophisticated frameworks can't insure against an awful secret key. There are the typical culprits — ABCDE, 12345, whatever else on the most speculated password list — however, attackers have progressively sophisticated tools available to them that make numerous different passwords progressively powerless. Presently, it's not simply making your password "password" that you need to stress over. It can be words all by themselves. Software exists that figure passwords that may be worded in the lexicon or generally utilized expressions [13].

7. CONCLUSION

An important issue in a database system is security because all data and information which they are stored and saved in the database are very important, valuable and very sensitive. The collected data and stored data in database system need to be secured and protected from perversion and should be protected from untrusted access and updates. This paper approached its task by defining the main threats that infect and crash the stored data in every database system also discussing most important points and ways that every developer and user of database system need to know and work with it, to make a challenge that keep his/her database safe and secure from any outside threats and attacks. Also, this paper discussed the important requirements which they are necessary for database security and different level of security.

8. FUTURE SCOPE

This case study paper will be helpful for every organization that creates or develops their own database. They will understand the main issues of attacks and threats that may be suspended to every database system and damage the reliability and integrity of the database system. In the future using this paper for database security of advantage technology that helps the implementation, design, and operation of data in the database system and many other functions that give the assurance to implement a database with security and privacy requirement.

REFERENCES

[1] Morrison, Paul. "Database Security." Network Security 2003, no. 6 (2003): 11-12.

[2] Baybulatov, A. A. "An Example of Industrial System Databases Security Assurance during the Maintenance Stage." IFAC Proceedings Volumes 46, no. 9 (2013): 1091-1095.

[3] Khanuja, Harmeet Kaur, and D. S. Adane. "Database security threats and challenges in database forensic: A survey." In Proceedings of 2011 International Conference on Advancements in Information Technology (AIT 2011), available at http://www. ipcsit. com/vol20/33-ICAIT2011-A4072. pdf. 2011.

[4] Shelly, Gurleen Kaur. "A Review on Database Security."

[5] Rhee, Keunwoo, Jin Kwak, Seungjoo Kim, and Dongho Won. "Challenge-response based RFID authentication protocol for distributed database environment." In International Conference on Security in Pervasive Computing, pp. 70-84. Springer, Berlin, Heidelberg, 2005.

[6] Band, Jonathan, and Makoto Kono. "The Database Protection Debate in the 106th Congress." Ohio St. LJ 62 (2001): 869.

[7] Mirkovic, Jelena, Sven Dietrich, David Dittrich, and Peter Reiher. "Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)." (2004).

[8] Shulman, Amichai, and C. T. O. Co-founder. "Top ten database security threats." How to Mitigate the Most Significant Database Vulnerabilities (2006).

[9] Buehrer, Gregory, Bruce W. Weide, and Paolo AG Sivilotti. "Using parse tree validation to prevent SQL injection attacks." In Proceedings of the 5th international workshop on Software engineering and middleware, pp. 106-113. ACM, 2005.

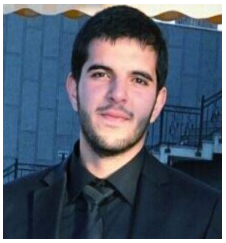
[10] Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. "Database security and encryption: A survey study." International Journal of Computer Applications 47, no. 12 (2012).

[11] Elmasri, Ramez, and Shamkant Navathe. Fundamentals of database systems. Addison-Wesley Publishing Company, 2010.

[12] Chen, Yu, and Wesley W. Chu. "Protection of database security via collaborative inference detection." In Intelligence and Security Informatics, pp. 275-303. Springer, Berlin, Heidelberg, 2008.

[13] Stallings, William, Lawrie Brown, Michael D. Bauer, and Arup Kumar Bhattacharjee. Computer security: principles and practice. Pearson Education, 2012.

ÖZGEÇMİŞ *(LER)*



Rasty Shakhawan Majeed

Rasty Shakhawan received the B.Sc. in Information system engineering from technical college of engineering, Erbil, Iraq In 2013. He is a student at the department of software engineering at Firat university, Turkey. He is working in National ID-Card for Iraqi government. He is CEO at Kaver company for engineering. He has interests in Computer Networking, Computer Programming,Computer Oranization and Design . He can fluently speak English and Arabic.

Asaf Varol

Dr. Asaf Varol is the Chair of the Software Engineering Department at College of Technology of Firat University in Turkey. He is the founder of the Department of Digital Forensics at Firat University which is first and still unique in Turkey. His research interests are cyber security, robotics, IoT Technologies, Digital Forensics, and Public Administration. He has published more than 300 articles, proceedings, books, etc. He can speak German, English and Turkish.