ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A Study on Threats Related to Databases and Data Security Measures

Nitin Nanda

B. Tech Scholar, Department of Computer Science and Engineering, JMIT, Radaur, Yamunanagar, India

ABSTRACT: In this paper, an emphasis has been made to outline the major threats to current database systems as they incur huge losses to the industry every year. The mistakes done by the system administrators and engineers that void the security of the databases have been outlined and the database security concepts have been discussed. The most commonly used cryptography techniques are also discussed along with their advantages and disadvantages. Various aspects of the encryption techniques have been studied and the immense scope of research and development in this field is identified. This paper serves as a path for further research in this field.

KEYWORDS: Database, Authentication, Integrity, Confidentiality, Cryptography, Encryption.

I. INTRODUCTION

The 21st century has seen some of the most revolutionary changes and developments related to databases. The shift from a manual query execution to automatic systems capable of handling up to a million queries per second has been dramatic. Nonetheless, it has posed huge security threats as most of the times, the data is centralized and a security breach could pose loss of highly valuable and personal data. Reports suggest that $16 billion worth of data was stolen in the year 2014. However, even with newer technologies in authentication techniques like biometrics and iris scanners, these threats continue to increase as more and more companies around the world are getting online and storing their information in the database.

At the ground zero, database security insures that only the authenticated users access the authorised data at authorised time frames. Database security is often overlooked by many firms and results in the vulnerability and frequent loss of information. There are many reasons for the risks involved in database security some of which are

- Lack of adequate guidance at the time of database setup
- Under-evaluating the possible threats
- Lack of skill
- Budget Constraints

The last factor is the most general one as developing a secure and personalized system can cost relatively high as compared to the overall cost of the system. Various database threats will be analysed and the latest security measures will be discussed in this paper, thus providing an insight into the current security systems.

II.THREATS TO THE DATABASE

As discussed previously that databases are mostly compromised when the overall expenditure in any firm is calculated. Unlike a decade ago, database thefts are now primarily done to sell sensitive information and earn money. Following are the major loopholes in the security systems.

Authentication abuse: The employees of the company or the database users are often given privileges that work beyond their domain. This might be intentional or un-intentional but in either way, cause a great loss to the concerned institution. For example, if a bank employee is able to perform banking operation from his home system during the off-working hours, then the security of the sensitive data cannot be ensured unless the computer is equipped with a biometric verification system.

Database Backup Vulnerabilities: Most of the data in any organisation is regularly backed up in a separate disk so that in case of loss of the data, it can be restored. But more often, these disks are not safeguarded properly and thus account for about 20% of the total data breaches. Smart methods must be implemented such as using multiple keys associated with multiple people so that even when one of the key has been disclosed, the data is still safe.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

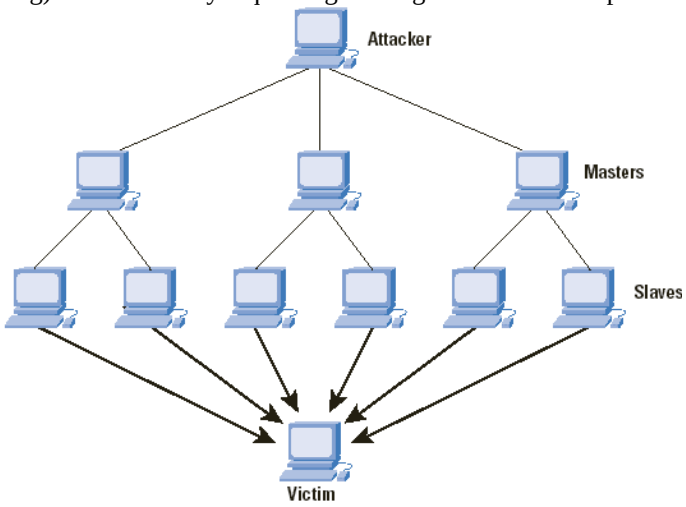
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Malwares: These spread through internet, infected devices and unauthorised programs that are run on the system. The malwares secretly watch the activities and the login credentials. Firewalls and anti-malware softwares can be used to protect against these threats.

Weak Audit Mechanisms: Audit mechanisms as the last line of defence for any database. Audit trials can detect any violation and help in tracing back to the point where the violation has occurred. Logging of data must be done through an automated mechanism with minimal human intervention. Industries such as e-commerce, retail, banking and finance are at a greater risk. Recently, a bank in the country India called back and replaced its 3 million debit cards when it found a possible threat in the security details of its customers.

Operating System Vulnerabilities: Vulnerabilities in the operating system like Windows and Unix can lead to unauthorised access. Sometimes, this lead to DoS (Denial of Service) attacks in which the system is unable to fulfil any request from the server as it has been flooded with more requests than it can handle. This is done by using thousands of IP addresses(IP address spoofing) simultaneously requesting the target machine to respond.



III. DATABASE SECURITY CONCEPTS

Database security can be defined mainly by three factors: Availability, Integrity and Confidentiality. Availability of data means that authorised users are able to access information at all the times. As discussed earlier that DoS attacks are used to prevent access of information even by the authorised users. Having an off-site backup of all the data is also very important for any institution. Integrity of the data means that data cannot be modified by any unauthorised person. Integrity of data can be maintained by using the following steps.

- Periodically changing the passwords and ensuring that its integrity is maintained.
- Allowing only the required rights to the employee or user. Any access allowed outside their domain will prove to be harmful.
- Setting strong passwords which includes both lower and upper class letter, numeric and other symbols such as the dollar($) or hash(#) sign.

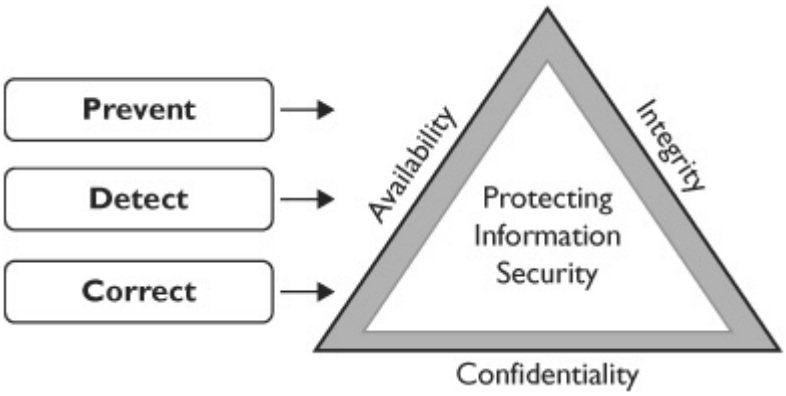
Confidentiality of information refers to protecting the information from unauthorised access. Every day we see that it's written on various websites that it is 128 bit encrypted or 256 bit encrypted. There are two different levels at which encryption can be done: data in transit and data at rest.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016



Data-in-transit is the data which is being moved from one location to another either via internet or any other system of networks. Such data is always at a higher risk of getting leaked or tampered. To prevent this, Encryption and Digital Signature techniques are used.

Data-at-rest is the data stored in the database. It is also vulnerable to theft as it may contain information such as credit card details and contact information. Different encryption algorithms are available such as DES (Data Encryption Standards), 3DES and the Advance Encryption Standards i.e. AES.

IV. SYSTEM SECURITY ASSESSMENT

A Database administrator can ensure that necessary security functions are integrated into the design and implementation of the system. The security check should provide the gaps in the security of the system which can be managed to ensure the security of the sensitive information:

Security policy creation: A strict security policy should be created while the database is being setup. The access rights for the various levels of employees, users and administrators should be clearly defined and no access right which is outside their field of work should be provided. Regular assessment and analysis of the system should be done with the help of security professionals.

Alerting and Blocking for Possible Threats: All database access must be regularly checked and any malicious activity must be immediately blocked. Security policies are useful for detecting privilege abuse by malicious users as well as for preventing most of the other database threats.

Removing Excessive Rights: Identifying the user who has access rights which are not required by them. Hackers might use these excess rights to reach the sensitive information. It helps in protecting against malware and targeted attacks. Moreover, the user who is not using his/her account for long must be blocked and their access rights must be suspended.

Detect Unusual Access Activity: Establish an audit log of each database user's routine activity. Deviation from the normal behavior of the users enables detection of DoS, malware and anomalous activities. Any user who attempts to perform any activity which in not in his/her domain must be immediately, by an automated system. The initial cost of such system might pose to be huge but it helps in preventing from possible threats in the long run. Creating such activity-based user records increases the possibility of detecting unauthorized access to sensitive data.

Auditing with a DAP Platform: (Distributed Application Platform) It enables much easier scalability, flexibility and cross- platform auditing which is otherwise quite difficult to perform on a heterogeneous system. Local database activity can also be closely monitored as the users with most access rights can cause a greater damage. A closer look at the issue suggest that auditing plays a primary role in securing the database but most of the companies fail to hire a dedicated workforce to constantly check and evaluate the log records.

Educating Workforce: The policy makers are responsible for guiding their sub-ordinates about the various aspects and security measures to be taken on their end. For example, creating a complex password and periodically updating it will help in curbing the possible threats. Similarly, any suspicious activity should be immediately reported to the concerned authorities.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

V. ENCRYPTION TECHNIQUES

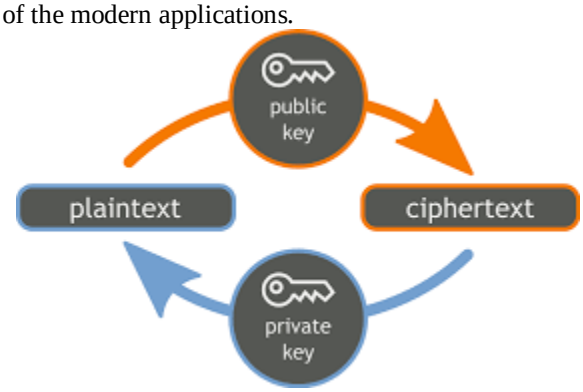
Encryption in the process of converting a piece of information (the plaintext) into encrypted form (the ciphertext). The sender encrypts it with the help of a public key which can be decrypted only by the use of a private key, which is at the end of the recipient. Initially symmetric-key encryption mechanisms were used but due to less security provided by it, its used is now abandoned and public key encryption techniques are used.

Data is very valuable for an organisation and framework which was proposed to store all the information on the disk and while transmitting the data has proved to be beneficial. However, the implementation of the encryption techniques is also very important. The Advanced Encryption Standard (AES) is now being used worldwide as a standard of encryption. AES uses fixed key sizes of 128, 192 and 256 bits, out of which 128 bit encryption is the most generally used. The level of security achieved by 256 bit encryption can be understood from the fact that it would take more than a trillion years to crack the encrypted data. The most widely used encryption techniques are as follows:

Internet Protocol Security (IPSec): IPSec is a protocol suite which works by authenticating and encrypting each IP Packet. It involves establishing a mutual consent between the sender and the receiver at the beginning of the session as they share the cryptographic keys to be used during the communication process. IPSec can be used to secure data flow between a pair of hosts, a host and a network of between two independent networks. This is an end to end encryption technique and thus it protects the information at the sender and receiver's end only and not during the actual transit of the IP packets. The advantage of IPSec over other security protocols is that it operates at layer 3 and has no impact on the higher network layers. The disadvantage being that it burdens the network with an overhead due to which the transmissions speeds have to be compromised. To overcome this, PCI chips and additional hardware is required.

Secure Multipurpose Internet Mail Extensions (S/MIME): The usability of SMIME in near future is expected to increase as it supports the encryption of both multimedia as well as plaintext files. However, due to some of its drawbacks such as the use of a 40-bit key to encrypt the messages seems to be not as secure as other protocols. It is said that a group of hackers can easily crack a message encrypted by a 40- bit key. SMIME is being developed by a group of companies (including the RSA Data Security) and work is being done to develop the 56-bit and the 168-bit keys in a more efficient manner. Another disadvantage of S/MIME is that the data is encrypted end to end. Therefore if a malware was present in the plaintext file and it is encrypted at the senders end then it would be impossible for malware detection system to scan it at the receivers end and thus poses great threat to the security.

Pretty Good Protocol (PGP): PGP encryption uses a combination of hashing, data compression, symmetric key cryptography and public key cryptography. It is the most popularly used encryption technique as it can be used for encrypting and decrypting e-mails, files and even large amounts of data in a disk and thus can be used to encrypt the whole database. Even if the data is stolen, it cannot be transformed into readable form unless its decryption key is known. Confidentiality is maintained by the use of a "session key" or simply a symmetric key. It is a one-time key which is sent along with the encrypted data to the receiver. The receiver can decrypt it using its public key. Digital signatures are another application of the PGP as it ensures that the data which was sent is delivered unaltered. They have become a necessary part of the modern applications.



The disadvantage of PGP is its inability to handle multimedia data and to resolve this PGP/MIME has been developed. Other protocols like MOSS(MIME Object Security Services) and MSP(Message Security protocol) were also developed but never used widely because of the popularity of the PGP and the PGP/MIME protocols.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

VI. CONCLUSION AND FUTURE WORK

The paper has discussed the threats to the databases and the innovations in this field. Various institutions and organizations are now getting dependent on databases and maintaining the integrity of the data is a major concern. The research paper has attempted to explore the reasons why proper security systems are not implemented by organizations using the databases to store their sensitive information and the strict budget and unawareness about the possible threats turns out to be the prominent reasons. Various techniques that can be used to secure databases of varying sizes are also discussed which range from implementing the general security policies to the complex algorithms and audit mechanisms. The paper briefly describes the fundamentals of encryption and the various techniques used nowadays to encrypt the stored as well as the data in transit. It is found that PGP is the most widely used mechanism because of its greater security and reliability factors. Work is being done to develop much better cryptography techniques and upgrade the existing ones to match the pace of the industry.

REFERENCES

1. Stephens, Ryan (2011). Sams teach yourself SQL in 24 hours. Indianapolis, Ind: Sams. ISBN 9780672335419.
2. Ravi Sandhu, Elisa Bertino, "Database Security-Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, vol. 2, no. , pp. 2-19, January-March 2005.
3. Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
4. Hershey, William; Easthope, Carol (1972). A set theoretic data structure and retrieval language. Spring Joint Computer Conference, May 1972
5. Proctor, Seth (12 July 2013). "Exploring the Architecture of the NuoDB Database, Part 1". Archived from the original on 15 July 2013
6. Ullman, Jeffrey; Widom, Jennifer (1997). A First Course in Database Systems. Prentice–Hall. ISBN 0138613370.
7. Chapple, Mike (2005). "SQL Fundamentals". Databases. About.com. Archived from the original on 22 February 2009. Retrieved 28 January 2009.
8. Singh, Simon (1999). The Code Book. Doubleday. pp. 279–292
9. Blakley, G. (June 1979). "Safeguarding cryptographic keys". Proceedings of AFIPS 1979. **48**: 313–317
10. Schneier, Bruce (15 June 2000). "The Data Encryption Standard (DES)". Crypto-Gram. Retrieved 26 March 2015.
11. Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques". AFIPS Proceedings. **45**: 109–112.
12. Turner, Dawn M. "Digital Authentication: The Basics". Cryptomathic. Retrieved 9 August 2016.
13. Goldreich, Oded. Foundations of Cryptography: Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.
14. Vijayan Prabhakaran (2006). "IRON FILE SYSTEMS" (PDF). Doctor of Philosophy in Computer Sciences. University of Wisconsin-Madison. Retrieved 9 June 2012

BIOGRAPHY

Nitin Nanda is a B. Tech scholar in the Computer Science Department, Jai Prakash Mukand Lal Institute of Technology, Kurukshetra University, India. His areas of interest are database management, security and software design.