ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Web Database Security Techniques

Sweety R. Lodha[1]
Dept. of Computer Science and Engineering
Sipna College of Engg. and Technology
Amravati, Maharashtra,
India

S. Dhande[2]
Assistant Professor
Dept. of Computer Science and Engg.
Sipna College of Engg. and Technology
Amravati, Maharashtra, India

Abstract: ***The paper mainly focuses on security issues that are associated with the database system. Data security is one of the most crucial and a major challenge in the digital world. Security, privacy and integrity of data are demanded in every operation performed on internet. Whenever security of data is discussed, it is mostly in the context of secure transfer data over unreliable communication networks. But the security of the data in databases is also an important. In this paper we will be presenting various issues in database security such as goals of the security measures, threats to database security and some of the common security techniques for the data that can be implemented in strengthening the databases.***

Keywords:

I. INTRODUCTION

Information or data is one of the most valuable properties in any organization. Almost all organization whether social, governmental, educational etc., have now computerized their information systems and other operational functions. They have maintained the databases that contain the vital information. So database security is a serious measure. Protecting the confidential/sensitive data which is stored in a database is actually the database security. It deals with making database secure from any kind of illegal access or threat at any level. Database security has difficulty while permitting or prohibiting user actions on the database and the objects inside it. Organizations that are running successfully have challenge for the confidentiality of their database. They do not allow the unauthorized user to access their data/information. And they are also having challenge to the assurance that their data is protected against any malicious or accidental modification. Data protection and confidentiality are the security concerns. Figure 1 below shows the properties of database security [1][2][3] :

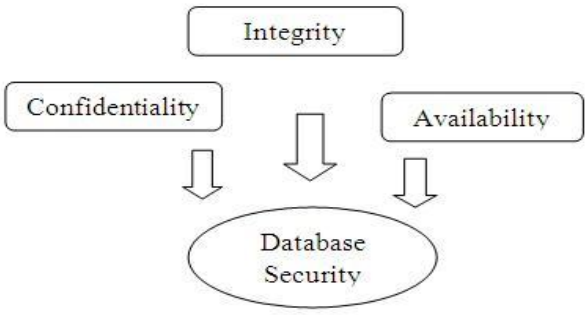

Fig. 1 Database Security Properties

Security in today's world is one of the important and challenging tasks that people are facing all over the world in every facet of their lives. Similarly security in electronic world having great demand. Protecting the confidential/sensitive data stored in a database is actually the database security [4]. There are different security layers in a database. These layers are: database administrator, system administrator, security officer, developers and employee [4] and security can be added at any of these layers by an attacker.

A. Categories of Attacker

An attacker can be categorized into three possible categories [4]:

- Intruder :

An intruder is a person who is an unauthorized user means accessing a computer system in an illegal manner and attempts to take out valuable information which is stored in database.

- Insider :

An insider is a person who is one of member of group of trusted users and makes violence of his/her privileges and tries to get information beyond his own access permissions.

- Administrator :

An administrator is a person who is the authorized user to administer a computer system, but uses her administration privileges in unauthorized way according to organization's security policy to spy on DBMS behavior and to get valuable information.

II. Different Types of Attacks

An attacker, after violating through all levels of protection, he will try to do one of the two following attacks [6]:

A. Direct attacks

A direct attack means attacking the targeted data directly. These types of attacks are obvious and are successful only if the database does not contain any protection mechanism. If this attack fails, the attacker tries to the next.

B. Indirect attacks

Indirect attacks are the attacks as the name indicates that are not directly executed on the target but information from or about the target can be received through other intermediate objects. Combinations of different queries are used and some of them having the purpose to cheat the security mechanisms. These attacks are difficult to find out or track. The attacker executes the above attacks in various ways.

Attacks on database can also be classified into two type's i.e. passive and active attacks [5]:

1) Passive Attack :

In passive attack, attacker only observes data present in the database. Here, attacker doesn't make modifications to the data. Passive attack can be done in following three ways:

- Static leakage: In this type of attack, information about database plaintext values can be acquired by observing the snapshot of database at any particular time.
- Linkage leakage: Here, information about plain text values can be obtained by linking the database values to position of those values in index.
- Dynamic leakage: In this, changes carried out in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

2) Active Attacks :

In active attack, actual database values are modified. These are more problematic than passive attacks because they can mislead a user. For example a user will receive wrong information in result of a query [5]. There are different ways of performing such kind of attack which are mentioned below:

- Spoofing – In this type of attack, cipher text value is replaced by a generated value.
- Splicing – Here, a cipher text value is replaced by different cipher text value.
- Replay – Replay is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

Databases are one of the favorite goal for attackers because of the data these are containing and also because of their volume [6].

III. WEB SECURITY THREATS

(a) AJAX SECURITY

As web applications become increasingly complex, it is essential for the performance of web services is also increasing. AJAX (Asynchronous JavaScript and XML) technology is mainstream technology of Web2.0 that facilitates the browser to provide users with more natural browsing experience. With asynchronous communication, user is able to submit, wait and refresh freely, update partial page dynamically. So it allows users to have a smooth experience similar in desktop applications.

However, different kinds of web applications has brought us countless convenience, produced a series of security problems. AJAX having lack of ability to solve the security problems, the traditional web security problems still exist, along with elements of the composition and structure of AJAX features, will lead to new security threats. In recent years, adding AJAX elements in sites has become a very popular style, and most of the websites are typical AJAX-based applications. As most of the website builders just enjoy the conveniences of AJAX technology, but they are not fully aware about its security threat, resulting in most of the AJAX application sites have different levels of security risks.

Here, we have reviewed and analyzed the AJAX security threats.

1. Security Threats of AJAX Technology:

The Deficit of JavaScript Language: JavaScript is a widely client-side scripting language, originally designed and implemented by Netscape, and it has been broadly used to reduce the load on the server. JavaScript is the scripting language determines its presence in all kinds of security risks. JavaScript is an interpreted language. In the process of interpretation, every error must be runtime error. Run-time error can only be found during running time of program, we cannot observe it before its execution. If somewhere in the code the bug has remain, but the logic of the code at run time is not running to the area, then the error will not be found, which leaving major risks to the application. To detect or locate the error position of interpreted language is somewhat difficult. JavaScript is a weak type language. Weak typing languages do not need to declare variables when the programmers declare the variable. This flexibility often easily leads to many difficulties. JavaScript code has active nature. It can be dynamically generated code, and used the eval() function dynamic execution; or you can directly make changes to the existing function. Once the attacker can acquire control of the JavaScript code, he can overwrite the other user-defined functions and even the browser built-in method, thus cause many severe malicious behaviors.

Problems of Asynchronous: Asynchronous communication is the highlights and basic idea of AJAX technology. But asynchronous will also introduce a sequence of competition problems.

2. Cross site scripting

Cross-site Scripting (also known as XSS or CSS) occurs when dynamically generated web pages display input that is not properly authenticated. In XSS, malicious attackers acted as normal users upload malicious script as JavaScript codes etc. to web server by utilizing the bugs of utility programs or codes in the web server. Attackers also send URL links including malicious script to objective users. When web users visit the pages having malicious script or open the received URL links codes in the web sites, users' browsers will auto-load and execute the malicious script codes. This attacking procedure indicates that XSS is actually a simple attack technology. In most cases, malicious attackers attack users in indirect way by utilizing web

server, and direct attack occurs simply. XSS is a passive attack. First of all, by utilizing the XSS bugs in the web programs, malicious attackers construct a trap page and the malicious script can be saved in the page content or URL. The URL of this page is then announced in the BBS after embedding to e-mails or disguising attractive titles. If the visitors visit URL, the JavaScript will be executed by attackers' browser. The procedure of XSS attack is shown in fig. 2.

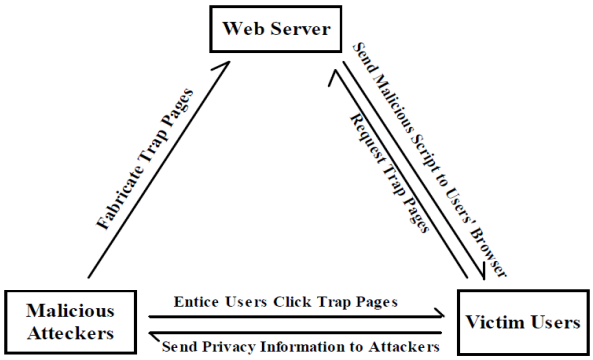

Fig. 2 Cross Site Scripting Attack Process

IV. DATABASE SECURITY CONSIDERATIONS

To eliminate the security threats every organization must having its own security policy. And that security policy should be strictly enforced. A strong security policy must contain well defined security features. Following figure shows some critical areas that need to take in consideration are explained below.[7][8][9]

A. Access Control

Access control ensures all communications with the databases and other system objects are according to the policies and controls defined. This makes sure that no obstruction occurs by any attacker neither internally nor externally and thus, protects the databases from potential errors. Errors that can make impact as big as stopping firm's operations. Access control also helps in minimizing the risks that may directly impact the security of the database on the main servers. For example, if any table is accidentally deleted or access is modified the results can be roll backed or for certain files, access control can restrict their deletion.

B. Inference Policy

Inference policy is required to protect the data at a particular level. It occurs when the interpretations from certain data in the form of analysis or facts are required to be protected at a certain higher security level. It also determines how to protect the information from being released.

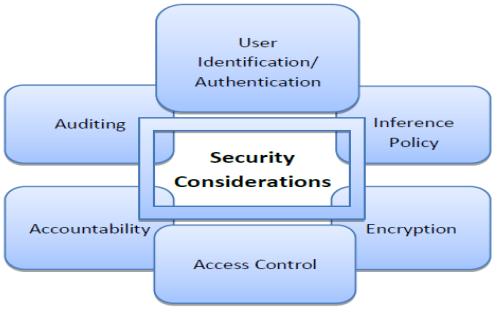

Fig. 3 Critical Areas Considered

C. User Identification /Authentication

User identification and authentication is the basic necessity to ensure security since the identification method describes a set of people that are allowed to access data and provides a complete mechanism of accessibility. To ensure security, the identity is authenticated and it keeps the sensitive data secure and from being modified by any ordinary user.

D. Accountability and auditing

Accountability and audit checks are required to ensure physical integrity of the data which requires defined access to the databases and that is managed through auditing and record keeping. It also helps in analysis of information held on servers for authentication, accounting and access of a user.

E. Encryption

Encryption is the process of transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. The resulting encoded information is called as encrypted information.

V. RECENT USED DATABASE SECURITY TECHNIQUES

In this section we list recently used security techniques that may prove useful in fortifying the database.

A. Securing Database using Cryptography

Sesay et al. proposed a database encryption scheme. In this scheme the users are divided into two levels: Level 1 (L1) and Level 2 (L2). Level 1 users have access to their own private encrypted data and the unclassified public data, whereas Level 2 users have access to their own private data and also classified data which is stored in an encrypted form.

Liu et al. proposed a novel database encryption mechanism [10]. The proposed mechanism performs column-wise encryption that allows the users to classify the data into sensitive data and public data. This classification helps in selecting to encrypt only that data which is critical and leaves the public data untouched thereby reducing the burden of encrypting and decrypting the whole database, as result of which the performance is not degraded.

Mixed Cryptography Database [1] scheme is presented by Kadhem et al. The technique involves designing a framework to encrypt the databases over the unsecured network in a diversified form that comprise of owning many keys by various parties. In the proposed framework, the data is grouped depending upon the ownership and on other conditions.

B. Securing Database using Steganography

Das et al. explained various techniques in steganography that can be implemented to hide critical data and prevent them from unauthorized and direct access. The various techniques include still image steganography, audio steganography, video steganography, IP Datagram steganography.

Naseem et al. presented a method that uses steganography to hide data. In the proposed scheme the data is embedded in the LSB's of the pixel values. The pixels values are categorized into different ranges and depending on the range certain number of bits is allocated to hide the sensitive data.

Kuo et al. presented a different approach to conceal data. In this scheme the image is divided into fixed number of blocks. Histogram of each block is calculated along with the maximum and minimum points to mask the data. This mechanism increases the hiding capacity of the data.

Dey et al. employs a diverse approach to efficiently hide the sensitive data and escalate the data hiding capacity in still images. The technique involves using prime numbers and natural numbers to enhance the number of bit planes to cloak the data in the images.

C. Securing Database using Access Control

Bertino et al. explains an authorization technique for video databases. In the proposed scheme, the access to the database and to a particular stream of the video is granted only after verifying the credentials of that user. The credentials may not just be

the user-id but it may be the characteristics that define the user and only after successful verification of the credentials the user is granted the permission to access the database.

Kodali et al. presented a generalized authorization model for multimedia digital libraries. The scheme involves integrating the three most common and widely used access control mechanisms namely: mandatory, discretionary and role-based models into a single framework to allow a unified access to the protected data. The technique also addresses the need of continuous media data while supporting the QoS constraints alongside preserving the operational semantics.

An authorization model is proposed by Rizvi et al. In the explained technique is based on authorization views which enable authorization transparent querying in which the user queries are formed and represented in terms of database relations and are acceptable only when the queries can be verified using the information contained in the authorization rules. The work presents the new techniques of validity and conditional validity which is an extension of the earlier work done in the same area.

VI. CONCLUSION

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. Databases are a favorite target for attackers because of their data. There are many ways in which a database can be compromised. There are various types of attacks and threats from which a database should be protected. For securing the data which considerations we have to take in account is mentioned in this paper and all the techniques which are recently used for database security.

References

1. Kadhem, H.; Amagasa, T.;Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 –170
2. Luc Bouganim; Yanli GUO; Database Encryption; Encyclo- pedia of Cryptography and Security, S. Jajodia and H. van Tilborg (Ed.) 2009, page(s):) 1-9
3. Khaleel Ahmad; Jayant Shekhar; Nitesh Kumar; K.P. Yadav; Policy Levels Concerning Database Security;
4. International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368-372.
5. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,"*Database Security and Encryption: A Survey Study*", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.
6. Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, "*Review of Attacks on Databases and Database Security Techniques*", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.
7. Emil Burtescu, "*DATABASE SECURITY - ATTACKS AND CONTROL METHODS*", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.
8. Ahmad Baraani-Dastjerdi; Josef Pieprzyk; Baraanidastjerdi Josef Pieprzyk ; ReihanedSafavi-Naini, Security In Databases: A Survey Study, 1996
9. Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.
10. Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009
11. E. Anupriya, Sachin Soni, Amit Agnihotri, Sourabh Babelay, "Encryption using XOR based Extended Key for Information Security – A Novel Approach", International Journal on Computer Science and Engineering (IJCSE), vol. 3, issue 1, Jan. 2011, pp. 146-154.

AUTHOR(S) PROFILE

Sweety Lodha received B.Tech. degree in Information Technology in 2013 from Government College of Engineering Amravati(An Autonomous Institute of Government of Maharashtra) and now pursuing M.E. from Sipna College of Engineering and Technology, Amravati.

