Database security and encryption: a survey study

This is an area of substantial interest In database because we know that, the use of database Is coming very important In today’s enterprise and databases contains Information that is major enterprise asset. This survey was conducted to identify the issues and threats in database security, requirements of database security, and how encryption Is used at different levels to provide the security. Abdul Wabash Mazurka There are four types of controls mentioned by Deeding [1] to obtain the database protection, those Includes: access control, Information flow control, cryptographic flow control and inference control.

Integrity Confidentiality OF 23 General Terms Your general terms must be any term which can be used for mineral classification of the submitted material such as Pattern Recognition, Security, Algorithms et. Al. Keywords Database Security Database, Security, Encryption, Access Control. 1. INTRODUCTION We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Information or data is a valuable asset in any organization. Almost all organization whether social, governmental, educational etc. , have now automated their information yester and other operational functions. They have maintained the databases that contain the crucial information. So database security is a serious concern. To go further, we shall first discuss what actually the database security is? Protecting the confidential/sensitive data stored in a repository is actually the database security.

It deals with making database secure from any form of illegal access or threat at any level. Database security demands permitting or prohibiting user actions on the database and the objects inside it. Organizations that are running successfully demand the confidentiality of heir database. They do not allow the unauthorized access to their data/information. And they also demand 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 that are: confidentiality, integrity and availability As discussed previously confidentiality imposes limits while retrieving the secure data and therefore averting the illegal access to the data. Integrity means that the data will not be tainted in any way. Availability of data on time is the property of secure databases. Access controls ensures that all direct accesses to the system are authorized. The access controls governs that that can access the system’s objects.

Often it happens that important information or data is leaked out or misused not because of defective access control but because of improper information flow. When policies for information flow are not properly defined than the system data is less protected. The cryptographic control, controls (secures) the data by encrypting it. Another approach has been adopted for securing the databases. It has been discussed that to make the databases secure different policies at organization level can be implemented. Data/information is always a most important asset for any organization whose security cannot be compromised.

With the advances in technology, the risk to these valuable assets increases. So their security is a big challenge. In [8] different database security layers are defined shown in figure (2) below. These layers are: database administrator, system administrator, security officer, developers and employee. For each layer some well-defined security policies have been anticipated. These policies ensure the security features, rivalry, confidentiality and integrity. This study mainly focuses on issues in databases security and measures taken to solve those issues.

Securing sensitive data from illegal access, theft and forging becomes a big challenge for different organizations, like government, no-government and privates sectors. Encryption of data in client or server side where data is shared between different parties is not sufficient. Basically the problem is to ensure that semi trusted database is secure or not. [6] 28 International Journal of Computer Applications (0975 – 888) Volume 47- No. 1 2, June A new hypothesis for database encryption is proposed in which database encryption can be provided as a service to applications with unified access to encrypted database.

Using such an encrypted data management model, applications can concentrate on their core businesses and protect data privacy against both malicious outsiders and the entrusted database service users without need to know encryption details. [12] example of university can be quoted in which an administrator who is given access t all databases and holds the privilege to change the records of any student. This may lead to misuse harmed to any student. As a result, all users who perform different tasks are given default level of privileges that grants access in excess.

Security Officer DAB System Admit Developer Employee Weak Authentication Denial of Service Security police Backup Data Exposure Risks s are check d at these Internet Data Communication Protocol Vulnerabilities layers Weak Audit Privilege Elevation SQL Injection Excessive Privilege Abuse Platform Legitimate privilege Abuse Fig 3: Databases Security Risks 2. 1. 2 Legitimate Privilege Abuse Intruder Legitimate privilege abuse can be in the form of misuse by database users, administrators or a system manager doing any unlawful or unethical activity.

It is, but not limited to, any misuse of sensitive data or unjustified use of privileges. Fig 2: Security layer at organizational level Further we shall discuss what actually has been implemented to reduce/eliminate the security threats and how the database security was enhanced in the past. And we shall see what needs to be done for securing a valuable asset, the databases, of organizations. 1. 1 Organization of Paper This paper is organized into different sections. In section 2, related work to databases security is deliberated.

Comparative analysis is presented in section 3 and conclusion is given in section 4. Section 5 sketches the future work. 2. RELATED WORK 2. 1 Security Risks to Databases The initiative database organization is subject to prodigious variety of threats. Some presented by Improver's Application Defense Center. [3] 2. 1. 1 Excessive Privilege Abuse When users are specified with the access rights that allow them to perform other tasks not included in their Job, harmful intent can be discovered through such tasks thus leading to misuse of such privileges. When we talk of such abuse, an . . 3 Privilege Elevation Excessive exposure leads to discovery of flaws which is

taken advantage of by attackers and may result in the change of privileges e. G. Ordinary user given the access of administrative privileges. The loss of which could result in bogus accounts, transfer of funds, misinterpretation of certain sensitive analytical information. Such cases are also found to be in database functions, protocols and even SQL statements. 2. 1. 4 Database Platform Vulnerabilities Vulnerabilities in the previous operating systems such as Widows 98, Windows 2000, etc. Ay create data loss from a database, data corruption or service denial conditions. For instance, the blaster worm created denial of service conditions from a vulnerability found in Windows 2000. 2. 1. 5 SQL Injection Random SQL queries are executed on server by some spiteful attacker. In this attack SQL statement is followed by a string identifier as an input. That is validated by the server. If it does not get validated it might get executed. Through these unobstructed rights may gain by the attackers to the whole database. 29 2. 1. 6 weak Audit Trail – 888) volume 47- NO. 2, June A database audit policy ensures automated, timely and proper recording of database orientations. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization’s databases and may cause instability in operations . Identification/ Auditing 2. 1. 7 Denial of Service It is the attack that prevents the legitimate users of a program/application/data to use or access that specific service.

DOS can take place using different technique. Attacker may get access to database and tries to crash the server or resource overloading, network loading and data corruption can be the techniques for creating conditions of

DOS attack. It is a serious threat for any organization. Considerations Accountability Inference Policy Encryption Access Control 2. 1. 8 Database Communication Protocol Large number of security weaknesses is being identified in the database communication protocols of all database retailers.

Deceitful activity directing these susceptibilities can varies from illegal data access, to data exploitation, to denial of service. 2. 1. 9 Weak Authentication A weak authentication strategy renders the databases more vulnerable to attackers. The identity of database users are stolen or the login credentials are obtained through some source which then helps in modification of data or obtaining sensitive information and if authentication is not properly implemented and is weak, it helps the attacker to steal data. 2. 1. 0 Backup Data Exposure Backup data exposure is an important threat that needs to be taken care of. Since backups on tapes, DVD’s or any external media are exposed to high risks, they need to be protected from attack such as theft or destruction. So far we he we shall see what can be done to limit these risks and threats. . 2 Database Security Considerations To eliminate the security threats every organization must define a security policy. And that security policy should be strictly enforced. A strong security policy must contain well defined security features.

Figure 2 shows some critical areas that need to be considered are explained below. 2. 2. 1 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 interference occurs by any attacker neither internally nor externally and thus, retests 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. 2. 2. 2 Inference Policy Inference policy is required to protect the data at a certain level. It occurs when the interpretations from certain data in the form of analysis or facts are required to be retorted at a certain higher security level. It also determines how to protect the information from being disclosed. Fig 4: Critical Areas under Consideration 2. 2. User Identification/Authentication User identification and authentication is the basic necessity to ensure security since the identification method defines 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 safe and from being modified by any ordinary user. 2. 2. 4 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. 2. 2. 5 Encryption 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. Data is valuable assets of an organization. So its security is always a big challenge for n organization. In recent times security of shared databases was studied through cryptographic viewpoint.

A new framework was proposed in which different keys are used by different parties to encrypt the databases in assorted form that was named as mixed cryptography database (MUCH). [6] Different governmental, non-governmental, and private and many other organizations have sensitive data on web servers that really need to be protected from attacker or intruders. To make the databases secure different security techniques were developed. One of them is encryption techniques. Though encryption improves the protection but its implementation decisions are also very important. Like what, how, when and where is to be encrypted..

Following figure 4 shows where encryption takes place. Developing the encryption strategies arises some important questions also, like how, when and where the encryption will be performed. Trusted Third Party To make the databases protected, encryption techniques are widely used. Implementing encryption on databases is though not an easy task [9]. But it is generally known as solitary the key concerns of data security. However preserving data rivalry providing boosted data sharing, an innovative encryption scheme is proposed. Secure data is protected and key management is done efficiently. That helps to share the encrypted data easily.

Encryption provides the confidentiality in databases. Server 1 Server 2 Server 3 Encryption algorithm, key size and keys protection are the parameters that ensure the security. The better the encryption algorithm is used the better will be the security. And with strong encryption algorithm, appropriate operation mode is also very important. To overcome the problem of unauthorized access of keys, two solutions were proposed. HAS and Security server approach. After the addition of security server or HAS that

lessen the disclosure of encryption keys, database is still vulnerable to threats.

Server n Fig 5: Three Levels where Encryption is performed. Encryption algorithm, symmetric or asymmetric is not explained in this framework. Query processing performance is badly affected by these algorithms. The encryption algorithms affect the performance of query processing and security analysis. Other important research issues related to this framework: first, the best encryption algorithm used in the mixed cryptography database on performance and security respective; second, access control methods used to control access for all parities using the database; and finally indexing and Joining between different databases.

According to [7], it does not matter which access control method is used; there are no of ways to avoid the authorization imposed by the database server. For instance, the information system can be intruded by stalker who tries to source the database impression on disk. Databases are being outsourced to database service providers (ADS) that also welcomes the threats. The database owner has no other choice than to trust the Adds. Than the database administrator can also miss use his rights and spay the Three encryption levels are defined.

Storage-level encryption, database-level encryption and application-level encryption. Storage level encryption encrypts the data in the storage subsystem. It is transparent thus avoids the risk of any change in existing application. In storage level encryption it has to be guaranteed that there

should be no copy left unencrypted so it is risky to selectively encrypt the files e. G. , in temporary files log files etc.