Security Policies in Modern Database System

Nutan Sharma[1], Pooja Garg[2]
HOD BCA Deptt[1]
Lect. in BCA Deptt2
AMM,
Bhiwani, Haryana (India)

ABSTRACT

Database security has become a vital issue in modern Web applications. Ensuring the confidentiality, privacy and integrity of data is a major issue for the security of database systems. Recent high profile data thefts have shown that perimeter defenses are insufficient to secure sensitive data. Securing organizations systems and data cannot be effective without the development of a written security policy.

In this paper security policies and procedures for protection of databases, security features and classical threats are described.

Keywords

Database, DBMS security, protection, smart card, ATM, swipe access cards, assertions.

1. INTRODUCTION

The goal of database security is the protection of data from accidental or intentional threats to their integrity and access. The database environment has grown more complex, with distributed database located on client/server architectures and personal computers as well as on mainframes. Access to data has become more open through the internet and corporate intranets and from mobile computing devices.

As a result managing data security effectively has become more difficult and time consuming because data are critical resources. [5] All persons in an organization must be sensitive to threats and take measures to protect data within their domains. Granting and revoke authorization to database resources is important, but it is by no means sufficient for modern database security. Most DBMS products are evolving to deliver additional levels of data protection. For example, DB2 offers multi-level security, providing ability to protect data and authorize its use at the row level. A multi-level security system allows the protection of data based on both traditional discretionary access controls, and controls that check the sensitivity of the data itself through mandatory access controls. These mandatory access controls are at the heart of a multi-level security environment, which prevents

Unauthorized users from accessing information at a classification level for which they are not

authorized or changing the classification of information they do have access to. These controls provide a way to segregate users and their data from others users and their data regardless of discretionary access they are given through standard access lists. Another method to secure database data is through encryption. There are actually two types of encryption with respect to database data-encryption at rest and encryption over the wire .Encryption at rest involves encrypting the persistent database data on disk. But encryption can be specified for data before it is sent across the network and then automatically decrypted once it is received. Encryption over the wire is helpful to prevent surreptitious access to your data as it files throughout your network, but it won't help combat thieves who target the database files on disk. Another burgeoning field in database auditing, sometimes called data activity monitoring. This type of solution monitors database activity (INSERT,UPDATE, DELETE, and even SELECT) and reports on who is accessing and changing which pieces of data and when. Such information can be very helpful to ensure that only appropriate personal are accessing appropriate data within the database. Database auditing solutions can help you to track the activity to privileged users.

2. FEATURES OF SECURITY

The most important security features Of Data management software follow:

2.1) Views

We define a view as a subset of the database that is presented to one or more users. [4] A view is created by querying one of more of the base tables, producing dynamic result table for the user at the time of the request. Thus a view is always based on the current data in the base tables from which it is built. The advantage of a view is that it can be built to present only the data (certain columns and/or rows) to which the user requires access, effectively preventing the user from viewing other data that may be private or confidential. The user may be granted the right to access the view, but not to access the base tables upon which the view is based. So, confining a user to a view may be more restrictive for that user than allowing him or her access to the involved base tables.

For example, we could build a view for a Pine Valley employee that provides information about materials needed to build a Pine Valley furniture product without providing other information, such as unit price, that is not relevant to the employee's work. This command creates a view that will list the wood required and the wood available for each product

```
CREATE VIEW MATERIALS_V AS
SELECTPRODUCT_T.PRODUCT_ID,PRODUCT_NAME,,
FOOTAGE,FOOTAGE_ON_HAND FROM
PRODUCT_T,RAW_MATERIALS_T,USES_T WHERE
PRODUCT_T.PRODUCT_ID=USES_T.PRODUCT_ID
AND
RAW_MATERIALS_T.MATERIAL_ID=USES_T.MATERI
AL_ID;
```

The contents of the view created will be updated each time the view is accessed, but here are the current contents of the view, which can be accessed with the SQL command:

```
SELECT FROM MATERIALS_V;
```

Modern Database Security

Table-2.1.1

Product_id	Product_name	Footage	Footage_on_hand
1	End Table 4	1	
2	Coffee Table	6	11
3	Computer Desk	15	11
4	Entertainment Centre	20	84
5	Writer's Desk	13	68
6	8-Drawer Desk	16	66
7	Dining Table	16	11
8	Computer Desk	15	0

The user can write SELECT statements against the view, treating it as though it were a table. Although views promote security by measures, because unauthorized persons may gain knowledge of or access to a particular view. [2]Also, several persons may ahsare a particular view, all may have authority to read the data, but only a restricted few may be authorized to update the data. Finally, with high-level query languages, an unauthorized person may gain access to data through simple experimentation. As a result, more sophisticated security measures are normally required.

2.2.) Integrity Controls

Integrity controls protect data from unauthorized use and update.

One form of integrity control is a domain. In essence, a domain is a way to create a user-defined data type. [3] Once a domain is defined, any field can be assigned that domain as its data type. For example, the following Price Change domain (defined in SQL) can be used as the data type of any database field, such as Price Increase and Price Discount, to limit the amount standard prices can be augmented in one transaction.

One advantage of a domain is that, if it ever has to change, it can be changed in one place-the domain definition-and all fields with this domain will be changed automatically.

Assertions are powerful constraints that enforce certain desirable database conditions. Assertions are checked automatically by the DBMS when transaction are run involving tables or fields on which assertions exist. If the assertion fails, the DBMS will generate an error message.

2.3.) Authorization Rules

Authorization rules are controls incorporated in the data management system that restrict access to data and also restrict the actions that people may take when they access data. For example, a person who can supply a particular password may be authorized to read any record in a database but cannot necessarily modify any of those records.

There model expresses authorization rules in the form of a table (or matrix) that includes subjects, objects, actions and constraints. Each row of the table indicates that a particular subject is authorized to take a certain action on an object in the database, perhaps subject to some constraint.

Table - 2.3.1

Subject	Object	Action	Constraint
Sales Dept	Customer record	Insert	Credit Limit LE$5000
Order trans.	Customer record	Read	None
Terminal 12	Customer record	Modify	Balance due only
Acctg. Dept.	Order record	Delete	None
Ann. Walkar	Order record	Insert	Order amt.LT $2000
Program AR4	Order record	Modify	None

This table contains several entries pertaining to records in an accounting database. For example, the first row in the table indicates that anyone in the Sales Department is authorized to insert a new customer record in the database, provided that the customer's credit limit does not exceed $5000. The last row indicates that the program AR4 is authorized to modify order records without restriction. Data administration is responsible for determining and implementing authorization rules that are implemented at the database level. Authorization schemes can also be implemented at the operating system level or the application level.

2.4.) Encryption

Data encryption can be used to protect highly sensitive data such as customer credit card numbers or account balances. Encryption is the coding or scrambling of data so that humans cannot read them. Some DBMS products include encryption routines that automatically encode sensitive data when they are stored or transmitted over communication channels. For example, encryption is commonly used in electronic funds transfer (EFT) systems. Other DBMS products provide exists that allow users to code their own encryption routines.

Two common forms of encryption exist:
one key and two key. With one-key method, also called data encryption standard (DES), both the sender and the receiver need to know the key that is used to scramble the transmitted or stored data. A two-key method, also called asymmetric encryption, employs a private and a public key.

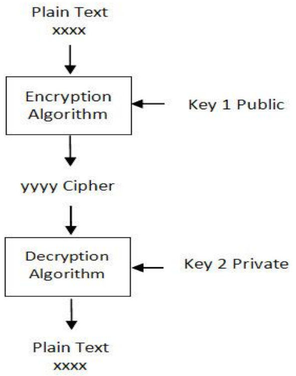

Fig. 2.4.1

2.5.) Strong Authentication

More reliable authentication techniques have become a business necessity, with the rapid advances in e-commerce and increased security threats in the form of hacking, identity theft, and so on.

Two factor authentication schemes require two of the three factors: something the user has and something the user knows. [6] We are already familiar with this system from using automated teller machines (ATMs) To use the ATM you must insert your bankcard in to the machine: then at the prompt we must key in our valid PIN. this scheme is much more secure than simple passwords because it is quite difficult for an unauthorized person to obtain both factors at the same time.

Three factor authentication is normally implemented with a high-tech card called a smart card. A smart card is a credit-card sized plastic card with an embedded microprocessor chip with the ability to store, process, and output electronic data in a secure manner. Some manufacturers encode each smart card with a unique serial number for card control. Sensitive data are stored on the cards in encrypted form, so the cards are highly tamper resistant.

Three factor authentication is implemented with smart cards in two stages. When the card is first issued to its owner, it is personalized with that owner's data. This data might include a digitized photograph, as well as the person's name, address and so on. the user selects a PIN which is encrypted and stored on the chip.

3. THREATS TO DATA SECURITY

Threats to data security may be thread to the data base for example to gain unauthorized access to a data base people may then browse, change or even still the data they can misuse the data. Focusing on database security alone, however ,will not ensure a secure database. [8] All parts of the system must be secure, including the database , the network, the operating system, the building in which the database resides physically, and the personnel who have any opportunity to access the system.

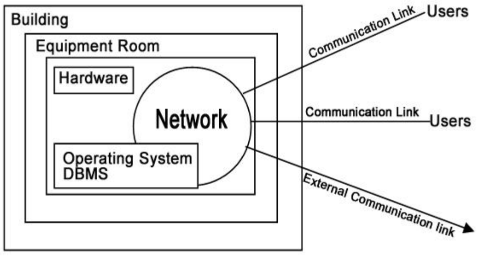

Fig.3.1

3.1. Accidental losses including human error

Establishing operating procedures such as user authorization, uniform software installation procedures, and hardware maintains schedulers are examples of actions that may be taken to address threats from accidental losses. [1] As in any effort that involves human beings, some losses are inevitable, but well-thought-out polices and procedures should reduce the amount and severity of losses

3.2 Theft and fraud

These activities are going to be perpetrated by people, quite possibly through electronic means, and may or may not alter data. Physical security must be established so that unauthorized are unable to gain access to rooms where computers, servers, telecommunicationfacilities, or computer files are located. Physical security should also be provided for employee offices and any other locations where sensitive data are stored or easily accessed. Establishment of a firewall to protect unauthorized access to inappropriate parts of the database through outside communication links will hamper people who are intent on theft or fraud.

3.3 Loss of privacy or confidentiality

Loss of privacy is usually taken to mean loss of protection of data about individuals, whereas loss of confidentiality is usually taken to mean loss of protection of critical organizational data that may have strategic value to the the organization. Failure to control privacy of information may lead to blackmail, bribery, public embarrassment, or stealing of user passwords. Failure to control confidentiality may lead to loss of competitiveness. State and federal laws now exist to require some type of organizations to create and communicate policies to ensure privacy of customer and client data.

4. SECURITY POLICIES AND PROCEDURES

Four types of security policies and procedures are the following :

4.1. Personnel Control

Adequate controls of personnel must be developed and followed, for the greatest threat to business security is often internal rather than external. [7] Organizations should develop procedures to ensure a selective hiring process that validates potential employees' representations about their backgrounds and capabilities. Monitoring to ensure that personnel are following established practices, taking regular vacations, working with other employees and so forth should be followed. Employees should be trained in those aspects of security and quality that are relevant to their jobs and encouraged to be aware of and follow standard security and data quality measures. Standard job controls, such as separating duties so no one.

4.2. Physical Access Control

Limiting access to particular areas within a building is usually a part of controlling physical access. Swipe or proximity access cards can be used to gain access to secure areas and each access can be recorded in a database with timestamps. Guests should be issued badges and escorted into secure areas. This includes vendor maintenance representatives. Sensitive equipment, including hardware and peripherals, such a printers can be controlled by placement in secure areas. Other equipment may be locked to a desk or cabinet or may have an alarm attached. Back-up data tapes should be kept in fireproof data safes and/or kept off-site at a safe location. Procedures that make explicit the schedules for moving media and disposing of media and that establish labeling and indexing of all materials stored.

4.3. Maintenance Controls

An area of control that helps to maintain data quality and availability but that is often overlooked is maintenance control. Organizations should review external maintenance agreement for all hardware and software they are using to ensure that appropriate response rates are agreed to for maintaining system quality and availability. It is also important to consider reaching agreements with the developers of all critical software so that the organization can get access to source code should the developer go out of business or stop supporting the programs. One way to accomplish this is by having a third party hold the source code, with an agreement that it will be released if such a situation develops. Controls should be in place to protect data from inappropriate access and use by outside maintenance staff and other contract workers.

4.4. Data Privacy Controls

Information privacy legislation generally gives individuals the right to know what data have been collected about them and to correct any errors in those data. As the amount of data exchanged continues to grow the need is also growing to develop adequate data protection. Also important are adequate provisions to allow the data to be used for legitimate legal purposes so that organizations that need the data can access them and rely on their quality. Individuals need to be given the opportunity to state with whom data retained about them may be shares, and then these wishes must be enforced, enforcement is more reliable if access rules based on privacy wishes are developed by the DBA staff and handled by the DBMS.

5. CONCLUSION

Security strategies include security policy and procedural controls, network firewalls, strong identification and authentication mechanisms, access control mechanisms , file and link encryption, file integrity checking, physical security measures and security training. A simple approach includes activization of protective mechanisms of a DB,protection of servers, workstations, a local area network, use of cryptography. The structured approach to protection of a DB is more expanded and includes :

1 improving federal information –system security by raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies.

2. researching ,studying, and advising techniques for the cost effective security and privacy of sensitive federal system.

3. developing standards, metrics , test,and validation programs.

4. developing guidance to increase secure IT planning, implementation, management, and operation.

6. REFERENCES

[1] Protecting Database, white Paper, http;//www.appsecinc.com.

[2] Stephen KOST,'An introduction to SQL Injection Attacks for Oracle

[3] Loiraina Hazel "A overview of Oracle Database Security features",GSEC Practical Assignment,2001

[4] PAUL Carmichael Securing Database, GSEC Practical Assignment 2002.

[5] Anderson, D.2005,'HIPAA Security and Compliance." Published on www.tadan.com,July,2005.

[6] Security and integrity. Reading MA: Addison-Wesley.

[7] Mullinsc 2001.'Modern Database Administration, Part 1.-DM

[8] 2004CSI/FBI Computer Crime and Security Survery Http://www.Gocsi..Com