Information Asset Security: Databases and Access Control

[1]Mission Franklin, [2] Prince Oghenekaro Asagba
[1]School of Post Graduate Studies, Department of Computer Science,
Faculty of Natural and Applied Sciences, Ignatius Ajuru University of Education.
[2]Department of Computer Science, Faculty of Science,
University of Port Harcourt, Choba, Port Harcourt

Abstract
Security of databases and control of access is a sure, safe and secure means of protecting information stored in a database. These is achievable through both physical and technological means, through the application of security schemes after the careful identification of the threats that an organisational database is exposed to, while not overlooking privacy and legal related issues. Control mechanisms such as encryption, digital certificate, digital signature have been adopted to ensure security, as we as the database survivability where the database system faces difficult challenges through the identified threats.

Introduction

Databases are essential corporate resources and the security of it is an important critical component of an organization. The security plan of an organization must ensure that databases are not left out. The protection of databases and privacy for individuals' data is within the purview of the role of database administrators. The means of protecting a database from illegal access, alteration, or damage is known as database security**.** (Ricardo et al., 2012). From the initial design stages of the database, reasonable efforts should be made to ensure that privacy is taken seriously, and therefore it is the right of individuals to know and have some control over information about them stored somewhere (Jones & Bartlett Learning, 2020; Mei, 2001).

Ricardo et al. (2012) and Biswas (2020) suggested that the CIA model (Confidentiality, Integrity, and Availability) of information security as shown in figure 1: should be adopted to secure any resource including a database; because security attacks against an organization can create availability issues and other security threats. Rubens (2016) recommended that securing any system should ensure the following: (i) physical security by securing physical locations, (ii) software based protection mechanism like firewall,(ii) inbuilt database security policies, (iv) use of strong encryption algorithms (v) effective management of access privileges, (vi) preemptive audit and monitoring of database activities. (DBSCSGWG, 2009).

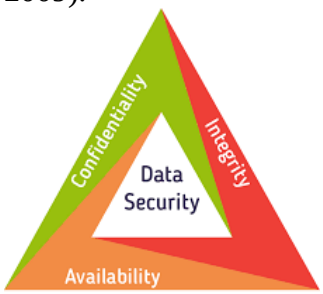

Figure 1: Data Security CIA Triangle

Types of Security Issues

Database system requires various security mechanisms for protection attacks and breaches. Elmasri et al. (2011) noted that issues of database security may involve (i) ethical and legal issues, (ii) policy issues, (iii) system-related issues, (iv) multi-level security identification. Thus the database administrator must be proactive in addressing these issues from the design stages of the database to its implementation and reviewing of the processes to keep the database safe and secure from imminent attacks. (Imperva, 2020).

Database Threats

As the information contained in the database becomes relevant, so does the threat level increases. The threat to database stems from different arenas and could impact the system, processes and users in an organisation, leading to different kind of losses such as financial loss, reputational loss, loss of confidence and loss of public trust. Principally data breaches results in loss of confidentiality, integrity and availability. For example, the impact of unauthorized disclosure of confidential information can result to violation of Data Privacy Act. Databases should be protected against threats of CIA model and countermeasures can be adopted to mitigate these threats such as; access control, inference control, flow control, encryption.(Elmasri et al., 2011). Beside these threats listed, databases are also exposed to other forms of threats, for example spurious performing unauthorized operations, deriving information from hidden data, SQL injection, physical removal of storage devices, copying and stealing of database files, administrative bypass of database privileges (Elmasri et al., 2011; Richardo et al., 2012).

Database Management Systems (DBMS) typically include security and authorization mechanism to ensure the security of a database against illegal and unauthorized access. DBMS must have protective mechanism to limit these threats. DBMSs access control mechanism ensures only authorized access to sensitive data and restrict access to unauthorized users, through authentication and authorization. Authentication is a way of validating the uniqueness of a user that is log on to the database; authentication alone is not adequate to protect data. An additional layer of security is required, which is authorization, to determine what data or transaction to be carried out, without which, there is no data security.

DataSunrise (2020) stated that two-step authentication be used to guarantee the security of the system, implemented through emails and one-time passwords (OTP); and using database access restriction mechanism to restrict access to all or certain parts of database objects such as operating system user; recorded login attempts; client application ID, IP address(hostname); username; Query string., etc.

Types of Access Control

Access control mechanisms are important and relevant security protocol that prevents or limits breaches to databases: these security mechanisms are discretionary or mandatory. Although these methods seem superseded, currently active methods like Role Based Access Control (RBAC) is in used, and recently, Attribute Based Access Control (ABAC). RBAC grants access based on a user's role and implements key security principles based on user's privilege while in ABAC resources and users are assigned a series of attributes (time, day, position and location) to make a decision on access to a resource.(Domingo-Ferrer, 2009).

Bayt (2020) identified some other security challenges to be addressed, which may include control of access to statistical database information or criteria based summaries like channels

flow problems, which invalidates the security policies through covert channels and encryption to protect sensitive data (Elmasri et al., 2011; Ricardo et al., 2012).

The role of the DBA and Database Security and audits

Securing a database is part of the routine of a database administrator (DBA) or the role of anyone who ensures the smooth running of a database. The DBA is the central role and the appropriate authority in a database for managing the system with superuser account; whose responsibilities includes: account creation, granting and revoking of user's privileges, security level assignment, classifying data and users in in line with security policy. (Oracle Help Center, 2020). While using the database, the system keeps record of transactions on the database and of the user who performed these transactions. The system log is relevant for recovery purposes from a transaction failure or system crash; where tampering with the database is suspected, a database audit is performed (Burleson, 2020). The DBA audits the database through the audit trail, to review the log and examine all accesses and operations applied to the database during the period. (Elmasri et al., 2011; Mei, 2001; Richardo et al., 2012).

Sensitive and Disclosures of Data

A measure of value assigned to the data by its owner, with the intension of classification and the need for safeguard is called data sensitivity. Not all databases contain sensitive data. (Elmasri et al., 2011). The classification of data for sensitivity may be due to: inherently sensitive(by its nature), sensitive source, sensitivity explicitly assigned by owner, sensitivity due to some attribute of the data, and sensitive in relation to previously disclosed data. However, the sensitivity of the data does not preclude its revelation to authorized users. To reveal such sensitive data, Elmasri et al. (2007) specified factors to consider before taking such a decision for its safety to reveal. They listed three important factors: authenticity assurance, access acceptability, and data availability while ensuring certain external characteristics about the user.

Most databases commonly used discretionary control mechanism to granting and revoking privileges. It is a selective access mechanism to relations in the database, and on specific accounts. The discretionary privileges used are the account level and the relation level, which specify the privileges assigned to the account irrespective of the relations, and that of control privileges assigned to the account on each relation or view in the database. (Elmasri et al., 2007).

The privileges assigned to the account level apply to the abilities provided for the account such as CREATE SCHEMA, CREATE TABLE , CREATE VIEW , ALTER , DROP , MODIFY, SELECT. The second level privileges are applicable to relation level, like base relations and virtual (view) relations. To control granting and revoking of relations privileges, each relation in a database is assigned an owner account. The owner has all the privileges on that relation, using the CREATE SCHEMA command. The owner account can pass privileges on any of the owned relation to other users by granting privileges to their accounts. (Elmasri et al., 2007; Mei, 2001).

SQL provides certain types of privileges, that can be granted on a relation: SELECT, MODIFY (*UPDATE, DELETE, and INSERT*) and REFERENCES. (Batini, et al., 1992; Elmasri et al., 2007; Natan, 2005).

Views are important discretionary authorization mechanism in its own right; by limiting some tuples: retrieving only certain tuples of the base table by means of a query that selects only those tuples from the base relations. (Batini et al., 1992; Elmasri et al., 2007). The owner of a relation may want to grant the SELECT privilege to a user for a specific task and then revoke that privilege once the task is completed, a REVOKE command is included for the purpose of canceling privileges. (Elmasri et al., 2007).

Propagation and Limitation of Privileges with GRANT OPTION

Privilege on a relation can be assigned to another account with the GRANT OPTION. Whenever the owner of a relation grants a privilege on that relation to another account, with the GRANT OPTION, this means the account with granted privilege can assign that object to other accounts. However, where it was granted without the GRANT OPTINON, then it would not have the privilege to assign that access privilege to another account. And when revoked, all the privileges that propagated accordingly on that privilege should spontaneously be retracted by the system (Batini et al., 1992; Elmasri et al., 2007, 2011).

There also exists limitation of the propagation of the privileges, such as horizontal and vertical propagation, though not implemented in most DMBS and not part of SQL language structure and implementation.

Role-Based Access Control (RBAC)

Large-scale enterprise systems have emerged with RBAC as a verified tool for enforcing and managing security effectively. This concept is based on the notion that permissions are linked with roles, and users are allocated to appropriate roles. Roles are created to manage functional roles in the database, for example CREATE ROLE and DESTROY ROLE commands, augmented with the GRANT and REVOKE commands to assign and revoke privileges from roles. RBAC is seen as a practicable substitute to the orthodox and obsolete access control methods, and ensures that only authorized users are given access to certain data or resources. RBAC model is a necessity to address key security requirements of Web-based applications. RBAC is properly managed through the paradigm of Separation of duties (SoD). SoD is important requirement in various commercial DBMSs and organisations. It prevents one user from doing work that requires more people, thereby elimination possible collusion. The hierarchy of roles in RBAC is a logical way to organize roles to reflect the organizations structures.

```
GRANT ROLE Lecture TO User_type1
GRANT ROLE Student TO User_type2
```

Web based access control mechanism are also available through the adoption of XML signature specification, XML Encryption Syntax for countersigning and transformations, and also for vocabulary and processing rules by protecting confidentiality of XML documents. In electronic commerce environments are characterized by electronic transactions; therefore require elaborate access control policies, beyond traditional DBMSs. In an e-commerce environment not only traditional data that need to be protected but also knowledge resources and experience. The access control mechanism must be flexible enough to support a wide range of heterogeneous protection objects. (Elmasri et al., 2011; Meghanathan, 2020).

Other threats to database security:

SQL Injection is one of the common threats to database systems. Such is necessitated by unauthorized privilege escalation, privilege abuse, denial of service (Dos), weak authentication. (Elmasri et al, 2011 and Richardo et al., 2012) and (Imperva, 2020). This type of attack is fashioned and executed through various SQL injection methods: commands are

sent to retrieve and display data from the database on a web browser. Some of the attacks include: SQL injection attack, SQL manipulation, code injection, function call injection.

Risks associated with SQL Injection and protection mechanisms

SQL injection attack creates threats, and harmful risk profiles are associated with the victim's database such as database fingerprinting, denial of service, bypassing authentication, identifying injectable parameters, remote command invocation, performing privilege escalation. (Elmasri et al., 2007). These risks are threat to the cooperate existence and going concerns of the organisation. Therefore protective machinery must be adopted to forestall these attacks; this can be achieved by applying certain programming rules to all web-accessible procedures and functions. Some of such procedures are: bind variables (using parameterized statements) and also improves performance, filtering input (input validation) and function security.

Database Security through Statistical Control

A database may contain data on individuals that is confidential. Statistical controls on databases are used primarily to produce statistics on various sets of populations. A population is a collection of relations (tables) that satisfy some selection criteria. Statistical control queries include the application statistical-aggregate functions to database tables. It is permissible to users to sieve out statistical information on the populations, like count, sum, minimum, maximum, average and standard deviation. But users are not at liberty to retrieve information about an individual. The DBMS must ensure confidentiality and privacy of information about individuals; at the same time provide beneficial statistical extractions of data about those individuals to users. It is vital that statistical control on database enforces the privacy protection of users. (Elmasri et al., 2011). Statistical security mechanisms should disallow the retrieval of data on individuals, by preventing queries that retrieve characteristic values and permitting only requests that involve statistical aggregate functions like count, summation, minimum, maximum, average, and standard deviation. Other functional means to secure information within a database could be through encryption and key infrastructures. This is a means of ensuring secure data in an insecure environment, by the use of encryption algorithm to scramble data with a pre-determined key for the recovery of the cipher through decryption. Thus, 16 bit block sized Data Encryption Standard (DES) was commonly used until it was replaced with 128 bit block sized Advanced Encryption Standards (AES), by the National Institute of Standards (NIST). DES and AES are encryption algorithms that uses secret key, also called symmetric key algorithms. (Cho et al, 2013). Public key encryption can also be used. Diffie and Hellman proposed the public key cryptosystem. Public key encryption uses two keys in encryption and decryption, although, the use of two separate keys have consequences in terms of key distribution, authentication and confidentiality. A public key encryption scheme has six ingredients: plaintext, encryption algorithm, public and private keys (encryption/decryption) ciphertext, and decryption algorithm. (Elmasri et al., 2007; Hoffman, 2008; Kamel, 2008 Thuraisinghami, 2005).

A digital signature is mechanism of using "encryption techniques to provide authentication services in electronic commerce applications". A digital signature is a means of associating a unique emblem to an individual with a body of text. The emblem should be unforgettable, meaning that others should have a way to authenticate and verify the originator of signature.
A digital certificate combines the value of a public key with the identification of the person or service that holds the corresponding private key into a digitally signed statement. Certificates are issued and signed by a certification authority (CA). "The entity receiving this certificate

from a CA is the subject of that certificate". (Elmasri, et al., 2007; Gertz et al., 2008; Thuraisingham, 2005).

Database Security Continuous Threats

With the tremendous scale and increase of terrorizations to databases and information resources, there are areas that would require more efforts to solve issues of intellectual property rights, data quality and database survivability. (i) Database users need techniques and answers to measure and evaluate the data quality, techniques such as quality stamps could be generated and posted on websites and other mechanisms that creates integrity semantics verification tools for quality assessment of data could also be used. Others are (ii) Intellectual Property Rights: The main purpose of digital watermarking is to protect content from unauthorized duplication and distribution by enabling provable ownership of the content.(Guarnieri et al., 2020), (iii) database survivability: database systems necessarily should operate and carry on their functions pertinently, even with degraded abilities, despite disruptive events such as information warfare attacks. Databases while in a bid to creating solution to avert attacks and discovering one in the event of occurrence, it should work towards (i) confinement, (ii) damage assessment, (iii) reconfiguration, (iv) repair, (iv) fault treatment.

The ultimate goal of the attacker is to damage the organisation's operation to fulfill his objective through disruption of the information systems and services. (Thuraisingham, 2005). On attacking the system, and the system struggles for survival and services are impacted, these attacks will receive immediate and concentrated attention; diagnosis on the procedures, preventive measures, and restoration should be considered (Gertz et al., 2008). However, issues related to database survivability are not sufficiently investigated and addressed. Hence, more research needs to be done into techniques and methodologies to guarantee database system survivability. (Elmasri et al., 2007).

Conclusion

Databases are critical infrastructures for an organisation's information assets. The security of these assets ensures the safety and availability of the organisation's information and services. Several security mechanisms are adopted to forestall that service breakdown is minimal, and ensure that service downtimes are drastically reduces.

However, it is not possible to achieve security without adequate physical and technological approaches. Therefore from inception, total security of information assets must be planned with both physical, non-physical and cyber security mechanisms to fortify security of database systems.

References

Batini, C., Ceri, S.,Navathe, S.B.(1992).Conceptual Database Design: An Entity-Relationship Approach. The Benjamin/Cummings Publishing Company, Inc. California

Biswas, P. (2020).Overview of an Information Security Management System. https://isoconsultantkuwait.com/2019/07/20/2392/

Burleson,D.K.(2020).An Enterprise Security Primer:Oracle Database Security Primer. Retrieved from http://www.dba-oracle.com/art_dbazine_security1.htm on 10/06/2020

Cho, E.-A., Moon, Ch.-J., Park, D.-H., Yim, K.-B.(2013). Database Security System For Applying Sophisticated Access Control Via Database Firewall Server, Computing and Informatics, Vol. 32, 2013, 1192-1211, retrieved from

https://cai.type.sk/content/2013/6/database-security-system-for-applying-sophisticated-access-control-via-database-firewall-server/12031.pdf on 10/06/2020

DataSunrise(2020).What is Access Control in Database Security?. Retrieved from https://www.datasunrise.com/blog/professional-info/what-is-access-control/#:~:text=What%20is%20Access%20Control%20in%20Database%20Security%3F,main%20components%3A%20authentication%20and%20authorization on 12/06/2020

DBSCSGWG [Database Security Consortium Security Guideline WG](2009).Database Security Guideline, Version 2.0. Retrieved from https://docplayer.net/6638838-Database-security-guideline-version-2-0-february-1-2009-database-security-consortium-security-guideline-wg.html on 11/06/2020

Domingo-Ferrer J.(2009). Inference Control in Statistical Databases. In: LIU L., ÖZSU M.T. (eds). Encyclopedia of Database Systems. Springer, Boston, MA

Elmasri,R and Navathe,S.B. (2007). Fundamentals of Database Systems.5th Edition. Retrieved from https://www.cs.purdue.edu/homes/bb/cs448_Fall2016/lecture-files/pdf/ch23-Database%20Security%20and%20Authorization.pdf on 11/06/2020

Elmasri,R and Navathe,S.B. (2011). Fundamentals of Database Systems.6th Edition. Library of Congress Cataloging-in-Publication Data ISBN-13: 978-0-136-08620-8

Gertz,M and Jajodia,S. (2008).Handbook of Database Security Applications and Trends,edited by Michael Gertz and Sushil Jajodia, Springer Publications

Guarnieri, M., Marinovic,S., Basin, D.(2020). Strong and Provably Secure Database Access Control. Retrieved from https://mguarnieri.github.io/files/papers/eurosp2016.pdf on 12/06/2020

Hoffman, D.V.(2008). Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control,Wiley Publishing

Imperva(2020).Relational Database Security. Retrieved from https://www.imperva.com/learn/data-security/database-security/ on 12/06/2020

Jones & Battlett Learning(2020). Introduction to Database Security. Retrieved from http://samples.jbpub.com/9781284056945/DBICHAP8.pdf on 11/06/2020

Kamel,A (2008).Chapter 23 Database Security. Retrieved from http://faculty.cord.edu/kamel/08F-330/Presentations/ch23.pdf on 11/06/2020

Meghanathan,D.(2020).Module 8: Database Security. Retrieved from http://www.jsums.edu/nmeghanathan/files/2015/05/CSC437-Fall2013-Module-8-DatabaseSecurity.pdf?x61976 on 10/06/2020

Mei Ke(2001). Computer database security and Oracle security implementation. Graduate Student Theses, Dissertations, & Professional Papers Graduate School, The University of Montana retrieved from https://scholarworks.umt.edu/cgi/viewcontent.cgi?article=6127&context=etd on 10/06/2020

Natan,R.B.(2005).Implementing Database Security and Auditing A guide for DBAs, information security administrators and auditors, Elsevier Digital Press

Ricardo,C.M., Urban,D.S.,(2012). Databases Illuminated, 3rd Edition Jones & Bartlett Learning, LLC publishing

Rubens,P.(2016). 7 Database Security Best Practices. Retrieved from https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html on 11/06/2020

Oracle Help Center(2020).Database Administrator's Guide: 22 Managing Users and Securing the Database. Retrieved from https://docs.oracle.com/cd/B19306_01/server.102/b14231/secure.htm on 10/06/2020

Thuraisingham Bhavani (2005).Applications Security:Integrating Information Security and Data Management, Auerbach Publications

Wikipedia(2020).Database Security. Retrieved from https://en.wikipedia.org/wiki/Database_security on 11/06/2020