A study on Advance Data Security for sustaining competitive edge

Amitesh Baghel, Abdeali Patanwala, Hasib Khan, Jay Joshi, Jayesh Surana
Information Technology, SVITS
Gram Baroli, Sanwer road, Indore, MP, INDIA

Abstract— Organizations apply data leakage prevention solutions to monitor and control data access and usage in the field of information security. As the organization progresses into the more technological environment, the amount of the digitally stored data increases dramatically, but keeping the track on data used in any organization is no longer as easy as before. While doing business there is a need to maintain the sensitive and confidential data. If the confidential data is leaked from the organization then it may influence on the organization heath. Advance Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. This study has examined the advance measures that could be taken to ensure digital security in today's world where data is not less than gold.

Keywords: identification, authentication, authorization, Monitoring and audit, Encryption, Network security, Database security.

1.INTRODUCTION

Security of data in today's digital world has become very important. So it is more important to take advance security measures to ensure the data remains secure. Proper step by step method should be followed for the security of data. Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers. It is delivered using information security technologies such as firewalls and antivirus, along with data security standards and policies for managing and governing the entire process. There is a large security gap between the existing systems which are used to prevent the data leakage and the real life scenario. The gap analysis is undertaken as means of bridging that space. It is a technique for determining the steps that are need to be taken in moving form a current state to desired future state. Security gaps are nothing but the vulnerabilities or weakness in the organization which is a threat and can be exploited to make an attack.

There are seven basic security measures.

1. **Identification**
2. **Authentication**
3. **Authorization**
4. **Monitoring & Audit**
5. **Encryption**
6. **Network security**
7. **Database security.**

These are basic security measures which are followed in any system makes data highly secure and reliable.

2. CONCEPTUAL MODEL

Identification, Authentication, & Authorization:

We all face these three concepts every day, but not everyone knows the difference. Since these terms are essential in data protection, they deserve to be explained better.

To begin, let's take an example from everyday life. It will help you to understand the difference between authentication and identification in general.

A new employee comes to work for the first time. At the entrance, he introduces himself to a security guard and says that he is a new manager. Thus, he **Identifies** himself – tells who he is.

The security guard does not believe the words he says. He demands to provide evidence that this person is a new manager and has the right to enter the office. To solve the problem, the employee has to show his pass with the photo. And the security guard should compare it with his list of registered employees. The employee confirms his authenticity – this is **Authentication**.

Finally, a forbidden door opens, and the guard lets the employee in. Once the employee receives the permission to enter the office the **Authorization** happens.

In the virtual world, everything is almost the same as in the real. Only the names of the "characters" are changing. The security guard is a server that controls the access to the website. And the manager who came to work – a user who wants to log in.

To perform any action on a website, the user must "introduce himself" to the system. User's identification means presenting grounds for the entry to the site or service. As a rule, your username or email address provided during registration serve as identificators. If the server finds in its database the data coinciding with that entered by the user, the user's identification is successful.

Login is a perfect thing. But where is the guarantee that it was entered by the person registered on the site? To finally verify the user's identity, the system typically authenticates the user.

Now, more and more often the two factor authentication is used. A usual static password serves as the first factor. The second factor may be different depending on the types of authentication methods used in this or that case:

- one-time password or PIN-code;
- magnetic stripe cards, smart cards, certificates with a digital signature;
- Biometric factors: voice, retina, fingerprints, etc.

From the new CJIS standards:

(The Criminal Justice Information Services Division (CJIS) is a division of the United States Federal Bureau of Investigation (FBI). The CJIS was established in February 1992, and it is the largest division in the FBI.)

Two factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token). something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).”

So while 2FA might sound complicated, it’s actually something we’re all familiar with. If you’ve ever used an ATM, you’ve used 2FA. At the ATM, you first present your debit or bank card (something you have), and then enter your 4-digit pin (something you know).

2FA provides a greatly enhanced level of security, because a system protected by 2FA is nearly impenetrable to a security breach from outside. After all, even if a hacker somehow acquires or guesses a system password, they would still need to enter another security “factor” in order to access the system—one they simply wouldn’t be able to provide.

Monitoring & Auditing:

Monitoring directly assists in the first step of this process—categorizing information systems—from which organizations can derive the secondary benefit of selecting and implementing the proper security controls. Monitoring tools start their processes with initial discovery, usually through passive listening, to determine, among other things, what devices and applications are on the network and the type of traffic, data, and user access with which they’re associated. This information helps organizations provide a baseline assessment to determine where they’ll need to monitor—but by no means is a replacement for manual discovery processes such as talking to business units, and other such information-gathering options.

Continuous monitoring enables information security professionals and others to see a continuous stream of near real-time snapshots of the state of risk to their security, data, the network, end points, and even cloud devices and applications. Assessing security controls as well as ongoing monitoring of security controls are both directly assisted by continuous monitoring through vulnerability monitoring processes, which many organizations already have in place.

We need **auditing** *because the ever changing cybersecurity landscape requires infosec professionals to stay abreast of new best practices on how to conduct information security assessments.* Your security policies are your foundation. Without established policies and standards, there's no guideline to determine the level of risk. But technology changes much more rapidly than business policies and must be reviewed more often. Software vulnerabilities are discovered daily. A yearly security assessment by an objective third party is necessary to ensure that security guidelines are followed.

As taught by SANS Insitute :

(The SANS Institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted and by far the largest source for information security training and security certification in the world.)

Basic Auditing and Monitoring Strategies

- Baselines
- Time Based Security
- Thinking like an Auditor
- Developing Auditing Checklists from Policies and Procedures
- Effective risk assessment
- 24/7 Monitoring

Encryption:

Encryption is defined as, "the translation of data into a secret code." Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text Source.

The data in an encrypted file is scrambled into a complex code that cannot be broken within a reasonable amount of time by any computer on earth. The key (or cipher) to unlock this code is a password that is created by whomever encrypted the file

Encryption is an effective method of protecting your corporate data, in the same way locking the doors to your business is an effective method of preventing trespassers. The hacking and selling of corporate data can be a very lucrative prospect for a potential hacker and, as such, protection against hacking is extremely important.

Leaving company data unencrypted on the company network is the equivalent of leaving your business' doors unlocked and all of the cash from the week in the register. Once hackers learn that your data is unencrypted, it becomes an easy target.

Comparing hacking (virtual theft) with burglary (physical theft), there is a much higher chance that your business will be hacked than there is that your business will be broken into. According to a recent survey, 90% of businesses say they have been hacked. Burglary statistics vary by region, but are typically extremely low (well under 1%).

The initial damage related to a burglary is obvious, but the damage related to the theft of sensitive company data, such as client lists or payroll information, could be far more deadly than a few thousand dollars in damages from a burglary.

Methods of Encryption

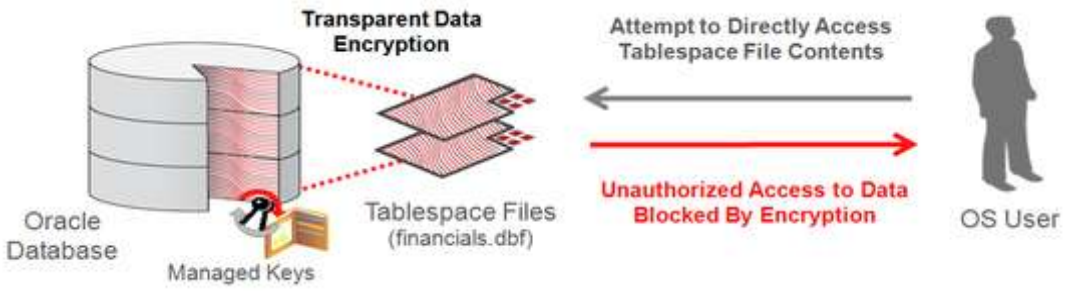
There are numerous ways to incorporate data encryption into your devices and networks. Business managers should speak to their IT departments about the best encryption for their networks and devices.

The simplest form of encryption for Windows based PCs is BitLocker. BitLocker is built into the "Professional" and "Ultimate" editions of Windows Vista, 7, 8 and 8.1. Once enabled, it will fully encrypt your hard drive without inconveniencing the user. A free alternative to BitLocker is TrueCrypt. Such methods can be activated for a small fleet of machines with only a few hours of work .

Transparent Data Encryption by Oracle

Transparent Data Encryption (TDE) protects Fusion Applications data which is at rest on the file system from being read or used. Data in the database files (DBF) is protected because DBF files are encrypted. Data in backups and in temporary files is protected. All data from an encrypted tablespace is automatically encrypted when written to the undo tablespace, to the redo logs, and to any temporary tablespace.

Advanced security enables encryption at the tablespace level on all tablespaces which contain applications data. This includes SOA tablespaces which might contain dehydrated payloads with applications data.



Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL). Tablespace keys are stored in the header of the tablespace and in the header of each operating system (OS) file that makes up the tablespace. These keys are encrypted with the master key which is stored in the Oracle Wallet. Tablespace keys are AES128-bit encryption while the TDE master key is always an AES256-bit encryption.

Network Security:

With the increasing reliance on technology, it is becoming more and more important to secure every aspect of online data and information. One of the best ways to secure your data is to make sure your network is protected.

Many network security threats today are spread over the Internet. The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

All of these different types of attacks can be grouped into two different groups; structured and unstructured. A structured attack is an attack by an individual who has advanced computer skills and intentionally targeted a specific group or company. An unstructured attack is an attack by an individual who does not understand who they are targeting and only use tools that can be found easily. Both types of attacks should be taken seriously because they can expose confidential information and create distrust between a company and their clients.

There are **four** steps to protect your network from attacks and they are:

1. Implement
2. Analyze
3. Test
4. Modify

Implement: The first step is to create and implement a network security system that provides protection and has sufficient authorization policies.

Analyze: Once the network security system is created and implemented, the system needs to be analyzed to determine if the current security system is appropriate for the network it is protecting.

Test: When an appropriate network security system is in place, it is time to conduct tests to make sure all of the securities are working and will completely protect your network against any threats.

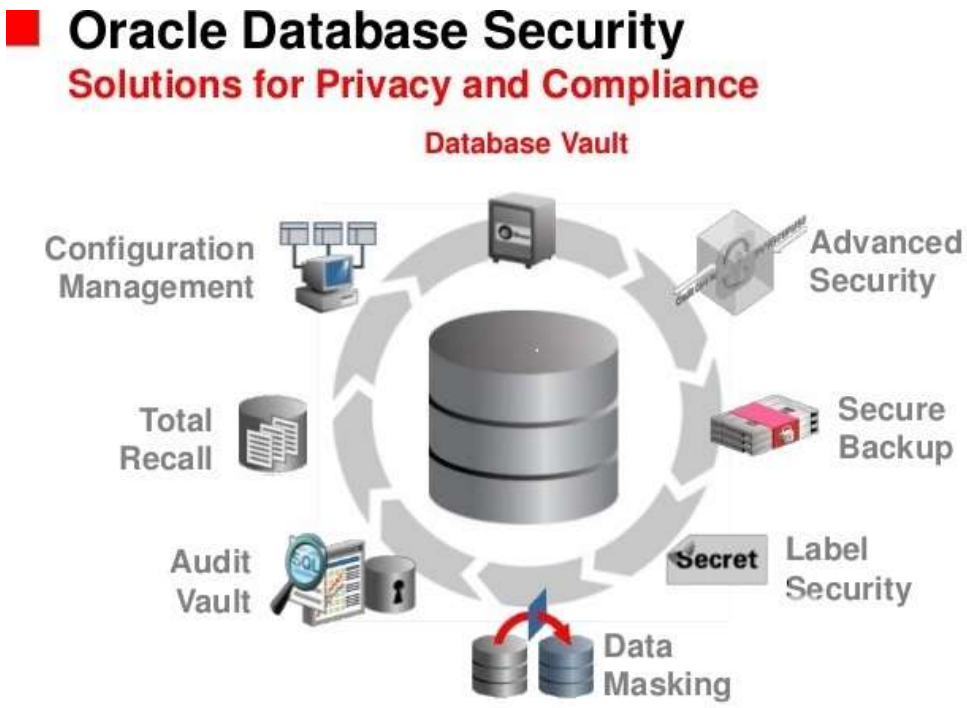
Modify: After conducting the tests, collect the data and enhance your protections. The results will reveal where your security system is effective and where it can be improved. Hackers are always improving their attacking procedures, so it is essential to test your system frequently to remain protected and stay one step ahead of them.

By having network security in place, your company will experience business benefits. Your company is protected against business disruption, this helps keep employees productive. Network security helps your company meet mandatory regulations. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.

Database security:

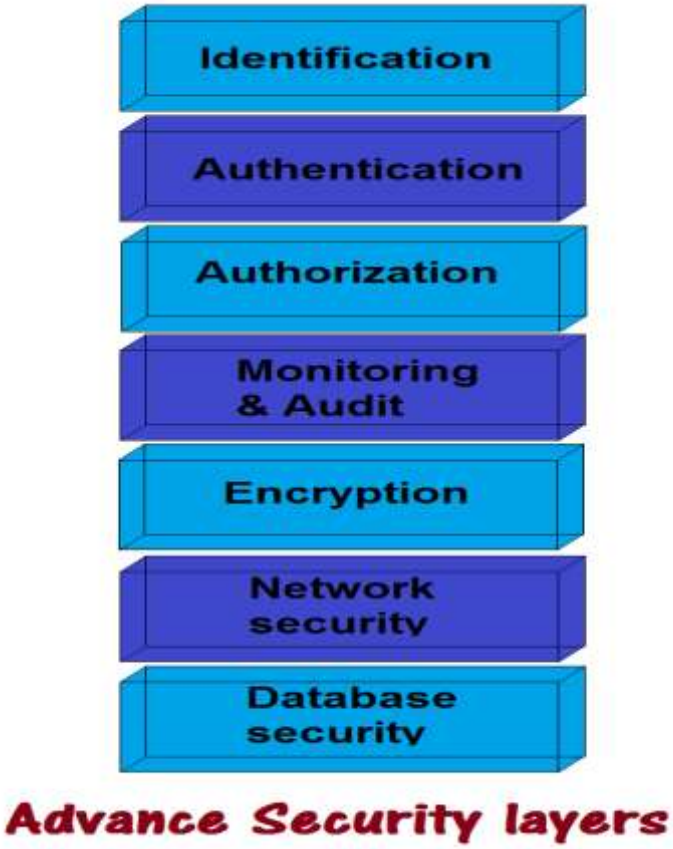
Advanced Data Security offers two types of extended data protections. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest. Advanced Data Security is available for Oracle Applications Cloud by subscription to Break-Glass service.

Oracle Database Vault



Database Vault reduces the risk of highly privileged users such as database and system administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects. Administrators can perform regular database maintenance activities, but cannot select from the application tables. If a DBA requires access to the application tables, she can request temporary access to the Fusion schema at which point keystroke auditing is enabled.

Conclusion:



If proper procedures, policies and controls are not taken Data leakages can be detrimental to an organizations. Management needs to understand what data leaks are, its effects, and proper measures should be taken as outlined in this study. However careful analysis and preparation is required to help monitor and prevent against data leaks through DLP solutions, especially if the communication involves open source protocols like NoSql or MQTT. In such cases, data is released in a shared buffer. Various schemes are suggested in order to prevent such undesirable information leakage. So if these security measures has been followed data can be highly secured.

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding all levels of security to make it applicable.

References:

1) A study on data leakage prevention for sustaining competitive edge Paper ISSN (2231-4571)
2) https://www.protectimus.com/blog/identification-authentication-authorization
3) http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits
4) http://www.packetworks.net/blog/encryption.htm
5) http://www.onlinetech.com/resources/videos/what-role-does-encryption-play-in-data-security
6) https://docs.oracle.com/cloud/latest/common/OCHUS/OCHUS1525255.htm
7) http://info.nutmegtech.com/it-insider-blog/the-importance-of-network-security.
8) https://docs.oracle.com/cloud/latest/common/OCHUS/OCHUS1525255.htm#OCHUS1525255