International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VIII, August 2018- Available at www.ijraset.com

Security Issues and Attacks in Sensitive Data over Cloud Environment

Dr. R. Sridevi [1], Sowmiya P R [2]
[1]*Assistant Professor in, Department of Computer Science, PSG College of Arts & Science Coimbatore.*
[2]*MPhil Research Scholar, Department of Computer Science, PSG College of Arts & Science Coimbatore.*

Abstract: Information Security is simply the process of keeping information secure: protecting its availability, integrity, and privacy. Information security (InfoSec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. InfoSec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. In this protection of information and its systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. This paper describes about the information security and also to escape from the hackers that are to prevent from the attacks some of the security methods are used.

I. INTRODUCTION

Effective Information Security incorporates security products, technologies, policies and procedures. No collection of products alone can solve every Information Security issue faced by an organization. More than just a set of technologies and reliance on proven industry practices is required, although both are important. Products, such as firewalls, intrusion detection systems, and vulnerability scanners alone are not sufficient to provide effective Information Security. Information Security is a process. An information system Security Policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure. Security Procedures document precisely how to accomplish a specific task.

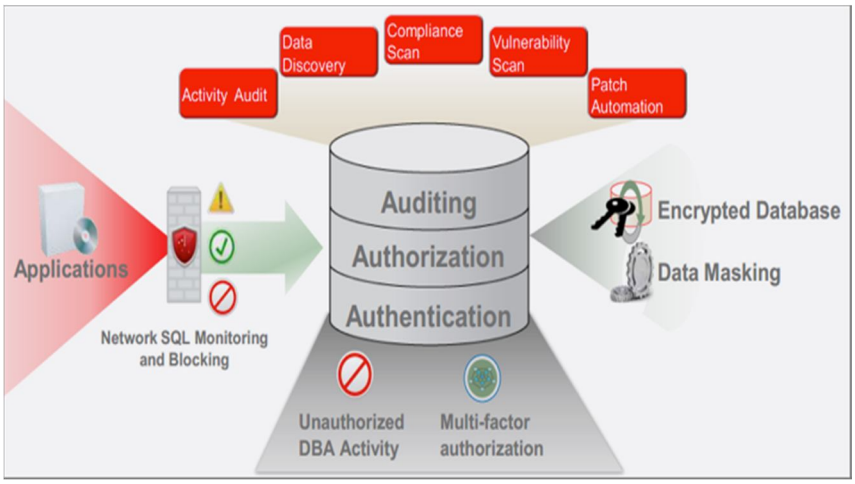
A. Overview Of Information Security

Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g., electronic, physical). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. To standardize this discipline, academics and professionals collaborate and seek to set basic guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability and user/administrator training standards. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, and transferred.

B. Issues In Information Security

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. Database security is a specialist topic within the broader realms of computer security, information security and risk management.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VIII, August 2018- Available at www.ijraset.com



C. Access Control

In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. Authorization is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular. Access control in computer systems and networks rely on access policies. The access control process can be divided into the following phases: policy definition phase where access is authorized, and policy enforcement phase where access requests are approved or disapproved.

D. Database Audit

Database auditing involves observing a database so as to be aware of the actions of database users. Database administrators and consultants often set up auditing for security purposes, for example, to ensure that those without the permission to access information do not access it. A data security audit starts with assessing what information you have, how it flows and identifying who has access to it and building a design flow to document it. Understanding how sensitive information moves into, through, and out of your business and who has (or could have) access to it is essential to assessing security risks.

E. Authentication

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected; the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

F. Encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as cipher text, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks.

G. Data Integrity

Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle,[1] and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. Data integrity is not to be confused with data security, the discipline of protecting data from unauthorized parties. Any unintended changes to data as the result of a storage, retrieval or processing operation, including malicious intent, unexpected hardware failure, and human error, is failure of data integrity. If the changes are the result of unauthorized access, it may also be a failure of data security.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VIII, August 2018- Available at www.ijraset.com

H. Backups

In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. Since a backup system contains at least one copy of all data considered worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model may be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.

I. Application Security

Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

Different techniques are used to surface such security vulnerabilities at different Stages of an applications lifecycle such design, development, deployment, upgrade and maintenance.

J. Attacks In Information Security

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, click jacking, brand jacking, botnet, phishing, spamming, inside and outside

Figure: various attacks in information security

K. Data Modification

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected; the more sensitive or valuable the information the stronger the control mechanisms need to be used. The foundation on which access control mechanisms are built start with identification and authentication.

L. Identity Spoofing (Ip Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data

M. Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

1) Obtain lists of valid user and computer names and network information.
2) Modify server and network configurations, including access controls and routing tables.
3) Modify, reroute, or delete your data.

N. Man-In-The-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information.

O. Denial-Of-Service Attack

Unlike other exploits, denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behavior of whole networks needs to be analyzed, not only the behavior of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, Trojan horse, or backdoor exploit to control them) are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion.

P. Direct-Access Attacks

An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions, install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system. Direct-access attacks are the only type of threat to Standalone computers (never connect to internet), in most cases.

Q. An Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

1) Read, add, delete, or modify your data or operating system.
2) Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
3) Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
4) Abnormally terminate your data applications or operating systems.
5) Disable other security controls to enable future attacks.

R. Indirect Attacks

An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonym zing systems, such as the tor onion router system.

S. Computer Crime

Computer crime refers to any crime that involves a computer and a network. It describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. Read on to find out what kinds of activities are considered computer crimes and how to prevent them.

II. CONCLUSION

In this protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Effective Information Security incorporates security products, technologies, policies and procedures he state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this. The above paper narrates how the information security is used and the security issues in order to protect from third party and some techniques which are used by the unauthorized persons to attack the data. They are done to prevent, detect, document and counter threats to digital and non-digital information.

REFERENCES

[1] Akyildiz, I.F. ; Georgia Inst. of Technol., Atlanta, GA, USA ; Weilian Su ; Sankarasubramaniam, Y. ; Cayirci, E "A survey on sensor networks." Communications magazine, IEEE 40.8 (2002): 102-114
[2] Ahmad Abed Alhameed Alkhatib, and Gurvinder Singh Baicher. "Wireless sensor network architecture." International conference on computer networks and communication systems (CNCS 2012)
[3] "A Study on Elliptic Curve Cryptography" in International Journal on Research Innovations in Engineering Science and Technology (IJRIEST), (ISSN 2455-8540), Volume 2, Issue 7, July-2017, pp: 546 – 550
[4] "A Survey on Cryptographic Cloud Storage Techniques" in International Journal of Engineering Sciences & Research Technology(IJESRT), ISSN: 2277-9655, July 2017, pp: 602-605.(Impact Factor: 4.116)
[5] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315
[6] "Secured Transmission of Data in cloud Environment Using Elliptic curve Cryptography" in International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE) (ISSN (online): 2320-9801), Vol. 3, Issue 8, August 2015(impact factor: 5.618).
[7] Vipul Goyal, Ajith Abraham, Sugata Sanyal and Sang Yong Han, "The N/R One Time Password System." Information Assurance and Security Track (IAS'05), IEEE International Conference on Information Technology: Coding and Computing (ITCC'05), USA, April, 2005. pp 733-738, IEEE Computer Society. [25]
[8] "A Novel Scheme for Remote Data Storage - Dual Encryption" in an International Journal of Research in Information Technology (IJRIT) ISSN: 2001-5569 Volume 2 Issue 4 April 2014.(Impact factor:1.738)
[9] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., "A pairwise key pre-distribution scheme for wireless sensor networks", Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51.
[10] "Selfish Carrier Monitoring In Wifi Using Distributed Sniffers" in an International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Issue 7, Volume 2(ISSN (Print): 2279-0047:ISSN (Online): 2279-0055) during February, 2014.(Impact factor:1.237)
[11] G. Bianchi, "A comparative study of the various security approaches used in wireless sensor networks," International Journal of Advanced Science and Technology, vol. 17, (2010) April, pp. 31-44. [10]
[12] "Reversible Data Embedding using Asymmetric Cryptosystem" in an International Journal of Advanced Research in Computer Science and Software Engineering(ISSN:2277-128X) in Volume 3, Issue 8 during August, 2013.(Impact factor:2.08)
[13] G. Padmavathi, and D. Shanmugapriya. "A survey of attacks, security mechanisms and challenges in wireless sensor networks." arXiv preprint arXiv: 0909.0576 (2009).
[14] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
[15] "An Approach for Secure Data Storage in Cloud Environment" in an International Journal of Computer and Communication Engineering (ISSN: 2010-3743) as one volume, and indexed by World Cat, Google Scholar, and Engineering & Technology Digital Library, Ulrich's Periodicals Directory.
[16] David J. Malan, Matt Welsh, Michael D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", Division of Engineering and Applied Sciences, Harvard University, Dec 2007