Network Security: Importance of Security, Audit & Related skills

Sanjivani Sumant [1], Shruti Joshi[2], Prof. Sweta Kale[3], Prof. Prachi Sorte[4]
[1] ME (IInd year), Department of IT, R. M. D. Sinhgad School of Engineering, Maharashtra, India
[2] ME (IInd year), Department of IT, R. M. D. Sinhgad School of Engineering, Maharashtra, India
[3] Assist. Professor, Department of IT, R. M. D. Sinhgad School of Engineering, Maharashtra, India
[4] Assist. Professor, Department of IT, R. M. D. Sinhgad School of Engineering, Maharashtra, India

Abstract - **Network Security plays a vital role in the field of Information Security. The number of attacks like Denial-Of-Service, Spoofing, Phishing, and Man-in-Middle violate the information security of the organisation. CIA Triangle- Confidentiality, integrity & availability are the important aspects in the network security. Confidentiality deals with the amount of secrecy which is enforced to prevent unauthorized disclosure. Integrity is the accuracy and reliability of information, the information is not altered while transmission. Availability assures reliability and timely access of the data to authorised users. One more term, Non-repudiation is also an important term in which user cannot deny about sending the information. To achieve the security there are different devices and techniques available. Techniques include Encryption & Hashing techniques, Digital signatures, Hardening of Devices, regular internal and external Audits and the devices like firewalls, IDS, IPS , Honeypots helps to secure the network from various external attacks. The network security skills must be implemented to recognize different attacks and to build the network and security architecture. Internal and external security audits must be conducted regularly for risk assessment and risk management. There are various standards and Certifications exists. ISO 27001:2005 is a standard which helps to establish, implement, and control the information security management system. By achieving this certification organization can move towards continuous improvement in regards of security management. This paper summarizes the importance of network security, various attacks, the devices and techniques which will assist students in learning these important concepts and helps to manage the information security.**

Key Words: Security, CIA triangle, Non-repudiation, Audit, Risk Assessment, Risk Management, ISO 27001:2005

1. INTRODUCTION

In Information Security, computer and Network Security play a vital role. Confidentiality, Integrity, Availability and Non-repudiation are the major aspects in Information Security. One should be aware of these terms when thinking about Information Security. In this, information is of any kind, data on hard disk, on the network, on tape drives, on storage devices, on compact disks or on a chit of paper.
The information which is related to business is important in the security point of view. Efforts should be made to protect this information. Security comes in the picture at this point when leakage of information leads to the negative impact on business values.
We will later see what exactly integrity, confidentiality, availability and non-repudiation means and how to achieve these to safe our information.
To achieve this, network and security administrator must be capable of handling the various security incidents. He or she should be capable to configure the network devices like Routers, Switches, Firewall and IPS/IDS to achieve the network and information security.

There are different kinds of attacks and threats that can access the traffic on the network segments or can take the access of network devices to hack the system to access the critical information. Some of the attacks are Brute Force attack, Spoofing, Phishing through which the intruder can take the access of the devices and hack the critical information.

To overcome these attacks the Security analyst must think like the cracker [1-2] that how he will attack the devices and make the preventive changes to his or her system.
Security audits must be conducted twice in a year to make sure that all the devices & system are in line with the security policies. Also it is useful to make awareness among the employees of an organization about security policies and procedures.

As security is today’s emerging career, an undergraduate student can study and learn from the simulations and labs to implement the security in the network. This will surely helpful for him/her to choose ‘Security’ as a career. Also this paper will be helpful to get the understanding about risk analysis & risk management and introduction to Security audit.

2. SECURITY FOCUS

The network security program highlights on the training the students to secure the network. For this, following information will surely helps the student in making right security decisions. For this one must be clearly aware about the CIA triangle. This speaks about Confidentiality, Integrity and Availability of information

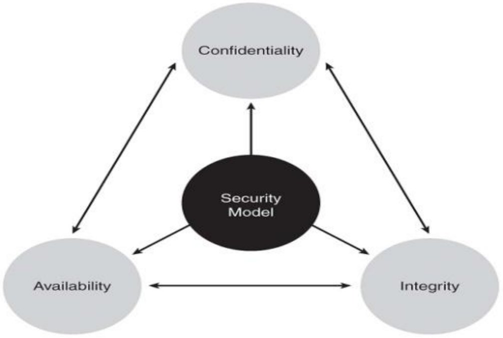


Fig -1: CIA Triangle

2.1. Confidentiality

It ensures that necessary amount of secrecy is enforced at each junction of data processing and prevent an authorized disclosure. This level of confidentiality can be achieved while data resides on the system and devices within the network as they transmit the data from source to destination. Users can intentionally or accidently disclose the sensitive information via shoulder surfing or social engineering. Confidentiality can be provided by encrypting the data as it is stored and transmitted, strict access control and by training personals on proper procedures.

2.2 Integrity

Integrity is the assurance of the accuracy and reliability of the information through which any unauthorized modification is prevented. Integrity means the data should not be modified or corrupt while in transit. There are various hashing techniques like MD5 or SHA which can be used to check the data integrity.

2.3 Availability

Availability ensures reliability and timely access to data and resources to authorized individuals. It can be affected by device or software failure. Necessary protection mechanisms must be in place to protect against inside and outside attacks that could intern affect availability productivity of the network.

One more term non-repudiation is also important in the security point of view, with this one cannot deny about sending the information. This can be achieved through encryption techniques and digital signature.

3. ATTACK RECOGNITION

There are various common attacks such as brute force attacks, spoofing, phishing, denial Of Service, and man-in-the–middle attack. [3, 7] Some of them are discussed below:

3.1 Brute force attack

It can be defined as trying every possible combination until the correct one is identified. The attacker usually tries handful number of combinations possible to exploit or to gain access into a system or a network. To overcome this, one can deploy IDS to watch the suspicious activity or set a lockout threshold. [7]

3.2 Phishing

Phishing is a more popular type of social engineering attack through which attacker can obtain personal information, credentials, credit card no., or financial data. The attacker, thus phishes for sensitive data through different methods. With this personal information, phisher can create new accounts in the victim's name, gain authorized access to bank accounts and make illegal credit card transactions. [7]

3.3 DoS

It is Denial of Service attack, in which the attacker continuously try to access the information through the particular service or port until it gets blocked. [8] Due to DoS attacks the system can become unavailable for a specific period of time. This is dangerous for the critical online servers like web servers, production and application servers.

3.4 Man-in-the-Middle attack

In Man-in-the–Middle attack, attackers monitor the packet from network, modify it and insert them back into the network. It allows the attacker to eavesdrop as well as to change, delete, add and divert data. [8]

3.5 Spoofing

Spoofing is a technique used to gain unauthorized access to computers where intruder sends a message with a source IP address that has been forged to indicate that the message are coming from a trusted host. In IP spoofing hackers use variety of techniques to obtain trusted IP address and then modify the packet headers to insert the forged IP address. [8]

4. NETWORK DEVICE SECURITY

To secure our network from such kind of attacks, certain skills must be practiced:

4.1 Hardening of Network Devices

Network devices deployed in the network must be hardened to prevent them an unauthorized access the routers, switches, and firewalls must be configured in such a way that intruder or hacker could not able to access these devices.

1. Default user names and passwords must be disabled
2. Telnet access should be allowed from authorized machines only otherwise denied.
3. Access control list –routers and firewalls should be configured to filter the packets accurately and efficiently by passing or dropping packets based on IP address and port address.
4. Unused services must be blocked.

5. Access through AAA- AAA stands for Authentication, Authorization & Accounting which must be configured in network so that each network device can be accessed through Tacacs or Radius servers so that proper authentication and authorization takes place and accounting of the network devices can be obtained which can be useful as a audit trail. Password management can be achieved through AAA server.

4.2 Firewall

Firewalls are used to restrict access to one network to another. Most companies use firewalls to restrict access to their network from internet or to restrict one internal segment from accessing another network segments. The firewall can give more defined and granual security policy through which the services are allowed to be accessed from the systems with authorized IP addresses. Ideally communication should flow through the firewall where traffic is inspected and restricted.

Firewall may be a router, server or specialized hardware device. Special skills are needed to configure the firewall according to requirements of security policy. Access –lists are needed to configure to allow or to restrict the access. Network address Translation can configured on the firewall to hide the internal IP addresses through outside

4.3 IDS/IPS

IDS (Intrusion Detection System) are designed to the security bridge. It is the system that takes care of detecting an unauthorized use of, attack upon a computer, network or telecommunication infrastructure. IDS are designed to mitigate the damage that can be caused by hacking. There are two types of IDS: Network based , which monitors network communication and Host based, which can analyze the activity within a computer system.IDS can be configured to watch the attacks, alert the administrators for the attacks, protect the system files.[7]

IPS(Intrusion Prevention System) which not only detects that something bad is taking place but also prevents the traffic to gain access to the target. So, IPS is the preventive and proactive technology and IDS is a detective and after the fact technology. [7]

4.4 Honey pot

Honey pot is a computer setup on the network which is the replica of authentic production system that has open ports and services enabled. It contains no real company information. So, it will not be at risk even if it will be attacked. With this, we can perhaps track down the attacker and can get more information about his techniques. [7]

4.5 Encryption

Encryption is method of transforming the readable data, plain text into unreadable format, cipher text. A system that provides the encryption and decryption is called the cryptosystem. Most of the encryption methods use the secret value called 'key' which works with algorithm to encrypt and decrypt the script. The key comprises a large sequence of random bits. Through cryptosystem we can achieve confidentiality, Integrity, Authentication, Authorization and non-repudiation.

Cryptography algorithms [7] are either symmetric or asymmetric. In symmetric cryptography, the sender and receiver uses the same key for encryption and decryption, while in asymmetric cryptography, each entity has different key- public key and private key. Public key is known to everyone but private key is only known to owner. By using the combination of public key and private key, we can achieve confidentiality, Integrity, Authentication, Authorization and non-repudiation.

Key management plays a critical role in encryption.

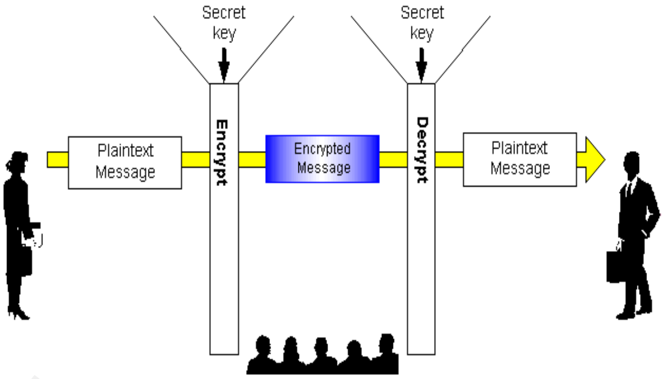


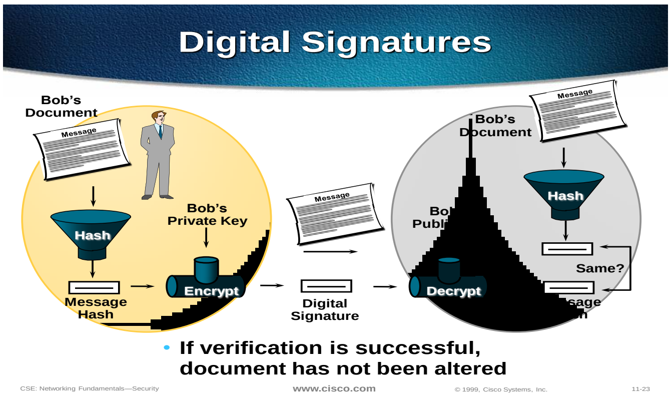
Fig -2: Example of Cryptography

4.6 Digital Signature

It is hash value that has been encrypted with sender's private key. The act of digitally signing the message means encrypting the message hash value with sender's private key. The hashing function ensures integrity of the message and signing of hash value provides authentication and non-repudiation. [7]

Figure 3 shows example of Digital Signature.

In this figure, Bob's message is hashed by using the hashing algorithms like SHA or MD5 and a message digest is formed. This message digest is again get encrypted by using the Private Key of Bob. This is a Digital Signature. This Digital Signature is sent along with the Document to sender. Sender upon receiving the document again calculates the Message digest of the same document by the same hashing algorithm. And by decrypting the received message hash value by using Bob's Public key, the document is verified for its Integrity.



- If verification is successful, document has not been altered

Fig -3: Example of Digital Signature

4.7 PKI (Public Key Infrastructure)

It is framework that uses public key cryptography. It consists of programs, procedures, protocols, security policies and public key cryptography which are working together in this framework. Each person that wants to participate in PKI requires digital certificate which is created and signed by certificate authority. [7]

4.8 IPSec:

IPSec is a protocol suit which set up a secure channel for protected data exchange between two devices. It is widely accepted standard for providing network layer protection. It is usually used to establish a virtual private network across the network. It has two modes: tunnel mode and transport mode. In transport mode the encapsulating security payload (ESP) of the message is encrypted. While in tunnel mode, along with the payload the authentication header (AH) is also get encrypted. It uses internet security association and key management protocol (ISAKMP). [7]

5. RISK ASSESSMENT AND MANAGEMENT

To secure the network the risks which are associated with the network devices must be assessed at regular intervals and the techniques should be implied to mitigate these risks.

5.1 Risk Assessment

Following are some steps to assess the risks-

- Identify the important assets. [4]
- Vulnerability testing- It is important audit exercise. Students need to research on the tools which addresses the vulnerability of the system. They can detect the vulnerabilities like password vulnerability or version checks of the system.[4]
- Once he/she determine that the system can be vulnerable for certain attacks for example, if in the system password management is not proper then system can be opened for Brute-Force attack.[4]

5.2 Risk Management

After the assessment of the risks, these risk need to be managed by applying certain security majors. It means, proper methods should be applied to mitigate this risk.

Risk appetite is also involved in Risk management; it is the amount of risk the organization can accept.

5.3 Audits

Audis are conducted to assess the risks and proper audit report need to prepare which can address all the risks for the system. Student can also practice and prepare audit plan and audit report according to vulnerability assessment which are also important skills. [5] Internal and External audits need to be conducted at regular intervals for the continuous improvement of the organization's security policy.

5.4 Standards related to Information Security

For auditing there are certain standards, ISO 27001:2005 [8] is a standard which is based on establishment, implementation, control and improvement of Information security management System (ISMS).The adaptation of ISMS should be strategic decision for an organisation. The design and implementation of organisation's ISMS is influenced by their needs, objectives, security requirements, the processes employed and the size and structure of organisation. These systems are expected to change over a time. This consists of COBIT, which includes the set of controls that should be in place for Information security management System.

6. CONCLUSIONS

As Security is an emerging carrier now a days, through this paper students can get the idea about the importance of security, various possible attacks, and risks in network and security field. They can also learn the various security and network devices. Students can get more exposure on audits and latest security standards and controls. The active learning in this direction will surely help students to be competent in performing security tasks required in the industry.

ACKNOWLEDGEMENT

We would like to thank our H.O.D. Prof. Dhara T. Kurian for her precious contribution and extended support.

REFERENCES

[1] P. Mateti, "A Laboratory-Based Course on Internet Security", Proc. Of 34th SIGCSE Technical Symp. on Computer Science Education, ACM,2003, 252-256.

[2] Computer Network Defense Course (CNDC), Army Reserve Readiness Training Center, Fort McCoy WI, http://arrtc.mccoy.army.mil, Jan.2004.

[3] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, 2006 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, GoCSI.com.

[4] U. A. Pabrai, The Art of Information Security, www.ecfirst.com, 2005.

[5] Auditing Networks, Perimeters, and Systems Hands-On Workbook, Audit 507 – Auditing Networks, Perimeters & Systems Course, SANS Institute, www.sans.org, 2005.

[6] M. Shema and B. C. Johnson, Anti-Hacker Toolkit, 2nd Ed., McGrawHill, 2004.

[7] CISSP All in one study Guide, 6th Edition ,Shon Harris, Publisher: McGraw-Hill Osborne Media Date: 2012

[8] Principles of information security, 4th Edition, Michael E. Whitman, Herbert J. Mattord

[9] http://en.wikipedia.org/wiki/ISO/IEC_27001

BIOGRAPHIES

Completed B.E.(Elect.) from Shivaji University. Pursuing M.E.in Information Technology from Savitribai Phule Pune University. Having 15 years of experience in Networking and security. Working in CMC Ltd, Pune.

Completed B.E.(I.T.) from University of Pune. Pursuing M.E in Information technology form Savitribai Phule Pune University.

Completed B.Tech.(CSE) from SNDT ,Mumbai and completed M.Tech.(CSE) from University of Nagpur. Currently working as Assistant Professor at R.M.D.Sinhgad College Of Engineering.

Completed B.E.(I.T.) from MIT Gondia and completed M.E.(I.T) from University of Pune. Currently working as Assistant Professor at R.M.D.Sinhgad College Of Engineering.