International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

Review on Information and Network Security

SREEHARI KUNDELLA

Independent Scholar, Hyderabad, Telangana, India, kundella.sreehari@gmail.com

---

Abstract - *This paper presents different techniques that deal with Information and Network Security. It presents brief overview of Cryptography, Information Security, and Network Security. Cryptography is a technique to protect the data safely while transforming from one computer to another computer through network. Information security is designed to protect the data from intruders, malicious intentions and viruses. Network Security is the huge topic to provide the security from unauthorized risks and potential security threats. Here we will discuss about different types of network security and how to protect from unauthorized risks.*

Key Words: Cryptography, Encryption, Decryption, Information Security, Network Security, Security Attacks, Malicious Software, Intruders, Firewalls.

1. INTRODUCTION

Nowadays Security is important aspect for information and network. Information is transmitted from one computer to another computer through networks either intranet or internet. Security is main concern to protect the information or data. Large volumes of data is electronically transmitted and stored every day on the net. The protection of systems and networks result in data availability, integrity and confidentiality. Cryptography is one of the major concept to provide the protection and securing the information by encrypting the data which is not understandable. Cryptography is an emerging technology for network security. Information security is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security.

2. COMPUTER SECURITY

William Stallings defines Computer Security as follows:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security:

2.1. Confidentiality

This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2.2. Integrity

This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

2.3. Availability

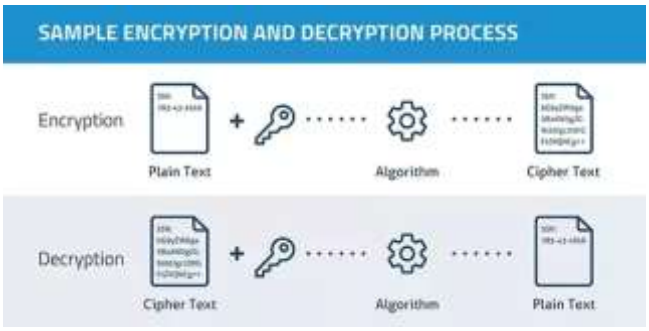
Assures that systems work promptly and service is not denied to authorized users.

3. CRYPTOGRAPHY

Cryptography is most often associated with scrambling plaintext into cipher text. This process is called encryption, then back again known as decryption. It provides for secure communication in the presence of malicious third-parties.

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.

Decryption is the conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.



There are two types of encryption in widespread use today: **symmetric** and **asymmetric** encryption. The name derives from whether or not the same key is used for encryption and decryption.

Symmetric encryption

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

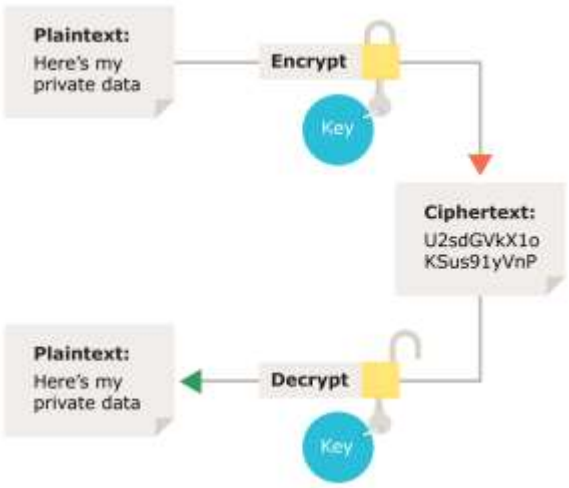


Figure 1: Symmetric encryption – Using the same key for encryption and decryption

Asymmetric encryption

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorized recipients or made available to the public at large.

Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorized or unlawful access to the data.

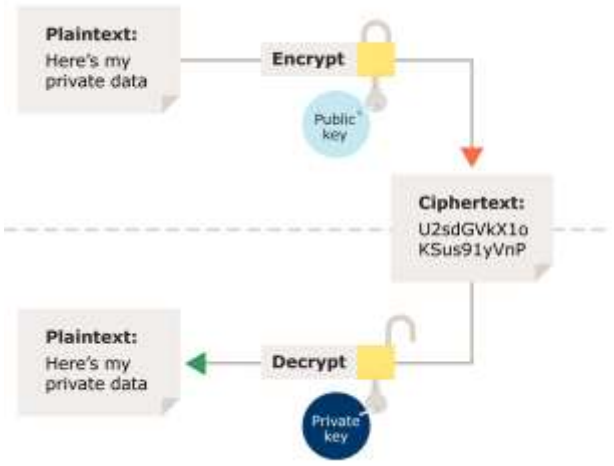


Figure 2: Asymmetric encryption – Using a different key for the encryption and decryption process

4. SECURITY ATTACKS

A useful means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks: Passive attacks (Figure 3) are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

Figure 3: Passive Attacks

Active Attacks: Active attacks (Figure 4) involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

Figure 4: Active Attacks

A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.

5. SECURITY SERVICES

Security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. These services divided into five categories.

5.1. Authentication

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

5.2. Access Control

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

5.3. Data Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

5.4. Data Integrity

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

5.5. Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the

sender can prove that the alleged receiver in fact received the message.

6. MALICIOUS SOFTWARE

a) Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.
b) A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
c) A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.
d) A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service.
e) A distributed denial of service attack is launched from multiple coordinated sources.

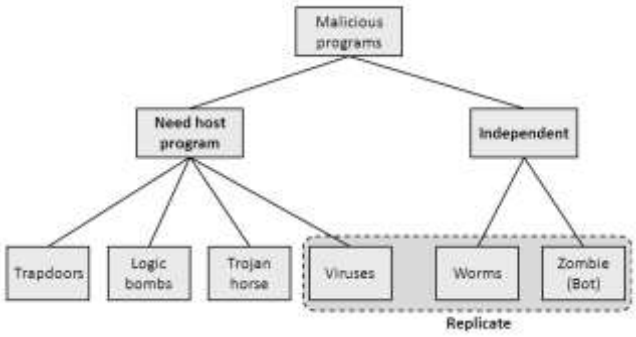


Figure 5: Malicious Programs

7. INTRUDERS

One of the two most publicized threats to security is the intruder (the other is viruses), generally referred to as a hacker or cracker. In an important early study of intrusion, Anderson [ANDE80] identified three classes of intruders:

Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

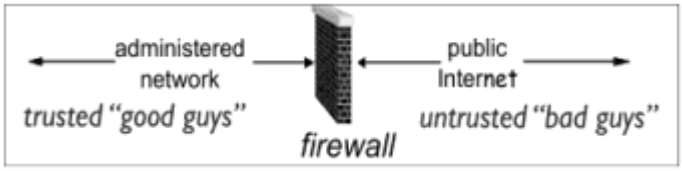
The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

8. FIREWALLS

Almost all small, medium and large organizations use the internet and have a connection to a company's network. At the boundary of the organization network, there must be a partition between the external and internal network that is essential for network security. The internal corporate network is known as the trusted zone while the external network is known as the untrusted zone. A Firewall is a network device that protects organizations' networks from intruders from inside and outside.

All data packets entering or leaving the internal network pass through the firewall. It inspects each packet and blocks any untrusted traffic.



8.1. Types of Firewalls

A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. Types of firewalls are shown in Figure 6.

8.1.1. Packet Filter

A packet filter is a first generation firewall that processes network traffic on a packet-by-packet basis (Figure 6a). Its main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network. Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted. Packet

filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.

8.1.2. Application-Level Gateway

An application-level gateway, also called a proxy server (Figure 6b), acts as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

A prime disadvantage of this type of gateway is the additional processing overhead on each connection. In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

8.1.3. Circuit-Level Gateway

A third type of firewall is the circuit-level gateway (Figure 6c). This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

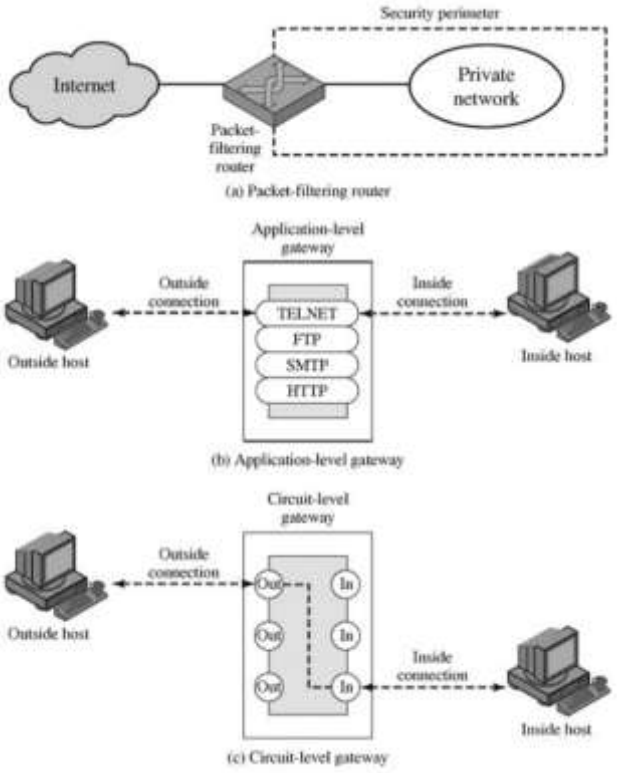


Figure 6: Types of Firewalls

9. CONCLUSION

This paper explains the security concepts of various network policies. Network and data security have become an inevitable concern for any organization whose internal private network is connected to the Internet. The security for the data has become highly important. The paper presented various schemes which are used in cryptography for Network security purpose. Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithms in network protocols and network applications. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security.

REFERENCES

[1] Cryptography and Network Security: Principles and Practice, Sixth Edition, William Stallings.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/types-of-encryption/

[3] M. Jagadheeswari, "Network Security- An Overview" Research Article Volume 7 Issue No.5 @2017 IJESE.

[4] Shyam Nandan Kumar, "Review on Network Security and Cryptography" International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11.

[5] Sandeep Kaur, C.K.Raina, "Firewall in Network Security" Research Article Volume 7 Issue No.4 @2017 IJESE.

[6] Smitha.G.L, Dr.E.Baburaj, "A Survey on Information Security" Research Article Volume 6 Issue No.9 @2017 IJESE.

[7] FATIMA MAIKUDI ABUBAKAR& SHITU ABDULLAHI LAME, "THE ROLE OF CRYPTOGRAPHY IN INFORMATION AND DATA SECURITY", Proceedings of the Academic Conference of African Scholar Publications & Research International on Sub-Sahara African Transformation and National Development Vol. 7 No. 1. 8th October, 2015 - C.E.S. Lecture Hall, Kaduna Polytechnic, Barnawa Campus, Kaduna, Kaduna State.