Gulshan Kumar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 11, November- 2014, pg. 24-32 **ISSN: 2321-8363**

Computer Network Attacks - A Study

Gulshan Kumar[1], Amanjeet Kaur[2], Sania Sethi[3]

[1]Assistant Professor, SBS State Technical Campus, Ferozepur (Punjab)-India

Email: gulshanahuja@gmail.com, Ph. +91-8146550540

[2]Reseach Scholar, Email: aman.mca07@gmail.com, Ph.: +91-8427000689

[3]Reseach Scholar, Email: saniasethi08@gmail.com, Ph.: +91-9915818513

Abstract: Network security consists of the provision and policies adopted by a network administration to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. In today's era, almost every single organization uses a computer and has a computer network to send, receive and store information. Whether it's sending emails, storing documents, or serving information through a web server, it is very important to focus on security, especially if your network contains sensitive, confidential and personal information. So with invent and increased use of internet security has become a major concern. The entire field of network security is vast and in an evolutionary stage so main focus of this paper is on the attacks against basic principle of network security or on CIA model of security as we are aware security became a fundamental component of every network design. In this paper, we presented an overview of different network attacks on confidentiality, integrity and availability of network resources. The study will help the readers to understand the current scenario of network security and provides clues for future directions.

There is a large amount of personal, commercial, military, and government information on networking infrastru cture worldwide.

Keywords: Availability, Confidentiality, Integrity, Network Security, Security Attacks

1. Introduction

The world is becoming more interconnected with the advent of the Internet and new networking technology (Computer N.N). There is a large amount of personal, commercial, military, and government information on networking infrastructure worldwide. Network security affects many organizations, whether they are large, small, or government organizations. If network security is breached an intruder can do all sorts of harm (Hilbert, 2013). That is why people need to be aware of and to be educated about network security and different attacks on network.

Network attack is usually defined as an intrusion on your network infrastructure that will first analyze your environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to your resources (Window, 2014). In such cases where the purpose of attack is only to learn and get some information from your system but the system resources are not altered or disabled in any way, we are dealing with a passive attack. Active attack occurs where the perpetrator accesses and either alters, disables or destroys your resources or data. Attack can be performed either from outside of the organization by unauthorized entity (Outside Attack) or from within the company by an "insider" that already has certain access to the network (Inside Attack).

Remembering that network security is the most important aim of any organizations (second to human lives, of course), the first principles ask what is being protected, why, and how do we control access? The fundamental goal of your network security program is to answer these questions by determining the confidentiality of the network, how can you maintain the integrity, and in what manner its availability is governed (Window, 2014). These three principles make up the CIA triad. Network Security revolves around three basic pillars i.e. Confidentiality, integrity and availability (Kumar et al., 2010).

2. Fundamental Principles of Network Security

Network Security revolves around three basic pillars i.e. Confidentiality, integrity and Availability (Kumar et al., 2010, Window, 2014). A network is not secure unless it can ensure the three basic security concepts; confidentiality, integrity and availability. Attack on confidentiality and integrity of data are emerging trends in network intrusion. In this paper we primarily focus on the confidentiality aspect. With more and more sophisticated tools being easily available the number of security incidents has been rapidly increasing.

The CIA triad is a very fundamental concept in security. Often, ensuring that the three facets of the CIA triad is protected is an important step in designing any secure system. Therefore study of CIA trend helps reader to predict future attacks on these trend and possible way out to restrict these attacks (Pearson).

2.1Confidentiality

Confidentiality means the preservation of data privacy from unwanted and illegal users. It is a passive form of attacks where the attacker attempts to obtain confidential information about network user like login credentials, SSN, Credit Card information or email password. With respect to the content of data transmission, several levels of protection can be identified.

A good example is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm and biometric verification is an option as well. In addition, users can take

precautions to minimize the number of places where the information appears, and the number of times it is actually transmitted to complete a required transaction (Patcha and Park, 2007).

Protections offered to confidential data are only as good as the security program itself. To maintain confidentiality, the security program must consider the consequences of an attacker monitoring the network to read the data. Although tools are available that can prevent the attacker from reading the data in this manner, safeguards should be in place at the points of transmission, such as by using encryption or physically safeguarding the network.

Another attack to confidentially is the use of social engineering to access the data or obtain access. Social engineering is difficult to defend because it requires a comprehensive and proactive security awareness program. Users should be educated about the problems and punishments that result when they intentionally or accidentally disclose information. This can include safeguarding usernames and passwords from being used by an attacker.

Protecting against Loss of Confidentiality: Organizations protect against loss of confidentiality in following way

- Access Control
- Encryption.

2.2Integrity

Data integrity refers to the preservation of the content and source of the data .It consists of checking whether the data has been transmitted from an authentic source and has not been tampered in transit. So, Integrity provides the assurance that the data is accurate and reliable. Without integrity, the cost of collecting and maintaining the data cannot be justified. Therefore, policies and procedures should support ensuring that data can be trusted.

To ensure integrity, you need to prevent information from being inappropriately modified. Data integrity can be compromised through accidental events or malicious means. Storage media problems, crashed or buggy programs and noisy transmission environments can cause accidental data corruption. Because the hardware, the Windows OS, or an application in the network typically catches accidental data corruption, accidental corruption problems usually become availability problems (Schneider, 2012).

Malicious individuals might corrupt or delete data just for the nihilistic thrill of it, for revenge, or for other reasons. However, malware (i.e., malicious software that's designed to compromise the privacy, integrity, or availability of a system or network) damages data more often than an actual person.

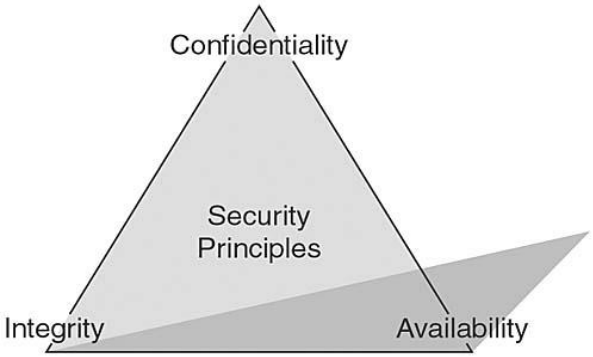

Figure 1: Fundamental principles of network security

2.3Availability

Availability is the ability of the users to access an information asset. Information is of no use if it cannot be accessed. Systems should have sufficient capacity to satisfy user requests for access, and network architects should consider capacity as part of availability. Policies can be written to enforce this by specifying that procedures be created to prevent denial-of-service (DoS) attacks (Pots, 2012, Schneider, 2012).

More than just attackers can affect system and network availability. The environment, weather, fire, electrical problems, and other factors can prevent systems and networks from functioning. To prevent these problems, organization's physical security policies should specify various controls and procedures to help maintain availability. Yet access does not mean that data has to be available immediately. Availability of information should recognize that not all data has to be available upon request. Some data can be stored on media that might require user or operator intervention to access. For example, if your organization collects gigabytes of data daily, you might not have the resources to store it all online. This data can be stored on an offline storage unit, such as a CD jukebox, that does not offer immediate access.

3. Types of network attacks

There are mainly two types of attack are present.

- **Passive attacks.**
- **Active attacks.**

3.1 Passive attacks

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the

disclosure of information or data files to an attacker without the consent or knowledge of the user. Passive attacks do not affect the target and the target is unaware of the attacks (Computer N.N). Examples of a passive attack are:

- Sniffing to record captured frames
- Eavesdropping
- Emanations detection
- Wiretapping

3.2Active attacks

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DOS, or modification of data. Active attacks do affect the target and the target is aware of the attack. Examples of active attacks are:

- Interruption
- Modification
- Fabrication(DOS)
- Replay attacks

The classification of network attacks described above can be summarized in Table 1.

Attacks	**Passive/Active**	**Threat**
Snooping Traffic analysis	Passive	Confidentiality
Wiretapping Eavesdropping DNS Poisoning	Active	
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of services	Active	Availability

Table 1: Categorization of passive and active attacks

4. Network attacks on security principles

Different types of network attacks can be aimed at three pillars of Network Security namely Confidentiality, Integrity and Availability. The three principles of security confidentiality, integrity, and availability can be threatened by security attacks in following ways.

4.1 Network attacks on confidentiality

A large number of attacks can be mounted to disrupt the confidentiality of network information. The attacks are as described in subsequent subsections.

4.1.1 ***Passive Attacks Threatening Confidentiality:*** The passives attacks are as described below:

a) **Snooping**: It is passive form of attack where the attackers attempts to obtain confidential information about network users like login credentials, SSN, Credit Card information or e-mail password. It is refers to unauthorized access to or interception of data. This type of attack causes a host or application to mimic the actions of another. Typically the attacker pretends to be an innocent host by following IP addresses in network packets. Snooping is in following ways:

- **Digital Snooping** - Monitoring a private or public network for passwords or data. This attack is at the network layer. This snooping is done on the physical cable. Attackers may reprogram network switches or other devices to allow them to capture data off a network. They may capture data that they should not have access to or they may capture user IDs and passwords, then run a password cracking program against them.
- **Shoulder Snooping** - This is a physical attack where someone tries to watch for typed passwords or see information on a monitor that they should not have access to.

b) **Traffic analysis:** In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis.

Countermeasures of these attacks include the traffic padding which involves releasing information or performing tasks that appear to be significant but are not. It is intended to mislead potential attackers.

4.1.2 ***Active attacks threatening Confidentiality:*** The active attacks are described below:

a) **Wiretapping:** Passive wiretapping monitors or records the traffic, while active wiretapping alters or otherwise affects it.

b) **Eavesdropping**: This is the simplest type of attack. A host is configured to "listen" to and capture data not belonging to it. Carefully written eavesdropping programs can take usernames and passwords from user login network connections. Broadcast networks like Ethernet are especially vulnerable to this type of attack. To protect against this type of threat, avoid use of broadcast network technologies and enforce the use of data encryption. IP firewalling is very useful in preventing or reducing unauthorized access, network

layer denial of service, and IP spoofing attacks. It not very useful in avoiding exploitation of weaknesses in network services or programs and eavesdropping.

c) **DNS Poisoning:** DNS poisoning is a process in which an attacker alters records in a DNS database so that a legitimate Web URLs point to a fraudulent Web site. In a DNS poisoning attack (Schneider, 2012, Kumar and Kumar, 2014):

- The attacker gains access to a DNS database.
- The attacker replaces a valid URL with the URL of a fraudulent Web site.
- In attempting to access the valid Web site, the target is directed to the fraudulent site.
- The fraudulent Web site requests the target to provide sensitive information.

4.2 Network attacks on integrity

A large number of attacks can be mounted to disrupt the integrity of network information. The attacks are as described in subsequent subsections.

4.2.1 Active attacks threatening Integrity

a) **Modification**: means that the some portion of a legitimate message is altered, or that message are delayed or reordered, to produce an unauthorized effect attacker intercepts the message and changes it.

b) **Masquerading or spoofing:** In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. It happens when the attacker impersonates somebody else. e.g. IP Spoofing

c) **Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it. It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

d) **Repudiation**: means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

4.3 Networks attacks on availability

Denial of service (DOS) is a very common attack that disrupts the availability of network resources (Security, 2002). Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors It may slow down or totally interrupt the service of a system. A denial of service attack is a special kind of Internet attack aimed at large websites. It is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Denial of Service can result when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real requests or talks. Yahoo! and e-bay were both victims of such attacks in February 2000 (Security, 2002).

A Dos attack can be perpetrated in a number of ways. There are three basic types of attack.

- Consumption of computational resources, such as band width, disk space or CPU time.
- Disruption of configuration information, such as routing information.
- Disruption of physical network components.

The consequences of a DOS attack are the following:

- Unusually slow network performance.
- Unavailability of a particular web site.
- Inability to access any web site.
- Dramatic increase in the amount of spam you receive in your account.

The description of network attacks on fundamental principles of security provided in above sections can be summarized in figure 1 as shown below.

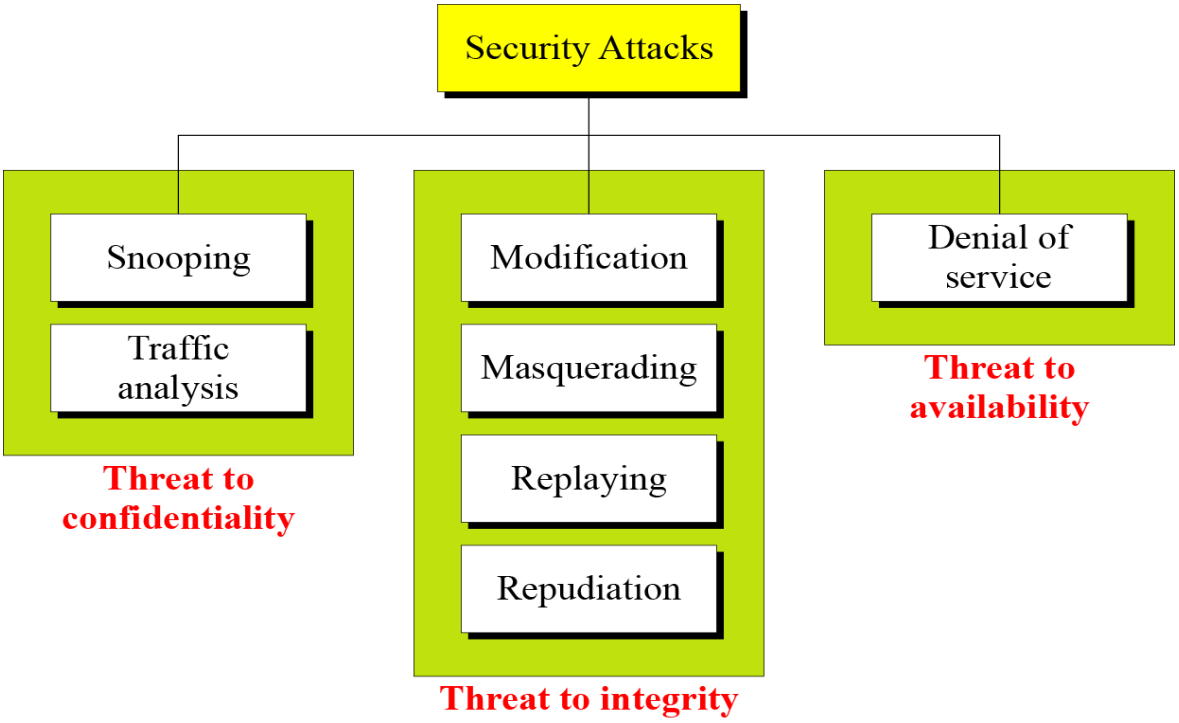

Figure 1: Network attacks on fundamental principles of security

5. Conclusions

In this research paper, we presented an overview of security attacks on basic building blocks of security. The findings of the study are that increasing reliance of network and communications facilities to build adequate security that enhance the level of security of CIA principle of network security. The requirements for security are best assessed by examining the various security attacks of active and passive nature faced by an organization on

confidentiality, Integrity and availability. The interruption of service is a severe threat to availability. The interception of information is a threat to secrecy. Finally, both the modification of legitimate information and the unauthorized fabrication of information are threats to integrity. The paper will facilitate the users to understand the attacks on network resources targeting the fundamental principles of security and provides clues for future directions.

References

[1] Computer N. N, http://computernetworkingnotes.com/network-security, Accessed on 18th Oct 2014.

[2] Hilbert, E.: Living with cybercrime. Network Security 2013 (11), 15-17 (2013).

[3] Kumar, G., Kumar, K., Sachdeva, M.: The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review 34(4), 369-387 (2010).

[4] Kumar, Gulshan, and Krishan Kumar. "Network security–an updated perspective." Systems Science & Control Engineering: An Open Access Journal 2.1 (2014): 325-334.

[5] MIT education, http://web.mit.edu/~bdaya/www/Network%20Security.pdf, Accessed on 15th Oct 2014.

[6] Patcha, A., Park, J.M.: An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks 51(12), 3448- 3470 (2007). DOI 10.1016/j.comnet.2007.02.001.

[7] Pearson, http://www.pearsonitcertification.com/ (2014) Accessed on 18th Oct 2014.

[8] Potts, M.: The state of information security. Network Security 2012 (7), 9 - 11 (2012)

[9] Ramamohanarao, K., Gupta, K., Peng, T., Leckie, C.: The curse of ease of access to the internet. Information Systems Security pp. 234-249 (2007)

[10] Schneider, D.: The state of network security. Network Security 2012(2), 14-20 (2012).

[11] Security PRO news, http://www.securitypronews.com/introduction-to-network-attacks-2002-06, (2002), Accessed on 30th Oct 2014.

[12] Windows Magazine IT PRO, http://windowsitpro.com/security/3-pillars-information-security#, (2014), Accessed on 15th Oct 2014.

