ISSN: 2321-7782

Volume 1, Issue 1, June 2013

International Journal of Advance Research in Computer Science and Management Studies

Research Paper

Available online at: www.ijarcsms.com

Computer & Network Security Threats

Abhishek P. Bhatt
Department of Postgraduate Education
Saint Petersburg State university
7-9, Universitetskaya nab
St. Petersburg
Russia

Abstract: ***Modern organizations depend heavily on their information systems and large investments are made on them annually. These systems are now computerized and networking has been the common trend during the last decade. The availability of information and computer resources within an organization as well as between cooperating organizations is often critical for the production of goods and services.***

Computer security is traditionally defined by the three attributes of confidentiality, integrity and availability. Confidentiality is the prevention of unauthorized disclosure of information. Integrity is the prevention of unauthorized modification of information and Availability is the prevention of unauthorized withholding of information or resources.

This paper study about the various types of security threats and computer system assets.

Keywords: Computer & Network Security, Types of Threats, Computer System Assets.

I. Introduction

System security can mean several things. To have system security we need to protect the system from corruption and we need to protect the data on the system. There are many reasons why these need not be secure.

- A system may not be able to function any longer because one user fills up the entire disk with garbage.
- Power failure might bring the system down.
- Malicious users may try to hack into the system to destroy it.

We can classify the security attacks into two types as mentioned below:

- **Direct:** This is any direct attack on your specific systems, whether from outside hackers or from disgruntled insiders.
- **Indirect:** This is a general random attack, most common computer viruses, computer worms or computer trojan horses.

II. Objectives

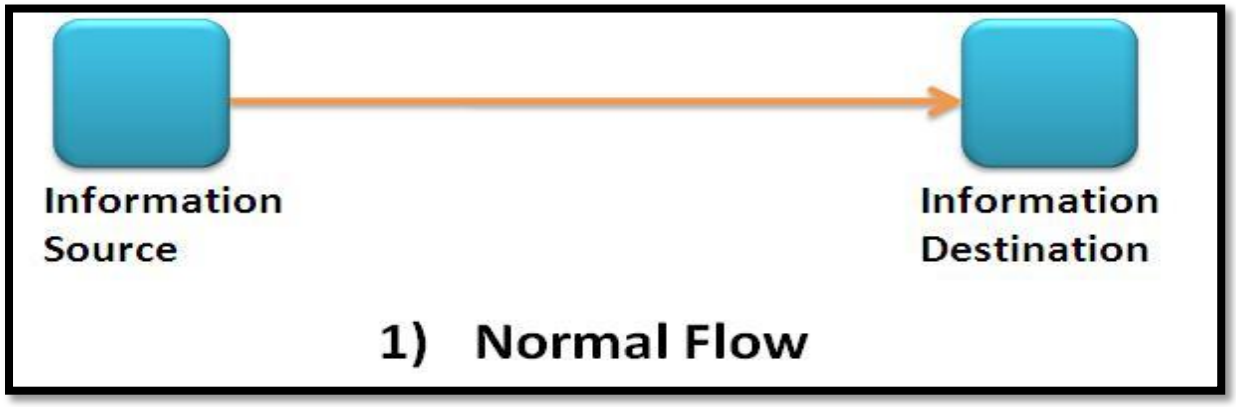
- Discover the security of computer and network level.
- Identify the security threats and goals.
- Mention the role of computer system assets in security.

III. Types of Threats

The types of attacks on the security of a computer system or network are best characterized by viewing the function of the computer system as providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user.

1) Normal Flow:

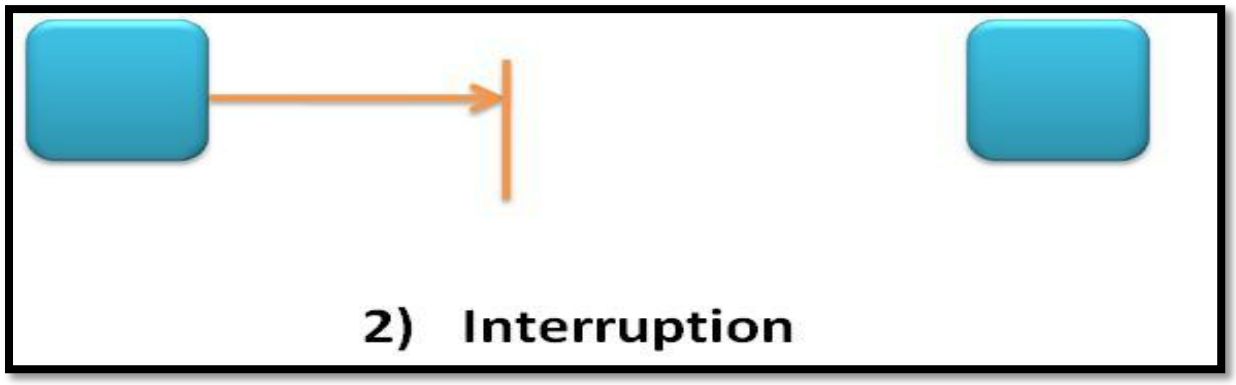
This normal flow is depicted in figure.



2) Interruption:

An asset of the system is destroyed or becomes unavailable or unusable. This is attack **availability**.

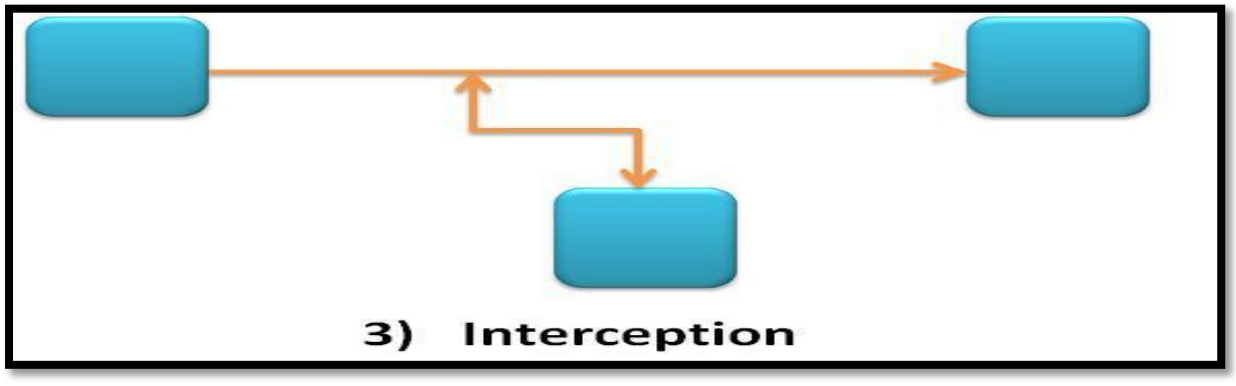
Examples include the destruction of a piece of hardware, such as a hard disk, the cutting of a communication line or disabling of the file management system.



3) Interception:

An unauthorized party gains access to an asset. This is an attack on **confidentiality**. The unauthorized party could be a person, a program or a computer.

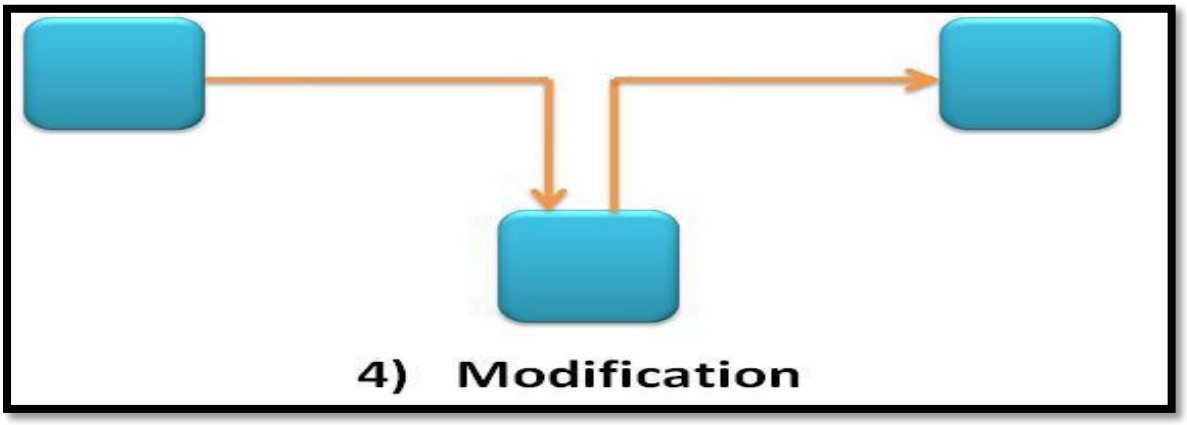
Examples include wire tapping to capture data in a network and the illicit copying of files or programs.



4) Modification:

An unauthorized party not only gains access to but tampers with the asset. This is an attack on **integrity**.

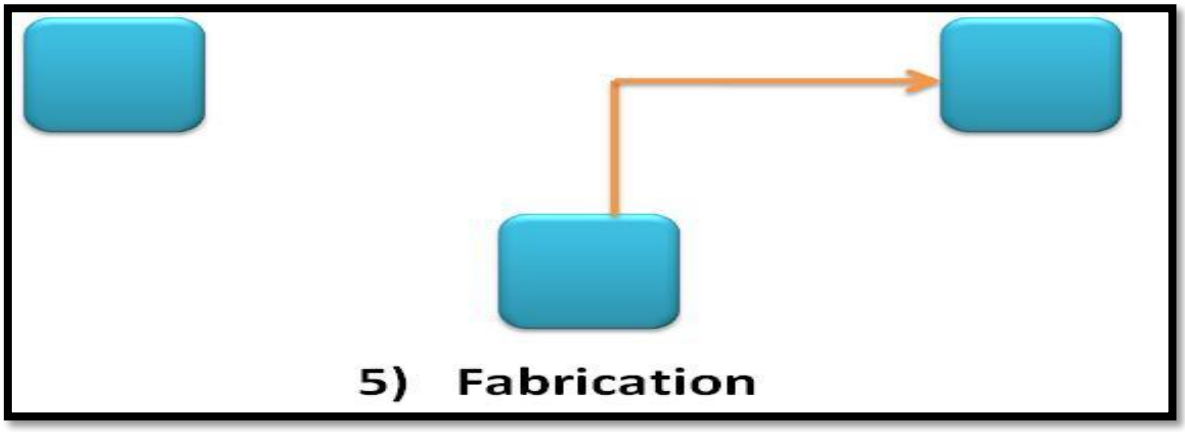
Examples include changing values in a data file, altering a program so that it performs differently and modifying the content of messages being transmitted on a network.



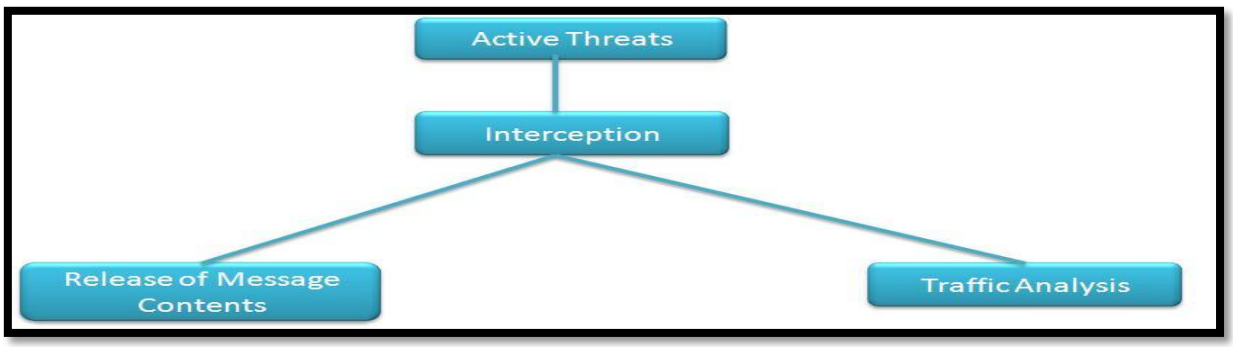
5) Fabrication:

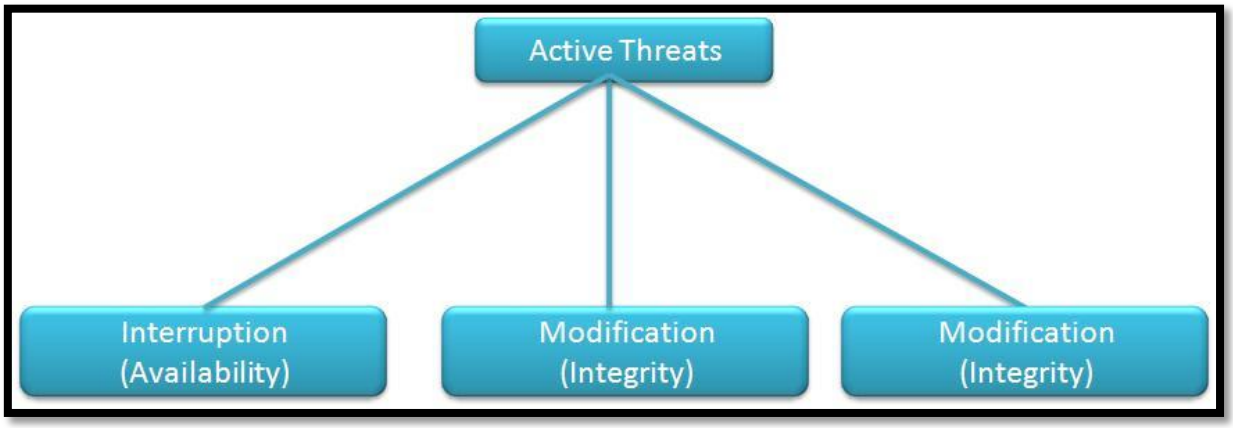
An unauthorized party inserts counterfeit objects into the system. This is an attack on **authenticity**.

Examples include the insertion of spurious messages in a network or the addition of records to a file.



Active and passive network security threats:





IV. Computer System Assets

The assets of a computer system can be categorized as hardware, software, data and communication lines.

Hardware: The main threat to computer system hardware is in the area of availability. Hardware is the most vulnerable to attack and the least amenable to automated controls. Threats include accidental and deliberate damage to equipment as well as theft. Physical and administrative security measures are needed to deal with these threats.

Availability:	Equipment is stolen or disabled, thus denying service.
Secrecy:	-
Integrity:	-

Software: The operating system, utilities and application programs make what computer system hardware useful to business and individuals.

Availability:	Programs are deleted, denying access to users.
Secrecy:	An unauthorized copy of software is made
Integrity:	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.

Data: Hardware and software security are typically concerned of computing center professionals or individual concerns of personal computer users. A much more widespread problem is data security, which involves filing and other forms of data controlled by individuals, groups and business organizations.

Availability:	Files are deleted, denying access to users.
Secrecy:	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.
Integrity:	Existing files are modified or new files are fabricated.

Communication Lines: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmission. The goal of the opponent is to obtain information that is being transmitted.

Availability:	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.
Secrecy:	Messages are read. The traffic pattern of messages is observed.
Integrity:	Messages are modified delayed, reordered, or duplicated. False messages are fabricated.

V. Conclusion

In this research work, we have studied the concept of security and various threats to it. The result of this study is that increasing reliance by business on the use of data processing system and the increasing use of network and communications facilities to build distributed systems have outcome in a strong requirement for computer and network security.

The requirements for security are best assessed by examining the various security threats faced by an organization. The interruption of service is a 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.

References

Books:

1. EC-Council, Network Defense: Security Policy and Threats – 1st Edition (Apr 2010) Cengage Learning.
2. James Michael Stewart, Network Security, Firewalls and VPN – 4th Edition (2011) Jones & Bartlett Learning Canada.
3. Willing Stallings. Operating System Internals and Design Principles – 3rd Edition New Jersey: Prentice-Hall International.
4. Avi Silberschatz, Peter Baer Galvin, Greg Gagne – Operating System Concept – 9th Edition John Wiley & Sons.

Web sites:

1. Network security available at: http://en.wikipedia.org/wiki/Network_security

2. Threat (computer) available at: http://en.wikipedia.org/wiki/Threat_%28computer%29

