Introduction to Information Technology

CSC109

2020

By: Rajiv Raman Parajuli

Unit 11: Computer Security

- Introduction;
- Security Threat and Security Attack;
- Malicious Software;
- Security Services;
- Security Mechanisms

(Cryptography, Digital Signature, Firewall, Users Identification and Authentication, Intrusion Detection Systems);

- Security Awareness;
- Security Policy

This Chapter make your base for further study of Network Security and Cryptography Subject

Introduction

We ensure security of our belongings, home, office, locality, city, country and so on, using different mechanism.

You lock your car and bike even you take your helmet with you when you park it, which gives you personal sense of security. Some even install GPS and alarm on bikes and cars as a security measures.

Could you imagine;

Your personal financial data, college works, key personal secrets etc are destroyed , changed or made public.

What are you willing to do to prevent it?

1st Step is Security awareness

Securing your data not only secure your computer hardware, software and data also secure yourself.

Introduction cont..

Computers being in use at every level– Need of Computer security

To:

- protect the computing system and to protect the data that they store and access.
- Transmission protection; to protect the data during transmission over the network.

This field of research and study has been linearly growing as new tech emerges.

Term **computer Security**; address both Computer security and network security.

Computer security focus:

1. **Security Attacks:** are the reasons for breach of security. Security attacks comprise of all actions that breaches the computer security.
2. **Security Mechanisms:** tools that include the algorithms, protocols or devices, that are designed to detect, prevent, or recover from a security attack.
3. **Security services:** provided by a system for a specific kind of protection to the system resources.

Security Threat And Security Attack

Point of Computer security is to eliminate or protect against threats.

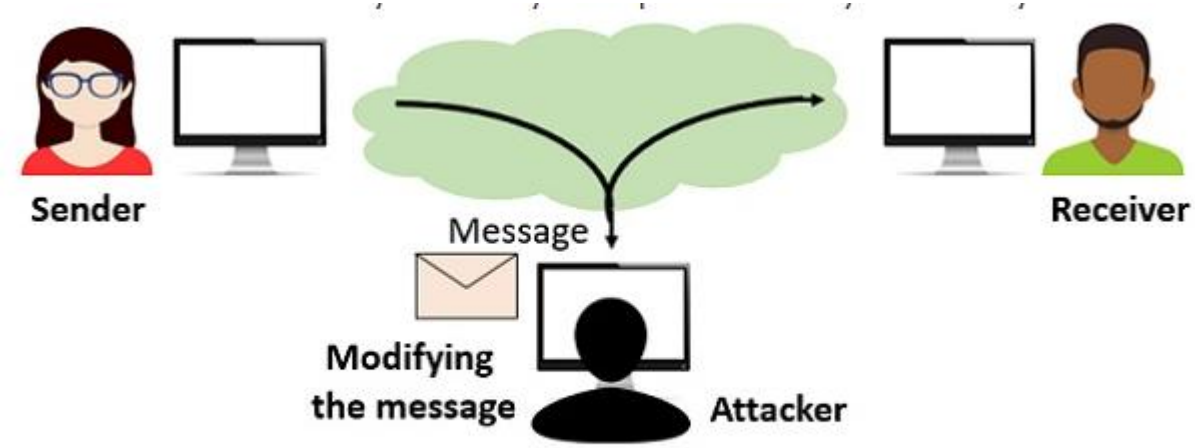
A threat is anything that can cause harm.

By itself its not harmful unless it exploits an existing vulnerability.

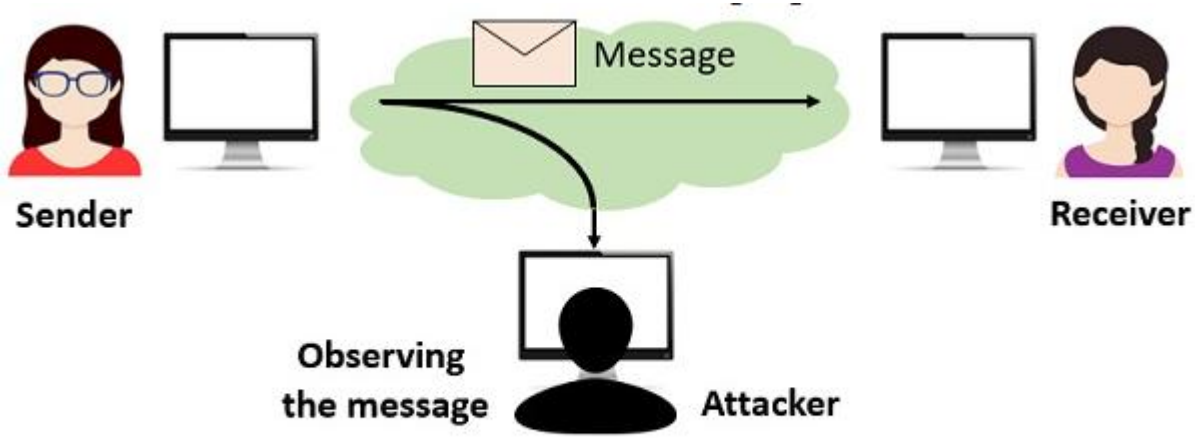
A Vulnerability is a weakness- anything that has been left unprotected and left it open to harm, easy on security attacks.

Passive Attack

Active Attack



Active Attack



Passive Attack

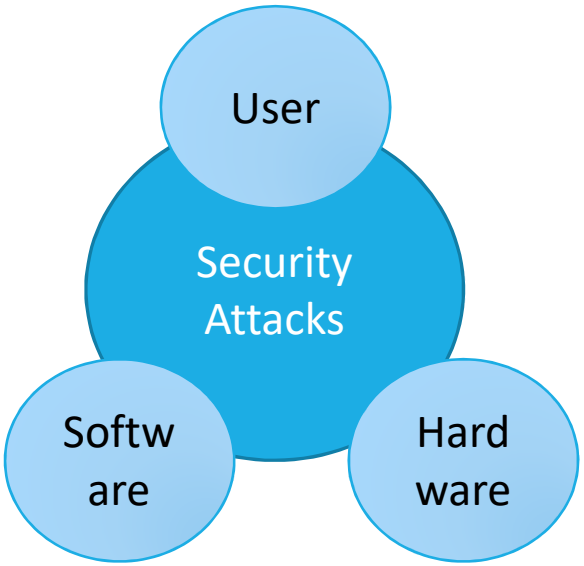
BASIS FOR COMPARISON	ACTIVE ATTACK	PASSIVE ATTACK
Basic	Active attack tries to change the system resources or affect their operation.	Passive attack tries to read or make use of information from the system but does not influence system resources.
Modification in the information	Occurs	does not take place
Harm to the system	Always causes damage to the system.	Do not cause any harm.
Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets informed about the attack.	The entity is unaware of the attack.
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link.	Just need to observe the transmission.
Emphasis is on	Detection	Prevention

users, computer hardware and computer software

Attacks on users : identity of user and to the privacy of user.

Attacks on computer hardware could be due to a natural calamity like floods or earthquakes

Software attacks harm the data stored in the computer. Software attacks may be due to malicious software, or, due to hacking.



Malicious Software

Malicious users use different methods to break into the systems

The software that is intentionally included into a system with the intention to harm the system is called *malicious software.*

These types of programs/ software are able to self-replicate and can spread copies of themselves, which might even be modified copies.

Malware, viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

Even Javascripts and Java applets written with the purpose of attacking

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse.

More advanced uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.