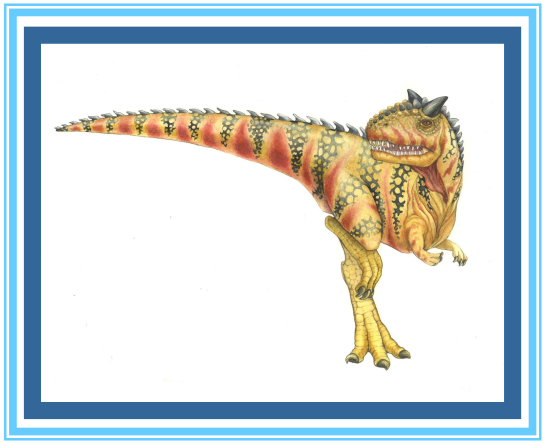
COM S 352 Operating Systems

Lecture 29: Security Basics



The Security Problem

- Goal of security is to protect
  - the integrity of the information stored in the system (both data and code)
  - and the physical resources of the computer system
- System is **secure** if resources are used and accessed as intended under all circumstances
  - Unachievable
- The security system prevents unauthorized access, malicious destruction or alteration of data, and accidental introduction of inconsistency
- **Intruders** are those who attempt to breach security
- A **vulnerability** is a weakness in the security of a system
  - Buffer that is not protected from overflow
- A **threat** is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure
  - Theft, fire, virus, spyware
- An **attack** is an attempt to breach security
  - Attack can be accidental or malicious

Requirements of Security Mechanisms

- **Confidentiality**: information maintained by a computer system is accessible only by authorized parties (users and the processes that run as/represent those users).
- **Integrity:** a computer system's resources can be modified only by authorized parties.
- **Availability**: a computer system be accessible at required times by authorized parties.
- **Authenticity**: a computer system can verify the identity of a user

Security Violation Categories

- **Breach of confidentiality**
  - Unauthorized reading of data
- **Breach of integrity**
  - Unauthorized modification of data
- **Breach of availability**
  - Unauthorized destruction of data
- **Theft of service**
  - Unauthorized use of resources
- **Denial of service (DOS)**
  - Prevention of legitimate use

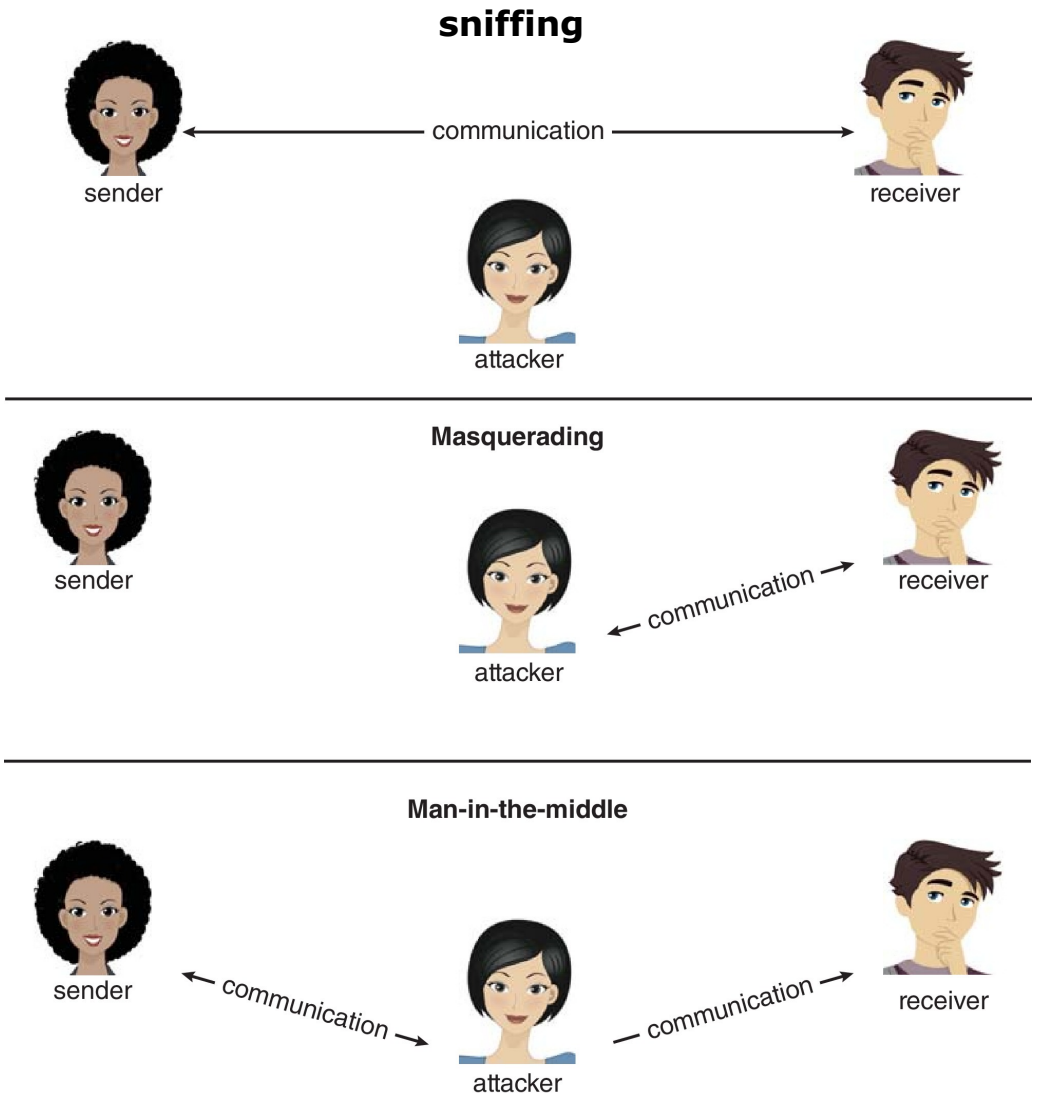
Program Threats

- **Malware -** Software designed to exploit, disable, or damage computer systems
- **Trojan Horse** – Program that looks legitimate but can take control of your computer.
  - **Spyware** – Program frequently installed with legitimate software to display ads, capture user data (Up to 90% of spam delivered by spyware-infected systems)
- **Ransomware** – Locks up data via encryption, demanding payment to unlock it
- Malware thrive when there is a violation of the Principle of Least Privilege

THE PRINCIPLE OF LEAST PRIVILEGE

"The principle of least privilege. Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. The purpose of this principle is to reduce the number of potential interactions among privileged programs to the minimum necessary to operate correctly, so that one may develop confidence that unintentional, unwanted, or improper uses of privilege do not occur."—Jerome H. Saltzer, describing a design principle of the Multics operating system in 1974: https://pdfs.semanticscholar.org/1c8d/06510ad449ad24fbdd164f8008cc730cab47.pdf.

System and Network Threats



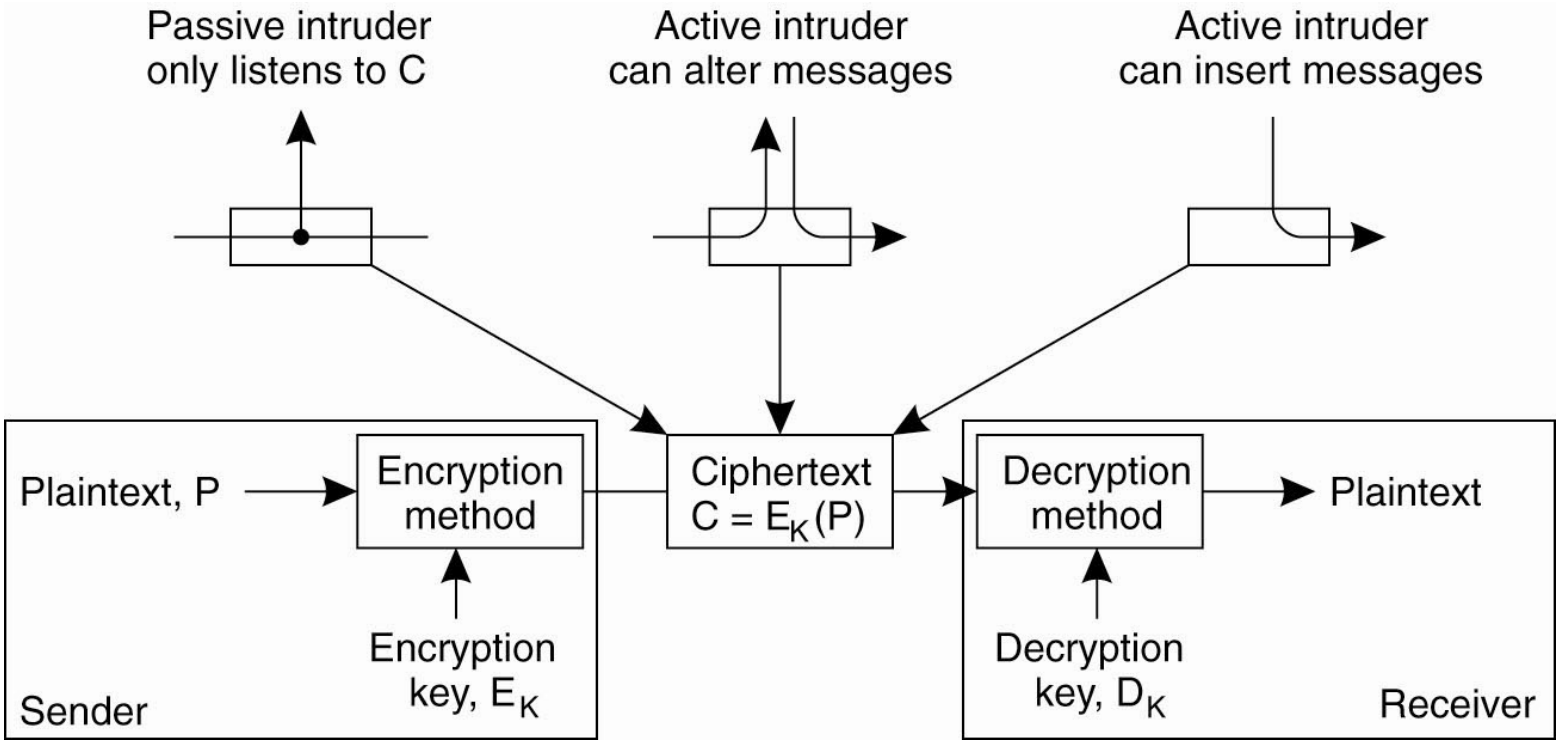
System and Network Threats (Cont.)

- **Denial of Service**
  - Overload the targeted computer preventing it from doing any useful work
  - **Distributed Denial-of-Service** (**DDoS**) come from multiple sites at once
  - Consider the TCP-connection handshake
    - How many connections can the OS handle?
  - Consider traffic to a web site
    - How can you tell the difference between being a target and being really popular?
- **Port scanning**
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
  - Detection of running services in order to identify vulnerabilities
  - Detection of OS and version running on system

Cryptography

- Goal: keep information from those who aren't supposed to see it
  - Do this by encrypting the data
  - Encryption constrains the set of possible receivers of a message
  - Algorithms have two inputs: data and key(s)
  - Some keys must be kept secret
- A good encryption algorithm should never depend on the secrecy of its implementation (assume attackers know the details of the algorithm), only the keys are secret

Basics of Cryptography



- plaintext: unencrypted message
- ciphertext: encrypted form of message