OPERATING SYSTEMS

Input - Output Management and Security - 6

Nitin V Pujari
Faculty, Computer Science
Dean - IQAC, PES University

OPERATING SYSTEMS

The Security Problem

Nitin V Pujari
Faculty, Computer Science
Dean - IQAC, PES University

OPERATING SYSTEMS

Course Syllabus - Unit 5

10 Hours

Unit-5:Unit 5: IO Management and Security

I/O Hardware, polling and interrupts, DMA, Kernel I/O Subsystem and Transforming I/O Requests to Hardware Operations - Device interaction, device driver, buffering System Protection: Goals, Principles and Domain of Protection, Access Matrix, Access control, Access rights. System Security: The Security Problem,Program Threats, System Threats and Network Threats. Case Study: Windows 7/Windows 10

OPERATING SYSTEMS

Course Outline

47	I/O Hardware, polling and interrupts	13.1,13.2
48	DMA	13.2.3
49	Transforming I/O Requests to Hardware Operations, Device interaction, device driver, buffering.	13.5
50	Goals, Principles and Domain of Protection	14.1-14.3
51	Access Matrix	14.4
52	Access control, Access rights	14.5-14.7
53	The Security Problem	15.1
54	Program Threats	15.2
55	System Threats and Network Threats	15.3
56	Case Study : Windows File System	17.5

- The Security Problem

The Security Problem

- **Protection**, as discussed earlier is strictly an internal problem deals with answering the question
  - How do we provide controlled access to programs and data stored in a computer system ?

The Security Problem

- **Security**, requires not only an adequate protection system but also consideration of the external environment within which the system operates.
    - A protection system is ineffective if user authentication is **compromised** or a program is run by an unauthorized user.
- Computer resources must be guarded against unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency.
- These resources include information stored in the system (both data and code), as well as the CPU , memory, disks, tapes, and networking that are the computer.

The Security Problem

- Large commercial systems containing payroll or other financial data are inviting targets to thieves.
- Systems that contain data pertaining to corporate operations may be of interest to unscrupulous competitors.
- Furthermore, loss of such data, whether by accident or fraud, can seriously impair the ability of the corporation to function.
- One can say that a system is **Secure** if its resources are used and accessed as intended under all circumstances.

The Security Problem

- Total security cannot be achieved.
- Mechanisms to make security breaches a rare occurrence, rather than the norm.
- Security violations or misuse of the system can be categorized as **intentional** or **malicious** or **accidental**.
- Protection mechanisms are the core of protection from accidents.

The Security Problem

- Several forms of accidental and malicious security violations

- **Intruder** and **Cracker** for those attempting to breach security.

- A **Threat** is the potential for a security violation, such as the discovery of a vulnerability

- An **Attack** is the attempt to break security

Accidental and Malicious Security Violations

- **Breach of Confidentiality:**
  - This type of violation involves unauthorized reading of data (or theft of information).
  - Typically, a breach of confidentiality is the goal of an intruder. Capturing secret data from a system or a data stream, such as credit-card information or identity information for identity theft, can result directly in money for the intruder.

Accidental and Malicious Security Violations

- **Breach of integrity:**
  - This violation involves unauthorized modification of data.
  - Such attacks can, for example, result in passing of liability to an innocent party or modification of the source code of an important commercial application.

Accidental and Malicious Security Violations

- **Breach of availability:**
  - This violation involves unauthorized destruction of data.
  - Some crackers would rather wreak havoc and gain status or bragging rights than gain financially.
  - Website defacement is a common example of this type of security breach

Accidental and Malicious Security Violations

- **Theft of service:**
  - This violation involves unauthorized use of resources.
  - For example, an intruder (or intrusion program) may install a daemon on a system that acts as a file server

Accidental and Malicious Security Violations

- **Denial of service:**
  - This violation involves preventing legitimate use of the system.
  - Denial-of-service (DOS) attacks are sometimes accidental.
  - The original Internet worm turned into a DOS attack when a bug failed to delay its rapid spread.

The Security Problem

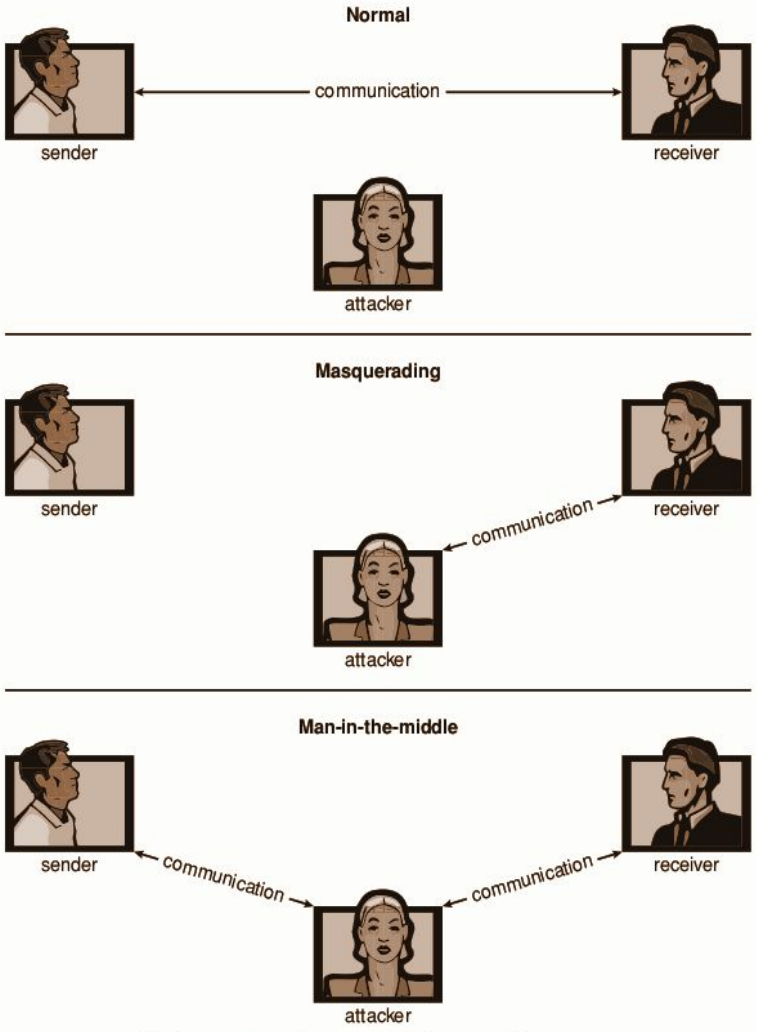
- Attackers use several standard methods in their attempts to breach security.

- **Masquerading:**

  - Here one participant in a communication pretends to be someone else another host or another person.

  - By masquerading, attackers breach authentication, the correctness of identification

  - They can then gain access that they would not normally be allowed or escalate their privileges and obtain privileges to which they would not normally be entitled.



Standard security attacks.

The Security Problem

- Attackers use several standard methods in their attempts to breach security.

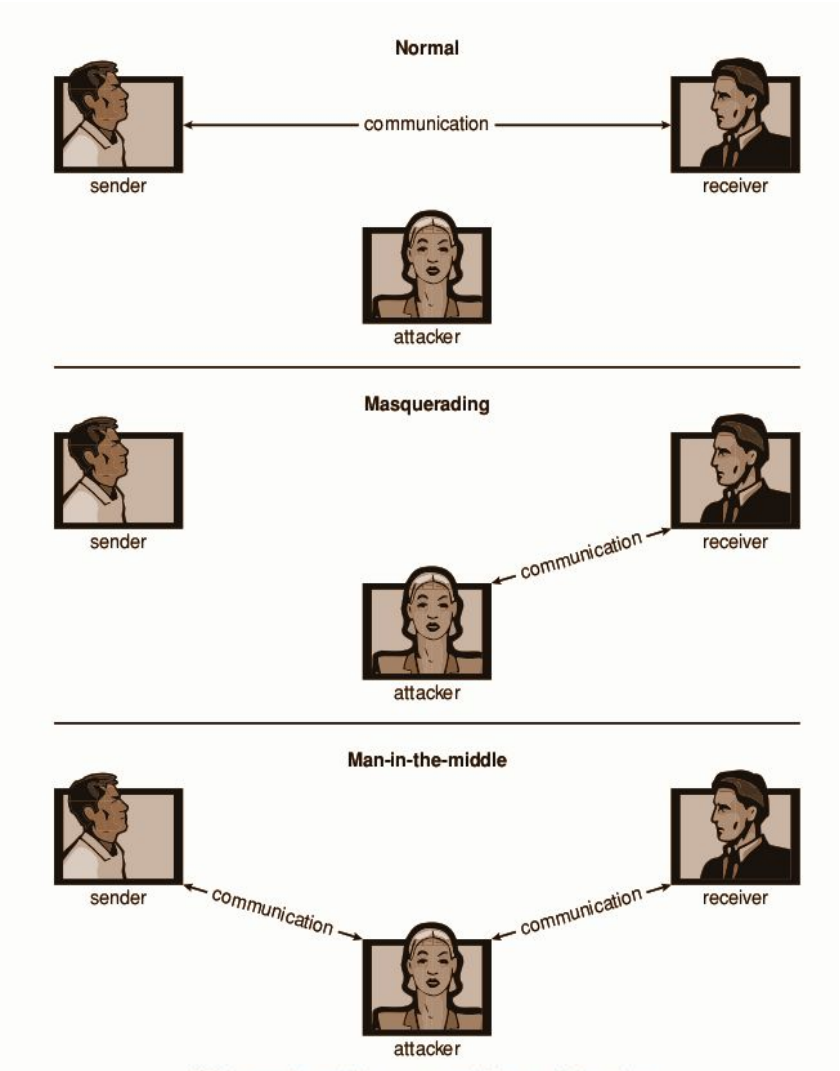
- **Replay Attack:**

  - Consists of the malicious or fraudulent repeat of a valid data transmission.

  - Sometimes the replay comprises the entire attack

  - As an example, in a repeat of a request to transfer money.

  - But frequently it is done along with message modification, again to escalate privileges.



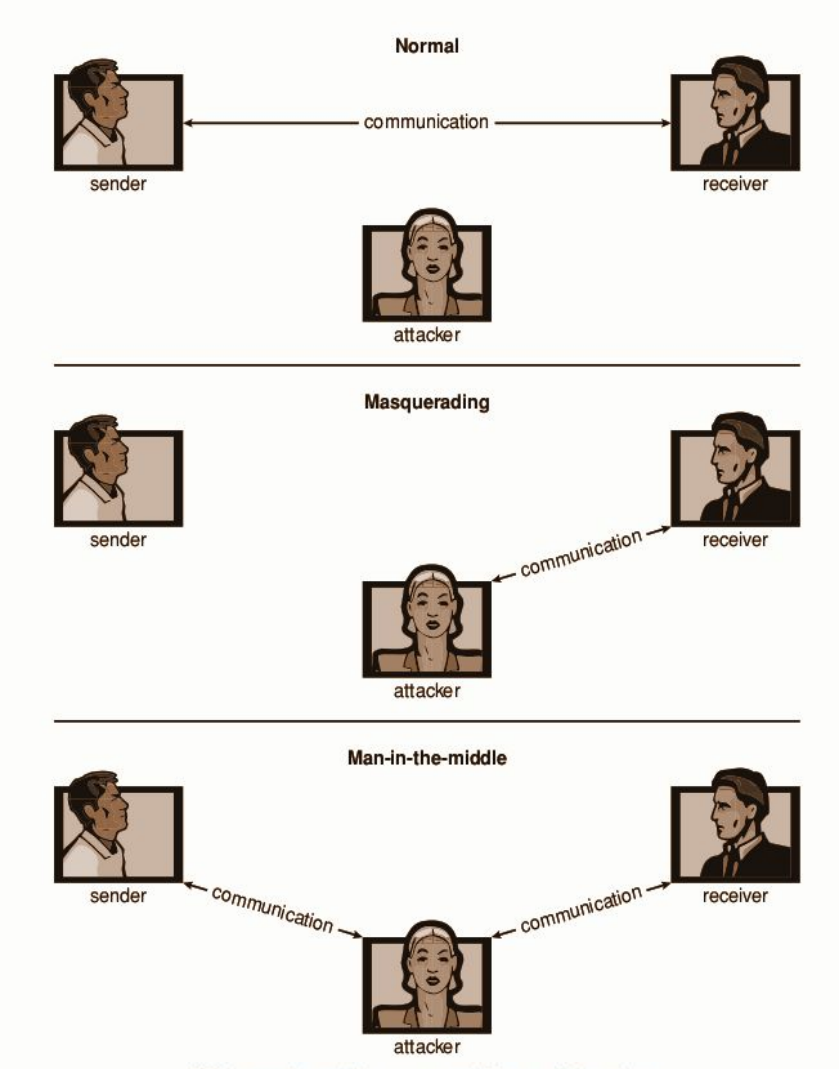
Standard security attacks.

The Security Problem

- Attackers use several standard methods in their attempts to breach security.

- **Man-in-the-middle attack:**

  - An attacker sits in the data flow of a communication, masquerading as the sender to the receiver, and vice versa.

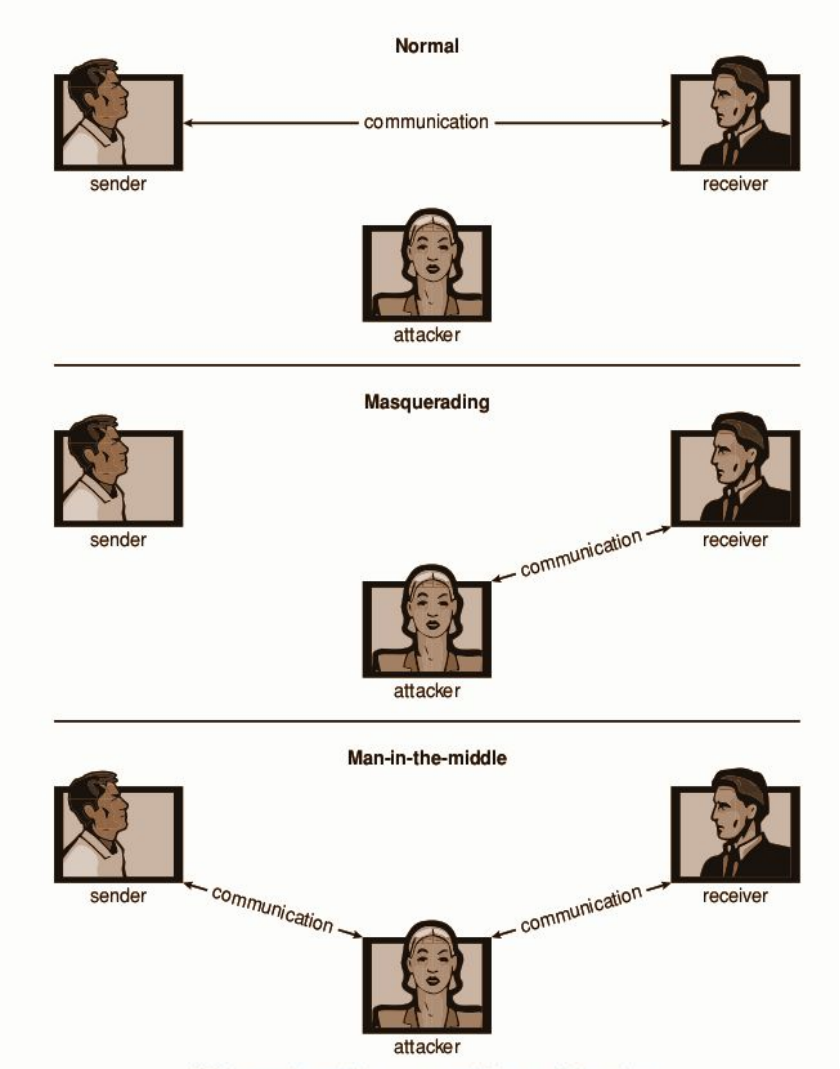


Standard security attacks.

The Security Problem

- Attackers use several standard methods in their attempts to breach security.

- **Session Hijacking:**
  - An active communication session is intercepted.



Standard security attacks.

The Security Problem

- To protect a system, one must take security measures at four levels

1. Physical:

- The site or sites containing the computer systems must be physically secured against armed or surreptitious entry by intruders.

- Both the machine rooms and the terminals or workstations that have access to the machines must be secured.

The Security Problem

- To protect a system, one must take security measures at four levels

2. Human:

- Authorization must be done carefully to assure that only appropriate users have access to the system.
- Even authorized users, however, may be “encouraged” to let others use their access (in exchange for a bribe, for example).
- They may also be tricked into allowing access via social engineering.

The Security Problem

- To protect a system, one must take security measures at four levels

2. Human:

- One type of social-engineering attack is **Phishing**.
- Here, a legitimate-looking email or web page misleads a user into entering confidential information.
- Another technique is dumpster diving, a general term for attempting to gather information in order to gain unauthorized access to the computer by looking through trash, finding phone books, or finding notes containing passwords, as an example.
- These security problems are management and personnel issues, not problems pertaining to operating systems.

The Security Problem

- To protect a system, one must take security measures at four levels

3. Operating system:

- The system must protect itself from accidental or purposeful security breaches.
- A runaway process could constitute an accidental denial-of-service attack.
- A query to a service could reveal passwords.
- A stack overflow could allow the launching of an unauthorized process.
- The list of possible breaches is almost endless.

The Security Problem

- To protect a system, one must take security measures at four levels

4. Network:

- Much computer data in modern systems travels over private leased lines, shared lines like the Internet, wireless connections, or dial-up lines.

- Intercepting these data could be just as harmful as breaking into a computer, and interruption of communications could constitute a remote denial-of-service attack, diminishing users' use of and trust in the system

The Security Problem

- Security at the first two levels must be maintained if Operating System security is to be ensured.
- A weakness at a high level of security (physical or human) allows circumvention of strict low-level (operating-system) security measures
- A chain is only as strong as its weakest link is especially true of system security.
- All of these aspects must be addressed for security to be maintained.
- Without the ability to authorize users and processes, to control their access, and to log their activities, it would be impossible for an operating system to implement security measures or to run securely
- Hardware protection features are needed to support an overall protection scheme.

The Security Problem

- Security within the operating system and between operating systems is implemented in several ways, ranging from passwords for authentication through guarding against viruses to detecting intrusions.

- The Security Problem

THANK YOU

Nitin V Pujari
Faculty, Computer Science
Dean - IQAC, PES University

nitin.pujari@pes.edu

For Course Deliverables by the Anchor Faculty click on www.pesuacademy.com