RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF ENGINEERING & TECHNOLOGY

BCS-501 Operating System

Lecturer-39

Manisha Verma
Assistant Professor
Computer Science & Engineering

Security

- Security:-The Security Problem
- Program Threats
- Security Violation Categories
- Security Measure Levels

Security

- To discuss security threats and attacks
- To explain the fundamentals of encryption, authentication, and hashing
- To examine the uses of cryptography in computing
- To describe the various countermeasures to security attacks

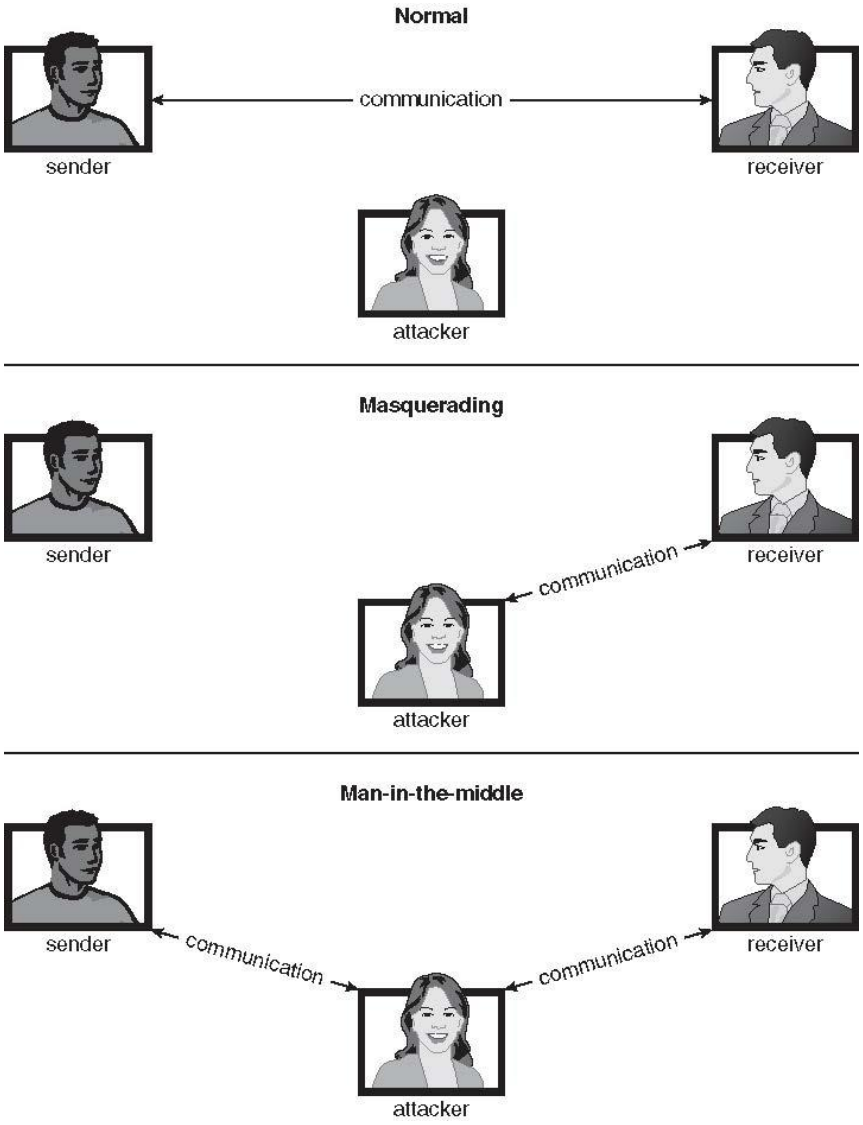
The Security Problem

- System secure if resources used and accessed as intended under all circumstances
- Unachievable
- Intruders (crackers) attempt to breach security
- Threat is potential security violation
- Attack is attempt to breach security
- Attack can be accidental or malicious
- Easier to protect against accidental than malicious misuse

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
- Masquerading (breach authentication)
  - Pretending to be an authorized user to escalate privileges
- Replay attack
  - As is or with message modification
- Man-in-the-middle attack
  - Intruder sits in data flow, masquerading as sender to receiver and vice versa
- Session hijacking
  - Intercept an already-established session to bypass authentication

Standard Security Attacks



Security Measure Levels

- Impossible to have absolute security, but make cost to perpetrator sufficiently high to deter most intruders

- Security must occur at four levels to be effective:
  - Physical
    - Data centers, servers, connected terminals
  - Human
    - Avoid social engineering, phishing, dumpster diving
  - Operating System
    - Protection mechanisms, debugging
  - Network
    - Intercepted communications, interruption, DOS

- Security is as weak as the weakest link in the chain
- But can too much security be a problem?

Program Threats

•Many variations, many names

•Trojan Horse
- ➢Code segment that misuses its environment
- ➢Exploits mechanisms for allowing programs written by users to be executed by other users
- ➢Spyware, pop-up browser windows, covert channels
- ➢Up to 80% of spam delivered by spyware-infected systems

•Trap Door
- ➢Specific user identifier or password that circumvents normal security procedures
- ➢Could be included in a compiler
- ➢How to detect them?

Logic Bomb
- ➢Program that initiates a security incident under certain circumstances

Stack and Buffer Overflow
- ➢Exploits a bug in a program (overflow either the stack or memory buffers)
- ➢Failure to check bounds on inputs, arguments
- ➢Write past arguments on the stack into the return address on stack
- ➢When routine returns from call, returns to hacked address
  - ➢Pointed to code loaded onto stack that executes malicious code
- ➢Unauthorized user or privilege escalation

MCQ

Which of the following are forms of malicious attack ?
A. Theft of information
B. Modification of data
C. Wiping of information
D. All of the mentioned

What are common security threats ?
A. File Shredding
B. File sharing and permission
C. File corrupting
D. File integrity

From the following, which is not a common file permission ?
A. Write
B. Execute
C. Stop
D. Read

Which of the following is least secure method of authentication ?
A. Key card
B. fingerprint
C. retina pattern
D. Password

Which of the following is a strong password ?
A. 19thAugust88
B. Delhi88
C. P@assw0rd
D. !augustdelhi