CS343 - Operating Systems

Module-8B

System Security and Threat Categories

Dr. John Jose

Assistant Professor

Department of Computer Science & Engineering

Indian Institute of Technology Guwahati, Assam.

http://www.iitg.ac.in/johnjose/

Objectives

- 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

Overview

- The Security Problem
- Program Threats
- System and Network Threats

The Security Problem

- Protection is strictly an internal problem →provide controlled access to programs and data stored in a computer
- A protection system is ineffective if user authentication is compromised or a program is run by an unauthorized user.
- System is **secure** if resources used and accessed as intended under all circumstances
- **Threat** is the potential for security violation
- **Attack** is attempt to break security
- **Intruders** (**crackers**) attempt to breach security
- Security violations can be accidental or malicious (intentional)
- Easier to protect against accidental than malicious misuse

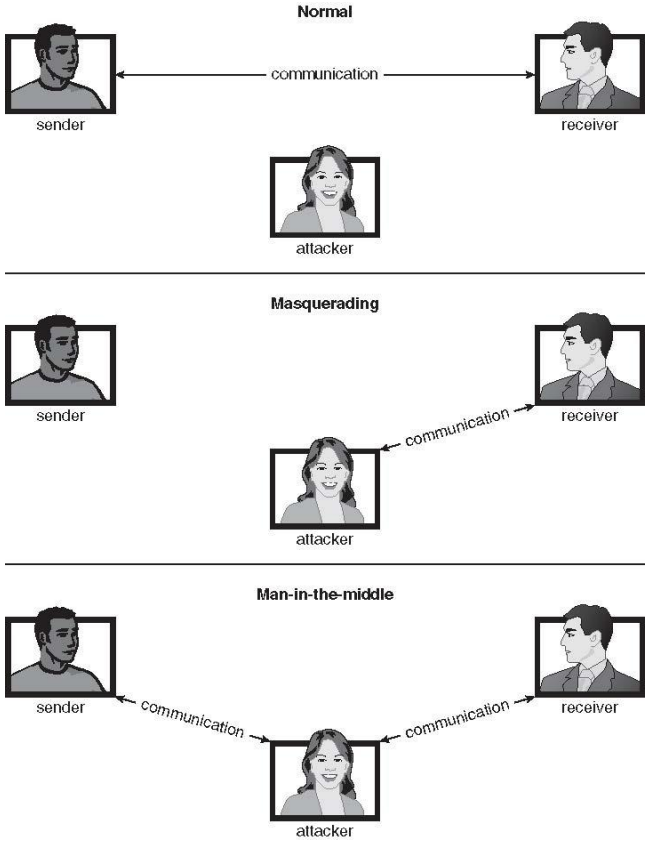
Security Violation Categories

- **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

Security Violation Methods

- **Masquerading** (breach **authentication**)
  - Pretending to be an authorized user to escalate privileges
- **Replay attack**
  - Fraudulent repeat of a valid data transmission.
- **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

- 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

- **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

Program Threats

- **Logic Bomb**
  - Program that initiates a security incident under certain circumstances
- **Stack** and **Buffer Overflow**
  - Exploits a bug in a program (overflow in 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

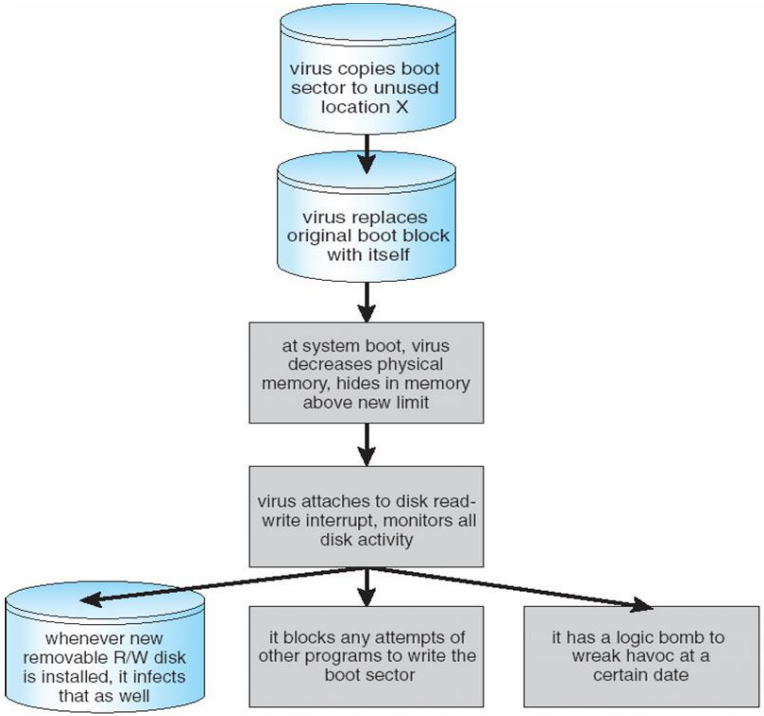
Program Threats

- **Viruses**
  - Code fragment embedded in legitimate program
  - Self-replicating, designed to infect other computers
  - Very specific to CPU architecture, operating system, applications
  - Usually borne via email or as a macro
  - **Virus dropper** inserts virus onto the system

Program Threats – Virus categories

- File / parasitic
- Boot / memory
- Macro
- Source code
- Polymorphic
- Encrypted
- Stealth
- Tunneling
- Multipartite
- Armored

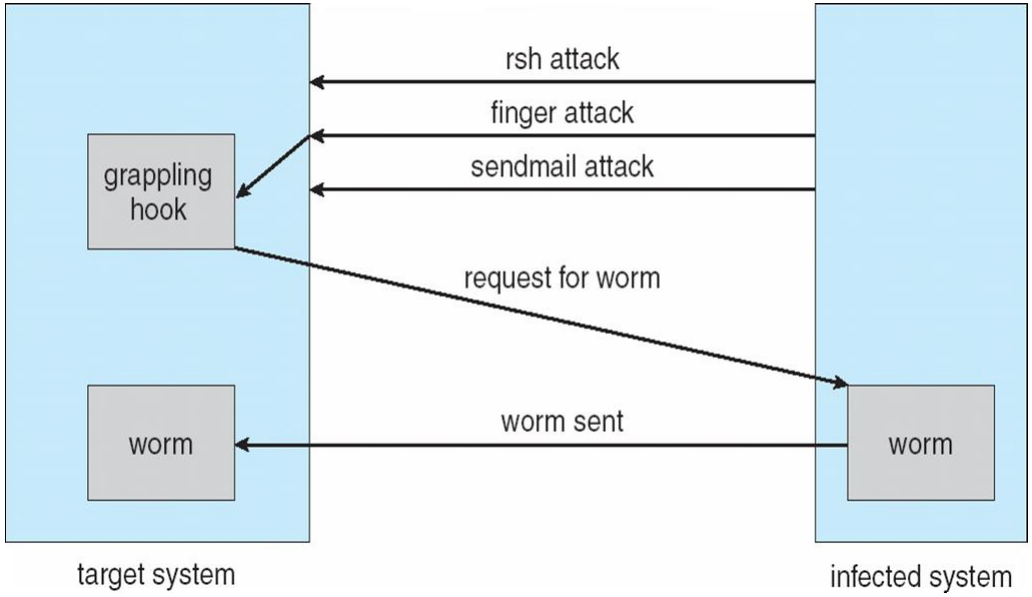
A Boot-sector Computer Virus



System and Network Threats

- **Worms** – use **spawn** mechanism; standalone program
- Internet worm (Morris worm)
  - Exploited UNIX networking features (remote access) and bugs in *finger* and *sendmail* programs
  - Exploited trust-relationship mechanism used by *rsh* to access friendly systems without use of password
  - **Grappling hook (bootstrap/ vector)** program uploaded main worm program – few lines of C code
  - Hooked system then uploaded main code, tried to attack connected systems
  - Also tried to break into other users accounts on local system via password guessing / rsh

The Morris Internet Worm



System and Network Threats

- **Port scanning**
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
  - Detection of answering service protocol
  - Detection of OS and version running on system
  - Frequently launched from **zombie systems** to decrease trace-ability

System and Network Threats

- **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 start of the IP-connection handshake (SYN)
    - How many started-connections can the OS handle?
  - Consider traffic to a web site - being a target and being really popular?

johnjose@iitg.ac.in
http://www.iitg.ac.in/johnjose/