Outline

- Information Protection
  - Security
- Q&A
Security [Silberschatz06]

- Introduction
  - Security
    - System protection
      - Controlled access to programs & data in a computer system
    - Protection environment
      - External environment for protection
  - Violation (or Misuse)
    - Intentional vs accidental
    - Threat (potential) vs attack (attempt)
Security (Cont’d)

Violation Types

- 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)
  - Preventing legitimate use of the system

Prevention vs Detection & Fix
Security (Cont’d)

- **Attack Methods**
  - **Masquerading**
    - Pretending to be another host or person in a communication for the breach of authentication
  - **Replay**
    - Malicious & fraudulent repeat of a valid data transmission frequently with message modification
  - **Man-in-the-Middle**
    - Masquerading as the sender to the receiver & vice versa, possibly preceded by a session hijacking (interception)
Security (Cont’d)

- **System Protection Levels**
  - **Physical**
    - Secured physical access to machines
  - **Human**
    - Authorized users
  - **Operating System**
    - Protection from security breaches
      - Runaway process constituting a DOS attack
      - Query to a service revealing passwords
      - Stack overflow possibly launching an unauthorized process
  - **Network**
    - Protection from intercepting transmitted data
    - Protection from interruption of communications
Security (Cont’d)

Program Threats

- Definition of a Trojan Horse
  - Code segment that misuses its environment

- Types of a Trojan Horse
  - Being slipped into the user’s path & executed
  - Emulating a login program
  - Spyware
    - Downloading ads to display on the user’s system
    - Creating pop-up browser windows when certain sites are visited
    - Capturing information & returning it to a central site (covert channels)

Violation of the Principle of Least Privilege: Human Error (w/ More Privileges) & Poor Design of OS (Allowing More Privileges)
Security (Cont’d)

- **Program Threats**
  - **Definition of Trap Door**
    - Hole in software that only the designer can use
  - **Example of Trap Door**
    - Circumvention of normal security procedures for a specific user ID & password
  - **Generator of Trap Door**
    - Designer vs Compiler
  - **Definition of Logic Bomb**
    - Creation of a security hole only under certain circumstances
Security (Cont’d)

- Program Threats
  - Goals of Stack & Buffer Overflow
    - To gain unauthorized access to the target system
    - To escalate privileges
  - Essence of Stack & Buffer Overflow
    - Exploiting a (no bounds checking) program bug
      - Writing into a daemon’s stack via overflowing an input field, command-line argument, or input buffer
      - Overwriting the current return address with the address of the exploit code
      - Writing a simple set of code for the next space in the stack: e.g., code for spawning a shell
Illustration: Stack & Buffer Overflow

Before

- Return address
- Saved frame pointer
- buffer(BUFFER_SIZE-1)
- ...
- buffer(1)
- buffer(0)

After

Address of modified shell code

- ... NO_OP ...

Modified shell code

Copied
Security (Cont’d)

Program Threats

- Definition of Viruses
  - Fragment of code embedded in a legitimate program
    - Self-replicating

- Characteristic of Viruses
  - Particular problem for Windows PC users
    - Protection of executables from writing by UNIX & other multiuser OS’s

- Common Forms of Virus Transmission
  - Email
  - Download of viral programs
  - Macros (or Visual Basic Programs) in MS documents

Works via a Virus Dropper, Usually a Trojan Horse
Security (Cont’d)

Program Threats

- Categories of Viruses
  - File
  - Boot
  - Macro
  - Source code
  - Polymorphic
    - Changing the virus’s signature each installation time
  - Encrypted
  - Stealth
  - Tunneling
    - Bypassing detection
  - Multipartite
  - Armored
Security (Cont’d)

- System & Network Threats

  - Characteristics of System & Network Threats
    - Abuse of services & network connections

  - Definition of Worms
    - Processes that use the spawn mechanism ravaging system performance

  - Definition of Port Scanning
    - Means to detect a system’s vulnerabilities

  - Denial of Service
    - Means to disrupt legitimate use of a system

  - Categories of Denial of Service
    - Using many facility resources
    - Disrupting the network of the facility

In Contrast to Program Threats Typically Using a Breakdown in System Protection Mechanisms
Reference