Information Systems and Network Security

Chapter 09

- Threats and attacks
- Classification of Threats and attacks

-Sanket Mohan Pandhare

Vulnerabilities, Threats, and Controls

- Understanding Vulnerabilities, Threats, and Controls
  - Vulnerability = a weakness in a security system
  - Threat = circumstances that have a *potential* to cause harm
  - Controls = means and ways to block a threat, which tries to exploit one or more vulnerabilities
- Example - New Orleans disaster (Hurricane Katrina)
  - Q: What were city vvulnerabilities, threats, and controls?
  - A: Vulnerabilities: location below water level, geographical location in hurricane area

    Threats: hurricane, dam damage, terrorist attack

    Controls: dams and other civil infrastructures, emergency response plan

- Attack (materialization of a vulnerability/threat)
  - = exploitation of one or more vulnerabilities by a threat; tries to defeat controls
    - Attack may be:
      - *Successful* (a.k.a. an *exploit*)
        - resulting in a breach of security, a system penetration, etc.
      - *Unsuccessful*
        - when controls block a threat trying to exploit a vulnerability

The Security Problem

- System is **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 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

A) Hardware Level of Threats

- Add / remove a h/w device
  - Ex: Snooping, wiretapping

    Snoop = to look around a place secretly in order to discover things about it or the people connected with it. [Cambridge Dictionary of American English]
  - Ex: Modification, alteration of a system
- Physical attacks on h/w => need physical security: locks and guards
  - Accidental (dropped PC box) or voluntary (bombing a computer room)
  - Theft / destruction
    - Damage the machine (spilled coffe, mice, *real* bugs)
    - Steal the machine
    - “Machinicide:” Axe / hammer the machine

B) Software Level of Threats

- Software Deletion
  - Easy to delete needed software by mistake
  - To prevent this: use *configuration management software*
- Software Modification
  - Trojan Horses, Viruses, Logic Bombs, Trapdoors, Information
- Software Theft
  - Unauthorized copying

C) Data Level of Threats

- How valuable is your data?
  - Credit card info vs. your home phone number
  - Source code
- Adequate protection
  - Cryptography
    - Good if intractable for a long time

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

Program Threats (Cont.)

- **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)
  - Unauthorized user or privilege escalation
  - Buffer Overflow - An application error that occurs when more data is sent to a buffer than it can handle. When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

Program Threats (Cont.)

- 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

The Threat Continues

- Attacks still common, still occurring
- Attacks moved over time from science experiments to tools of organized crime
  - Targeting specific companies
  - Creating botnets to use as tool for spam and DDoS delivery
  - **Keystroke logger** to grab passwords, credit card numbers
- Why is Windows the target for most attacks?
  - Most commonly used
  - Everyone is an administrator
    - Licensing required?
  - **Patches/Updates**

System and Network Threats

- Some systems “open” rather than **secure by default**
  - Reduce **attack surface**
  - But harder to use, more knowledge needed to administer
- Network threats harder to detect, prevent
  - Protection systems weaker
  - No physical limits once system attached to internet
    - Or on network with system attached to internet
  - Even determining location of connecting system difficult
    - IP address is only knowledge

System and Network Threats (Cont.)

- **Worms** – use spawn mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs multiple programs.
  - Exploited trust-relationship mechanism used by *rsh* to access friendly systems without use of password

System and Network Threats (Cont.)

- **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
  - `nmap` scans all ports in a given IP range for a response
  - `nessus` has a database of protocols and bugs (and exploits) to apply against a system

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 start of the IP-connection handshake (SYN)
    - How many started-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?
  - Purposeful – extortion, punishment

Attacks

- Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by threat agent that damages or steals organization’s information.
- An exploit is a technique to compromise a system.
- Vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective.
- An attack is then the use of an exploit to achieve the compromise of a controlled system.

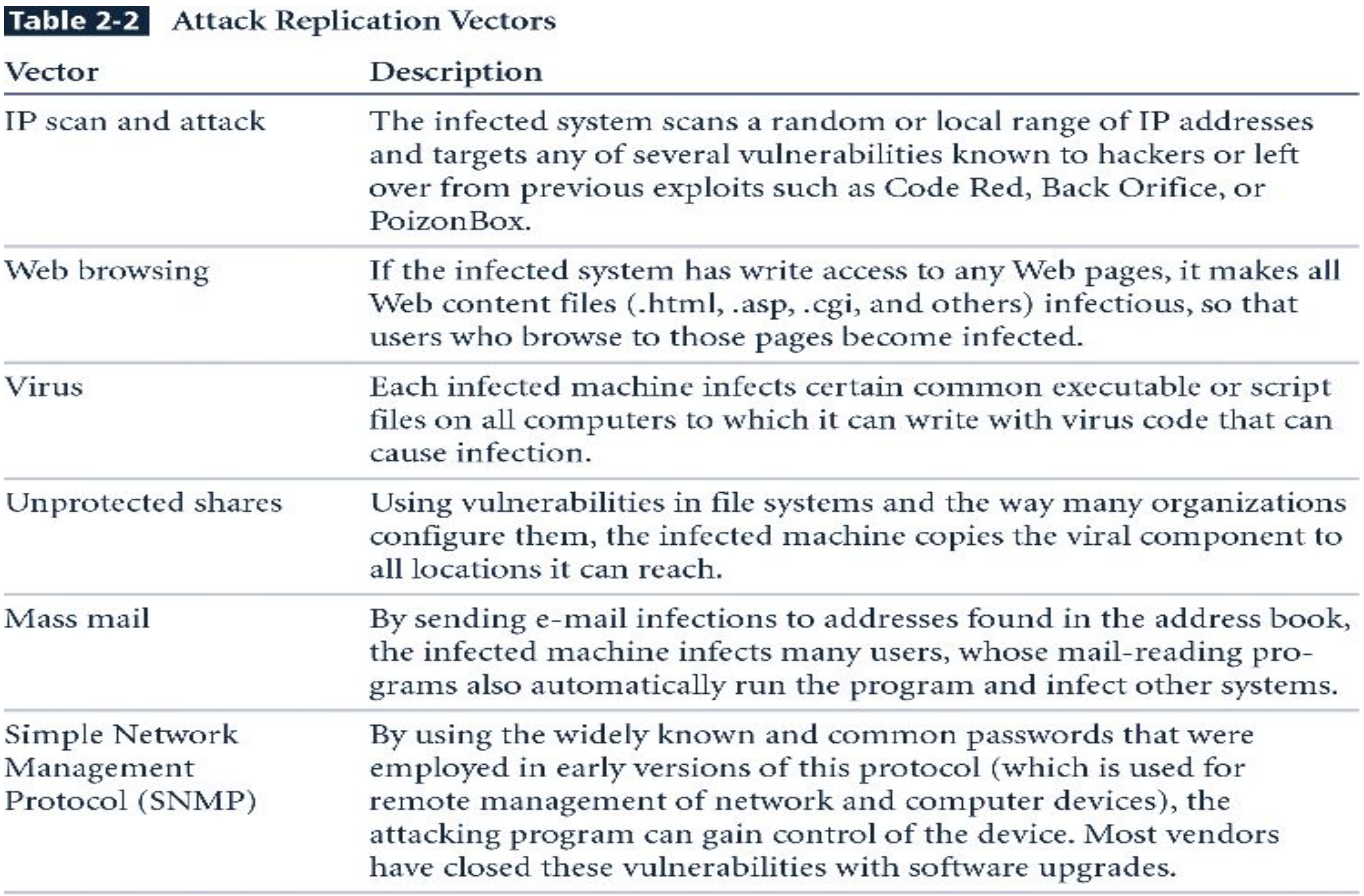

Table 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox.
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected.
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
Unprotected shares	Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to addresses found in the address book, the infected machine infects many users, whose mail-reading programs also automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	By using the widely known and common passwords that were employed in early versions of this protocol (which is used for remote management of network and computer devices), the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Attacks (continued)

- Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information
- Hoaxes: transmission of a virus hoax with a real virus attached; more devious form of attack
- Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism

Attacks (continued)

- Password crack: attempting to reverse calculate a password
- Brute force: trying every possible combination of options of a password
- Dictionary: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses

Attacks (continued)

- Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
  - Target system cannot handle successfully along with other, legitimate service requests
  - May result in system crash or inability to perform ordinary functions
- Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously

Attacks (continued)

- Spoofing: technique used to gain unauthorized access; intruder assumes a trusted IP address

- Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network

- Spam: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks

Attacks (continued)

- Mail bombing: also a DoS; attacker routes large quantities of e-mail to target
- Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
- Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker

Attacks (continued)

- “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” — Kevin Mitnick

- (Spear) Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity

Attacks (continued)

- Pharming: redirection of legitimate Web traffic (e.g., browser requests) to illegitimate site for the purpose of obtaining private information

- Timing attack: relatively new; works by exploring contents of a Web browser’s cache to create malicious cookie

Summary

- Unlike any other aspect of IT, information security's primary mission to ensure things stay the way they are
- Information security performs four important functions:
  - Protects organization's ability to function
  - Enables safe operation of applications implemented on organization's IT systems
  - Protects data the organization collects and uses
  - Safeguards the technology assets in use at the organization

Summary (continued)

- Threat: object, person, or other entity representing a constant danger to an asset
- Management effectively protects its information through policy, education, training, and technology controls
- Attack: a deliberate act that exploits vulnerability
- Secure systems require secure software