Computer and Network Security

Computer Security Attacks
Viruses and Malware

Introduction

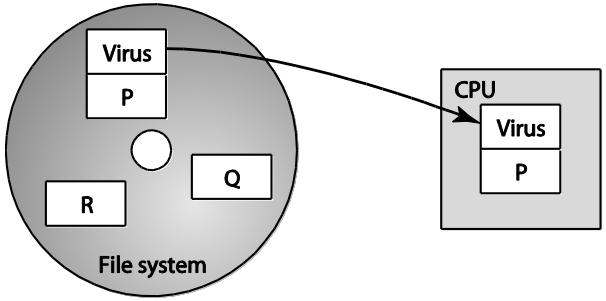
- Computers getting faster and less expensive
- Utility of networked computers increasing
  - Shopping and banking
  - Managing personal information
  - Controlling industrial processes
- Increasing use of computers $\rightarrow$ growing importance of computer security

Malware

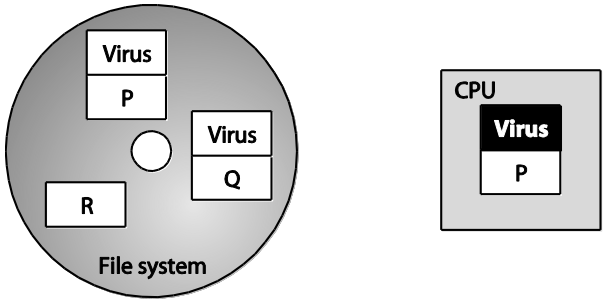
Viruses

- Virus: Piece of self-replicating code embedded within another program (host)
- Viruses associated with program files
  - Hard disks, floppy disks, CD-ROMS
  - Email attachments
- How viruses spread
  - Diskettes or CDs
  - Email
  - Files downloaded from Internet

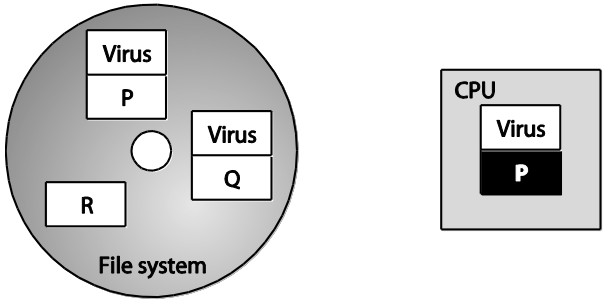
How a Virus Replicates



(a)

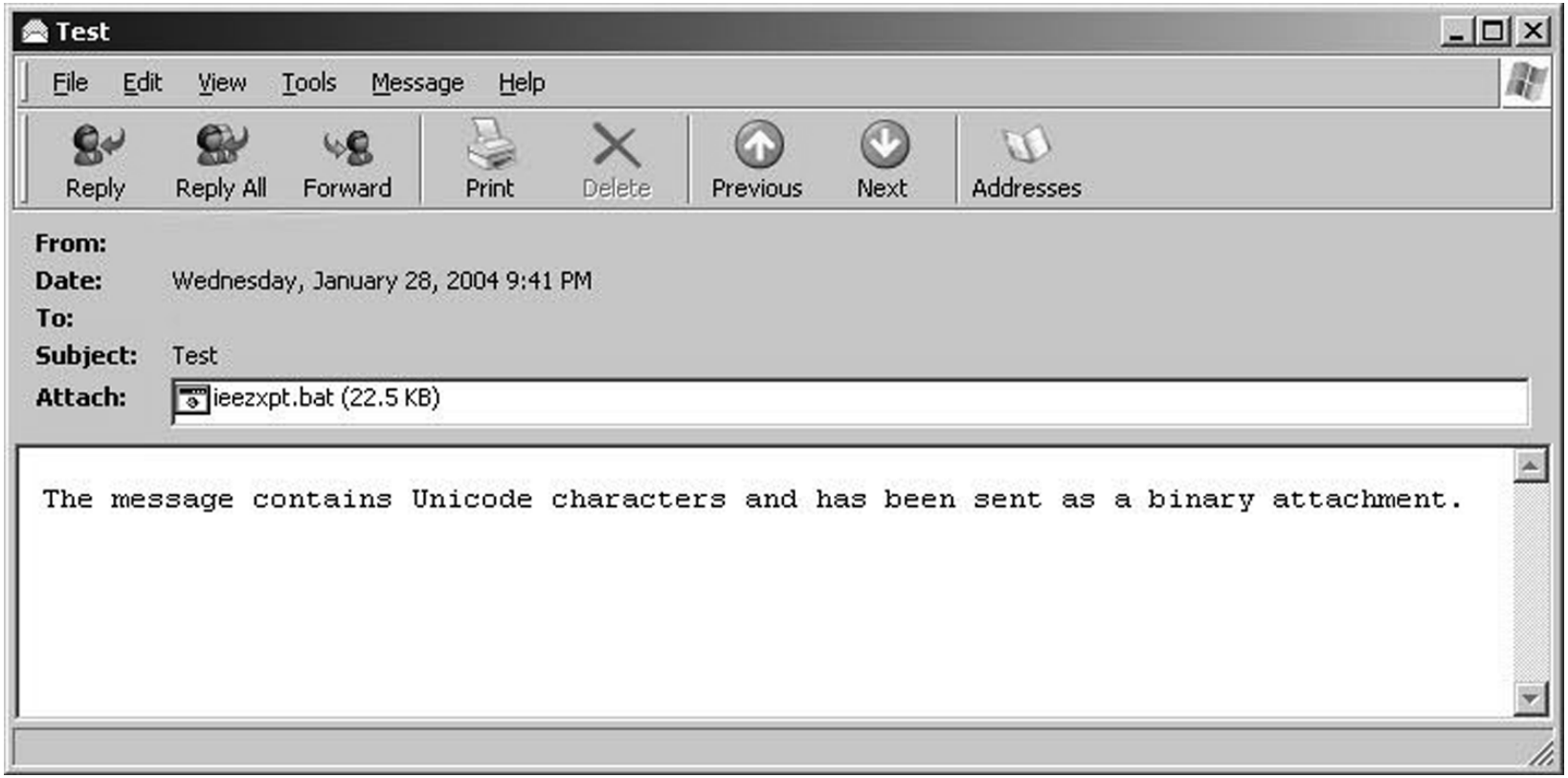


(b)

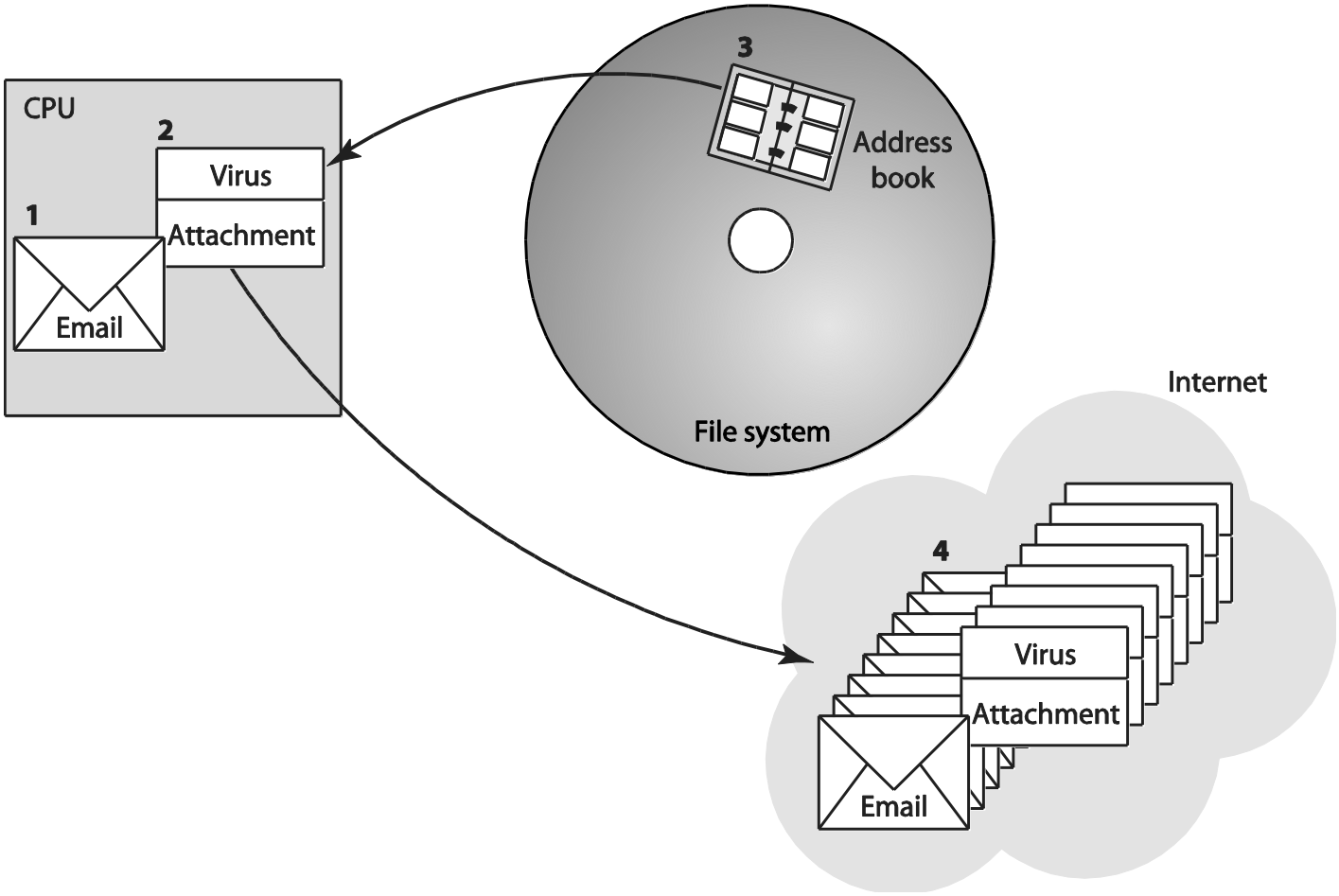


(c)

Email Attachment with Possible Virus



How an Email Virus Spreads



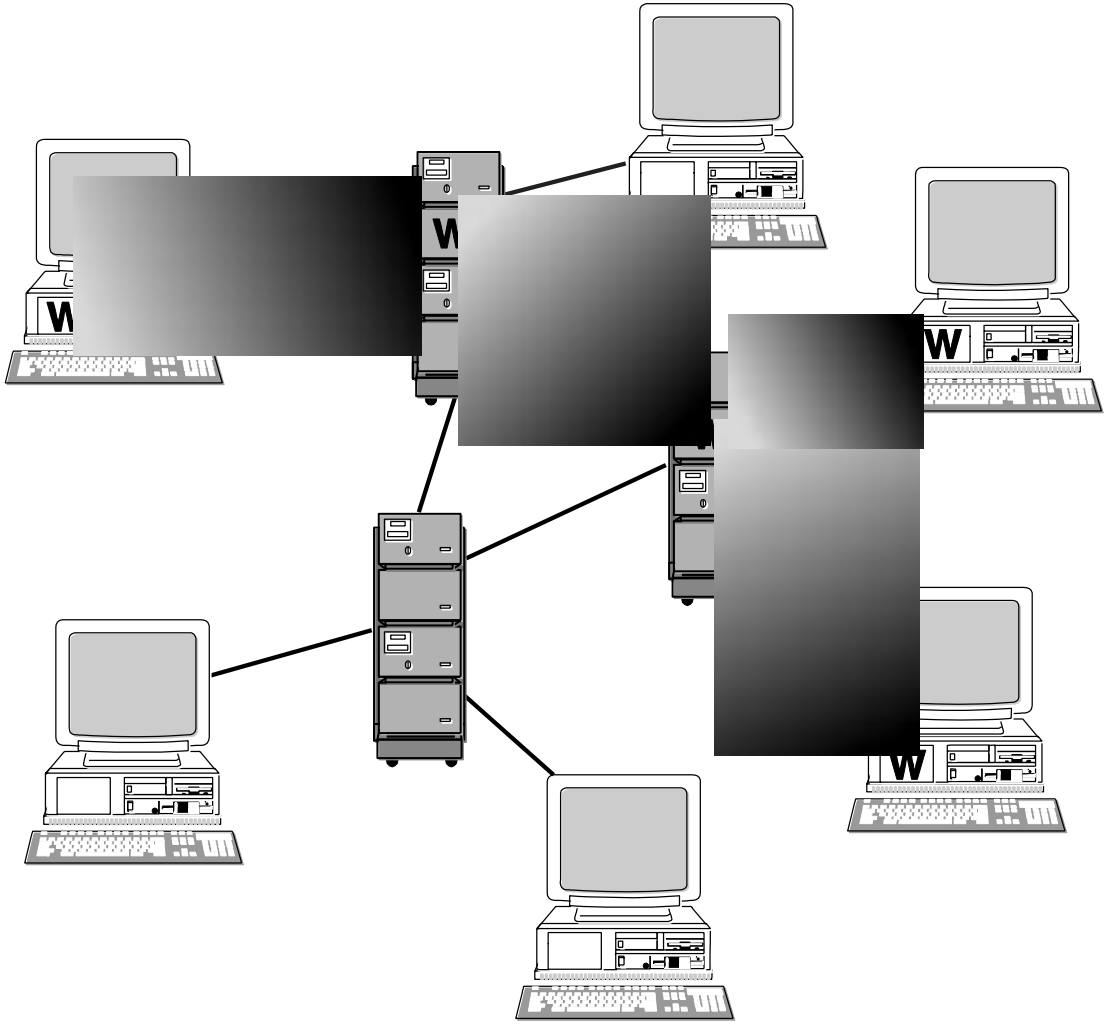
Antivirus Software Packages

- Allow computer users to detect and destroy viruses
- Must be kept up-to-date to be most effective
- Many people do not keep their antivirus software packages up-to-date
- Consumers need to beware of fake antivirus applications

Worm

- Self-contained program
- Spreads through a computer network
- Exploits security holes in networked computers

How a Worm Spreads



The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - Released worm onto Internet from MIT computer
- Effect of worm
  - Spread to significant numbers of Unix computers
  - Infected computers kept crashing or became unresponsive
  - Took a day for fixes to be published
- Impact on Morris
  - Suspended from Cornell
  - 3 years' probation + 400 hours community service
  - $150,000 in legal fees and fines

Ethical Evaluation

- Kantian evaluation
  - Morris used others by gaining access to their computers without permission
- Social contract theory evaluation
  - Morris violated property rights of organizations
- Utilitarian evaluation
  - Benefits: Organizations learned of security flaws
  - Harms: Time spent by those fighting worm, unavailable computers, disrupted network traffic, Morris's punishments
- Morris was wrong to have released the Internet worm

Cross-site Scripting

- Another way malware may be downloaded without user's knowledge
- Problem appears on Web sites that allow people to read what others have posted
- Attacker injects client-side script into a Web site
- Victim's browser executes script, which may steal cookies, track user's activity, or perform another malicious action

Drive-by Downloads

- Unintentional downloading of malware caused by visiting a compromised Web site
- Also happens when Web surfer sees pop-up window asking permission to download software and clicks “Okay”
- Google Anti-Malware Team says 1.3 percent of queries to Google’s search engine return a malicious URL somewhere on results page

Trojan Horses and Backdoor Trojans

- Trojan horse: Program with benign capability that masks a sinister purpose
- Backdoor Trojan: Trojan horse that gives attack access to victim’s computer

Malware (1)

- ***Viruses***: **Self-replicating** programs that can infect other programs by modifying them to include a version of itself. Most viruses are spread through email vectors. All viruses make copies of themselves, infecting boot sectors, programs, or “data files” whenever possible.
  - *3 distinct parts: a vector, a replicator/infector, and a payload.*
  - *Vector: The way that a virus propagates.*
    - *Most popular vector in use today is via e-mail attachments. T*
    - *The second most popular delivery vector is via worms.*
  - *Replication code: Can be classified by infection condition. Infector code relies on rules or conditions to propagate itself to other files on the infected system or to other systems across a network.*
    - *Examples conditions include replicating after a predetermined number of infections, or over a given period of time, spreading on a certain date, or in response to the presence of a certain file or files. Finally,*
  - *Payload: Virus payloads can damage, destroy, or modify executable or data files.*

- ***Trojan Horses***: Trojan horses are **non-replicating** programs that perform some unwanted action while pretending to be useful. Many trojan horses activate when they are executed and at times destroy the structure of the current drive and self-destructing themselves in the process.

- ***Worms***: **Self-replicating** program that spreads onto other computers by breaking into them via network connections and unlike a virus starts itself on the remote machine without infecting other programs.

Malware (2)

- ***Binary File Virus/Worm***: File viruses infect executables (program files) and are implemented in machine code. File worms are also written in machine code, but instead of infecting other files, worms focus on spreading to other machines.
- ***Binary Stream Worm***: This type of network spreading worms never manifest themselves as files but rather travel from computer to computer just as pieces of code that exist only in memory.
  - The most well known example of this group is the Code Red series of worms that spread between IIS servers.
- ***Script File Virus and Worm***: A script virus is technically a file virus, but script viruses are written as pure text and thus easily readable for everybody.
  - Since computers cannot understand text instructions directly, the text first has to be translated from text to machine code. This procedure is called interpretation", and is performed by separate programs on the computer.
- ***Macro Virus****:* Macro viruses infect data files, including files, like documents and spreadsheets. Many "data file types" have the possibility to include instructions along with the normal content, e.g., Microsoft Word files can contain instructions that tells Word how to show a particular document

Malware (3)

- ***Blended Threats or Hybrid Threats***
  - New threat on the horizon.
  - Mainly, this type of threat is characterized by the utilization of various combinations of attack tools,
  - e.g., virus using IM communication.
    - Use a virus technique to incorporate P2P communication such as IM to propagate itself by using IM's "file send" process and having an unsuspecting user to execute the malicious code

Evolution of Malicious Software*

- **1st Generation**
  - Viruses spread via diskettes and DOS
  - Worm experimentation (Xerox)
- **2nd Generation**
  - Encrypted viruses.
  - Emergence of polymorphic-based viruses (different code, same functionality)
  - Virus toolkits
  - Emergence of cross-platform macro viruses
- **3rd Generation**
  - Emailed viruses
  - Social engineering
  - Dangerous worms
- **4th Generation**
  - New infection vectors
  - Blended attacks
  - Disable virus scanners

* Adapted from Chen/Robert 2004

Rootkits

- Rootkit: A set of programs that provides privileged access to a computer
- Activated every time computer is booted
- Uses security privileges to mask its presence

Spyware and Adware

- Spyware: Program that communicates over an Internet connection without user's knowledge or consent
  - Monitor Web surfing
  - Log keystrokes
  - Take snapshots of computer screen
  - Send reports back to host computer
- Adware: Type of spyware that displays pop-up advertisements related to user's activity
- Backdoor Trojans often used to deliver spyware and adware

Bots

- Bot: A kind of backdoor Trojan that responds to commands sent by a command-and-control program on another computer
- First bots supported legitimate activities
  - Internet Relay Chat
  - Multiplayer Internet games
- Other bots support illegal activities
  - Distributing spam
  - Collecting person information for ID theft
  - Denial-of-service attacks

Botnets and Bot Herders

- Botnet: Collection of bot-infected computers controlled by the same command-and-control program
- Some botnets have over a million computers in them
- Bot herder: Someone who controls a botnet

Defensive Measures

- Security patches: Code updates to remove security vulnerabilities
- Anti-malware tools: Software to scan hard drives, detect files that contain viruses or spyware, and delete these files
- Firewall: A software application installed on a single computer that can selectively block network traffic to and from that computer

Stuxnet Worm (2009)

- Attacked SCADA systems running Siemens software
- Targeted five industrial facilities in Iran that were using centrifuges to enrich uranium
- Caused temporary shutdown of Iran’s nuclear program
- Worm may have been created by Israeli Defense Forces