Chapter 7: Computer and Network Security

COMP422 Ethics and Professional Issues in Computing
Dr. Patrick Pang

Based on
Ethics for the Information Age (5ᵗʰ Ed.)
by
Michael J. Quinn

Chapter Overview

- Introduction

- Hacking

- Malware

- Cyber crime and cyber attacks

- Online voting

7.1 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

7.2 Hacking

Hackers, Past and Present

- Original meaning of hacker: explorer, risk taker, system innovator
  - MIT's Tech Model Railroad Club in 1950s
- 1960s-1980s: Focus shifted from electronics to computers and networks
  - 1983 movie *WarGames*
- Modern meaning of hacker: someone who gains unauthorized access to computers and computer networks

Obtaining Login Names and Passwords

- ## Eavesdropping
  - looking over the shoulder of a legitimate user to learn his login name and password

- ## Dumpster diving
  - looking through garbage for interesting information

- ## Social engineering
  - manipulation of a person inside the organization to gain access to confidential information

Computer Fraud and Abuse Act

- Criminalizes wide variety of hacker-related activities
  - Transmitting code that damages a computer
  - Accessing any Internet-connected computer without authorization
  - Transmitting classified government information
  - Trafficking in computer passwords
  - Computer fraud
  - Computer extortion

- Maximum penalty: 20 years in prison and $250,000 fine

Sidejacking

- Sidejacking: hijacking of an open Web session by capturing a user's cookie

- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"

- Internet security community complained about sidejacking vulnerability for years, but ecommerce sites did not change practices

Case Study: Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser

- Firesheep made it possible for ordinary computer users to easily sidejack Web sessions

- More than 500,000 downloads in first week

- Attracted great deal of media attention

- Early 2011: Facebook and Twitter announced options to use their sites securely

Utilitarian Analysis

- Release of Firesheep led media to focus on security problem

- Benefits were high: a few months later Facebook and Twitter made their sites more secure

- Harms were minimal: no evidence that release of Firesheep caused big increase in identity theft or malicious pranks

- Conclusion: Release of Firesheep was good

Kantian Analysis

- Accessing someone else's user account is an invasion of their privacy and is wrong

- Butler provided a tool that made it much simpler for people to do something that is wrong, so he has some moral accountability for their misdeeds

- Butler was willing to tolerate short-term increase in privacy violations in hope that media pressure would force Web retailers to add security

- He treated victims of Firesheep as a means to his end

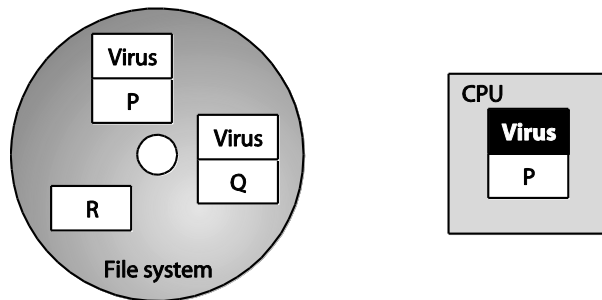- It was wrong for Butler to release Firesheep

7.3 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
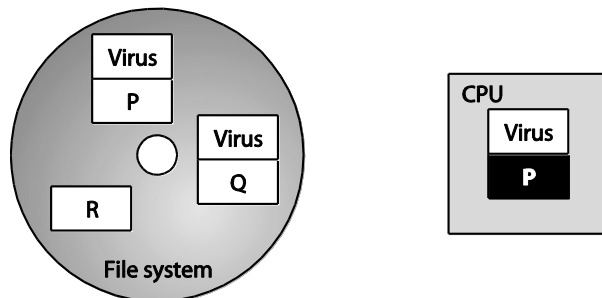 - Files downloaded from Internet
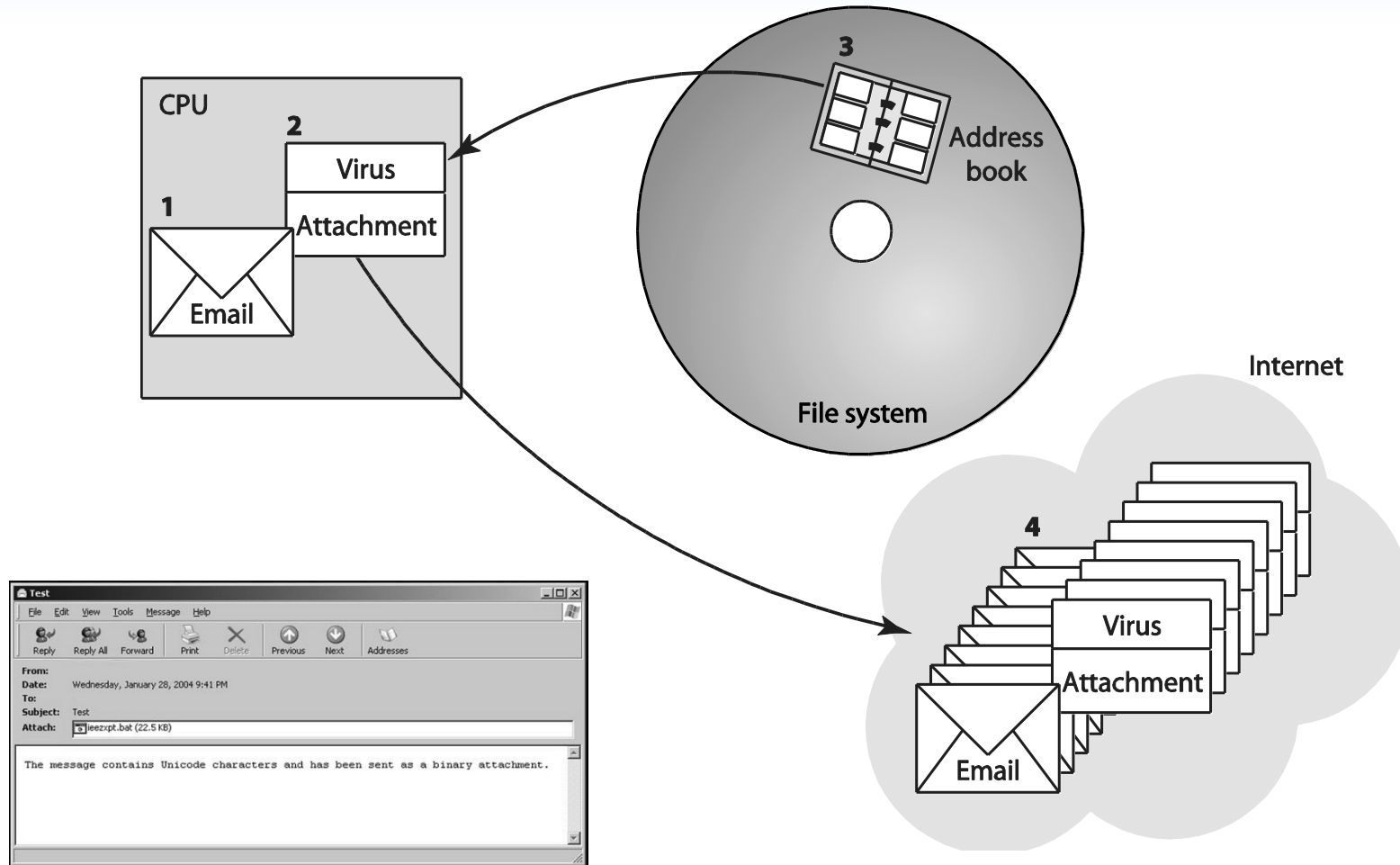
How a Virus Replicates
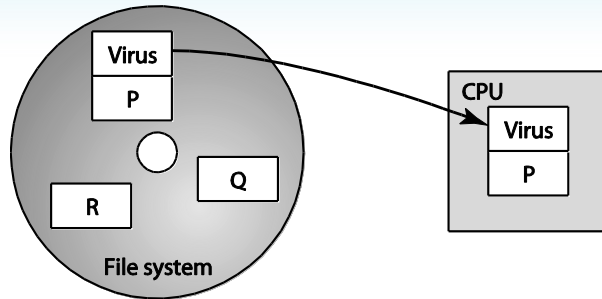
(a)

(b)

(c)

a) Program P, which is infected with a virus, is executed

b) The virus code executes. It finds another program Q and creates a new version of Q infected with the virus

c) The virus passes control to program P. The user is unaware of the presence of the virus

How an Email Virus Spreads


Email Attachment with Possible Virus

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
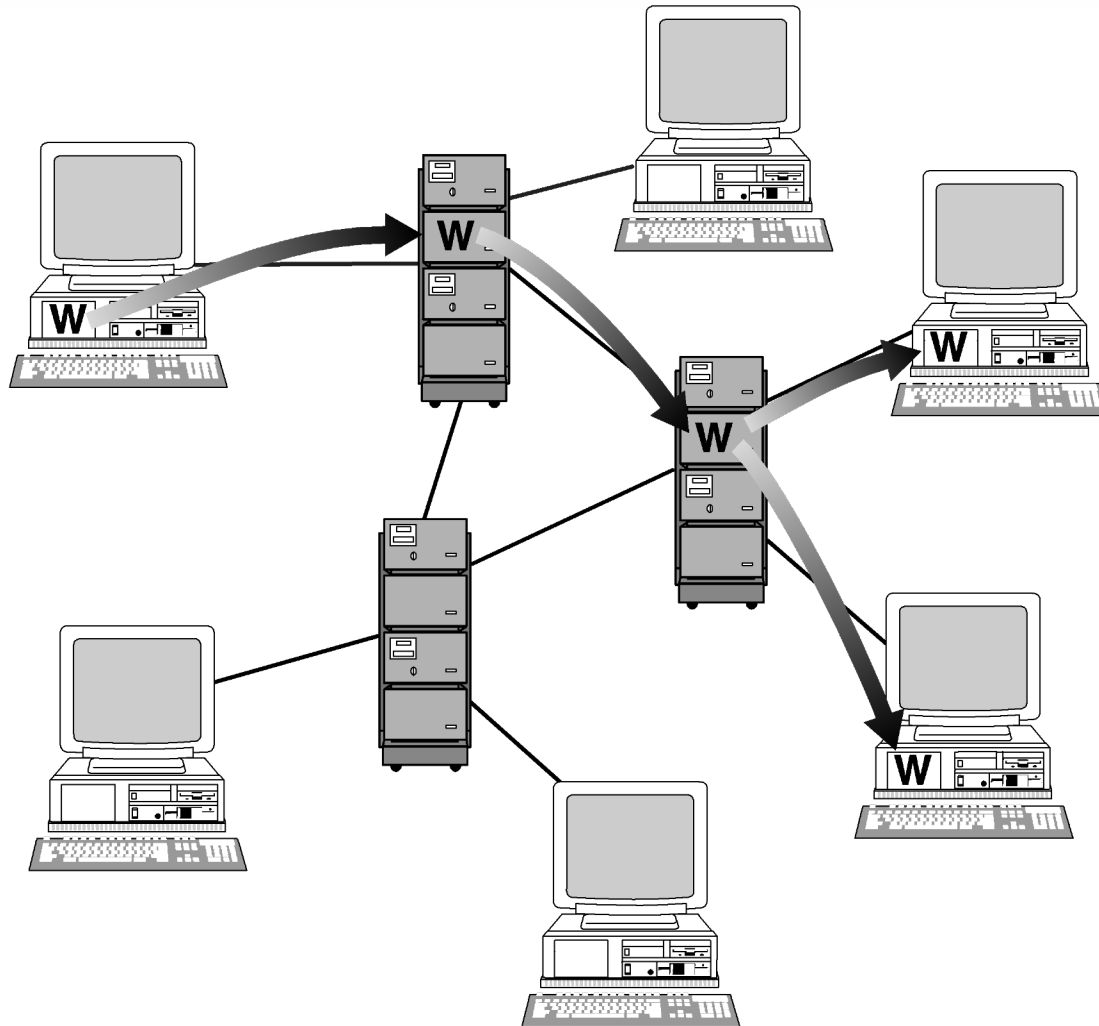
The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell (1988)
  - 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

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

7.5 Online Voting

Motivation for Online Voting

- 2000 U.S. Presidential election closely contested
- Florida pivotal state
- Most Florida counties used keypunch voting machines
- Two voting irregularities traced to these machines
  - Hanging chad
  - "Butterfly ballot" in Palm Beach County

The Infamous "Butterfly Ballot"
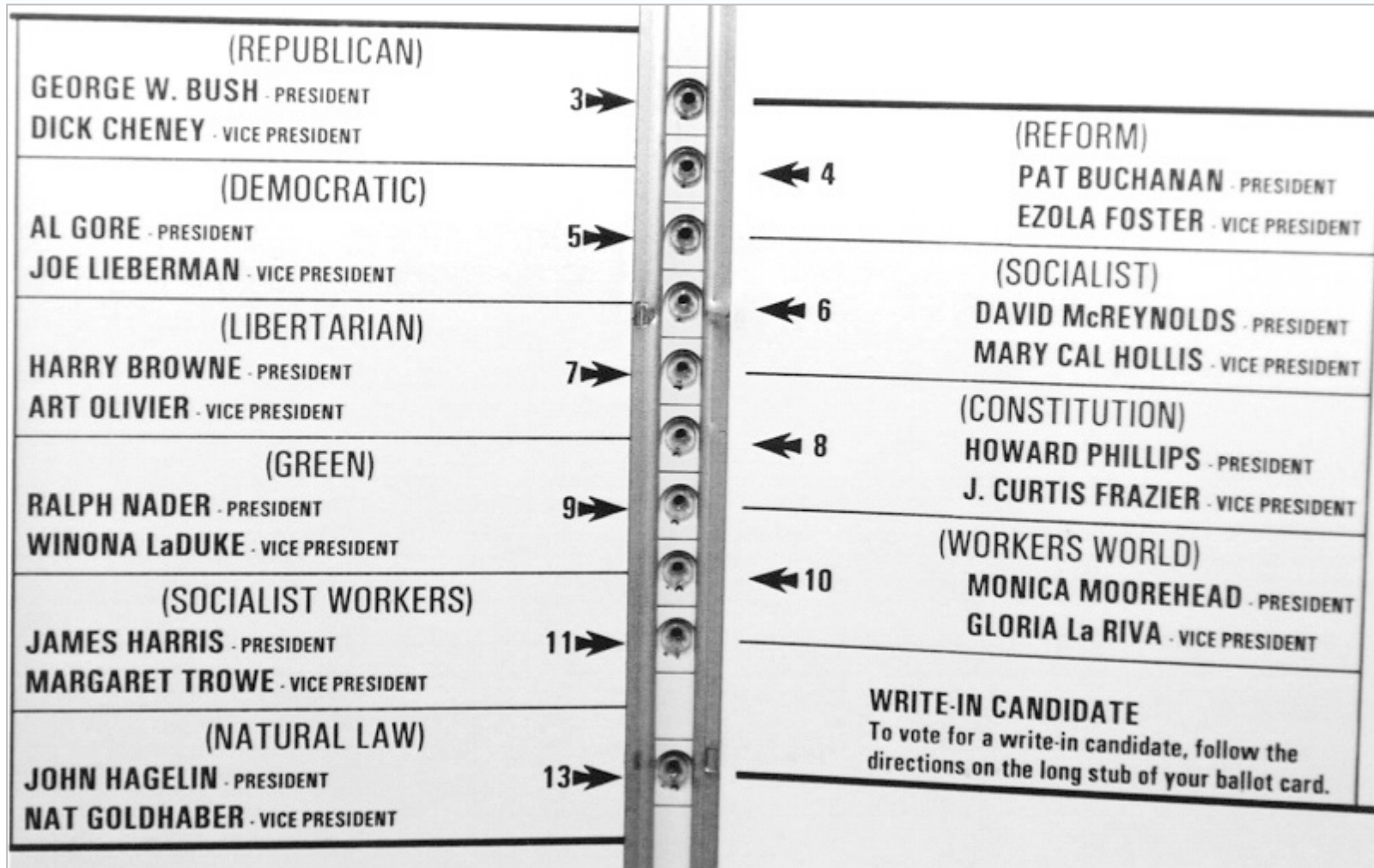
AP Photo/Gary I. Rothstein

Benefits of Online Voting

- More people would vote

- Votes would be counted more quickly

- No ambiguity with electronic votes

- Cost less money

- Eliminate ballot box tampering

- Software can prevent accidental over-voting

- Software can prevent under-voting

Risks of Online Voting

- Gives unfair advantage to those with home computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to vote-changing virus
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

Utilitarian Analysis

- Suppose online voting replaced traditional voting
- Benefit: Time savings
  - Assume 50% of adults actually vote
  - Suppose voter saves 1 hour by voting online
  - Average pay in U.S. is $18.00 / hour
  - Time savings worth $9 per adult American
- Harm of DDoS attack difficult to determine
  - What is probability of a DDoS attack?
  - What is the probability an attack would succeed?
  - What is the probability a successful attack would change the outcome of the election?

Kantian Analysis

- The will of each voter should be reflected in that voter's ballot

- The integrity of each ballot is paramount

- Ability to do a recount necessary to guarantee integrity of each ballot

- There should be a paper record of every vote

- Eliminating paper records to save time and/or money is wrong

Conclusions

- Existing systems are highly localized
- Widespread tainting more possible with online system
- No paper records with online system
- Evidence of tampering with online elections
- Relying on security of home computers means system vulnerable to fraud
- Strong case for not allowing online voting

7.4 Cyber Crime and Cyber Attacks

Phishing and Spear-phishing

- Phishing: Large-scale effort to gain sensitive information from gullible computer users
  - At least 67,000 phishing attacks globally in second half of 2010
  - New development: increase in phishing attacks on Chinese e-commerce sites
- Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients

SQL Injection

- Method of attacking a database-driven Web application with improper security

- Attack inserts (injects) SQL query into text string from client to application

- Application returns sensitive information

Denial-of-service and Distributed Denial-of-service Attacks

- Denial-of-service attack: Intentional action designed to prevent legitimate users from making use of a computer service

- Aim of a DoS attack is not to steal information but to disrupt a server's ability to respond to its clients

- Distributed denial-of-service attack: DoS attack launched from many computers, such as a botnet

Cyber Crime (PP. 332-334)

- Criminal organizations making significant amounts of money from malware

- Jeanson James Ancheta

- Pharmamaster

- Albert Gonzalez

- Avalanche Gang

The Rise and Fall of Blue Security Part I: The Rise

- Blue Security: An Israeli company selling a spam deterrence system

- Blue Frog bot would automatically respond to each spam message with an opt-out message

- Spammers started receiving hundreds of thousands of opt-out messages, disrupting their operations

- 6 of 10 of world's top spammers agreed to stop sending spam to users of Blue Frog

The Rise and Fall of Blue Security Part II: The Fall

- One spammer (PharmaMaster) started sending Blue Frog users 10-20 times more spam

- PharmaMaster then launched DDoS attacks on Blue Security and its business customers

- Blue Security could not protect its customers from DDoS attacks and virus-laced emails

- Blue Security reluctantly terminated its anti-spam activities

Politically Motivated Cyber Attacks (PP. 334-337)

- Estonia (2007)

- Georgia (2008)

- Georgia (2009)

- Exiled Tibetan Government (2009)

- United States and South Korea (2009)

- Stuxnet Worm (2009)

Attacks on Twitter and Other Social Networking Sites

- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009

- Three other sites attacked at same time: Facebook, LiveJournal, and Google

- All sites used by a political blogger from the Republic of Georgia

- Attacks occurred on first anniversary of war between Georgia and Russia over South Ossetia

Fourth of July Attacks

- 4th of July weekend in 2009: DDoS attack on governmental agencies and commercial Web sites in United States and South Korea

- Attack may have been launched by North Korea in retaliation for United Nations sanctions

Supervisory Control and Data Acquisition (SCADA) Systems

- Industrial processes require constant monitoring

- Computers allow automation and centralization of monitoring

- Today, SCADA systems are open systems based on Internet Protocol

  – Less expensive than proprietary systems

  – Easier to maintain than proprietary systems

  – Allow remote diagnostics

- Allowing remote diagnostics creates security risk

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