CS 4001: Computing, Society & Professionalism

Munmun De Choudhury | Assistant Professor | School of Interactive Computing

Week 12: Computer and Network Security

March 30, 2017

Chapter Overview

- Introduction
- Hacking
- Malware
- Online voting
- Cyber crime and cyber attacks

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 🎭 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

- Brute force methods and dictionary attacks
- Eavesdropping
- Dumpster diving
- Social engineering

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

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

Other Laws

- Other laws – Electronic Commission Privacy Act (cannot intercept electronic communications or read email without authorization)

- Wire Fraud Act, National Stolen Property Act, Identity Theft and Assumption Deterrence Act

Class Activity 1: Case Study of Firesheep

Firesheep: Act 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

Firesheep: 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

Firesheep: Virtue Ethics Analysis

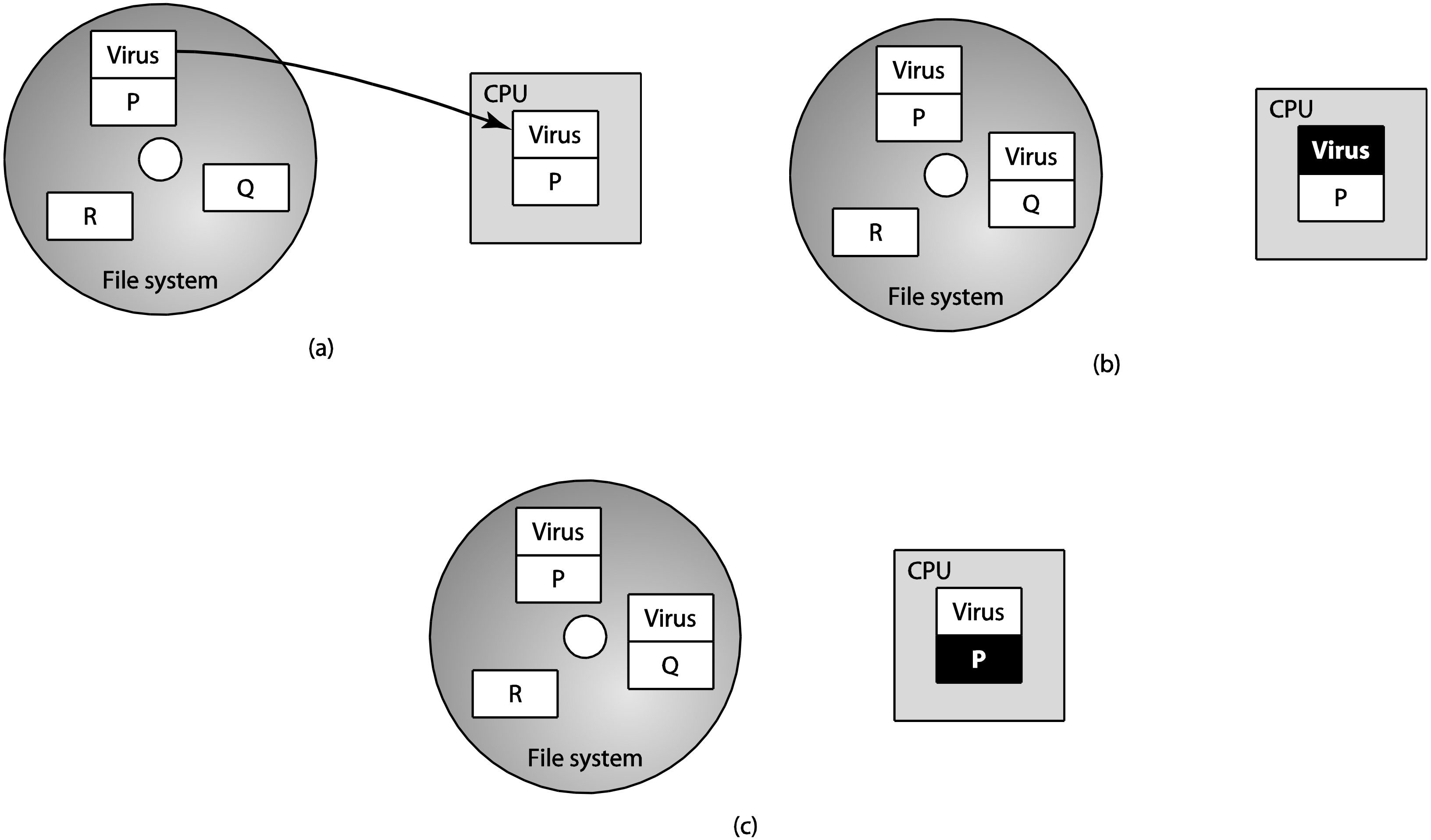
- Butler shared expertise and knowledge to help people and educate them of the privacy risks of using some non-encrypted websites
- Butler exhibited courage by taking personal responsibility for creating Firesheep, and he demonstrated benevolence by making it freely available
- Butler's interest in promoting the common good

7.3 Malware

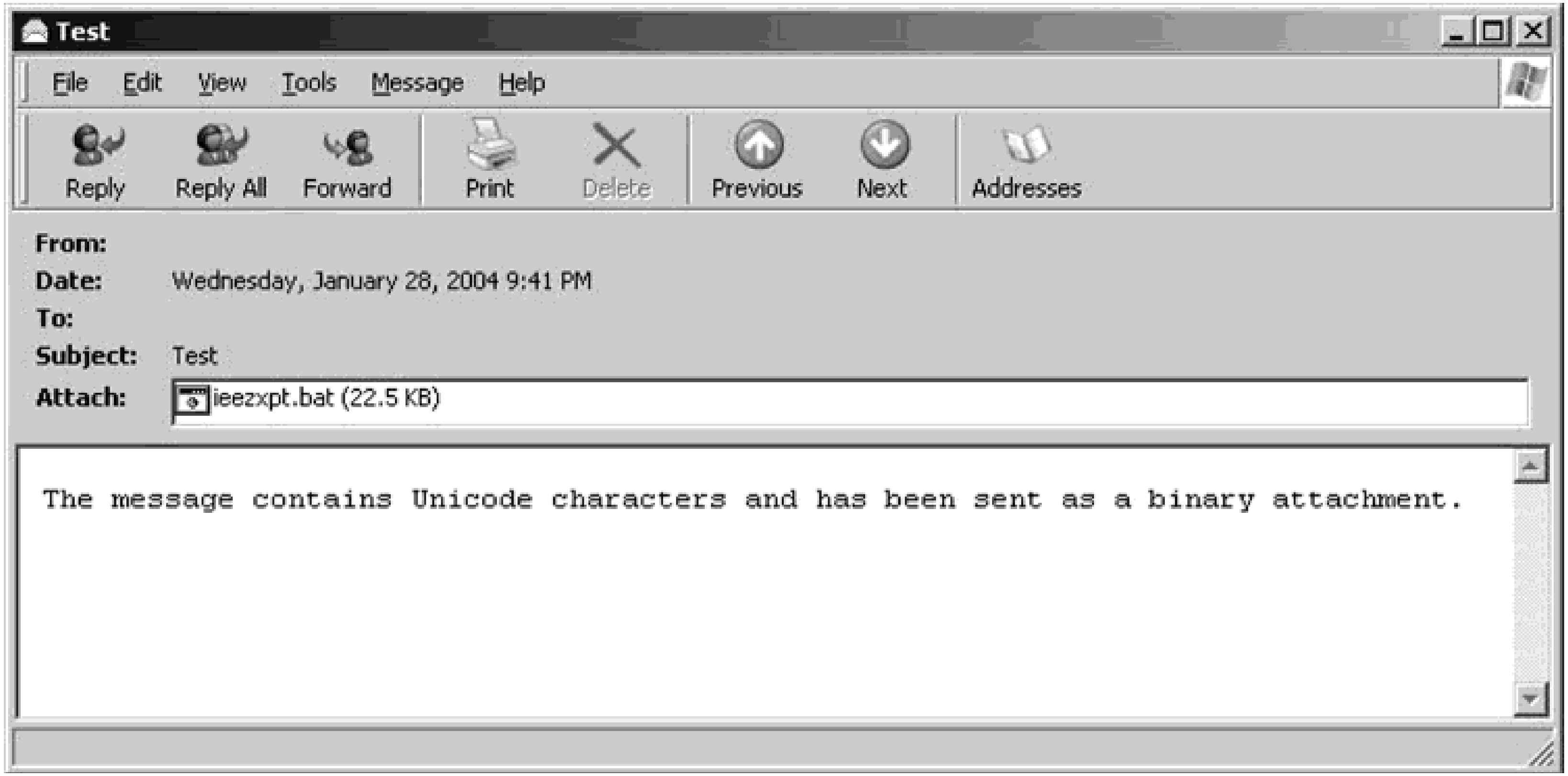
Viruses

- 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



Email Attachment with Possible Virus



From:

Date: Wednesday, January 28, 2004 9:41 PM

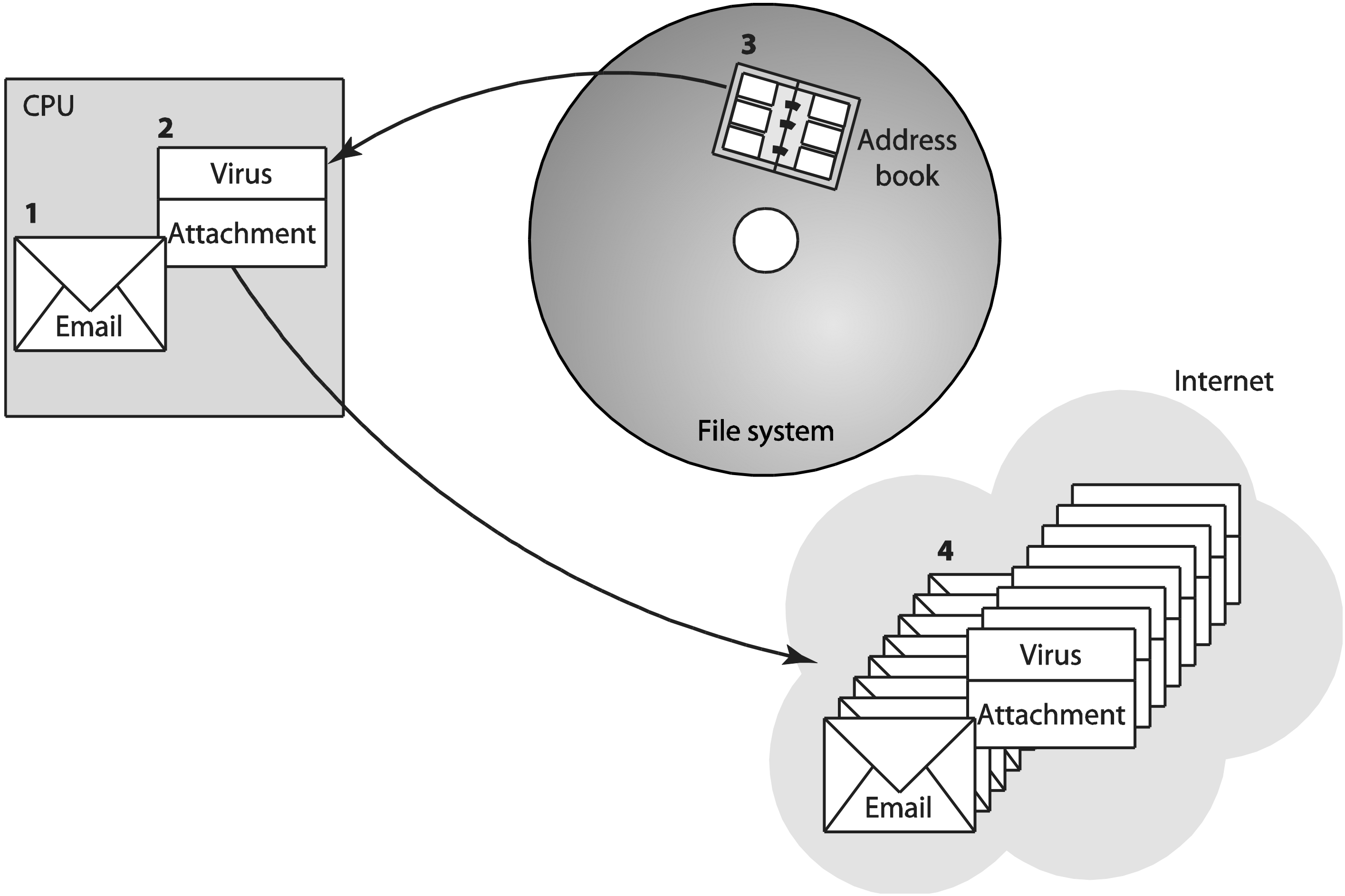
To:

Subject: Test

Attach: ieezxpt.bat (22.5 KB)

```
The message contains Unicode characters and has been sent as a binary attachment.
```

How an Email Virus Spreads



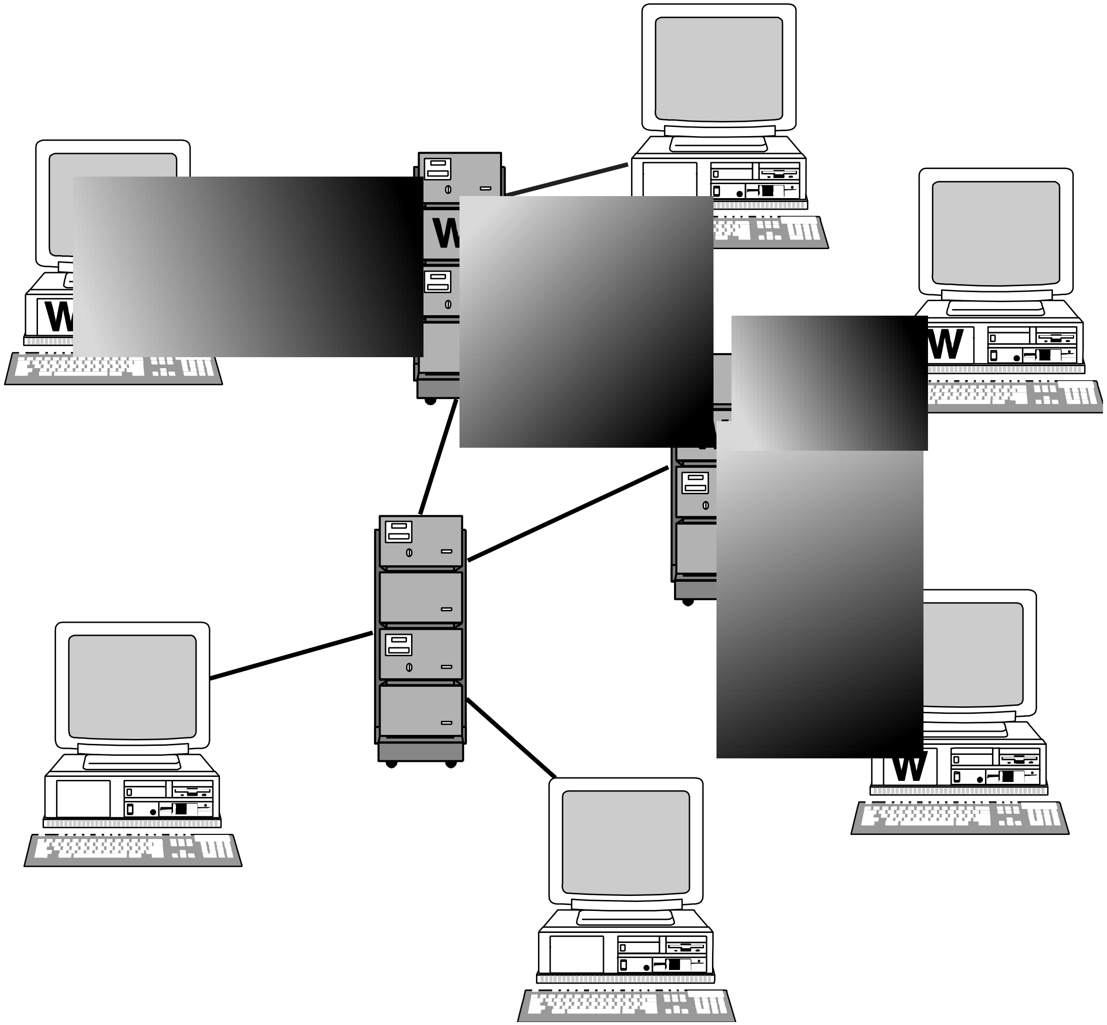
Antivirus Software Packages

- 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



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 Website
- Victim's (the next user'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 attacker access to victim's computer
  - May claim to cleanse malware from a user's computer, but in reality it installs spyware

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

Class Activity 2: The Internet Worm (Robert Tappan Morris Case Study)

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

Defensive Measures

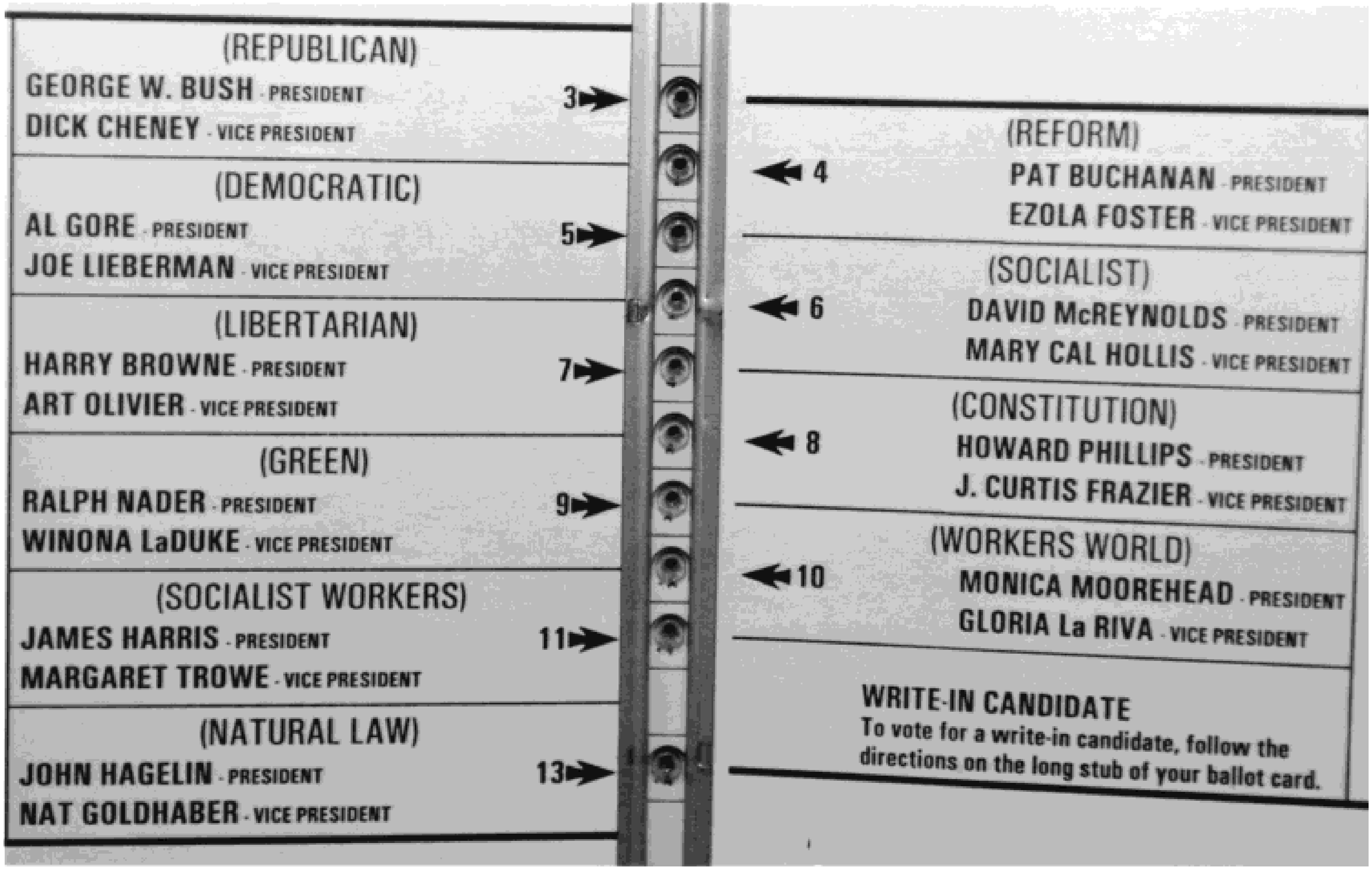
- Security patches: Code updates to remove security vulnerabilities
- Anti-malware tools: Software to scan hard drives, detect files that contain viruses or spyware, and delete these files
- Firewall: A software application installed on a single computer that can selectively block network traffic to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



(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13

4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

AP Photo/Gary I. Rothstein

Suppose online voting replaced traditional voting

Group Activity: Ethical Evaluation of Online Voting:

1) Act Utilitarian Perspective;
2) 2) Kantian Perspective

Utilitarian Analysis

- 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

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 or RAT
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

7.4 Cyber Crime and Cyber Attacks

Phishing and Spear-phishing

- Phishing: Large-scale effort to gain sensitive information from gullible computer users
  - Phishing emails are sent to users asking them to enter sensitive information on an imposter website
  - At least 67,000 phishing attacks globally in second half of 2010
  - New development: 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 DDOS 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

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

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

Anonymous

- Anonymous: loosely organized international movement of hacktivists (hackers with a social or political cause)
- Various DDoS attacks attributed to Anonymous members

Year	Victim	Reason
2008	Church of Scientology	Attempted suppression of Tom Cruise interview
2009	RIAA, MPAA	RIAA, MPAA's attempt to take down the Pirate Bay
2009	PayPal, VISA, MasterCard	Financial organizations freezing funds flowing to Julian Assange of WikiLeaks
2012	U.S. Dept. of Justice, RIAA, MPAA	U.S. Dept. of Justice action against Megaupload