Lecture 7: Computer Security

(Some slides are from M. Quinn, *Ethics for the Information Age*, Pearson © 2013.)

Lecture 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 → growing importance of computer security

1-3

7.2 Hacking

1-4

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
- Is hacking ever justified?

1-5

Computer Fraud and Abuse Act (CFAA) 1984

- Criminalizes wide variety of interstate and foreign hacker-related activities where there is a compelling federal interest
  - 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
- Amended by Patriot Act 2001 and Identity Theft Act 2008
  - Crime to commit conspiracy of fraud and abuse
- Maximum penalty: 20 years in prison and $250,000 fine

1-6

Obtaining Login Names and Passwords

- Eavesdropping
- Dumpster diving
- Social engineering

1-7

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
- Only effective fix is full end-to-end encryption (HTTPS or SSL)

1-8

Case Study: Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser to demonstrate sidejacking security vulnerability
- 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

1-9

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

1-10

Kantian Analysis

- Accessing someone else's user account is an invasion of their right to privacy and is wrong. It is also a form of theft.
- 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

1-11

7.3 Malware

1-12

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

1-13

Worm

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

1-14

The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - 1988 Released worm onto Internet from MIT computer
    - Bugs in Sendmail & Finger, trusted host feature, password brute-force attacks
- 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
- Convicted under the ComputerFraud and Abuse Act
  - Suspended from Cornell
  - 3 years' probation + 400 hours community service
  - $150,000 in legal fees and fines

1-15

Ethical Evaluation

- Kantian evaluation
  - Morris used others by gaining access to their computers without permission
- Rights 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

1-16

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

1-17

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

1-18

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

1-19

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

1-20

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

1-21

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

1-22

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

1-23

Defensive Measures

- Firewall: A software application installed on a single computer that can selectively block network traffic to and from that computer
  - Packet filter
  - Specialized filters for DoS attacks
- Software monitors
  - Intrusion detection
- Filtering systems scans email for spam or viruses
- Security patches to OS: Code updates to remove security vulnerabilities
- Anti-malware tools: Software to scan hard drives, detect files that contain viruses or spyware, and delete files
- Encryption for securing information itself

1-24

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

1-25

Encryption

- Types of encryption
  - Private key: strong encryption 128 bit algorithm
  - Public key: private & public keys for both parties
    - RSA and PGP
  - SSL protocol: web browsers and web servers
  - Authentication: validity of identification of parties
- Protects e-commerce, privacy, free speech
- Competing social issues
  - Protection vs. national security
  - Back door access by the government
    - Wiretapping vs. surveillance

7.4 Cyber Crime and Cyber Attacks

1-27

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: phishing attacks on Chinese e-commerce sites
- Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients

1-28

Phishing #1

DiMedio , Annette <ADiMedio@uarts.edu> May 13, 2013 2:29 AM
To: info@web.com
Dear Mail Box Account User

Dear Mail Box Account User

A phish attempt, banned phrase or sensitive information was detected in a message sent to you and the original message has been quarantined. This message is a copy of the original with the content replaced with this text. The subject line and sender information has been unaltered from the original.Please you are to re-validate your WEB-MAIL. email address immediately.

To Confirm Your E-mail Account click on the link below

http://www.iworkinhotels.com/filemanager/userfiles/sym/update/emailadmin.php.htm

And if you can not click the above link, kindly copy the link and paste on your web address.

Thank you for your cooperation.
System Administrator.

Phishing #2

AUDITOR INDEX <prestige@cogeco.ca> May 13, 2013 7:11 AM
Reply-To: indexaopt@gmail.com Hide Details
Transaction Ref No.: FNB/TELEX/00900076695/2013

Attn: The Manager / Director CEO
Sir/Madam,

This proposal is meant to notify you the outstanding Company's project funds transfer from our Bank,marked pending.
Kindly acknowledge for the transcript details.
With regards,

FNB Foreign Exchange Operation / Audit & Claim Dept Office
Tel: 0027 86 6693 209 / agenttfnb@gmail.com.
Jhb, South Africa

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

1-31

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

1-32

Cyber Crime

- Criminal organizations making significant amounts of money form malware
- Jeanson James Ancheta
  - 2006 convicted of controlling botnets, 5 yrs prison
- Pharmamaster
  - 2006 Hacker attack on Blue Security system
- Albert Gonzalez
  - 2010 convicted of credit card theft reselling, 20 yrs
- Avalanche Gang
  - 2008-2010 Eastern European, phishing with spam mail infected with malware: log keystrokes, allows remote access, still operating?

1-33

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

- Blue Security: An Israeli company selling a spam deterrence system 2006
- 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

1-34

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

1-35

Politically Motivated Cyber Attacks

- Estonia (2007)
- Georgia (2008)
- Georgia (2009)
- Exiled Tibetan Government (2009)
- United States and South Korea (2009)
- Stuxnet Worm (2009)

1-36

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

1-37

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

1-38

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

1-39

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

1-40

7.5 Online Voting

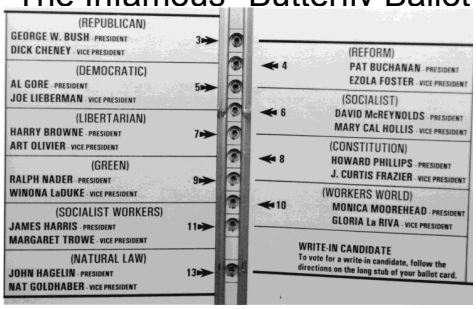
1-41

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

1-42

The Infamous "Butterfly Ballot"



AP Photo/Gary I. Rothstein

1-43

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

1-44

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

1-45

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?

1-46

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

1-47

On-Line Voting: 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

1-48