### Introduction

- Computers are 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

### Consider the following questions:

- What key trade-offs and ethical issues are associated with the safeguarding of data and information systems
- Why has there been a dramatic increase in the number of computer-related security incidents in recent years
- What are the most common types of computer security attacks?
- Who are the primary perpetrators of computer crime, and what are their objectives?

---

### IT Security Incidents: A Major Concern

- Security of information technology is of utmost importance
  - Safeguard:
    - Confidential business data
    - Private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Balance against other business needs and issues
- Number of IT-related security incidents is increasing around the world

### Why Computer Incidents Are So Prevalent

- Increasing complexity increases vulnerability
  - Computing environment is enormously complex
    - Continues to increase in complexity
    - Number of entry points expands continuously
    - Cloud computing and virtualization software
  - Higher user expectations
    - Computer help desks under intense pressure
    - Forget to verify users’ IDs or check authorizations
- Number of IT-related security incidents is increasing around the world

- Increased reliance on commercial software with known vulnerabilities
  - Exploit
    - Attack on information system
    - Takes advantage of system vulnerability
    - Due to poor system design or implementation
  - Patch
    - “Fix” to eliminate the problem
    - Users are responsible for obtaining and installing
    - Delays expose users to security breaches
Why Computer Incidents Are So Prevalent

- Zero-day attack
  - Before a vulnerability is discovered or patched
- U.S. companies rely on commercial software with known vulnerabilities

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

The Hacker Ethic

Argue that they follow an ethic that both guides their behavior and justifies their break-ins
- All information should be free
  - Belongs to everyone and there should be no boundaries or restraints to prevent anyone from examining information
- GNU Manifesto (Richard Stallman)

Types of Perpetrators

- Perpetrators include:
  - Thrill seekers wanting a challenge
  - Common criminals looking for financial gain
  - Industrial spies trying to gain an advantage
  - Terrorists seeking to cause destruction
- Different objectives and access to varying resources
- Willing to take different levels of risk to accomplish an objective

Types of Perpetrators

<table>
<thead>
<tr>
<th>Type of Perpetrator</th>
<th>Typical Motives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>Test limits of system and gain publicity</td>
</tr>
<tr>
<td>Cracker</td>
<td>Game problems, steal data, and corrupt systems</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>Gain financially and disrupt company’s information systems and business operations</td>
</tr>
<tr>
<td>Industrial spy</td>
<td>Capture trade secrets and gain competitive advantage</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Gain financially</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>Promote political ideology</td>
</tr>
<tr>
<td>Cyberterrorist</td>
<td>Destroy infrastructure components of financial institutions, utilities, and emergency response units</td>
</tr>
</tbody>
</table>

Source: Course Technology/Conedge Learning.

Kevin Mitnick

- Famous controversial U.S. hacker
- Utilized “social engineering” for obtaining user names / passwords, modem phone numbers, etc.
- Served 46 months in federal prison for wire fraud, computer fraud, and illegally intercepting a wire communication

Acts by Kevin Mitnick
- Using the L.A. bus transfer system to get free rides
- Evading the DEC UNIX security (DEC reportedly spent $160,000 in cleanup costs)
- Gaining full admin privileges to an IBM mainframe at the Computer Learning Center in L.A. in order to win a bet
- Hacking into DEC’s mainframe and later into Boeing’s systems
- Wiretapped FBI agents according to John Markoff, although denied by Kevin Mitnick.

Alleged
- Stole computer manuals from a Pacific Bell telephone switching center in Los Angeles
- Read the e-mail of computer security officials at MCI Communications and Digital
- Wiretapped the California DMV
- Made free cell phone calls
- Hacked SCO, PacBell, FBI, University of Southern California, and federal systems.
<table>
<thead>
<tr>
<th>Hackers and Crackers</th>
<th>Malicious Insiders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hackers</strong></td>
<td></td>
</tr>
<tr>
<td>– Test limitations of systems out of intellectual curiosity</td>
<td>• Major security concern for companies</td>
</tr>
<tr>
<td>• Some smart and talented</td>
<td>• Fraud within an organization is usually due to weaknesses in internal control procedures</td>
</tr>
<tr>
<td>• Others inept; termed “lamers” or “script kiddies”</td>
<td>• Collusion</td>
</tr>
<tr>
<td><strong>Crackers</strong></td>
<td></td>
</tr>
<tr>
<td>– Cracking is a form of hacking</td>
<td>– Cooperation between an employee and an outsider</td>
</tr>
<tr>
<td>– Clearly criminal activity</td>
<td>• Insiders are not necessarily employees</td>
</tr>
<tr>
<td></td>
<td>• Can also be consultants and contractors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industrial Spies</th>
<th>Cybercriminals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use illegal means to obtain trade secrets from competitors</strong></td>
<td>• Hack into corporate computers to steal</td>
</tr>
<tr>
<td><strong>Trade secrets are protected by the Economic Espionage Act of 1996</strong></td>
<td>• Engage in all forms of computer fraud</td>
</tr>
<tr>
<td><strong>Competitive intelligence</strong></td>
<td>• Loss of customer trust has more impact than fraud</td>
</tr>
<tr>
<td>– Uses legal techniques</td>
<td>• To reduce potential for online credit card fraud:</td>
</tr>
<tr>
<td>– Gathers information available to the public</td>
<td>• Use encryption technology</td>
</tr>
<tr>
<td><strong>Industrial espionage</strong></td>
<td>• Verify the address submitted online against the issuing bank</td>
</tr>
<tr>
<td>– Uses illegal means</td>
<td>• Request a card verification value (CVV)</td>
</tr>
<tr>
<td>– Obtains information not available to the public</td>
<td>• Use transaction-risk scoring software</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybercriminals</th>
<th>Cyber Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smart cards</strong></td>
<td>In our context, cyber crime might be defined as:</td>
</tr>
<tr>
<td>– Contain a memory chip</td>
<td>Software piracy</td>
</tr>
<tr>
<td>– Updated with encrypted data each time card is used</td>
<td>Computer sabotage</td>
</tr>
<tr>
<td>– Used widely in Europe</td>
<td>Electronic break-ins</td>
</tr>
<tr>
<td>– Becoming more widely used in the U.S.</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Crime

- Criminal organizations making significant amounts of money from malware
- Jeanson James Ancheta
  - Built botnet, sold access to “customers”
- Pharmamaster
  - Israeli anti-spam program
- Albert Gonzalez
  - SQL injection attacks
- Avalanche Gang
  - Phishing gang

Hacktivists and Cyberterrorists

- Hacktivism
  - Hacking to achieve a political or social goal
- Cyberterrorist
  - Attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives
  - Seeks to cause harm rather than gather information
  - Uses techniques that destroy or disrupt services

Federal Laws for Prosecuting Computer Attacks

<table>
<thead>
<tr>
<th>Federal Law</th>
<th>Subject area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft and Assumption Statute (U.S. Code Title 18, Section 1028)</td>
<td>Violates identity theft: Federal crimes with penalties up to 15 years imprisonment and a maximum fine of $250,000</td>
</tr>
<tr>
<td>Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)</td>
<td>False claims regarding unauthorized use of credit cards</td>
</tr>
<tr>
<td>Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)</td>
<td>Fraud and related activities in connection with computers: - Accessing a computer without authorization or exceeding authorized access - Transmitting a program, code, or command that causes harm to a computer - Trafficking of computer passwords - Threatening to cause damage to a protected computer</td>
</tr>
<tr>
<td>Stored Voice and Electronic Communications and Transaction Records Access Statute (U.S. Code Title 18, Chapter 32)</td>
<td>Unlawful access to stored communications to obtain, alter, or prevent authorized access to wire or electronic communications while it is in electronic storage</td>
</tr>
</tbody>
</table>

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

The Security Arguments

- Break-ins illustrate security problems to a community that will otherwise not note the problems
- Originally the Worm example
  - Security problem awareness
  - Inspires copy-cat acts
  - High cost

The Idle System Argument

- Systems not in service to provide a general-purpose user environment
  - Used in commerce, medicine, public safety, research, and government functions
  - Unused capacity is present for future needs and sudden surges of activity
  - Hacker view: not causing harm to production systems if we attack these systems.
### The Student Hacker Argument

- Doing no harm and changing nothing
  - simply learning about how computer systems operate or writing complex programs

Arguments against
- Not educational
- Intruder can cause accidental damage
- Systems can no longer be fully trusted

### The Social Protector Argument

- Hackers break into systems to watch for instances of data abuse and to help keep “Big Brother” at bay
  - They claim to be Protectors rather than criminals

Arguments against
- Ends justify means – assumes ability to achieve good end
- Results in more data restrictions

### Obtaining Login Names and Passwords

- 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
  - Today many sites have changed to encrypted web sessions (https).

### Case Study: Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser
  - Security people previously tried to convince web sites/browser manufacturers to use encryption.
- 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

Types of attack “tools”

Viruses

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

How a Virus Replicates

Antivirus Software Packages

- Allow computer users to detect and destroy viruses
  - Work by looking for virus “signatures”
    - False positives!
- 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
- Typically spreads through a computer network
  - email/spam
  - Web site
- Exploits security holes in networked computers
The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - Released worm onto Internet from MIT computer
    - "To demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that I had discovered."
- 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 some percentage 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 personal 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

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
  - The number of worldwide phishing attacks detected by Kaspersky hit 129.9 million during the second quarter of 2019
  - The total number of phishing sites detected in July through September 2019 was 266,387. This was up 46 percent from the 182,465 seen in the second quarter of 2019, and almost double the 138,328 seen in Q4 2018.
- Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients
  - 91% Of Data Breaches Start With Spear Phishing Attacks On Organizations.
  - Hackers attack every 39 seconds, on average 2,244 times a day.

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
Distributed Denial-of-Service (DDoS) Attacks

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
  - Botnet is a very large group of such computers
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot access target machine

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

Defensive Measures

- Security patches: Code updates to remove security vulnerabilities
- Anti-malware tools: Software to scan hard drives, detect files that contain viruses, worms, 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
  - A hardware device that provides protection for an entire network.

Case studies and wrapup

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

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**

- Estonia (2007)
- Georgia (2008)
- Georgia (2009)
- Exiled Tibetan Government (2009)
- United States and South Korea (2009)
- Stuxnet Worm (2009)
- United States and South Korea (2013)
- United States Elections (2016, 2020?)

**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

**Implications**

- Privacy is no longer possible
- Not individual property
  - Anyone may access / alter
  - Loss of control
  - Accuracy cannot be trusted
- Economic arguments
  - Expense of info collection and protection
CONCLUSION

• Computer break-ins, even when no obvious damage results, are unethical
  – Disruptive, immoral
  – Examine act itself – difficult to determine all effects

• Justified computer break-in
  – Save life
  – Preserve national security