Computer Crime & Privacy

• **Computer crime** (cybercrime) includes any illegal act involving a computer
  – A multibillion-dollar business often performed by criminals

• **Information privacy** refers to the rights of individuals and companies to control how information about them is collected and used
  – *ACM Code of Ethics 1.1*: “An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy.”
Hardware Loss and Damage

- **Hardware loss** occurs when hardware is stolen, damaged, or lost
  - Both security and privacy concern
- **Hardware theft**
  - Theft for the hardware itself
  - Risk identity theft and other fraudulent activities
- **Damage** => power fluctuations, heat, dust, static electricity, water, and abuse
System Failure => Disasters & Attacks

• **System failure**
  – Complete malfunction of a computer system
    => hardware/software problem (corrupt/missing file)
    => computer sabotage
    => natural disaster/terrorist attack
Physical Security First

- Door and computer equipment locks
  - Locked doors
  - Access control
  - Locks/Alarms on devices
  - Staff security protocols
Device Tracking Software and Antitheft Tools

• Device tracking software
  – Designed to locate lost or stolen hardware
  – Location typically determined by GPS or Wi-Fi
• Kill switches -> disable/delete

FIGURE 9-3
Remote locking.
Backups and Disaster Recovery Plans

• **Backups**
  – Businesses should backup new data daily
    
    Review 3 different backups presented in Storage & OS

• **Continuous data protection (CDP)**
  – backs up data in real time as it changes

• **A disaster recovery plan** (business continuity plan)
  – How organizations recover from a disruptive event
  – Hot sites and cold sites provide alternate location
  – Cloud data recovery
Unauthorized Access and Unauthorized Use

- **Unauthorized access**
  - Gaining access without permission

- **Unauthorized use**
  - Using for unapproved activities

- **Codes of conduct/Acceptable use policies**
  - Used to specify rules for behavior, typically by a business or school

- **Hacking**
  - Break into another computer system
War Driving and Wi-Fi Piggybacking

- **War driving**
  - Driving around an area to find a Wi-Fi network to access and use without authorization

- **Wi-Fi piggybacking**
  - Accessing an unsecured Wi-Fi network from the hacker’s current location without authorization

- Wi-Fi finders can be used to find free and fee-based hotspots
Encryption

- Encryption makes data unreadable to unauthorized individuals
  - Used with secure Wi-Fi networks and VPNs to secure data that is transferred over those networks
  - **Secure Web pages** use encryption in order to protect information transmitted via that Web page
    - Transport Layer Security (TLS) (Secure Sockets Layer (SSL))
      - Self-encrypting hard drives automatically encrypt all content stored on those drives
      - Can be used with stored files as well as files sent over the Internet
Encryption

- **Private key encryption** (symmetric key encryption)
  - Uses a single key
  - Most often used to encrypt files on a computer
  - If used to send files to others, the recipient and sender must agree on the private key to be used

- **Public key encryption** (asymmetric key encryption)
  - Uses two keys (a private key and a public key) to encrypt and decrypt documents
    - Public key encrypts file
    - Private key decrypts file
  - Key pairs are obtained through a Certificate Authority
Access Control

• Access control systems control access to facilities, computer networks, company databases, and Web site accounts
  – Identification systems
    • Verify that the person trying to access the facility or system is an authorized user
  – Authentication systems
    • Determine if the person is who he or she claims to be
  – Businesses => identity management (IDM) systems
Access Control

- **Knowledge** – Something I know
- **Possessed** – Something I have
- **Biometric** – Something I am

- **Two-factor authentication** uses two different methods to authenticate users
Wireless Networks

– Implement WPA or WPA2 security
  • Network key is then required for access
– Can hide network name (SSID) to prevent war driving or Wi-Fi piggybacking
  • Authorized users will need to supply the SSID to access the network
Additional Precautions

• Individuals
  – public hotspots => use a firewall, VPN, and encryption
  – Turn off automatic Wi-Fi connections
  – Disable ad hoc connections
  – Turn off file sharing and Bluetooth

• Employers
  – Screen hires carefully
  – Limit employee access to resources
  – Use software to manage devices and prevent data leaks
Computer Sabotage

• **Computer sabotage** refers to acts of malicious destruction to a computer or computer resource
  – Launching a malicious program
    => viruses, worms, Trojans, bots, etc.
  – Altering the content of a Web site
  – Changing data or programs located on a computer
• Let’s look at the various attacks
Botnets

- A **botnet** is a group of **bots** (computers controlled by a hacker) that are controlled by one individual and work together in a coordinated fashion
  - Used by botherders (criminals) to send spam, launch Internet attacks, and spread malware
  - Distributed Denial of Service (DDoS)
Denial of Service (DoS) Attacks

• **Denial of service (DoS) attacks** are acts of sabotage that attempt to flood a network server or Web server with so much activity that it cannot function
  – Server either shuts down or can no longer handle requests
  – Legitimate users are denied service
  – Distributed DoS (DDoS) attacks are carried out via multiple computers
    • Often botnets
  – Costly in terms of lost business and the time and expense to bring the server back online
Malware

• **Malware** is any type of malicious software
  – Written to perform destructive acts (damaging programs, deleting files, erasing drives, etc.)
  • Can take place immediately after infection or at a later time
    – Logic bomb: Triggered when a certain condition is met
    – Time bomb: Triggered by a particular date or time
  – Writing malware is considered unethical; distributing is illegal
  – Is very costly to businesses
A **computer virus** is a software program installed without the user’s knowledge and designed to alter the way a computer operates or to cause harm to the computer system.

- Often embedded in downloaded programs and e-mail messages (games, videos, music files)
- Spread when the infected file reaches a new device

A **computer worm** is a malicious program designed to spread rapidly by sending copies of itself to other computers via a network.

- Typically sent as an e-mail attachment**
Trojan Horses and Mobile Malware

• A Trojan horse is a malicious program that masquerades as something else, usually an application program
  – Rogue anti-malware apps (scareware)
  – Ransomware
  – Spread via downloaded files, e-mail attachments, etc.

• Mobile malware infects smartphones, tablets, etc.
  – Primary goal is to obtain mobile banking credentials
Data, Program, or Web Site Alteration

• Hacker can breach a computer system in order to delete/change data or modify programs
• Data on Web sites can also be altered
  – Hacking into and changing social networking account contents (Facebook pages, Twitter tweets, etc.)
  – Altering legitimate site to perform malware attacks
• Estimated that more than half of malicious sites are actually legitimate sites that were compromised
Protecting Against Computer Sabotage

- **Security software** is typically a suite of programs used to protect your computer against a variety of threats
  - **Antivirus software** is used to detect and eliminate computer viruses and other types of malware
    - Should be set up to run continuously to check incoming e-mail messages, instant messages, Web page content, and downloaded files
    - Quarantines any suspicious content as it arrives
    - Should be set to perform regular system scans
  - **Antispyware software** detects and removes spyware
Firewalls

• **Firewalls** are a collection of hardware and/or software intended to protect a computer or computer network from unauthorized access
  
  – Typically two-way: Check all incoming (from the Internet) and outgoing (to the Internet) traffic
    
    => Stateful Packet Inspection (SPI)
  
  – Important for home computers that have a direct Internet connection, as well as for businesses
  
  – Work by closing down external communications ports
Intrusion Prevention Systems

- **Intrusion prevention system (IPS)** software monitors traffic to detect and block possible attacks
  - Help businesses detect and protect against denial of service (DoS) attacks
  - Recommend WiFi logs be turned on
Identity Theft

- **Identity theft** involves using someone else’s identity to purchase goods or services, obtain new credit cards or bank loans, or illegally masquerade as that individual
  - Information can be obtained:
    - Online via hacking, spyware, etc.
    - Via offline documents gathered via trash dumpsters, mailboxes, etc.
    - Via skimming devices
    - Via social engineering and social media
  - Expensive and time consuming to recover from
Phishing and Spear Phishing

- **Phishing** is the use of spoofed communications to gain credit card numbers and other personal data
  - Often via e-mail; typically looks legitimate but links go to a spoofed Web site
  - Information obtained is used in identity theft or fraud
  - Can occur via spyware, text messages, social media messages, etc.
  - Typosquatting: Setting up spoofed Web sites with URLs slightly different from legitimate sites

- **Spear phishing**
  - A personalized phishing scheme targeted to specific individuals
Digital IDs

- A **digital ID** (**digital certificate**) is a group of electronic data that can be used to verify the identity of a person or organization
  - Are also used with secure Web sites to guarantee that the site is secure and actually belongs to the stated individual or organization
    - Can be SSL/TLS or EV SSL
      - Includes public/private key pair
Personal Safety Issues: Cyberbullying

• **Cyberbullying** involves the use of online communications to bully another person
  – E-mail, social media, etc.
  – Often anonymous
  – Prevalent among teens; estimated to affect more than one-third of all U.S. teenagers
• NYS 240.30 - Aggravated harassment in the second degree *

A person is guilty of aggravated harassment in the second degree when, with intent to harass, annoy, threaten or alarm another person, he or she:

(a) communicates with a person, anonymously or otherwise, by telephone, by telegraph, or by mail, or by transmitting or delivering any other form of written communication, in a manner likely to cause annoyance or alarm;

*http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=@SLPEN0P3TNA240+&LIST=LAW+&BROWSER=EXPLORER+&TOKEN=36544786+&TARGET=VIEW)
Databases and Electronic Profiling

• **Electronic profiling**: Collecting in-depth information about an individual; name, address, income, and buying habits
  - Information is sold to companies upon request to be used for marketing purposes
• Most business Web sites have a **privacy policy** that explains how personal information is used and share
Spam and Other Marketing Activities

- **Spam** refers to unsolicited e-mail sent to a large group of individuals at one time
  - The electronic equivalent of junk mail
  - At best, an annoyance to recipients
  - At worst, can disable a mail network completely
Presence Technology

- **Presence technology** is the ability of one computing device to identify another device on the same network and determine its status
  - Integrated into many messaging programs, like Facebook
  - Used in some business communications programs
- Privacy advocates are concerned about the use of this technology
Electronic Surveillance and Monitoring

• Electronic tools can be used to watch individuals, listen to their conversations, monitor their activities, etc.

• Computer monitoring software is used for monitoring someone’s computer activity
  – Some can block specific Web sites
  – Some notify a designated party of the use of specified keywords or inappropriate Web sites
  – Keystroke logging software can be used to record e-mail messages and documents before they are encrypted
  – Used by parents, spouses, law enforcement agencies, and employers
Video Surveillance

• **Video surveillance** is the use of video cameras to monitor activities
  – For security and law enforcement purposes
  – Used in businesses, schools, outdoors, etc.
  – With face recognition technology, it can help detect suspicious behavior

• Privacy concerns
  – How captured video is used
  – How mobile device cameras are used
Summary

• Why Be Concerned About Network and Internet Security?
• Hardware Loss, Hardware Damage, and System Failure
• Unauthorized Access and Unauthorized Use
• Computer Sabotage
• Online Theft, Online Fraud, and Other Dot Cons
• Personal Safety Issues
• Databases, Electronic Profiling, Spam, and Other Marketing Activities