Privacy and Security

COMPUTER FRAUD AND ABUSE TECHNIQUES

Identity Theft

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - Assuming someone's identity, typically for economic gain, by illegally obtaining and using confidential information such as the person's social security number, bank account number, or credit card number.
  - Identity thieves benefit financially by:
    - Taking funds out of the victim's bank account.
    - Taking out mortgages or other loans under the victim's identity.
    - Taking out credit cards and running up large balances.
  - If the thief is careful and ensures that bills and notices are sent to an address he controls, the scheme may be prolonged until such time as the victim attempts to buy a home or car and finds out that his credit is destroyed.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - Victims can usually clear their credit, but the effort requires a significant amount of time and expense.
  - Identity theft was made a federal offense in 1998, but it is a growing crime industry.
  - One U.S. postal inspector, whose job duties involved investigation of identity thefts, was himself a victim. The thief ran up $80,000 in debt under the postal inspector's identity before the inspector discovered the problem.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - The U.S. Department of Justice suggests the following four ways to minimize the chances of being victimized by identity theft:
    - Do not give out corporate or personal information unless there is a good reason to trust the person to whom it is given.
    - Check financial information regularly for what should be there, as well as for what should not be there.
    - Periodically review your credit report.
    - Maintain careful records of banking and financial accounts.

COMPUTER FRAUD AND ABUSE TECHNIQUES

Phishing Fraud

- Sending out a spoofed email that appears to come from a legitimate company, such as a financial institution. EBay, PayPal, and banks are commonly spoofed.
- The recipient is advised that information or a security check is needed on his account, and advised to click on a link to the company's website to provide the information.
- The link connects the individual to a website that is an imitation of the spoofed company's actual website. These counterfeit websites appear very authentic, as do the emails.

- **Phishing**

COMPUTER FRAUD AND ABUSE TECHNIQUES

- One newly graduated college student recently took a job in California and deposited his first paycheck of approximately $5,000 in the bank.
- That same night, he received an email from the bank, inviting him to click on the link in the email to set up online banking for his new bank account.
- He followed directions and provided the requested information to set up online banking.
- Two hours later, he was nervous and called the bank—only to find out that his bank account had been cleaned out and closed.

- **Phishing**

- As a rule of thumb, it is a good idea not to click on any link provided in an email and to go directly to the website instead.
- PayPal, whose email address is commonly spoofed for phishing scams, offers the following advice:
  - If PayPal ever sends you an email, they will include your first and last name in the salutation of the email.
  - If you need to enter PayPal's website, type "https:" in the URL instead of "http:" in order to enter on the company's secured server.
  - If you receive a suspicious email, get out of your browser and go back in before proceeding directly to a company website.

- **Phishing**

COMPUTER FRAUD AND ABUSE TECHNIQUES

- In 2004, a phishing-related scam took place in South America with respect to three large South American banks. Once an individual opened the related email, a script was downloaded on their computer. The script would alter the individual's web browser so that if the user entered the URL of one of these three banks, the browser would redirect them to a counterfeit website for that bank. The oblivious user would provide ID and password information, and was instantly set up for a high-tech robbery of his bank account.

- **Phishing**

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Logic time bombs
- Masquerading or impersonation
- Packet sniffers
- Password cracking

- *Consumer Reports* suggests that if you have any questions about the legitimacy of a website, you should try entering the wrong password. A phishing website will typically accept an incorrect password—which cues you that it is a phishing scam.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- **Example of a website produced for a phishing scam.**

COMPUTER FRAUD AND ABUSE TECHNIQUES

Spyware

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:

- Software that monitors computing habits, such as web-surfing habits, and sends the data it gathers to someone else, typically without the user's permission.
  - One type, called *adware* (for advertising-supported software) does two things:
    - Causes banner ads to pop up on your monitor as you surf the net.
    - Collects information about your Web-surfing and spending habits and forwards it to a company gathering the data—often an advertising or large media organization.

COMPUTER FRAUD A

- Perpetrators have devised
- computer fraud and abuse
  - Social engineering
  - Software piracy
  - Spamming
  - **Spyware**

- Usually comes bundled with freeware and shareware downloaded from the Internet.
- May be disclosed in the licensing agreement, but users are unlikely to read it.
- Reputable adware companies claim they don't collect sensitive or identifying data.
  - But there is no way for users to control or limit the activity.
  - It is not illegal, but many find it objectionable.
- Software has been developed to detect and eliminate spyware, but it may also impair the downloaded software.
  - Some is intentionally difficult to uninstall.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - **Social engineering**

- Perpetrators trick employees into giving them information they need to get into the system.
- A perpetrator might call an employee and indicate he is the systems administrator and needs to get the employee's password.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud ar
  - Social engineering
  - Software piracy
  - Spamming
  - Spyware
  - Keystroke loggers
  - Superzapping
  - Trap doors
  - **Trojan horse**

- A set of unauthorized computer instructions planted in an authorized and otherwise properly functioning program.
- Allows the creator to control the victim's computer remotely.
- The code does not try to replicate itself but performs an illegal act at some specific time or when some condition arises.
- Programs that launch denial of service attacks are often Trojan horses.

COMPUT

- Perpetrato
  computer f
  - **Virus**

- Damage may take many forms:
  - Send email with the victim's name as the alleged source.
  - Destroy or alter data or programs.
  - Take control of the computer.
  - Destroy or alter file allocation tables.
  - Delete or rename files or directories.
  - Reformat the hard drive.
  - Change file content.
  - Prevent users from booting.
  - Intercept and change transmissions.
  - Print disruptive images or messages on the screen.
  - Change screen appearance.
- As viruses spread, they take up much space, clog communications, and hinder system performance.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fra
  - **Virus**

- Virus symptoms:
  - Computer will not start or execute
  - Performs unexpected read or write operations
  - Unable to save files
  - Long time to load programs
  - Abnormally large file sizes
  - Slow systems operation
  - Unusual screen activity
  - Error messages

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fra
  - **Virus**

- Viruses are contagious and easily spread from one system to another.
- They are usually spread by:
  - Opening an infected email attachment or file (most common); or
  - Running an infected program.
- Some viruses can mutate, which makes them more difficult to detect and destroy.
- The emails often appear to come from sources like Microsoft and seem very convincing.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - **Virus**

- Viruses attack computers, but any device that is part of the communications network is vulnerable, including:
  - Cell phones
  - Smart phones
  - PDAs

COMPUTER FRAUD AND ABUSE TECHNIQUES

- A worm is similar to a virus except for:
  - A worm is a stand-alone program, while a virus is only a segment of code hidden in a host program or executable file.
  - A worm will replicate itself automatically, while a virus requires a human to do something like open a file.
- Worms often reproduce by mailing themselves to the recipient's mailing list.
- They are not confined to PCs and have infected cell phones in Japan.
- A worm typically has a short but very destructive life.
- It takes little technical knowledge to create worms or viruses; several websites provide instructions.
- Most exploit known software vulnerabilities that can be corrected with a software patch, making it important to install all patches as soon as they are available.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit
  - You receive an email from a friend, apologizing profusely that he/she has previously sent you an email that was infected with a virus.
  - The friend's email gives you instructions to look for and remove the offending virus.
  - You delete the file from your hard drive. The only problem is that the file you just deleted was part of your operating system.
  - Your friend was well-intended and has done the same thing to his/her computer.
  - REMEDY: Before even considering following instructions of this sort, check the list of hoaxes that are available on any virus protection website, such as:
    - www.norton.com
    - www.mcafee.com

nformation Systems Concerns for People

- Privacy – What are the threats to personal privacy and how can we protect our selves?
- Security – How can access to sensitive information be controlled and how can we secure hardware and software?

10-21

Large Databases

- Large organizations are constantly compiling information about us.
- The federal government alone has over 2,000 databases.
- Our **social security numbers** have become a national identification number.
  - The vast majority of forms we fill out today require our social security number.
- For billing purposes, telephone companies compile lists of the calls we make, the numbers called, and so on.
- The reverse directory lists telephone numbers followed by subscriber names.
  - Government authorities and others could easily get the names, addresses, and other details about the persons we call.
- Credit card companies keep similar records.
- Supermarket scanners in grocery checkout counters record what we buy, when we buy it, how much we buy, and the price.
- Publishers of magazines, newspapers, and mail-order catalogs have our names, addresses, phone numbers, and what we order.
- This is just a small example of data contained about us in large databases

Cookies

- A cookie works as follows:
- A user opens a Web browser and selects a site to visit.
- The user's computer sends a request for information to the computer running at the Web site.
- The Web site computer is called the server, since it allows the user's computer to display the Web site.
  - At the same time it sends a cookie – a data file containing information like an encrypted user ID and information about when the user visited and what he did on the site.
- The user's computer receives the cookie and places it in a file on the hard drive.
- Whenever the user goes back to the Web site, the server running the site retrieves the cookie to help identify the user

Types of Cookies

- **Traditional** cookies monitor your activities at a single site.
  - When you leave the site, the cookie becomes dormant.
- **Ad network** or **Adware** cookies monitor your activities across all sites you visit.
  - Once deposited on your hard drive, they are continually active collecting information on your Web activities. Interacts with spyware.
  - These are deposited by organizations that compile and market the information including individual personal profiles, mailing lists, and e-mail addresses.
- There are specialized programs, **called cookie-cutter** programs, that allow users to selectively filter or block the most intrusive ad network cookies while allowing selective traditional cookies to operate.

Spyware

- Wide range of programs that are designed to secretly record and report an individual's activities on the Internet; in addition to Internet Ad cookies, there are also
  - Web bugs (key term) – small programs typically hidden within the HTML code for a Web page or e-mail message and can be used to secretly read e-mail message or work with cookies to collect and report information back to a predefined server on the Web
  - Computer monitoring software (key term)– invasive and dangerous type of spyware; programs record every activity and keystroke made on a computer system including credit card numbers, bank account numbers, and e-mail messages
    - Sniffer programs (key term) and keystroke loggers (key term)– can be deposited on a hard drive without detection from the Web or by someone installing programs directly onto a computer
  - Category of programs known as spy removal programs – designed to detect Web bugs and monitoring software

Why HIPAA?

- The 13-year-old daughter of a hospital employee took a list of patients' names and phone numbers from the hospital when visiting her mother at work.
  - As a joke, she contacted patients and told them they had HIV. (The Washington Post, March 1, 1995)
- Health insurance claim forms blew out of a truck carrying them to a recycling center. The forms scattered on a busy interstate highway during evening rush hour.
  - The insurer quickly sent employees to scoop up forms containing names and personal health information.
  - Company policy stated that the forms should have been shredded. (The Hartford Courant, May 14, 1999)

SECURITY

- Attacks on information and computer resources come from inside and outside the company
- Computer sabotage costs about $10 billion per year
- In general, employee misconduct is more costly than assaults from outside

8-34
McGraw-Hill

Security and Employees

- Statistics on white-collar crime
  - Costs an estimated $400 billion annually
  - Average nonmanagerial embezzlement is $60,000
  - Average managerial embezzlement is $250,000
  - Two-thirds of insider fraud is not reported
  - Of known losses, one-quarter cost more than $1 million

8-35
McGraw-Hill

Security and Computer Criminals

- Threats to computer security are criminals, computer crime, and hazards
- Computer criminals are of five types:
  - Employees
  - Outside users
  - Hackers and crackers
  - Organized crime
  - Terrorists

10-36
Return

Computer Crime

Computer Crimes have tripled in the past two years

- Malicious Programs
  - Viruses
  - Worms
  - Trojan horse
- Denial of service (DoS)
- Internet Scams
- **Theft**
  - **Hardware or software**
  - **Data**
  - **Computer time**
- **Data Manipulation**
  - **Computer Fraud and Abuse Act of 1986**

10-37

Examples of Computer Crimes

Computers as	Inside the Organization	Outside the Organization
Weapons/Tools	• Intellectual property theft • Accessing information on others for personal reasons • Acts of spite or revenge • Acts of extortion • Reading the e-mail of others	• Murder • Theft of information • Embezzlement • Harassment • Extortion • Credit card theft • Cargo theft by diverting shipments
Targets	• Information destruction • Planting destructive code • Stealing customer information • Altering information	• Virus attacks • Denial-of-service attacks • Web defacing • Rerouting network traffic • Crashing servers

Crimes in Which Computers Usually Play a Part

- Illegal gambling
- Forgery
- Money laundering
- Child pornography
- Hate message propagation
- Electronic stalking
- Racketeering
- Fencing stolen goods
- Loan sharking
- Drug trafficking
- Union infiltration

Outside the Organization

- In 2008 the greatest financial loss stemmed from
  - Virus and worm attacks
  - Unauthorized access
  - Theft of hardware
  - Theft of information
  - Malware

Types of Malware

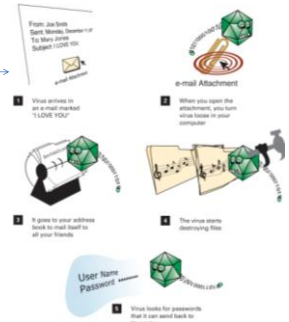
- Malware – software designed to harm you computer or computer security
  - Viruses
  - Worms
  - Misleading e-mail
- Types of Malware
  - Denial-of-service attacks
  - Web defacing
  - Malware bots

Viruses

- ***Computer virus (virus)*** – software that was written with malicious intent to cause annoyance or damage
- ***Worm*** – a computer virus that replicates and spreads itself from computer to computer

The Love Bug Worm

In 2000, a worm shut the Massachusetts state government's e-mail system and caused problems for Capitol Hill and Parliament. It cost approximately $8.7M to fix. What



Stand-Alone Viruses

- ***Spoofing*** – forging of return address on e-mail so that it appears to come from someone other than sender of record
- *Klez* family of worms
  - Introduced spoofing of sender and recipient

Trojan Horse Viruses

- ***Trojan horse virus*** – hides inside other software, usually an attachment or download
- Examples:
  - ***Key logger (key trapper) software*** – program that, when installed on a computer, records every keystroke and mouse click
  - Ping-of-Death DoS attack designed to crash Web sites

Misleading E-mail: Virus Hoax

- Objective is to cause damage to your system
- Virus hoax is an e-mail telling you of a non-existent virus
  - Makes recipients believe that they already have a virus and gives instructions on removal which actually delete a Windows file
  - Often purports to come from Microsoft -Microsoft always sends you to a Web site to find the solution to such a problem

Denial-of-Service Attacks

- ***Denial-of-Service (DoS) attack*** – floods a Web site with so many requests for service that it slows down or crashes
- Objective is to prevent legitimate customers from using Web site

Distributed DoS

- ***Distributed denial-of-service attack (DDoS)*** – attacks from multiple computers that flood a Web site with so many requests for service that it slows down or crashes.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - **Denial of service attacks**

    - An attacker overloads and shuts down an Internet Service Provider's email system by sending email bombs at a rate of thousands per second—often from randomly generated email addresses.
    - May also involve shutting down a web server by sending a load of requests for the web pages.

COMPUTER FRAU

- Perpetrators have dev
  computer fraud and a
  - Denial of service attac

- Carried out as follows:
  - The attacker infects dozens of computers that have broadband Internet access with denial-of-service programs. These infected computers are the *zombies*.
  - The attacker then activates the denial-of-service programs, and the zombies send pings (emails or requests for data) to the target server. The victim responds to each, not realizing they have fictitious return addresses, and waits for responses that don't come.
  - While the victim waits, system performance degrades until the system freezes up or crashes.
  - The attacker terminates the program after an hour or two to limit the victim's ability to trace the source.

COMPUTER FRAUD AND ABUSE TECHNIQUES

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - **Denial of service attacks**

- Experts estimate there as many as 5,000 denial-of-service attacks weekly in the U.S.
- A denial-of-service can cause severe economic damage to its victim or even drive them out of business.

Malware Bots

- ***Bot*** – a computer program that runs automatically.
- ***Malware bots*** – bots that are used for fraud, sabotage, denial-of-service attacks, or some other malicious purpose
- ***Zombies (or drones)*** – malware-bot-infected computers

Botnets and Rootkits

- ***Botnet*** – a network of malware-bot infected computers
- ***Rootkit*** – software that gives you administrator rights to a computer or network and whose purpose is to allow you to conceal processes, files, or system data from the operating system

Web Defacing

- ***Web defacing*** – maliciously changing another's Web site
- Electronic equivalent of graffiti

Other Hazards

- Natural hazards
  - Fires & floods
  - Winds
  - Hurricanes
  - Tornadoes
  - Earthquakes

- **Civil strife and terrorism**
  - **Wars, riots and terrorist acts**
- **Technological failures**
  - **Voltage surge**
    - **Use surge protector**
    - **Hard disk crashes**
- **Human errors**

10-57

Measures to Protect Computer Security

- Encrypting messages
- Restricting access
- Anticipating disasters
- Backing up data

How to Dispose of Your Computer

- If you are disposing of your computer along with its hard drive:
  - delete personal files,
  - defrag your computer,
  - and run a disk cleanup