

Cyber Forensics

Understanding Cyber Forensics-
Emerging IT Devices

Dr. Pradeepthi K V
Assistant Professor

C R Rao Advanced Institute of Mathematics, Statistics and Computer Science,
University of Hyderabad Campus,
Gachibowli, Hyderabad.

What is Cyber Forensics ?

- Definition: *Cyber forensics involves collecting, analyzing, and conserving digital evidence to investigate cybercrimes.*
- Importance: *Highlight its role in identifying criminals and reconstructing digital events.*

Formal Definition:

The application of computer science and investigative procedures for a legal purpose involving the

- analysis of digital evidence (**binary form**)
- after proper **search authority, chain of custody,**
- **validation** with mathematics (**hash function**),
- use of **validated tools, repeatability,**
- **reporting** and possible expert **presentation in court of law** .

Significance of Cyber Forensics

- **Definition of Cyber Forensics:** Cyber forensics refers to the methodologies and processes employed to collect, preserve, analyze, and present digital evidence in a manner that is legally admissible. It encompasses a broad spectrum of investigative practices across multiple technological platforms.
- **Importance in IT Security:** Cyber forensics is pivotal for enhancing IT security. It not only aids in the identification of cybersecurity breaches and attacks but also plays a crucial role in understanding attack vectors, which is essential for formulating effective prevention strategies.
- **Overview of Emerging Devices:** The field of cyber forensics must adapt to the rising prevalence of innovative devices. Mobile phones, IoT devices, and wearables are now prime sources of digital evidence, each presenting unique challenges and opportunities for forensic analysis.



Crisis

- Internet has grown very fast and security has lagged behind.
- Legions of hackers have emerged as impedance to entering the hackers club is low.
- It is hard to trace the perpetrator of cyber attacks since the real identities are camouflaged
- It is very hard to track down people because of the ubiquity of the network.
- Large scale failures of internet can have a catastrophic impact on the economy which relies heavily on electronic transactions



Computer Crime - The Beginning

- In 1988 a "worm program" written by a college student shut down about 10 percent of computers connected to the Internet. This was the beginning of the era of cyber attacks.
- Today we have about 10,000 incidents of cyber attacks which are reported and the number grows.

Computer Crime - 1994



- A 16-year-old music student called Richard Pryce, better known by the hacker alias Datastream Cowboy, is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, Nasa and the Korean Atomic Research Institute. His online mentor, "Kuji", is never found.
- Also this year, a group directed by Russian hackers broke into the computers of Citibank and transferred more than \$10 million from customers' accounts. Eventually, Citibank recovered all but \$400,000 of the pilfered money.

Computer Crime - 1995



-
- In February, Kevin Mitnick is arrested for a second time. He is charged with stealing 20,000 credit card numbers. He eventually spends four years in jail and on his release his parole conditions demand that he avoid contact with computers and mobile phones.
 -
 - On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Mr Pile, who called himself the Black Baron, was sentenced to 18 months in jail.
 - The US General Accounting Office reveals that US Defense Department computers sustained 250,000 attacks in 1995.

Computer Crime - 1999



- In March, the Melissa virus goes on the rampage and wreaks havoc with computers worldwide. After a short investigation, the FBI tracks down and arrests the writer of the virus, a 29-year-old New Jersey computer programmer, David L Smith.
- More than 90 percent of large corporations and government agencies were the victims of computer security breaches in 1999

Computer Crime - 2000



-
- In February, some of the most popular websites in the world such as Amazon and Yahoo are almost overwhelmed by being flooded with bogus requests for data.
 - In May, the ILOVEYOU virus is unleashed and clogs computers worldwide. Over the coming months, variants of the virus are released that manage to catch out companies that didn't do enough to protect themselves.
 - In October, Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen.

Why Security?



-
- Some of the sites which have been compromised
 - U.S. Department of Commerce
 - NASA
 - CIA
 - Greenpeace
 - Motorola
 - UNICEF
 - Church of Christ ...
 - Some sites which have been rendered ineffective
 - Yahoo
 - Microsoft
 - Amazon ...

Understanding the Need for Security Measures



Basic Security Concepts

- Threats
 - Anything that can harm a computer
 - Vulnerabilities are weaknesses in security
 - Security attempts to neutralize threats



Basic Security Concepts

- Degrees of harm
 - ☐ Level of potential damage
 - ☐ Include all parts of system
 - ❖ Potential data loss
 - ❖ Loss of privacy
 - ❖ Inability to use hardware
 - ❖ Inability to use software



Basic Security Concepts

❑ Countermeasures

- Steps taken to block a threat
- Protect the data from theft
- Protect the system from theft



Threats To Users

- Identity Theft
 - Impersonation by private information
 - Thief can 'become' the victim
 - Reported incidents rising
 - Methods of stealing information
 - Shoulder surfing
 - Snagging
 - Dumpster diving
 - Social engineering
 - High-tech methods



Threats To Users

- Loss of privacy
 - Personal information is stored electronically
 - Purchases are stored in a database
 - Data is sold to other companies
 - Public records on the Internet
 - Internet use is monitored and logged
 - None of these techniques are illegal



Threats to Users

- Cookies
 - Files delivered from a web site
 - Originally improved a site's function
 - Cookies now track history and passwords
 - Browsers include cookie blocking tools



Threats to Users

- Spyware
 - Software downloaded to a computer
 - Designed to record personal information
 - Typically undesired software
 - Hides from users
 - Several programs exist to eliminate



Threats to Users

- Web bugs
 - Small programs embedded in gif images
 - Gets around cookie blocking tools
 - Companies use to track usage
 - Blocked with spyware killers



Threats to Users

- Spam
 - Unsolicited commercial email
 - Networks and PCs need a spam blocker
 - Stop spam before reaching the inbox
 - Spammers acquire addresses using many methods
 - CAN-SPAM Act passed in 2003



Threats to Hardware

- Affect the operation or reliability
- Power-related threats
 - Power fluctuations
 - Power spikes or browns out
 - Power loss
 - Countermeasures
 - Surge suppressors
 - Line conditioners
 - Uninterruptible power supplies
 - Generators



Threats to Hardware

- Theft and vandalism
 - Thieves steal the entire computer
 - Accidental or intentional damage
 - Countermeasures
 - Keep the PC in a secure area
 - Lock the computer to a desk
 - Do not eat near the computer
 - Watch equipment
 - Chase away loiterers
 - Handle equipment with care



Threats to Hardware

- Natural disasters
 - Disasters differ by location
 - Typically result in total loss
- Disaster planning
 - Plan for recovery
 - List potential disasters
 - Plan for all eventualities
 - Practice all plans



Threats to Data

- The most serious threat
 - Data is the reason for computers
 - Data is very difficult to replace
 - Protection is difficult
 - Data is intangible



Threats to Data

- Cyber terrorism
 - Attacks made at a nations information
 - Targets include power plants
 - Threat first realized in 1996
 - Organizations combat cyber terrorism
 - Computer Emergency Response Team (CERT)
 - Department of Homeland Security



Why do Hackers Attack?

- Because they can
 - A large fraction of hacker attacks have been pranks
- Financial Gain
- Espionage
- Venting anger at a company or organization
- Terrorism



Hacking

Definition:

Hacking is an attempt to exploit a computer system or a private network inside a computer.

Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose. They can destroy, steal or even prevent authorized users from accessing the system.



Types of Hackers

Black Hat Hacker



White Hat Hacker



Gray Hat Hacker



Black-hat

Unethical Hacker or a Security Cracker. They hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.



• White hat

- Ethical Hackers or a Penetration Tester.
- good guys of the hacker world.
- use the same technique used by the black hat hackers.
- hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system.
- focus on security and protecting IT system.
- White hat hacking is legal.

• Gray hat Hackers

- Hybrid between Black hat Hackers and White hat hackers.
- hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.
- tell the administrator of that system.
- illegal because they test the security of the system that they do not have permission to test.
- Grey hat hacking is sometimes acted legally and sometimes not.

Types of Hacking

- 1.Social Engineering & Phishing
- 2.Malware-Injecting Devices
- 3.Missing Security Patches
- 4.Cracking Passwords
- 5.Distributed Denial-of-Service (DDoS)



Types of Hacker Attack

- Active Attacks
 - Denial of Service
 - Breaking into a site
 - Intelligence Gathering
 - Resource Usage
 - Deception
- Passive Attacks
 - Sniffing
 - Passwords
 - Network Traffic
 - Sensitive Information
 - Information Gathering



Modes of Hacker Attack

- Over the Internet
- Over LAN
- Locally
- Offline
- Theft
- Deception



Web Spoofing



-
- Basic
 - Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com
 - Man-in-the-Middle Attack
 - Attacker acts as a proxy between the web server and the client
 - Attacker has to compromise the router or a node through which the relevant traffic flows
 - URL Rewriting
 - Attacker redirects web traffic to another site that is controlled by the attacker
 - Attacker writes his own web site address before the legitimate link
 - Tracking State
 - When a user logs on to a site a persistent authentication is maintained
 - This authentication can be stolen for masquerading as the user

Web Spoofing - Tracking State



-
- Web Site maintains authentication so that the user does not have to authenticate repeatedly
 - Three types of tracking methods are used:
 1. Cookies: Line of text with ID on the users cookie file
 - Attacker can read the ID from users cookie file
 2. URL Session Tracking: An id is appended to all the links in the website web pages.
 - Attacker can guess or read this id and masquerade as user
 3. Hidden Form Elements
 - ID is hidden in form elements which are not visible to user
 - Hacker can modify these to masquerade as another user

Session Hijacking

Definition:

1. Process of taking over an existing active session
-

Modus Operandi:

1. User makes a connection to the server by authenticating using his user ID and password.
2. After the users authenticate, they have access to the server as long as the session lasts.
3. Hacker takes the user offline by denial of service
4. Hacker gains access to the user by impersonating the user



Denial of Service (DOS) Attack



Definition:

Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it.

Types:

1. Crashing the system or network
 - Send the victim data or packets which will cause system to crash or reboot.
2. Exhausting the resources by flooding the system or network with information
 - Since all resources are exhausted others are denied access to the resources
3. Distributed DOS attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks

Denial of Service (DOS) Attack

Types:

1. Ping of Death
2. SSping
3. Land
4. Smurf
5. SYN Flood
6. CPU Hog
7. Win Nuke
8. RPC Locator
9. Jolt2
10. Bubonic
11. Microsoft Incomplete TCP/IP Packet Vulnerability
12. HP Openview Node Manager SNMP DOS Vulnerability
13. Netscreen Firewall DOS Vulnerability
14. Checkpoint Firewall DOS Vulnerability



Password Attacks - Process

- Find a valid user ID
- Create a list of possible passwords
- Rank the passwords from high probability to low
- Type in each password
- If the system allows you in - success !
- If not, try again, being careful not to exceed password lockout (the number of times you can guess a wrong password before the system shuts down and won't let you try any more)



Password Attacks - Types



-
- **Dictionary Attack**
 - Hacker tries all words in dictionary to crack password
 - 70% of the people use dictionary words as passwords
 - **Brute Force Attack**
 - Try all permutations of the letters & symbols in the alphabet
 - **Hybrid Attack**
 - Words from dictionary and their variations used in attack
 - **Social Engineering**
 - People write passwords in different places
 - People disclose passwords naively to others
 - **Shoulder Surfing**
 - Hackers slyly watch over peoples shoulders to steal passwords
 - **Dumpster Diving**
 - People dump their trash papers in garbage which may contain information to crack passwords

System Hacking

- System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information.
- The malware and the attacker identify and exploit the weaknesses of the computer system to gain unauthorized access.



Hacking Web Servers

- When practicing ethical hacking, a hacker is searching for vulnerabilities. An ethical hacker has several reasons to try gaining unauthorized control of a web server, though the primary reason is to test a server and its software for vulnerabilities.
- By using the same tools and methods that malicious attackers rely on, you can attempt to gain access to a server. If successful, you can identify necessary fixes and upgrades that must be performed to improve security and to detect and respond to malicious activity.



Hacking Methods

- Gathering intelligence
- Reconnaissance tools
- Hacking in
- Backdoors and covered tracks



What is a social engineering attack?

- an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.





What is a phishing attack?

- Phishing is a form of social engineering.
- Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.
- For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

What is a vishing attack?

- Vishing is the social engineering approach that leverages voice communication.



What is a smishing attack?

- Smishing is a form of social engineering that exploits SMS, or text, messages.



What are common indicators of phishing attempts?

- Suspicious sender's address
- Generic greetings and signature
- Spoofed hyperlinks and websites
- Spelling and layout
- Suspicious attachments



How do you avoid being a victim?

- Be suspicious of unsolicited phone calls
- Do not reveal personal or financial information in email,
- Don't send sensitive information over the internet before checking a website's security.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.



What do you do if you think you are a victim?

- report it to the appropriate people
- contact your financial institution immediately
- Watch for other signs of identity theft.



Social Engineering -- Examples

1. On the phone
2. In the office
3. Online



Social engineering attack techniques

- Baiting
- Scareware
- Pretexting
- Phishing
- Spear phishing



Social engineering prevention

- Don't open emails and attachments from suspicious sources
- Use multifactor authentication
- Be wary of tempting offers
- Keep your antivirus/antimalware software updated



Security of Information Assets

Learning Objectives

- Security threats to
 - data
 - hardware and
 - users
- common types of hacking
- protective measures





IT Security

- ❖ IT security is the protection of computer systems and networks from **information disclosure**, **theft of** or **damage** to their hardware, software, or electronic data, as well as from the **disruption or misdirection** of the services they provide.
- ❖ IT security performs four important functions for an organization:
 - Protects the organization's ability to function
 - Enables the safe operation of applications implemented on the organization's IT systems
 - Protects the data the organization collects and uses
 - Safeguards the technology assets in use at the organization

IT Security: Features

Confidentiality:-

- Assurance that information is shared only among authorized persons or organizations.

Integrity:-

- Assurance that the information is authentic and complete.
- Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Availability:-

- Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.



Vulnerabilities

- A **vulnerability** is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system.
- Vulnerabilities are classified according to the asset class they are related to:-
 - ❖ **Hardware:-** Susceptibility to humidity/dust ; Unprotected storage; Over-heating.
 - ❖ **Software:-** Insufficient testing; insecure coding; lack of audit trail; Design flaw.
 - ❖ **Network:-** Unprotected communication lines; Insecure network architecture.
 - ❖ **Personnel:-** Inadequate recruiting process; Inadequate security awareness; insider threat
 - ❖ **Physical site:-** Area subject to natural disasters (e.g. flood, earthquake); interruption to power source
 - ❖ **Organizational:-** Lack of regular audits; lack of continuity plans;



Threats

- A **threat** is a potential negative action or event facilitated by a **vulnerability** that results in an unwanted impact to a computer system or application.
- Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- A **countermeasure** is any step you take to ward off a threat to protect user, data, or computer from harm.
- Various Security threats:-
 - ❖ **Users:-** Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
 - ❖ **Hardware:-** Power-related problems; theft; vandalism; and natural disasters.
 - ❖ **Data:-** Malwares; Hacking; Cybercrime; and Cyber-terrorism.



Threats to Information Security

TABLE 2-1 Threats to Information Security⁴

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies



Threats(Keywords)

- ❖ Spam:-Unsolicited commercial e-mail/Junk e-mail
- ❖ Cookie:- Small text file that a Web server put on computer
- ❖ Web Bugs:-a small gif embedded in webpage/email
- ❖ **Malwares:-Malicious Software**
 - ❖ Virus(require Some executables), Worms(Self executables), Spyware, Trojan Horses, Botnet (Robot Network)
- ❖ Shoulder Surfing
- ❖ Hacking:-
 - ❖ Sniffing:- finding user's password(Password Sharing, Password Guessing or Password Capture
 - ❖ Social Engineering:- Dumpster Diving, Phishing(Email) & Vishing(Phone Calls)
 - ❖ Spoofing
- ❖ DDoS:-Distributed Denial of Services.
- ❖ Cybercrime; and Cyber-terrorism.



Attack Descriptions

- **Denial-of-service (DoS)**

- attacker sends a large number of connection or information requests to a target
- so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
- may result in a system crash, or merely an inability to perform ordinary functions

- **Distributed Denial-of-service (DDoS)**

- an attack in which a coordinated stream of requests is launched against a target from many locations at the same time



In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

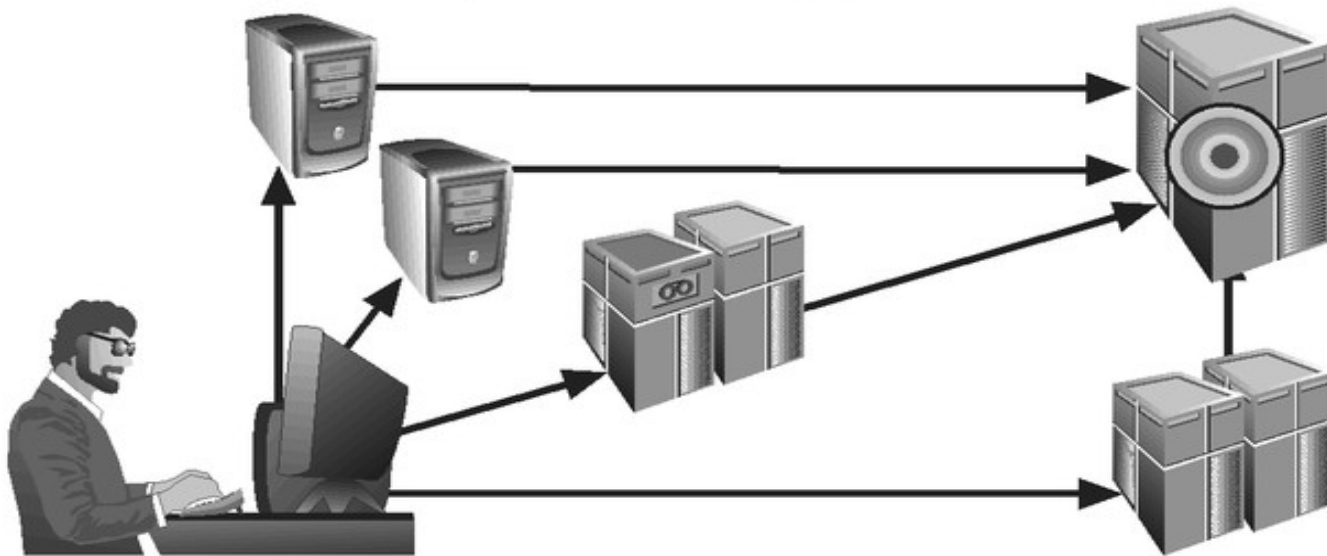


FIGURE 2-9 Denial-of-Service Attacks

Attack Descriptions

- **Spoofing** - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network



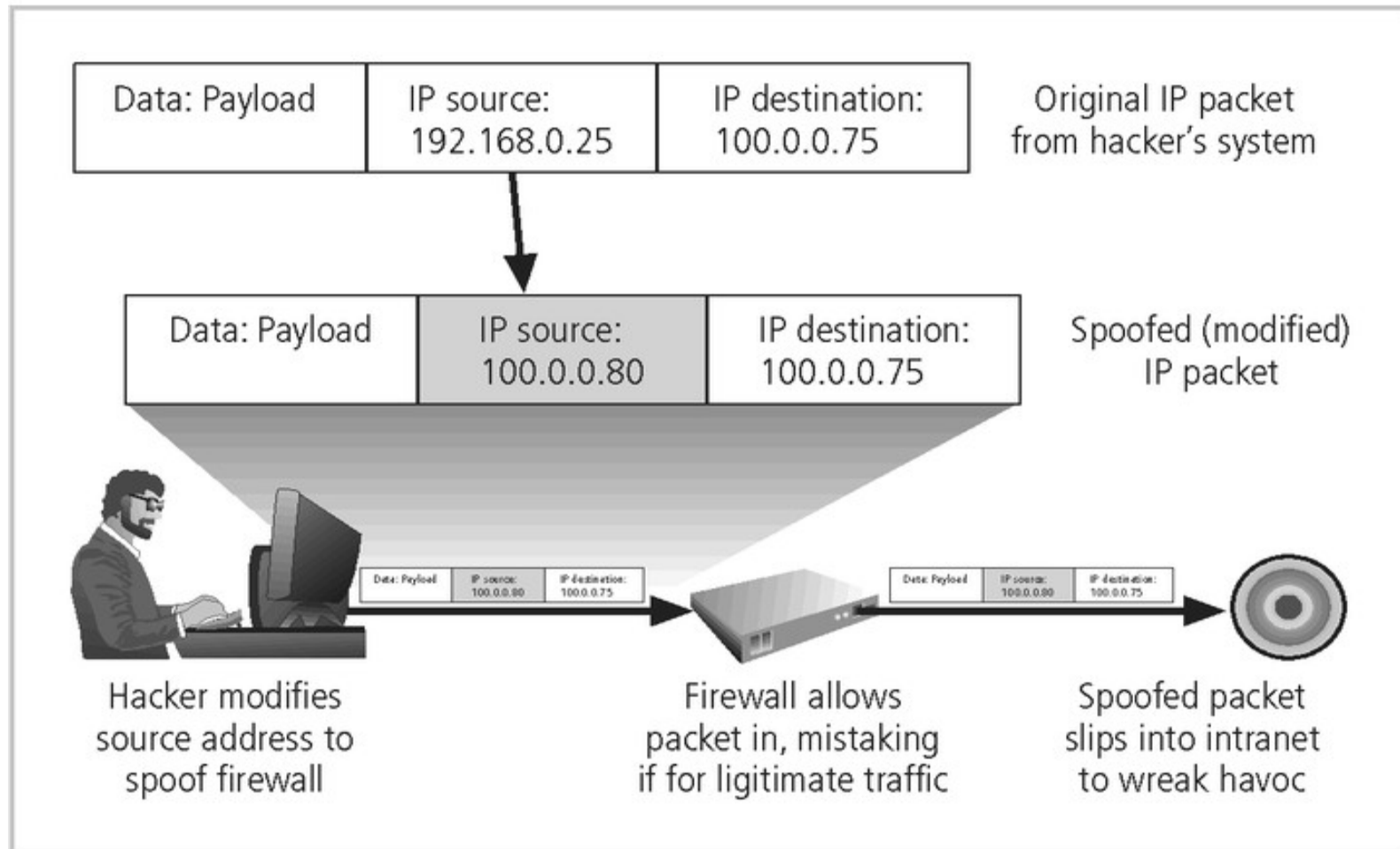


FIGURE 2-10 IP Spoofing



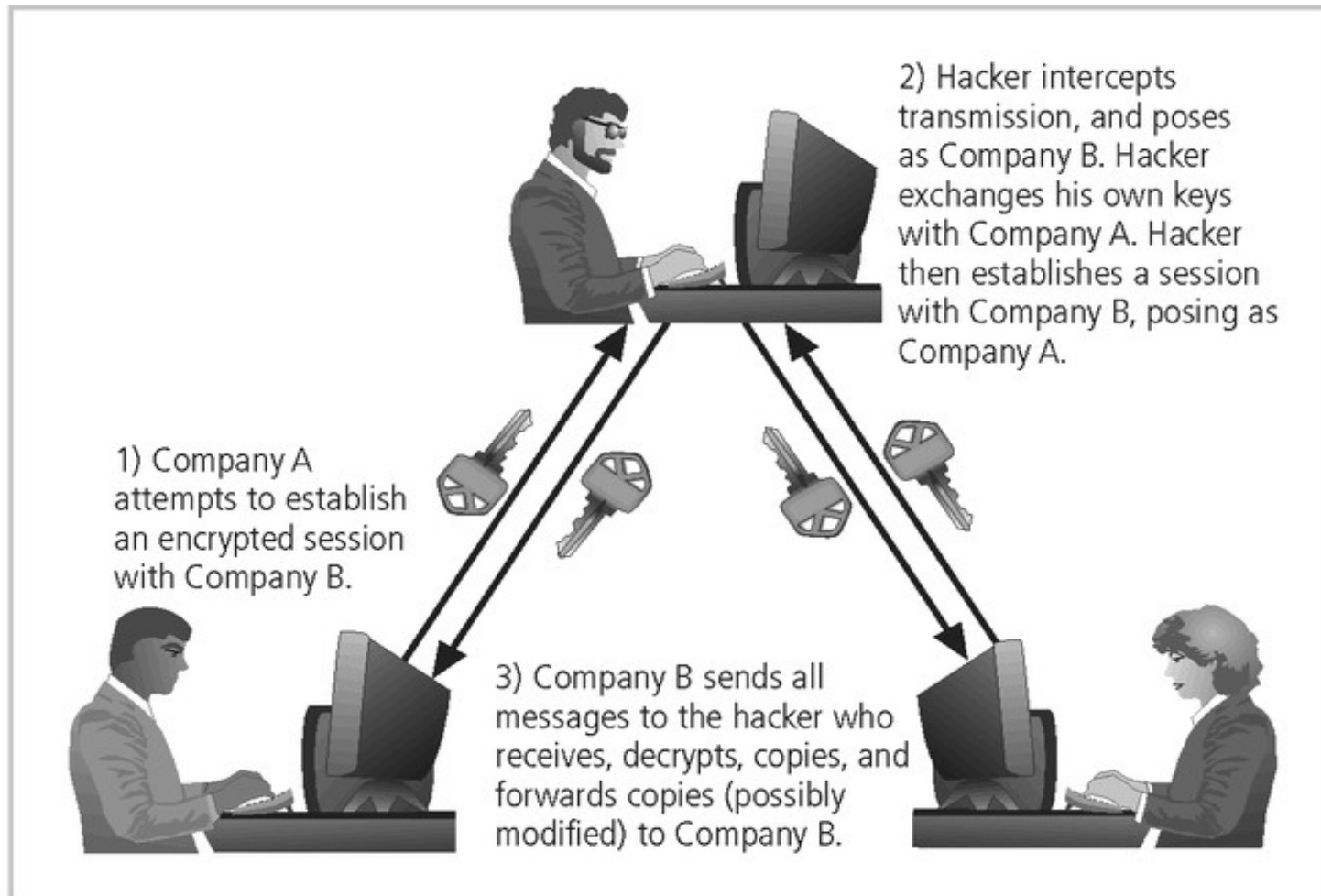


FIGURE 2-11 Man-in-the-Middle Attack



1. Bolster Access Control

- by using a strong password system. You should have a mix of uppercase and lower case letters, numbers, and special characters.
- Also, always reset all default passwords.
- Finally, create a strong access control policy.

2. Keep All Software Updated

- From anti-virus software to computer operating systems, ensure your software is updated.
- When a new version of software is released, the version usually includes fixes for security vulnerabilities.
- Manual software updates can be time-consuming. Use automatic software updates for as many programs as possible.



3. Standardize Software

- Keep your systems protecting by standardizing software like Operating system, Browser, Media player, Plug-in.
- Ensure that users cannot install software onto the system without approval.

4. Use Network Protection Measures

- Install a firewall
- Ensure proper access controls
- Use IDS/IPS to track potential packet floods
- Use network segmentation
- Use a virtual private network (VPN)
- Conduct proper maintenance



5. Employee Training

- Sometimes external threats are successful because of an insider threat. The weakest link in data protection can be your own employees.
- Ensure your employees understand network security.
- Employees should be able to identify threats.
- They should also know who to contact to avoid a security breach

6. Schedule backups

- You can schedule backups to external hard drives or in the cloud in order to keep your data stored safely.
- The right frequency is weekly but you can do incremental backups every few days.



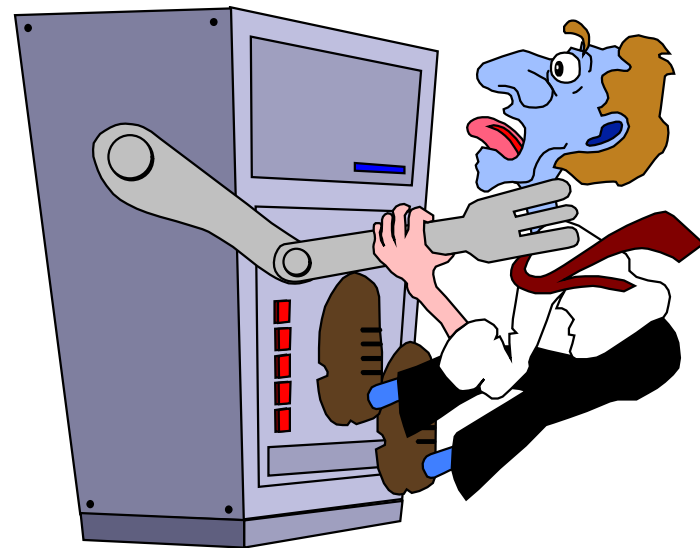
Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
 - Inexperience
 - Improper training
 - Incorrect assumptions
 - Other circumstances
- Employees are greatest threats to information security - They are closest to the organizational data



Acts of Human Error or Failure

- Employee mistakes can easily lead to the following:
 - revelation of classified data
 - entry of erroneous data
 - accidental deletion or modification of data
 - storage of data in unprotected areas
 - failure to protect information
- Many of these threats can be prevented with controls



Compromises to Intellectual Property

- Intellectual property is “the ownership of ideas and control over the tangible or virtual representation of those ideas”
- Many organizations are in business to create intellectual property
 - trade secrets
 - copyrights
 - trademarks
 - patents



Compromises to Intellectual Property

- Most common IP breaches involve software piracy
- Watchdog organizations investigate:
 - Software & Information Industry Association (SIIA)
 - Business Software Alliance (BSA)
- Enforcement of copyright has been attempted with technical security mechanisms



Espionage/Trespass

- Broad category of activities that breach confidentiality
 - Unauthorized accessing of information
 - Competitive intelligence vs. espionage
 - Shoulder surfing can occur any place a person is accessing confidential information
- Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace
- Hackers use skill, guile, or fraud to steal the property of someone else



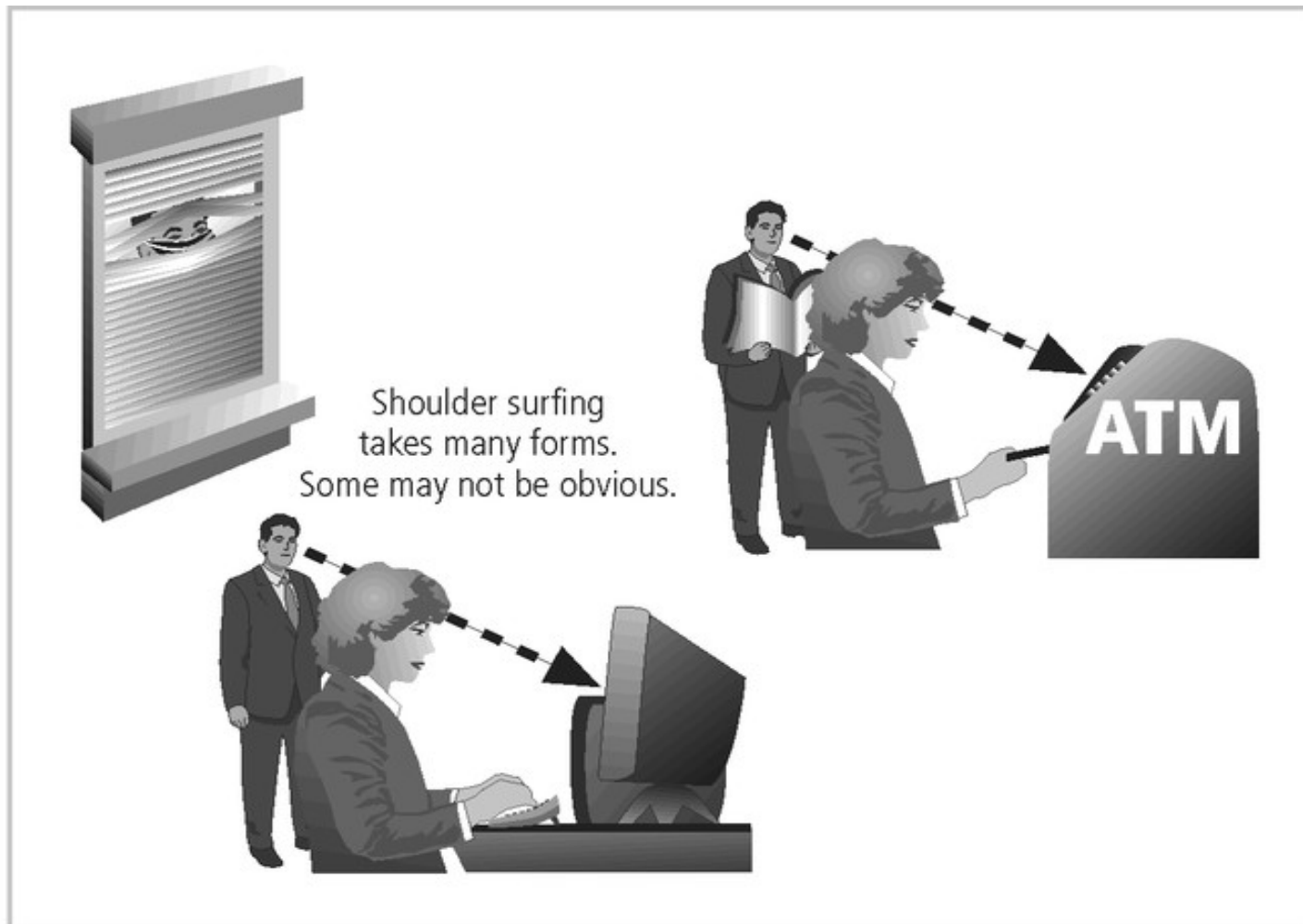


FIGURE 2-2 Shoulder Surfing





Espionage/Trespass

- Generally two skill levels among hackers:
 - Expert hacker
 - develops software scripts and codes exploits
 - usually a master of many skills
 - will often create attack software and share with others
 - Script kiddies
 - hackers of limited skill
 - use expert-written software to exploit a system
 - do not usually fully understand the systems they hack
- Other terms for system rule breakers:
 - Cracker - an individual who “cracks” or removes protection designed to prevent unauthorized duplication
 - Phreaker - hacks the public telephone network



Traditional hacker profile:
Age 13-18, male with limited
parental supervision spends all his
free time at the computer



Modern hacker profile:
Age 12-60, male or female, unknown
background, with varying technological
skill levels; may be internal or external
to the organization

FIGURE 2-3 Hacker Profiles



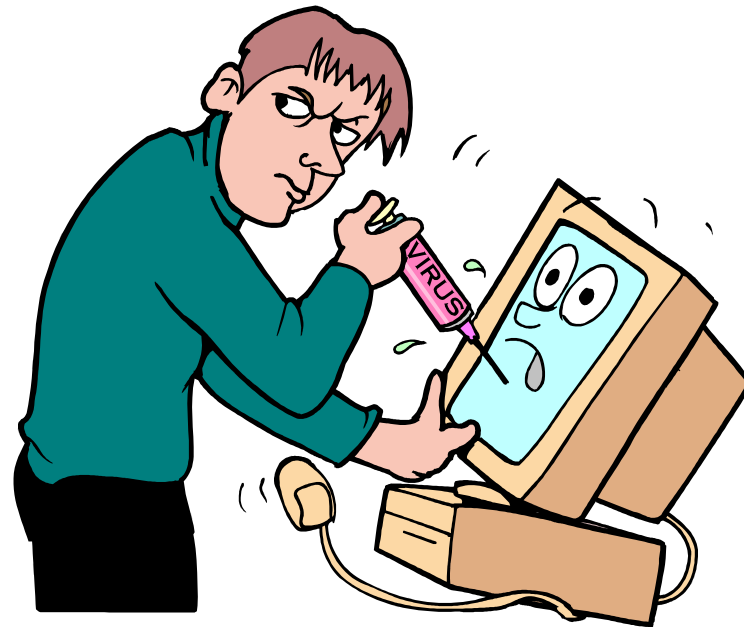
Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use
- Extortion found in credit card number theft



Sabotage or Vandalism

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations - the most extreme version is cyber-terrorism





Deliberate Acts of Theft

- Illegal taking of another's property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner's knowledge
- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred



Internet Service Issues

- Loss of Internet service can lead to considerable loss in the availability of information
 - organizations have sales staff and telecommuters working at remote locations
- When an organization outsources its web servers, the outsourcer assumes responsibility for
 - All Internet Services
 - The hardware and operating system software used to operate the web site



Communications and Other Services

- Other utility services have potential impact
- Among these are
 - telephone
 - water & wastewater
 - trash pickup
 - cable television
 - natural or propane gas
 - custodial services
- The threat of loss of services can lead to inability to function properly

Power Irregularities

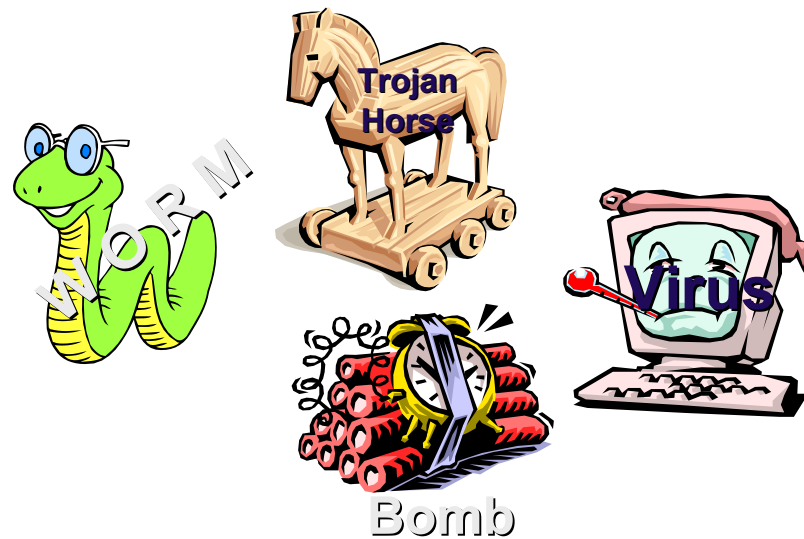
Voltage levels can increase, decrease, or cease:

- spike - momentary increase
 - surge - prolonged increase
 - sag - momentary low voltage
 - brownout - prolonged drop
 - fault - momentary loss of power
 - blackout - prolonged loss
- Electronic equipment is susceptible to fluctuations, controls can be applied to manage power quality



Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware
 - Designed to damage, destroy, or deny service to the target systems
- Includes:
 - macro virus
 - boot virus
 - worms
 - Trojan horses
 - logic bombs
 - back door or trap door
 - denial-of-service attacks
 - polymorphic
 - hoaxes



Deliberate Software Attacks

- Virus is a computer program that attaches itself to an executable file or application.
- It can replicate itself, usually through an executable program attached to an e-mail.
- The keyword is “attaches”. A virus can not stand on its own.
- You must prevent viruses from being installed on computers in your organizations.



Deliberate Software Attacks

- There is no foolproof method of preventing them from attaching themselves to your computer
- Antivirus software compares virus signature files against the programming code of known viruses.
- Regularly update virus signature files is crucial.



Deliberate Software Attacks

- A worm is a computer program that replicates and propagates itself without having to attach itself to a host.
- Most infamous worms are Code Red and Nimda.
- Cost businesses millions of dollars in damage as a result of lost productivity
- Computer downtime and the time spent recovering lost data, reinstalling programming's, operating systems, and hiring or contracting IT personnel



Deliberate Software Attacks

- Trojan Programs disguise themselves as useful computer programs or applications and can install a backdoor or rootkit on a computer.
- Backdoors or rootkits are computer programs that give attackers a means of regaining access to the attacked computer later.



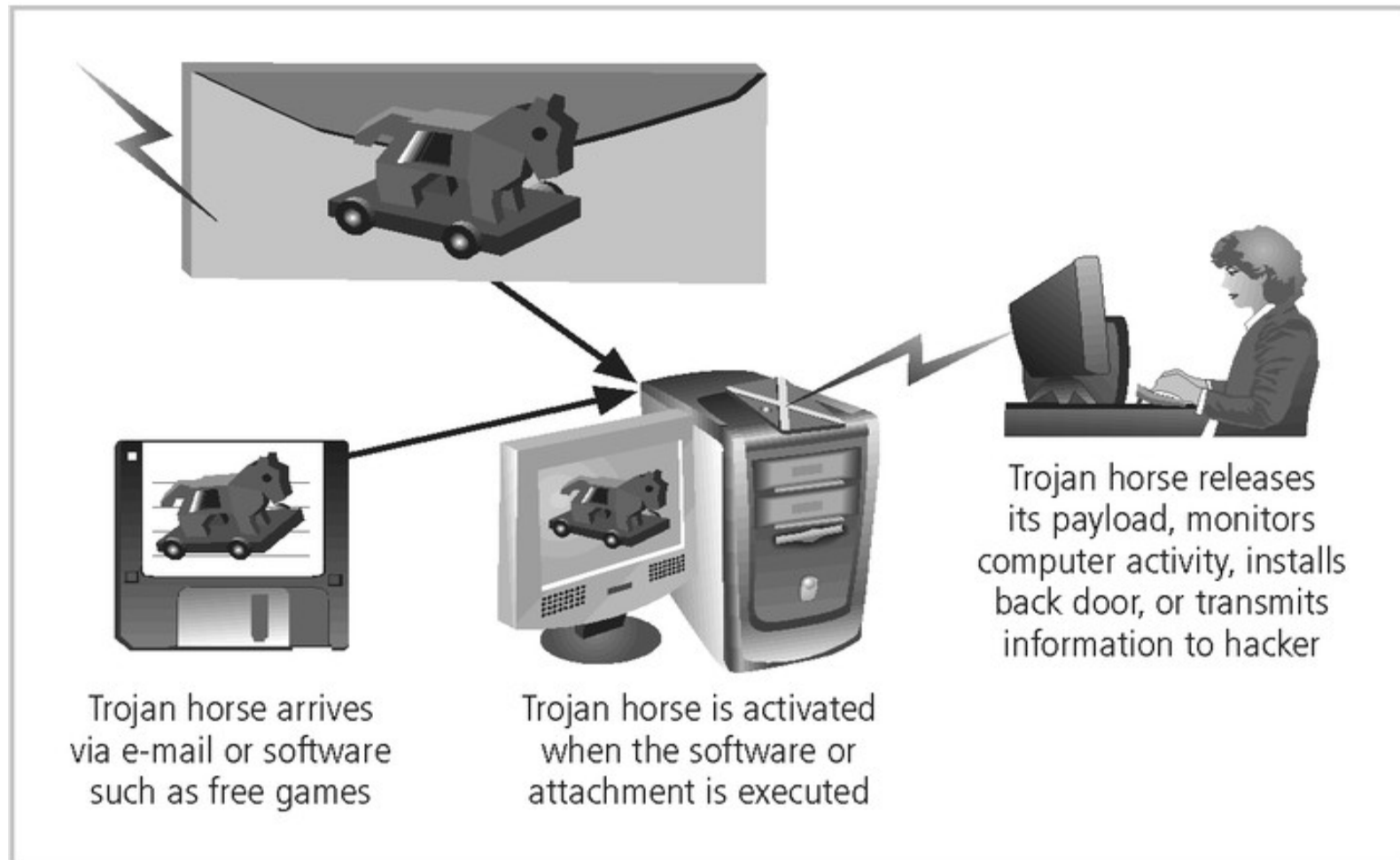


FIGURE 2-8 Trojan Horse Attack



Deliberate Software Attacks

Challenges:

- Trojan programs that use common ports, such as TCP 80, or UDP 53, are more difficult to detect.
- Many software firewalls can recognize port-scanning program or information leaving a questionable port.
- However, they prompt user to allow or disallow, and users are not aware.
- Educate your network users.
- Many Trojan programs use standard ports to conduct their exploits.



Deliberate Software Attacks

- **Spyware**

- A Spyware program sends info from the infected computer to the person who initiated the spyware program on your computer
- Spyware program can register each keystroke entered.
- www.spywareguide.com

- **Adware**

- Main purpose is to determine a user's purchasing habits so that Web browsers can display advertisements tailored to that user.
 - Slow down the computer it's running on.
 - Adware sometimes displays a banner that notifies the user of its presence
- Both programs can be installed without the user being aware of their presence



Protecting against Deliberate Software Attacks

- **Educating Your Users**

- Many U.S. government organizations make security awareness programs mandatory, and many private-sector companies are following their example.
- Email monthly security updates to all employees.
- Update virus signature files as soon as possible.
- Protect a network by implementing a firewall.

- **Avoiding Fear Tactics**

- Your approach to users or potential customers should be promoting awareness rather than instilling fear.
- When training users, be sure to build on the knowledge they already have.



TABLE 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
Shares	Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems
Simple Network Management Protocol (SNMP)	In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of





Attack Descriptions

- **IP Scan and Attack** - Compromised system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits
- **Web Browsing** - If the infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected
- **Virus** - Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection



Attack Descriptions

- **Unprotected Shares** - using file shares to copy viral component to all reachable locations
- **Mass Mail** - sending e-mail infections to addresses found in address book
- **Simple Network Management Protocol** - SNMP vulnerabilities used to compromise and infect
- **Hoaxes** - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached



Attack Descriptions

- **Back Doors** - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- **Password Crack** - Attempting to reverse calculate a password
- **Brute Force** - The application of computing and network resources to try every possible combination of options of a password
- **Dictionary** - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

Attack Descriptions

- **Denial-of-service (DoS)** -

- attacker sends a large number of connection or information requests to a target
 - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
 - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS)** - an attack in which a coordinated stream of requests is launched against a target from many locations at the same time



In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

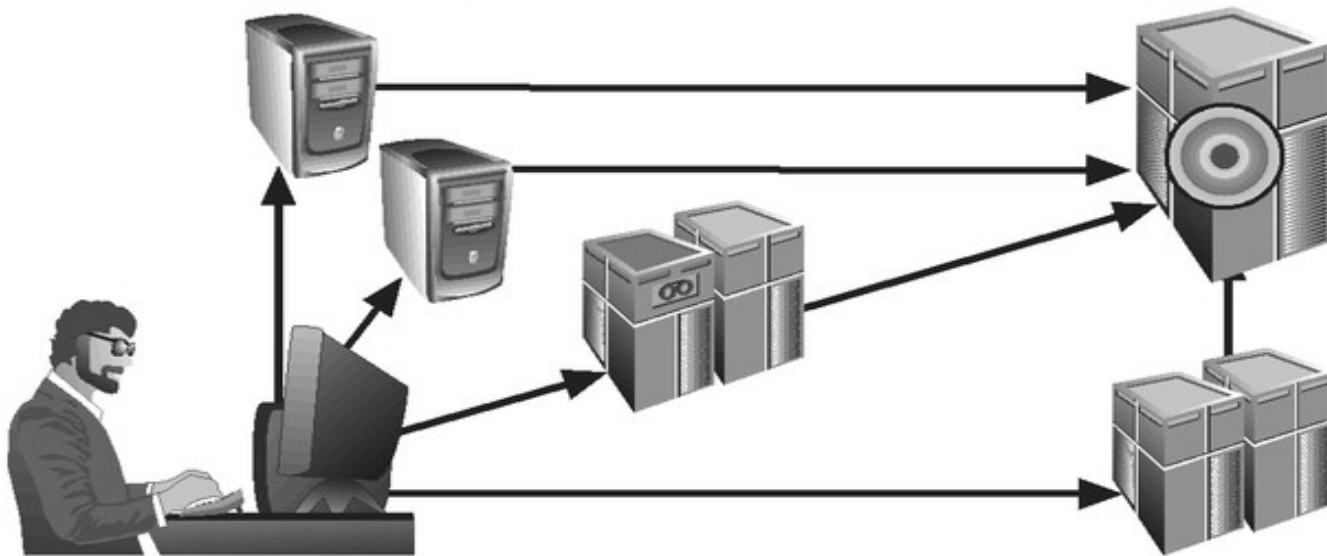


FIGURE 2-9 Denial-of-Service Attacks

Attack Descriptions



- **Spoofing** - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network
- **Spam** - unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

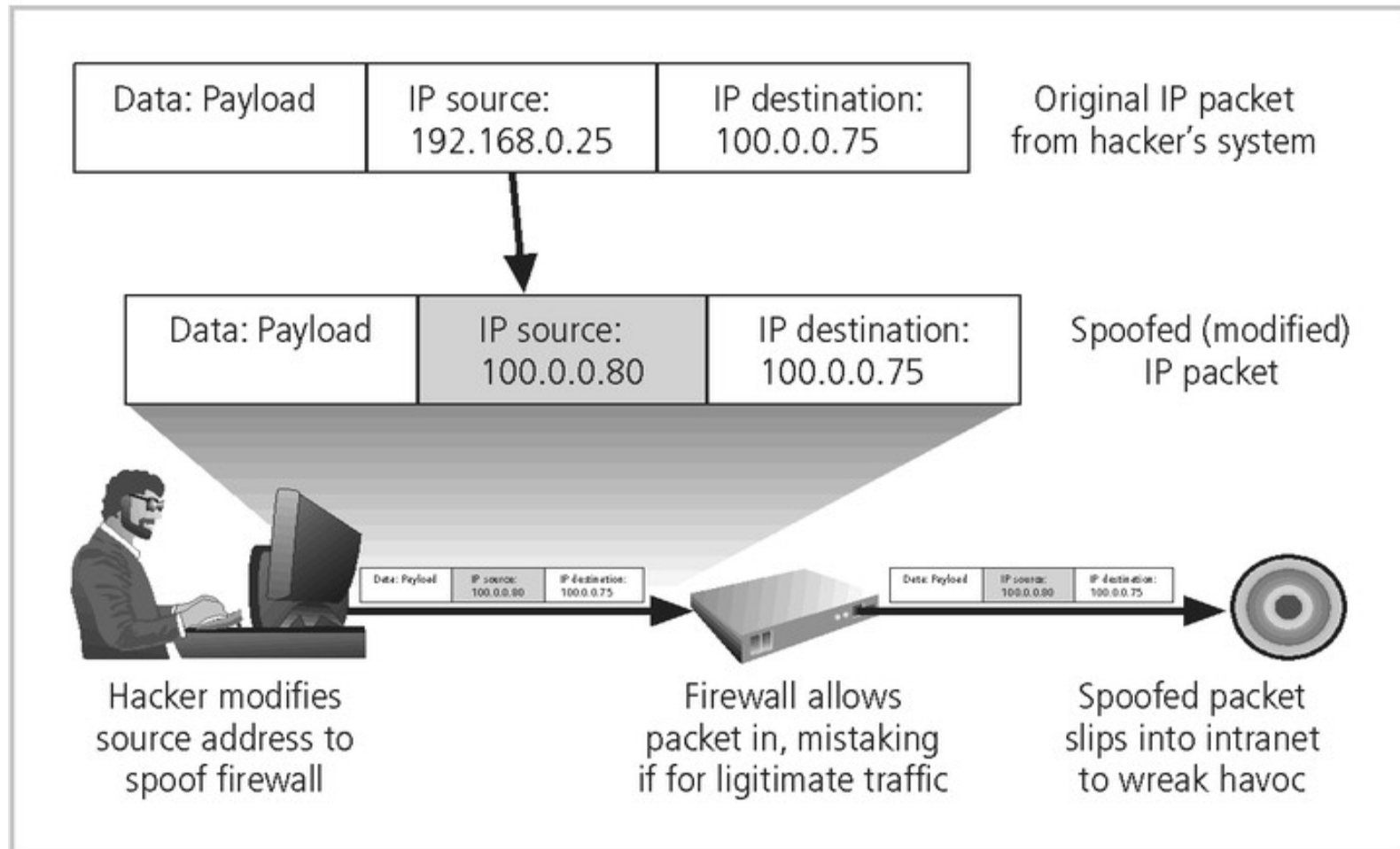


FIGURE 2-10 IP Spoofing



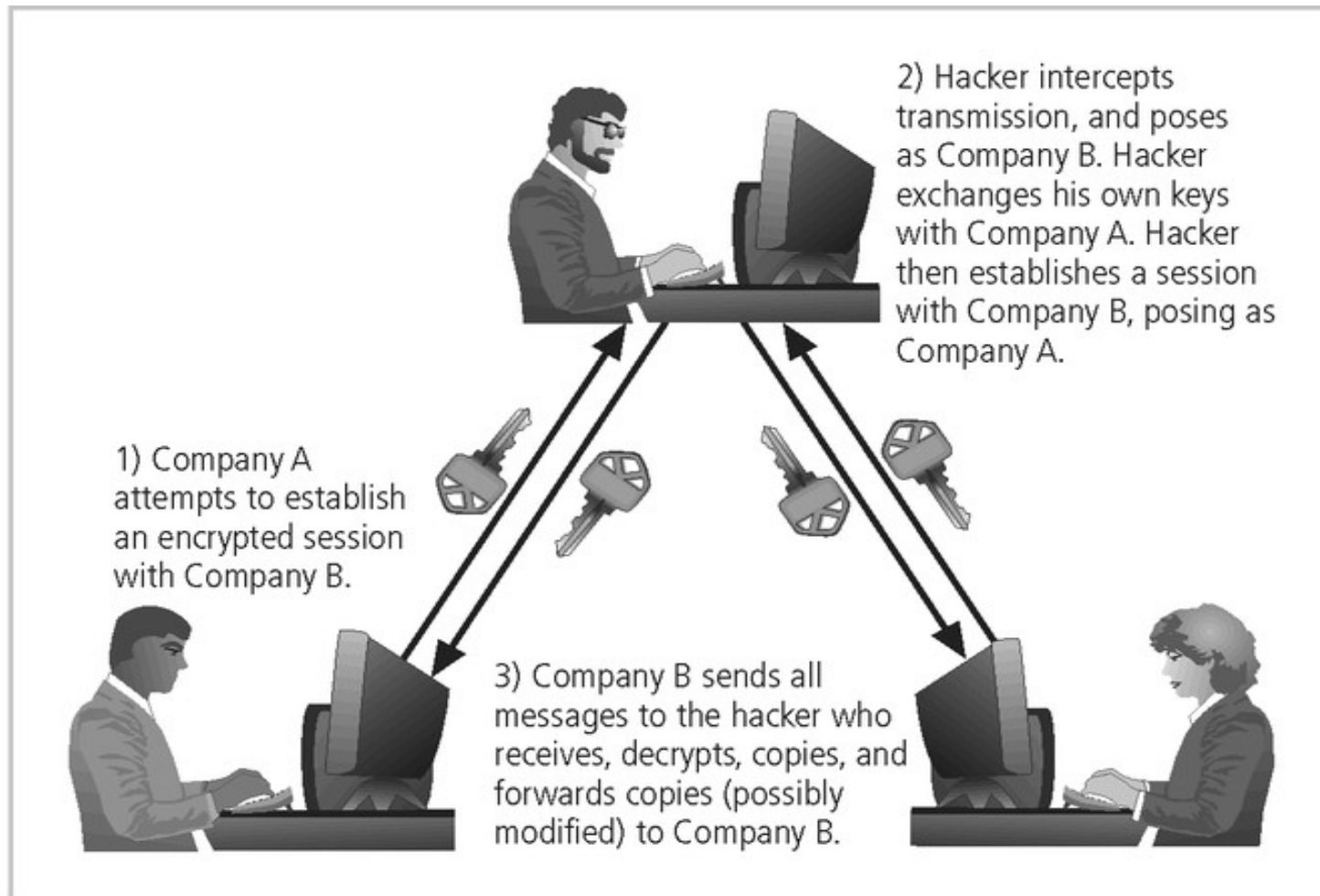


FIGURE 2-11 Man-in-the-Middle Attack

Attack Descriptions

- **Mail-bombing** - another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target
- **Sniffers** - a program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network
- **Social Engineering** - within the context of information security, the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker



Attack Descriptions

- “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”
-
- “brick attack” - the best configured firewall in the world can't stand up to a well placed brick



Attack Descriptions

- **Buffer Overflow -**

- application error occurs when more data is sent to a buffer than it can handle
- when the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure
- Usually the attacker fill the overflow buffer with executable program code to elevate the attacker's permission to that of an administrator.



Attack Descriptions

- **Ping of Death Attacks**

- A type of DoS attack
- Attacker creates an ICMP packet that is larger than the maximum allowed 65,535 bytes.
- The large packet is fragmented into smaller packets and reassembled at its destination.
- Destination user cannot handle the reassembled oversized packet, thereby causing the system to crash or freeze.



Attack Descriptions

- **Timing Attack** -
 - relatively new
 - works by exploring the contents of a web browser's cache
 - can allow collection of information on access to password-protected sites
 - another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms



Digital Forensics

What is Digital Forensics?

- Emerging discipline in computer security
 - “voodoo science”
 - No standards, few research
- Investigation that takes place after an incident has happened
- Try to answer questions: Who, what, when, where, why, and how

Types of investigations

- Determine what the incident was and get back to a working state
- Internal investigation
 - Should be based on IR policy
 - May lead to criminal investigation
- Criminal investigation
- Support for “real world” investigations

Typical investigation phases

1. Acquisition
2. Recovery
3. Analysis
4. Presentation

Phase 1: Acquisition

- Analogous to crime scene in the “real world”
- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Maintain *Chain of Custody*

Acquisition (2)

- Determine if incident actually happened
- What kind of system is to be investigated?
 - Can it be shut down?
 - Does it have to keep operating?
- Are there policies governing the handling of the incident?
- Is a warrant needed?

Acquisition (3)

- Get most fleeting information first
 - Running processes
 - Open sockets
 - Memory
 - Storage media
- Create 1:1 copies of evidence (imaging)
- If possible, lock up original system in the evidence locker

Phase 2: Recovery

- Goal is to extract data from the acquired evidence
- Always work on copies, never the original
 - Must be able to repeat entire process from scratch
- Data, deleted data, “hidden” data

File systems

- Get files and directories
- Metadata
 - User IDs
 - Timestamps (MAC times)
 - Permissions, ...
- Some deleted files may be recovered
- Slack space

File deletion

- Most file systems only delete directory entries but not the data blocks associated with a file.
- Unless blocks get reallocated the file may be reconstructed
 - The earlier the better the chances
 - Depending on fragmentation, only partial reconstruction may be possible

Slack space

- Unallocated blocks
 - Mark blocks as allocated to fool the file system
- Unused space at end of files if it doesn't end on block boundaries
- Unused space in file system data structures

Steganography

- Data hidden in other data
- Unused or irrelevant locations are used to store information
- Most common in images, but may also be used on executable files, meta data, file system slack space

Encrypted data

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.

Recovery (cont.)

- Locating hidden or encrypted data is difficult and might even be impossible.
- Investigator has to look at other clues:
 - Steganography software
 - Crypto software
 - Command histories

File residue

- Even if a file is completely deleted from the disk, it might still have left a trace:
 - Web cache
 - Temporary directories
 - Data blocks resulting from a move
 - Memory

Phase 3: Analysis

- Methodology differs depending on the objectives of the investigation:
 - Locate contraband material
 - Reconstruct events that took place
 - Determine if a system was compromised
 - Authorship analysis

Contraband material

- Locate specific files
 - Databases of illegal pictures
 - Stolen property
- Determine if existing files are illegal
 - Picture collections
 - Music or movie downloads

Locating material

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
 - Misleading file suffix
 - Misleading file name
 - Unusual location

Event reconstruction

- Utilize system and external information
 - Log files
 - File timestamps
 - Firewall/IDS information
- Establish time line of events

Time issues

- Granularity of time keeping
 - Can't order events that occur in the same time interval
- Multiple systems:
 - Different clocks
 - Clock drift
- E-mail headers and time zones

The needle in the haystack

- Locating files:
 - Storage capacity approaches the terrabyte magnitude
 - Potentially millions of files to investigate
- Event reconstruction:
 - Dozens, hundreds of events a second
 - Only last MAC times are available
 - Insufficient logging

Compromised system

- If possible, compare against known good state
 - Tripwire
 - Databases of “good” files
- Look for unusual file MACs
- Look for open or listening network connections (trojans)
- Look for files in unusual locations

Unknown executables

- Run them in a constrained environment
 - Dedicated system
 - Sandbox
 - Virtual machine
- Might be necessary to disassemble and decompile
 - May take weeks or months

Authorship analysis

- Determine who or what kind of person created file.
 - Programs (Viruses, Trojans, Sniffers/Loggers)
 - E-mails (Blackmail, Harassment, Information leaks)
- If actual person cannot be determined, just determining the skill level of the author may be important.

Phase 4: Presentation

- An investigator that performed the analysis may have to appear in court as an expert witness.
- For internal investigations, a report or presentation may be required.
- Challenge: present the material in simple terms so that a jury or CEO can understand it.

Forensics Tools

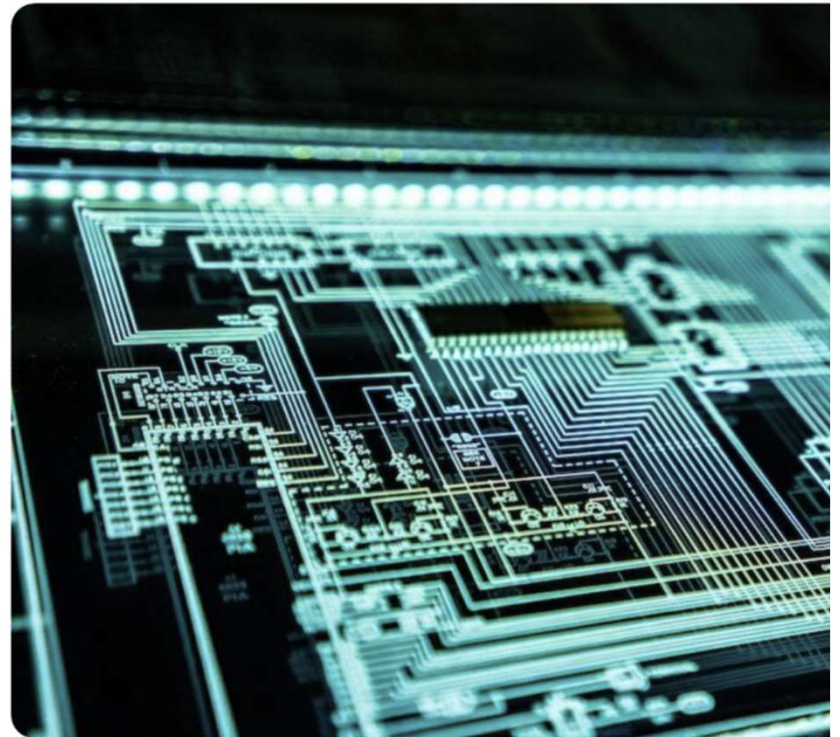
- Acquisition
 - dd, pdd
 - SafeBack, ...
- Recovery
 - Encase
 - TCT and SleuthKit
- Analysis
 - ?
- Presentation
 - ?

DF Investigator Profile

- Understanding of relevant laws
- Knowledge of file systems, OS, and applications
 - Where are the logs, what is logged?
 - What are possible obfuscation techniques?
 - What programs and libraries are present on the system and how are they used?
- Know what tools exist and how to use them
- Be able to explain things in simple terms

Emerging IT Devices in Cyber Forensics

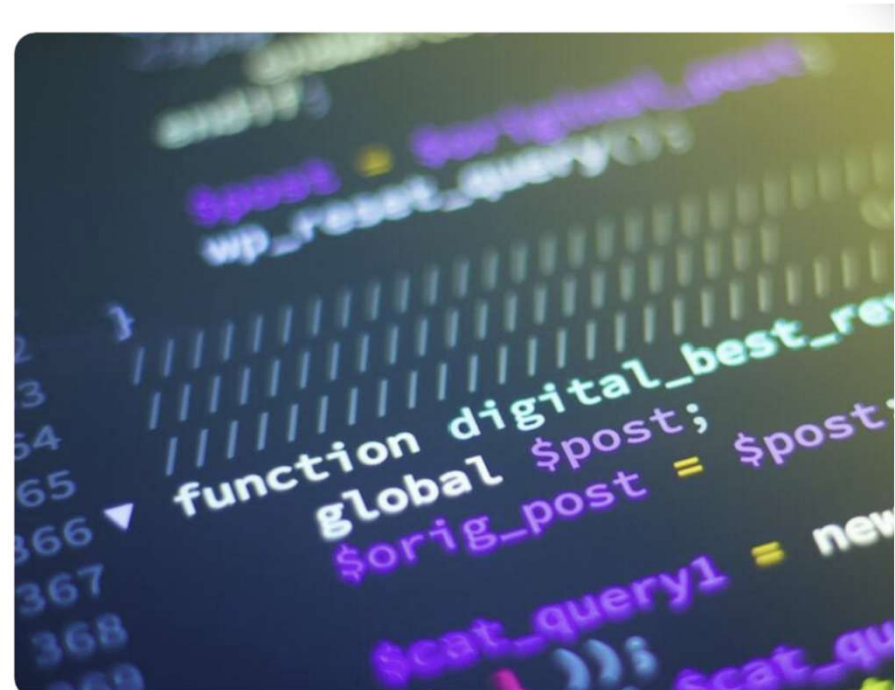
- **Smartphones:** Smartphones serve as multi-functional devices that store a wealth of personal information, including communication records and geolocation data, making them critical in cyber forensic investigations for both criminal and civil cases.
- **IoT Devices:** The Internet of Things (IoT) encompasses interconnected devices that often collect and transmit data. Their rapid proliferation presents forensic challenges, including voluminous data management and varying protocols for data extraction.
- **Wearable Technology:** Wearables like smartwatches and fitness trackers offer unique insights into user behavior and health metrics. These devices can provide timelines and additional context that are increasingly relevant in forensic inquiries.



Challenges in Cyber Forensics with New Devices

Navigating obstacles in Evidence Collection

- **Data Encryption:** As data encryption becomes more prevalent, forensic experts face hurdles in accessing protected information. Techniques utilized for encryption often complicate the extraction of usable evidence, necessitating advanced decrypting skills.
- **Device Diversity:** The vast array of device types and manufacturers results in heterogeneous data formats and storage systems, complicating analysis. For forensic processes, such diversity can lead to inconsistencies in evidence interpretation and retrieval.
- **Legal and Ethical Issues:** The evolving nature of technology raises complex legal and ethical considerations regarding privacy and rights. Forensic professionals must navigate these waters carefully to ensure compliance without compromising integrity.



Techniques and Tools for Cyber Forensics

Mechanism for Effective Evidence Analysis



Digital Evidence Collection

Digital evidence collection involves systematic procedures that ensure the integrity of data from the moment it is captured. Basic protocols include the use of write-blockers and forensically sound imaging methods, ensuring that no alterations occur during the process.



Forensic Analysis Software

Forensic analysis software enables analysts to sift through vast amounts of digital information efficiently. These tools offer functionalities such as data carving, timeline analysis, and pattern recognition to uncover critical insights from digital evidence.



Data Recovery Methods

Data recovery techniques are crucial for retrieving lost or deleted information. Methods range from file system recovery to more sophisticated approaches that can extract remnants of data from damaged devices, expanding the possibilities for evidence discovery.

Case Studies:

Analysing Real-world Scenarios and Implications



Real-world Examples

Numerous high-profile cases have highlighted the role of cyber forensics, from cybercrime investigations to corporate espionage, illustrating the substantial impact of forensic evidence in legal proceedings.



Lessons Learned

Each case provides valuable insights into best practices and challenges encountered in forensic processes. Understanding these lessons aids in refining methodologies and improving future investigative outcomes.



Impact on Investigation

The impact of employing cyber forensics in investigations can be profound, often leading to the resolution of complex cases, the identification of perpetrators, and the enhancement of cybersecurity measures for organizations.

Future Trends in Cyber Forensics

Anticipating Tomorrows Developments

AI and Machine Learning

Artificial Intelligence and machine learning present the opportunity to automate data analysis and enhance pattern recognition in forensic investigations, greatly increasing efficiency and accuracy in detecting anomalies and predicting potential threats.

Blockchain Technology

Blockchain technology offers transparent and immutable record-keeping possibilities for forensic evidence, ensuring data integrity and chain of custody, fundamentally enhancing the reliability of digital evidence in legal settings.

Evolving Threat Landscape

The nature of cyber threats is continuously evolving, creating a pressing need for forensic professionals to adapt to new tactics employed by cybercriminals. Staying ahead of these trends is vital in protecting assets and ensuring effective responses to incidents.

Best Practices

Guiding Principles for effective practice

- **Continuous Education:** The cyberforensics landscape is ever-changing; hence, continuous education is essential for professionals to stay informed about the latest threats, technologies, and methodologies in digital forensics.
- **Collaboration with Law Enforcement:** Building solid partnerships with law enforcement agencies ensures that forensic evidence is not only well-prepared for litigation but also effectively utilized in broader investigations, enhancing the overall effectiveness of inquiries.
- **Adopting New Technologies:** As new technologies emerge, adopting innovative forensic tools and methodologies can provide a significant advantage, ensuring that cyber forensics practices remain effective and relevant in the face of evolving challenges.

Conclusion

Reflecting on Key Insights and Future Directions

- **Summary of Key Points:** The presentation underlined the definition of cyber forensics, the role of emerging IT devices, the challenges posed by these innovations, and the techniques that can be employed to gather and analyze evidence.
- **Future Outlook:** The foreseen developments in AI, blockchain, and an evolving threat landscape present both opportunities and challenges. Understanding these dynamics is crucial for enhancing the effectiveness of cyber forensic practices in the years to come.
- **Call to Action:** It is imperative for professionals in the field to engage with the evolving nature of cyber forensics proactively. Embracing education, innovative practices, and collaboration will ensure they remain at the forefront of digital investigations.