

Security of Information Assets

By Vinod Sencha

Core Faculty(IS), RTI Jaipur

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.

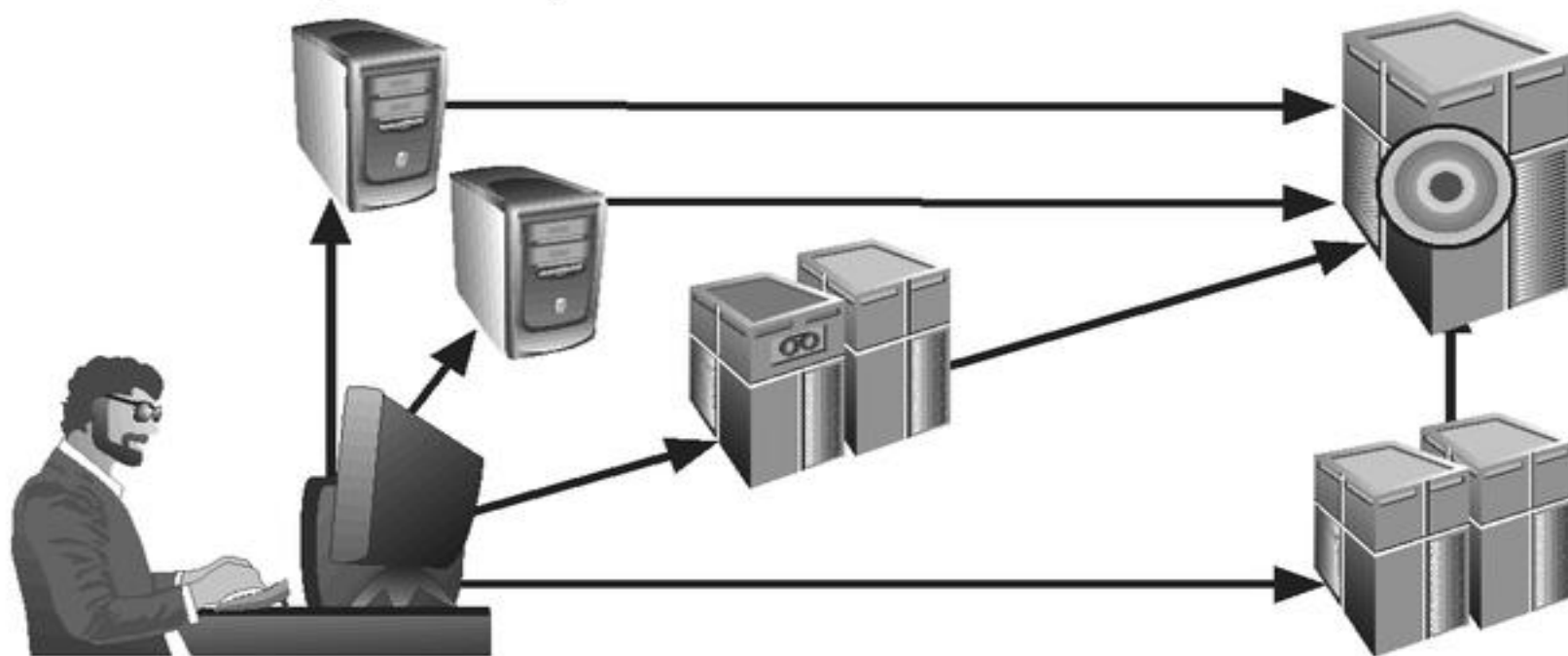


FIGURE 2-9 Denial-of-Service Attacks

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

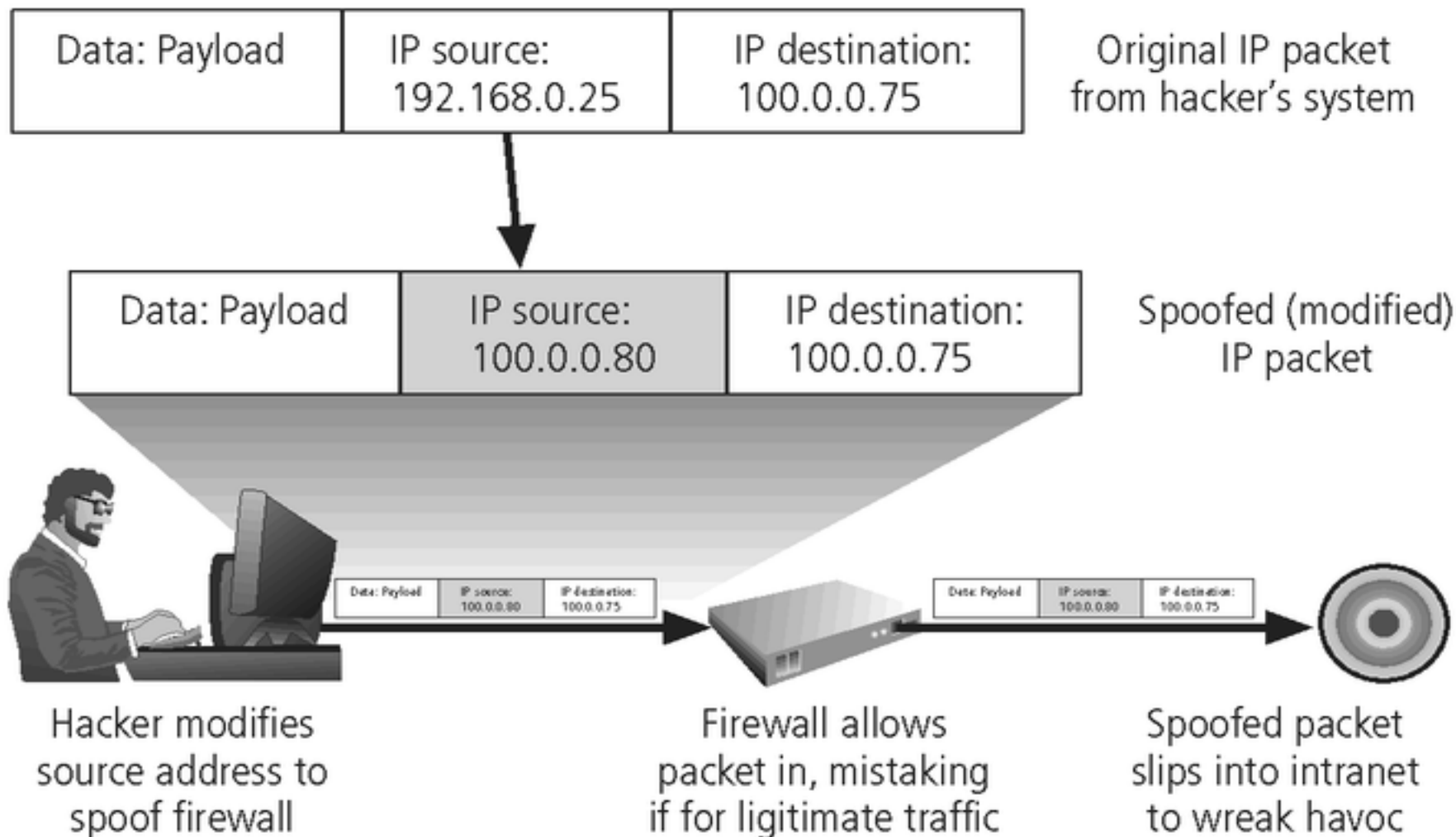


FIGURE 2-10 IP Spoofing

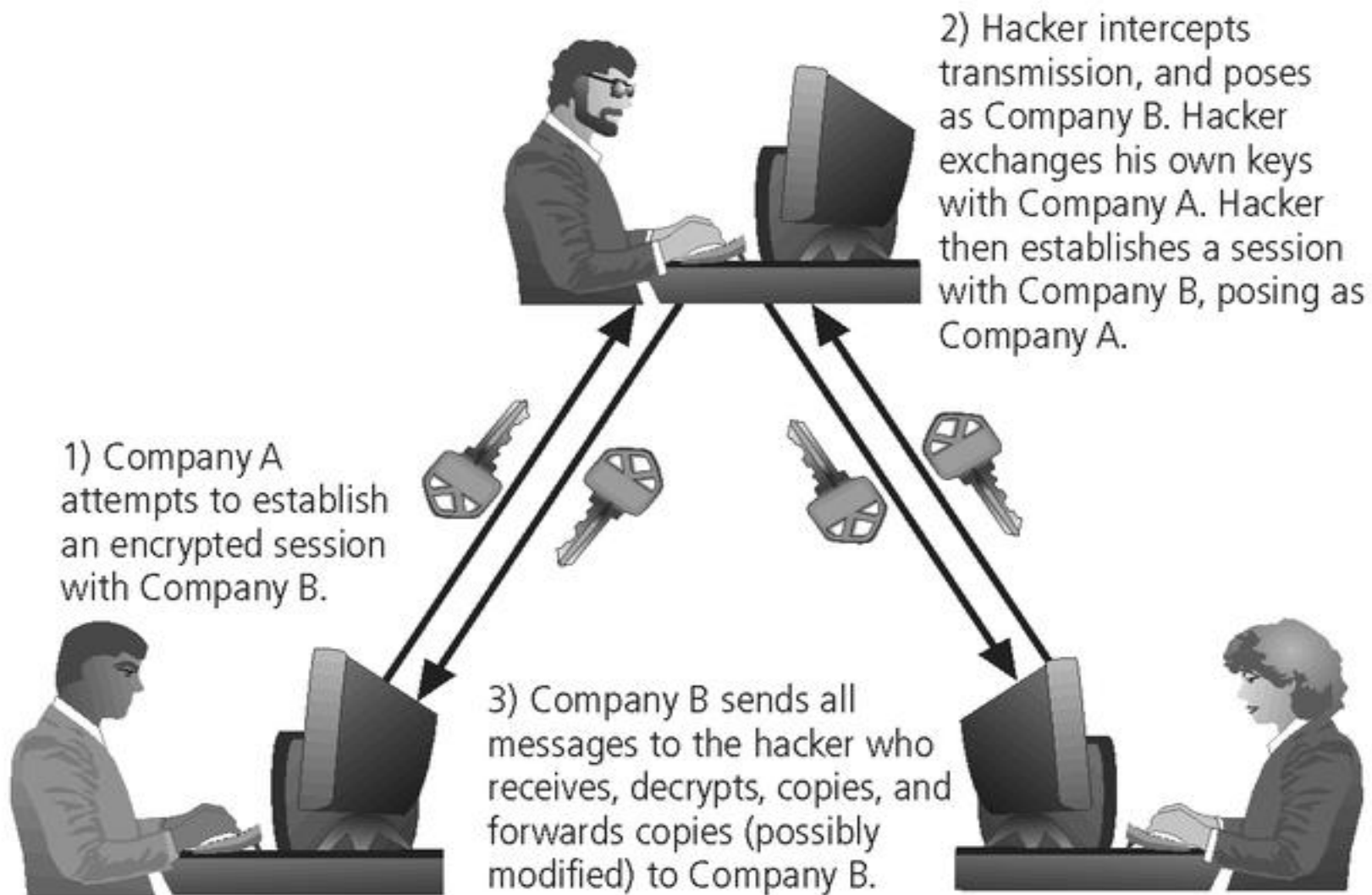


FIGURE 2-11 Man-in-the-Middle Attack

Protective Measures

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.

Protective Measures

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

Protective Measures

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.

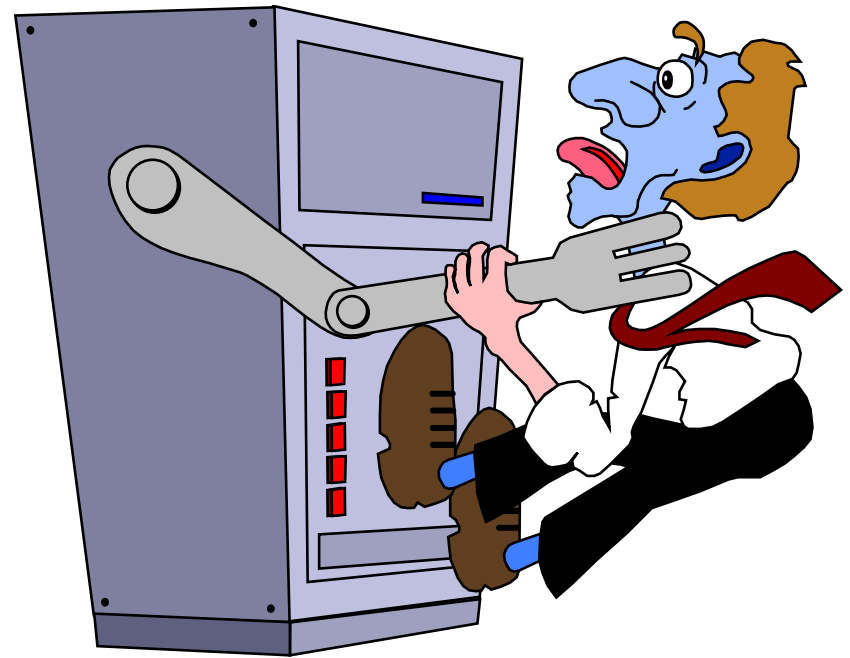
Acts of Human Error or Failure

- 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





Shoulder surfing
takes many forms.
Some may not be obvious.



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

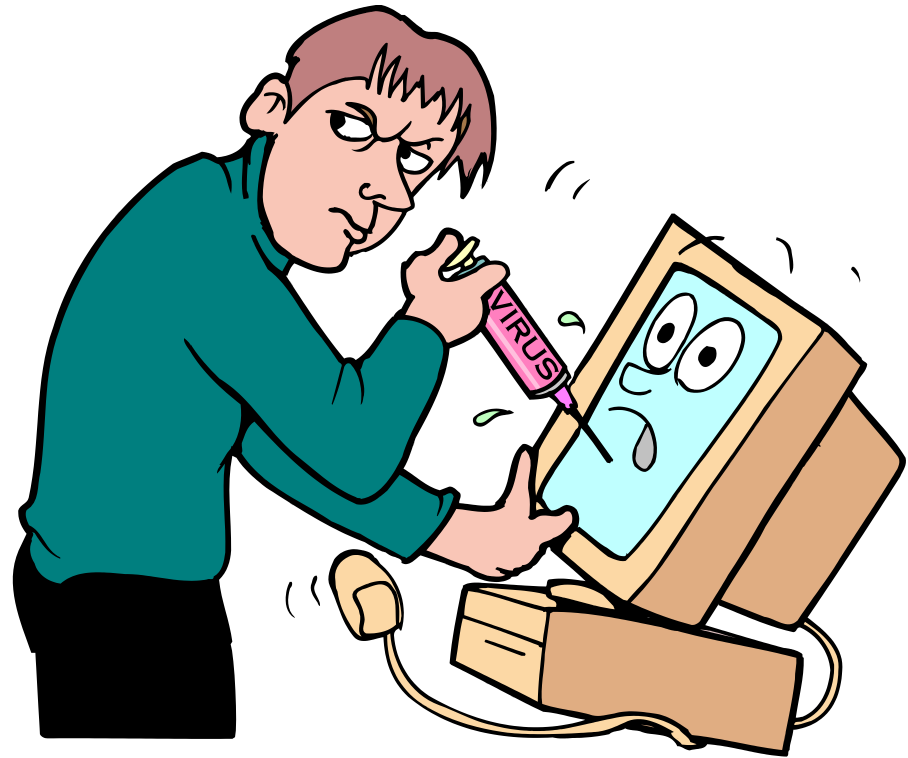
Information Extortion

- 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.

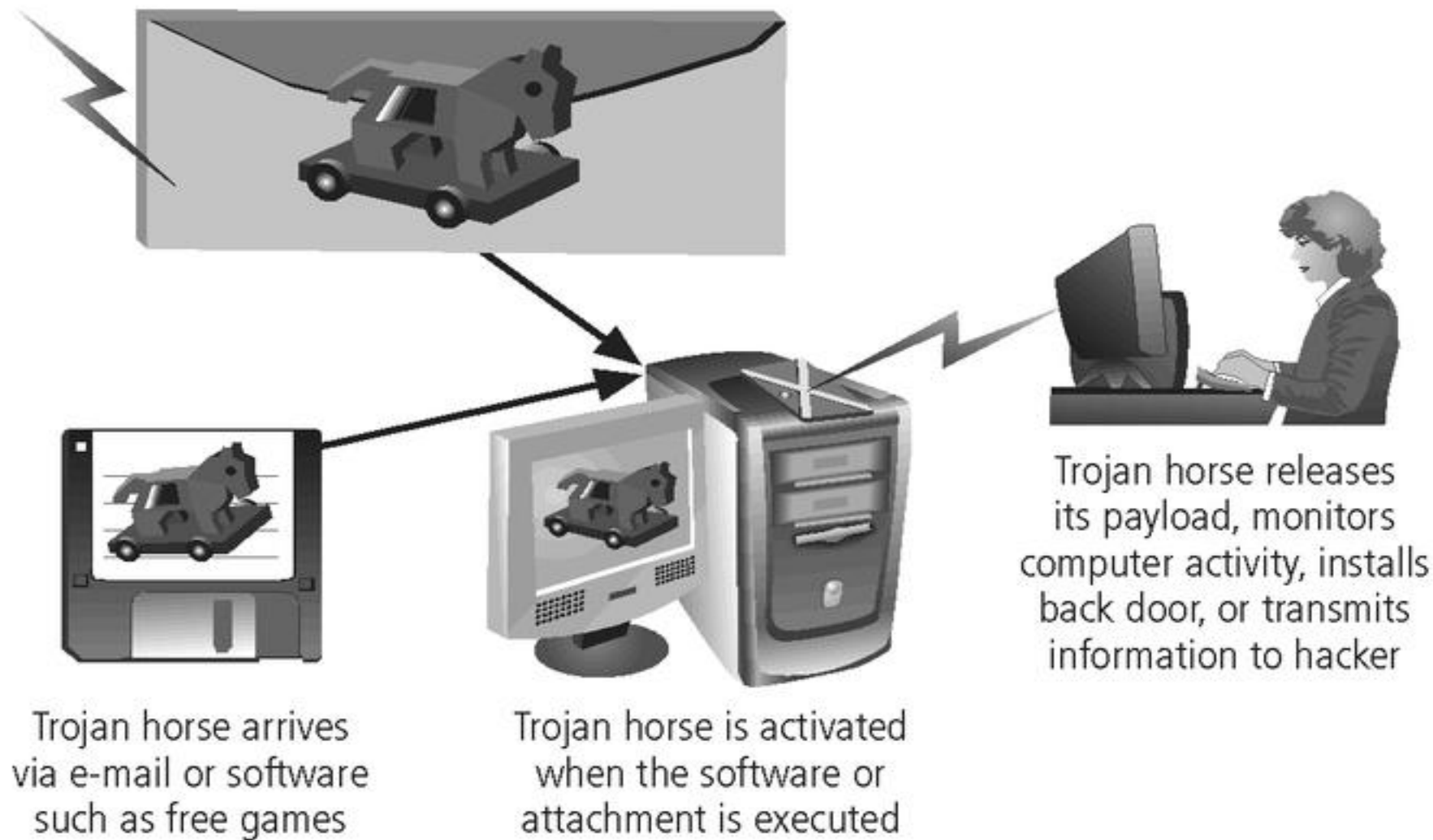







FIGURE 2-8 Trojan Horse Attack

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

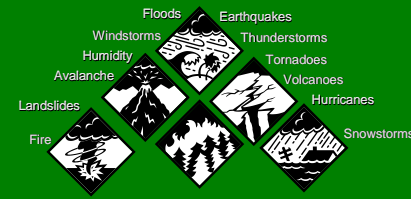
Educating Your Users

-  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.

Forces of Nature



- Forces of nature, *force majeure*, or acts of God are dangerous because they are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected
- Information system depends on many inter-dependent support systems
- Three sets of service issues that dramatically affect the availability of information and systems are
 - Internet service
 - Communications
 - Power irregularities

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in the unrecoverable loss of the equipment
- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

Technical Hardware Failures or Errors

- This category of threats comes from purchasing software with unrevealed faults
- Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
- Sometimes, unique combinations of certain software and hardware reveal new bugs
- Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

Technological Obsolescence

- When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks
- Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action

Attacks

- An attack is the deliberate act that exploits vulnerability
- It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
 - An exploit is a technique to compromise a system
 - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
 - An attack is then the use of an exploit to achieve the compromise of a controlled system

Malicious Code

- This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
- The state of the art in attacking systems in 2002 is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices



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 2002

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.

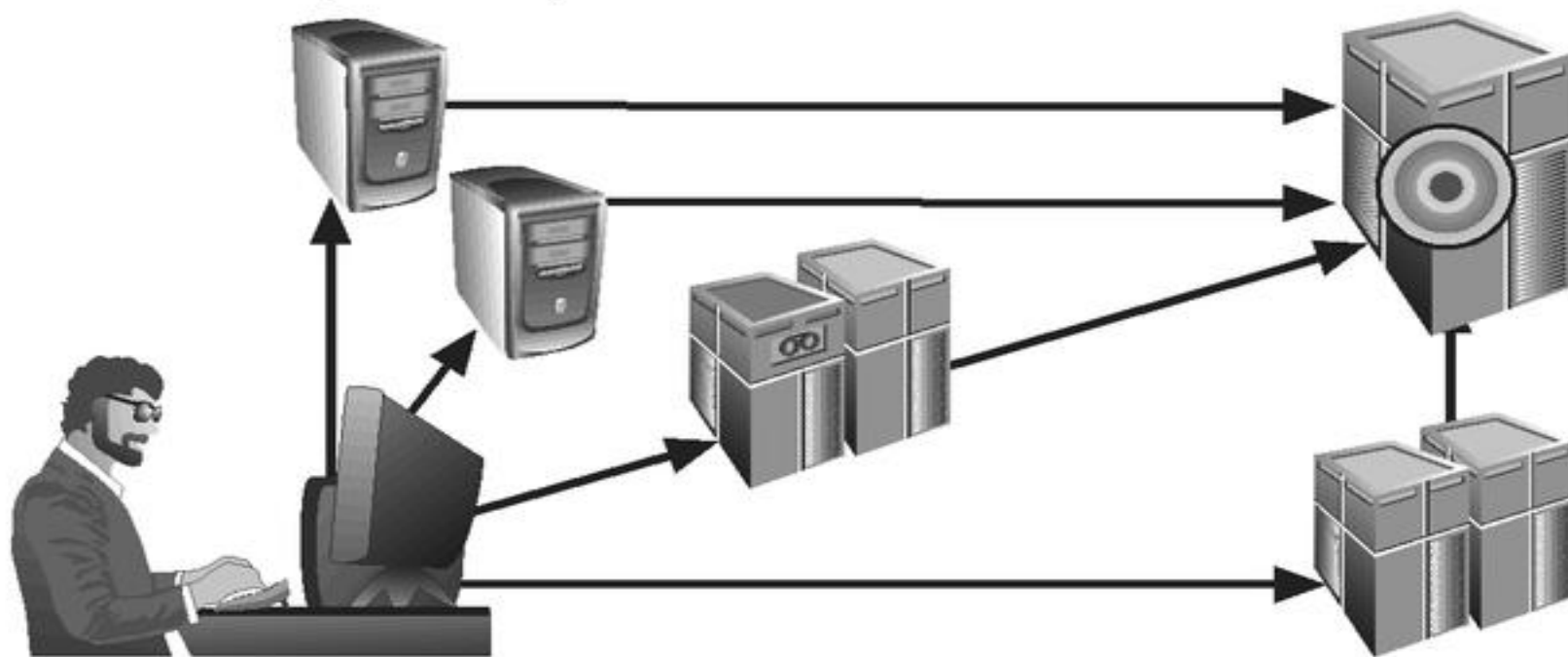


FIGURE 2-9 Denial-of-Service Attacks

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

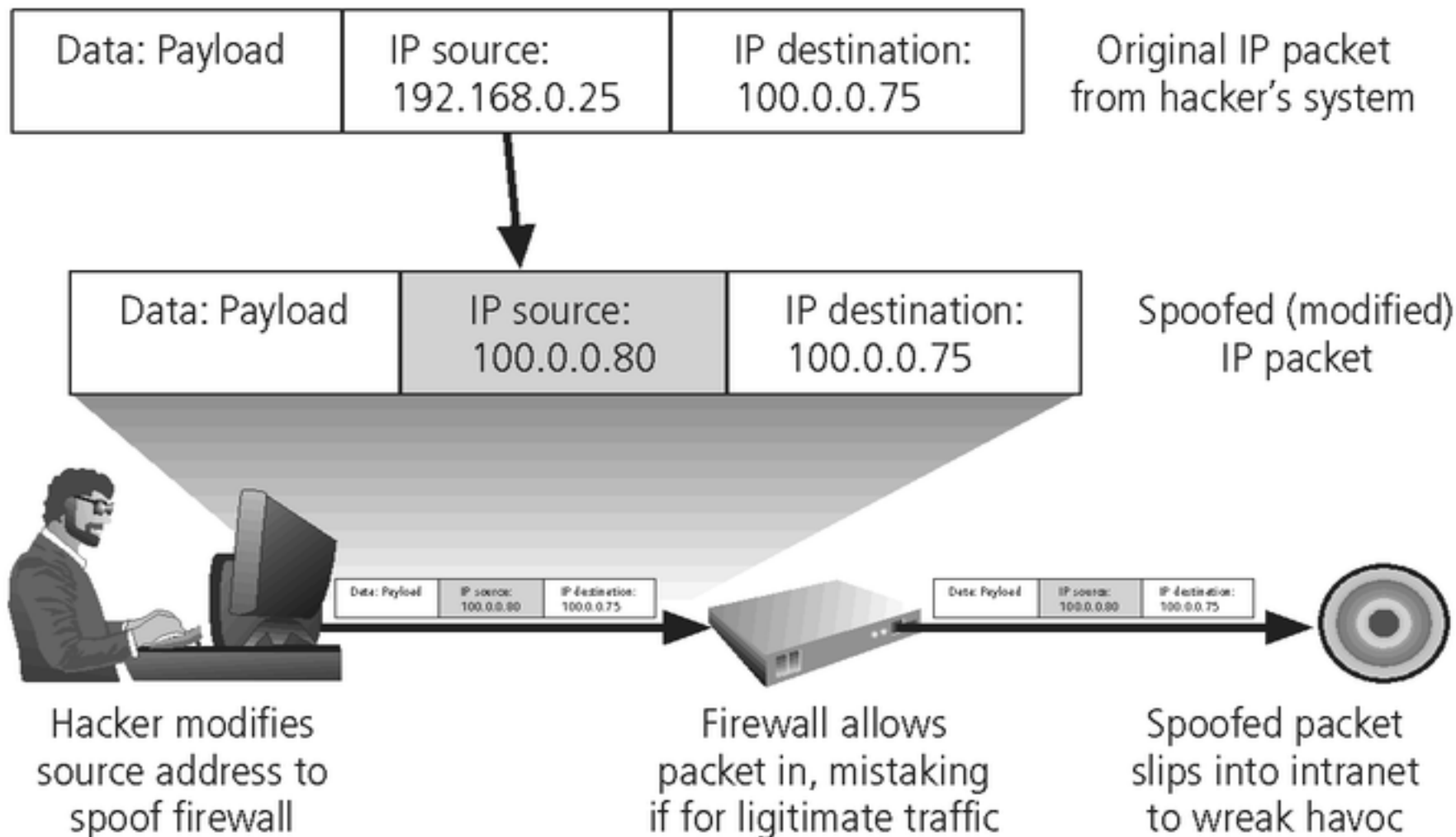


FIGURE 2-10 IP Spoofing

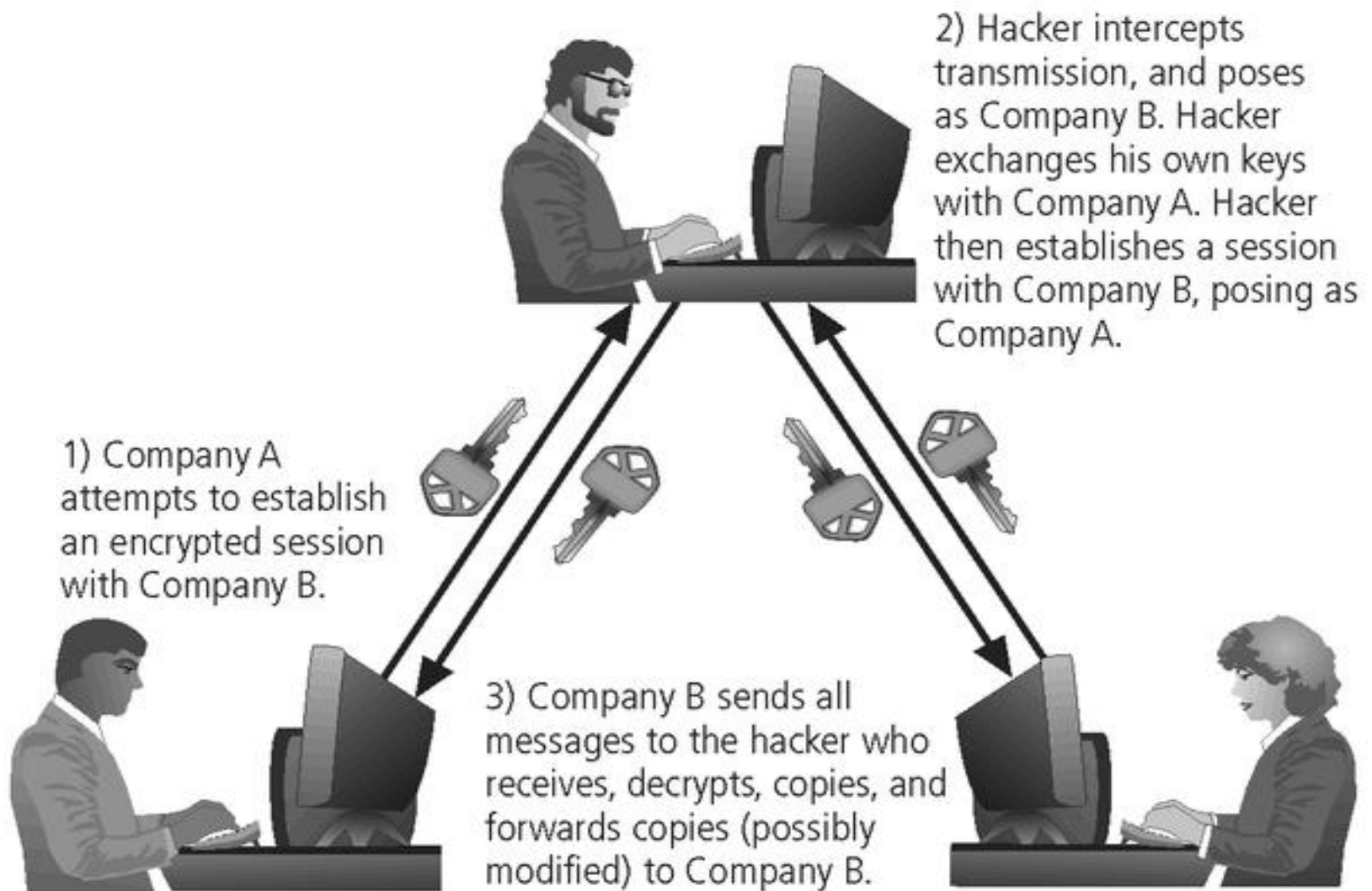


FIGURE 2-11 Man-in-the-Middle Attack

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