Information Security

The Need For Security

Learning Objectives

Upon completion of this lecture, you should be able to:

- Understand the need for information security.
- Understand a successful information security program is the responsibility of an organization's general management and IT management.
- Understand the threats posed to information security and the more common attacks associated with those threats.
- Differentiate threats to information systems from attacks against information systems.

Business Needs First, Technology Needs Last

Information 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

Protecting the Ability to Function

- Management is responsible
- Information security is
  - a management issue
  - a people issue
- Communities of interest must argue for information security in terms of impact and cost

Enabling Safe Operation

- Organizations must create integrated, efficient, and capable applications
- Organization need environments that safeguard applications
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions

Protecting Data

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers
- An effective information security program is essential to the protection of the integrity and value of the organization's data

Safeguarding Technology Assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided
- More robust solutions may be needed to replace security programs the organization has outgrown

Assets

An asset is the resource being protected, including:

- **physical assets:** devices, computers, people;
- **logical assets:** information, data (in transmission, storage, or processing), and intellectual property;
- **system assets:** any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.

Assets have value so are worth protecting.

Subjects and Objects

Often a security solution/policy is phrased in terms of the following three categories:

Objects: the items being protected by the system (documents, files, directories, databases, transactions, etc.)

Subjects: entities (users, processes, etc.) that execute activities and request access to objects.

Actions: operations, primitive or complex, that can operate on objects and must be controlled.

Both subjects and objects have associated **attributes**. The security mechanisms may operate in terms on the attributes and manipulation of the attributes can be used to subvert security.

Critical Aspects

Information assets (objects) may have critical aspects:

availability: authorized users are able to access it;

accuracy: the information is free of error and has the value expected;

authenticity: the information is genuine;

confidentiality: the information has not been disclosed to unauthorized parties;

integrity: the information is whole, complete and uncorrupted;

utility: the information has value for the intended purpose;

possession: the data is under authorized ownership and control.

Threats

- Management must be informed of the various kinds of threats facing the organization
- A threat is an object, person, or other entity that represents a constant danger to an asset
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Terms: Threat and Threat Actors

A *threat* is a *category* of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

- Threats can be categorized by intent: accidental or purposeful (error, fraud, hostile intelligence);
- Threats can be categorized by the kind of entity involved: human (hackers, someone flipping a switch), processing (malicious code, sniffers), natural (flood, earthquake);
- Threats can be categorized by impact: type of asset, consequences.

A *threat actor* is a specific instance of a threat, e.g. a specific hacker, a particular storm, etc.

Examples of Threats

- Interruption: an asset becomes unusable, unavailable, or lost. E.g. a denial of service attack on a website
- Interception: an unauthorized party gains access to an information asset. E.g. compromise of confidential data, e.g., but packet sniffing
- Modification: an unauthorized party tampers with an asset. E.g. hacking to deface a website
- Fabrication: an asset has been counterfeit. E.g spoofing attacks in a network

Examples of each Threats

- **Interruption:** a denial of service attack on a website
- **Interception:** compromise of confidential data, e.g., but packet sniffing
- **Modification:** hacking to deface a website
- **Fabrication:** spoofing attacks in a network

Impactful Cybersecurity Facts and Stats

- Data breaches exposed 4.1 billion records in the first half of 2019
- Hackers attack every 39 seconds, on average 2, 244 times a day
- 57% of companies experienced social engineering or phishing attacks
- 53% of companies had over 1, 000 sensitive files open to every employee
- The cost of a data breach in the healthcare industry was highest at $6.5 Million
- $3.9 Million is the average cost of a data breach worldwide and $8.2 Million in the United States
- By 2021, their will be 3.5 Million unfulfilled cybersecurity jobs globally

Threats

Threats to Information Security

TABLE 2-1 Threats to Information Security[4]

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

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

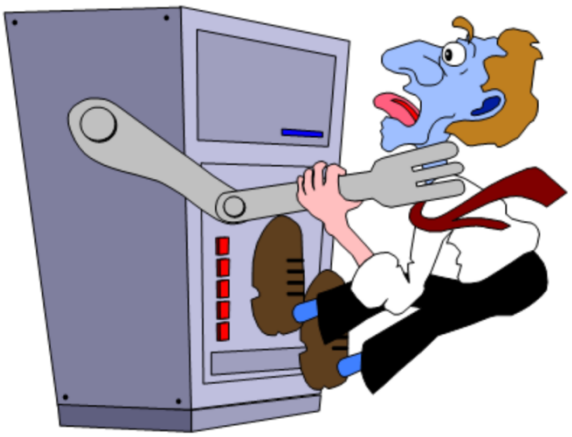


FIGURE 2-1 Acts of Human Error or Failure

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

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

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 uses skill, guile, or fraud to steal the property of someone else

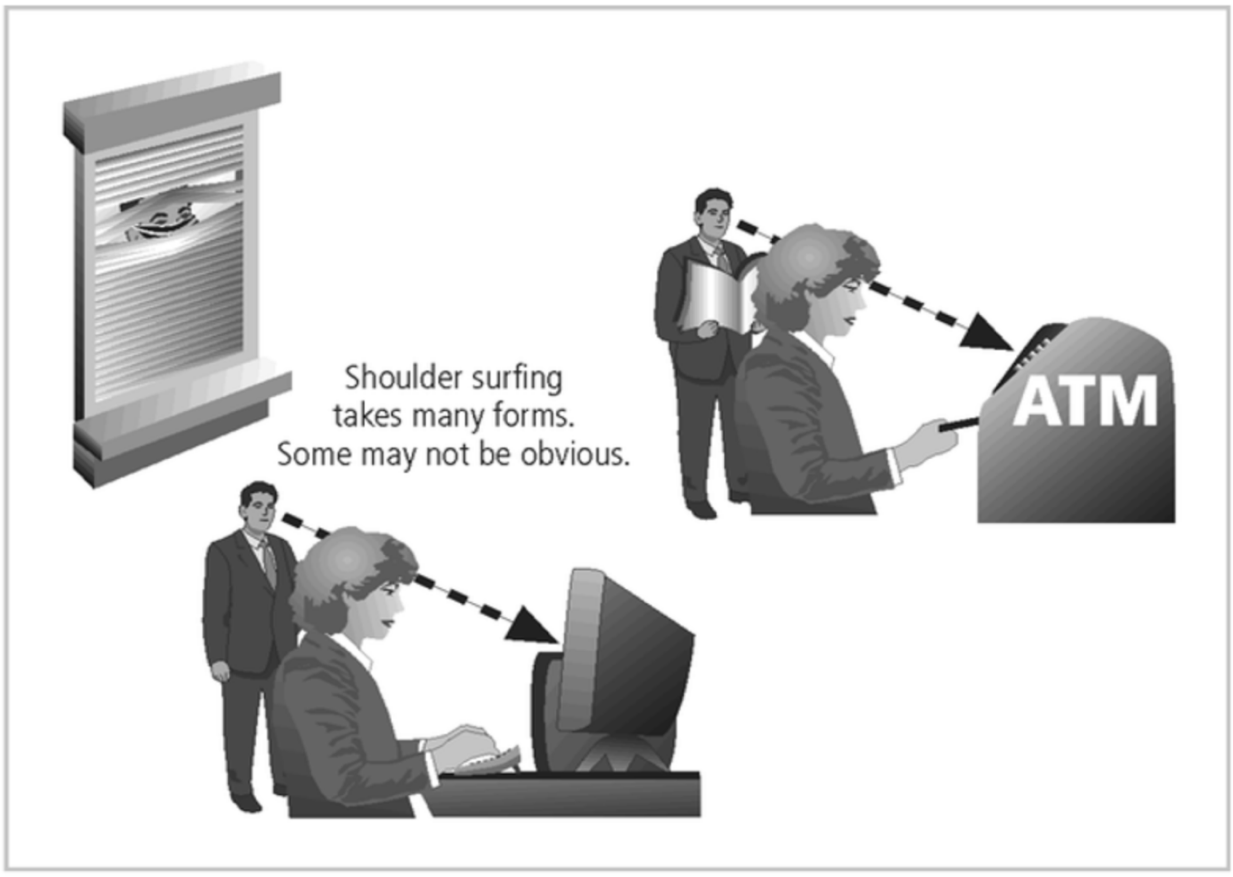


FIGURE 2-2 Shoulder Surfing

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

Espionage/Trespass

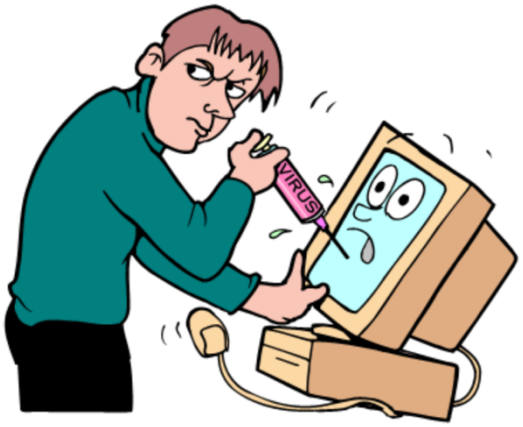
- Generally two skill levels among hackers:
  - Expert hacker
    - develops software scripts and codes exploits
    - usually a master of many skills
    - will often create attack software and share with others
  - Script kiddies
    - hackers of limited skill
    - use expert-written software to exploit 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

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

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 know 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.

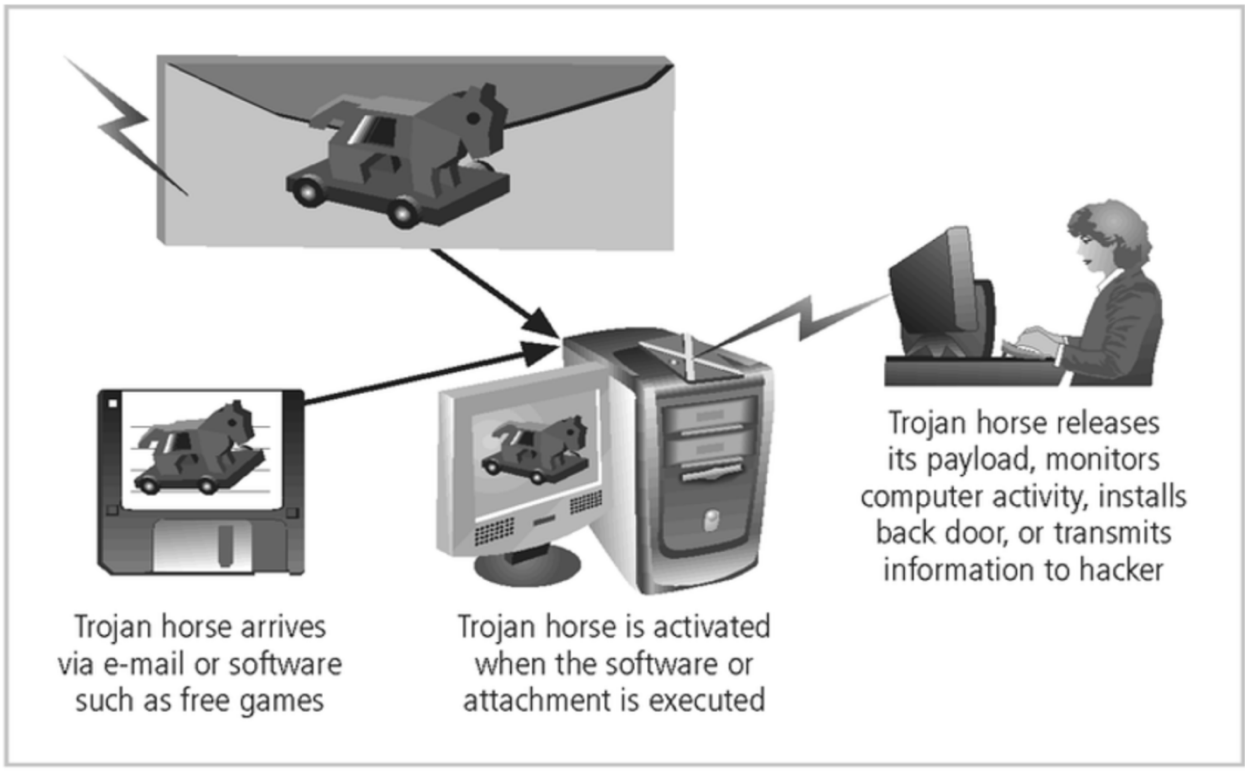


FIGURE 2-8 Trojan Horse Attack

Deliberate Software Attacks

- Challenges:
  - Trojan programs that use common ports, such as TCP 80, or UPD 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 Trajan 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.

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

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

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

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

Attacks

- An attack is an attempt to gain access, cause damage to or otherwise compromise information and/or systems that support it.
- Passive attack: an attack in which the attacker observes interaction with the system.
- Active attack: at attack in which the attacker directly interacts with the system.
- Unintentional attack: an attack where there is not a deliberate goal of misuse

Attacks

- Attacks have a subject and object.

Attack subject: the active entity, usually a threat actor, that interacts with the system.

- Attack object: the targeted information system asset.
- The *attack surface* of an organization/entity is the set of ways in which an adversary can enter the system and potentially cause damage. For example:

The attack surface of a software environment is the code within a computer system that can be run by unauthenticated users. This includes, but is not limited to: user input fields, protocols, interfaces, and services.

Malicious Code

- This kind of attack includes the executio viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
- The state of the art in attacking systems 2002 is the multi-vector worm using up t 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.

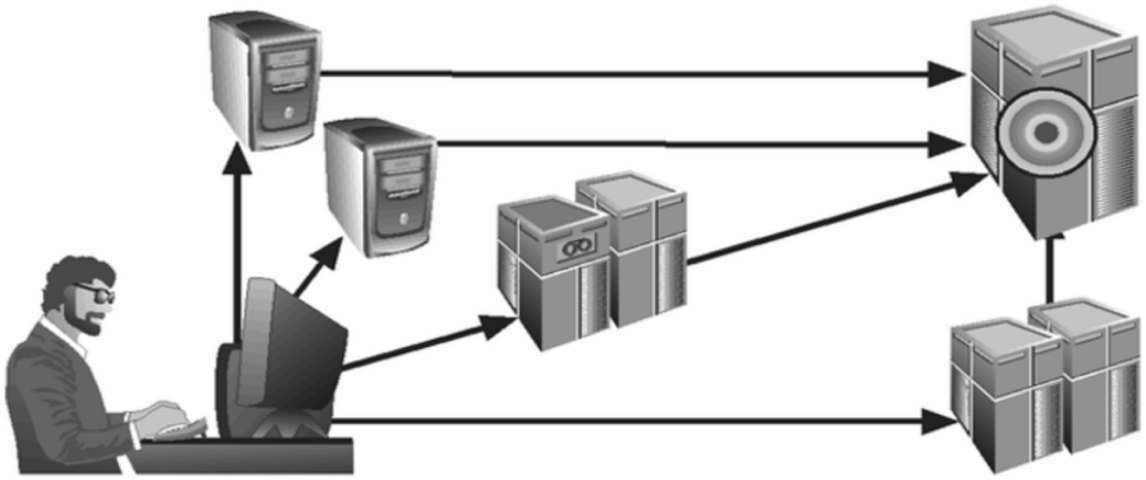


FIGURE 2-9 Denial-of-Service Attacks

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

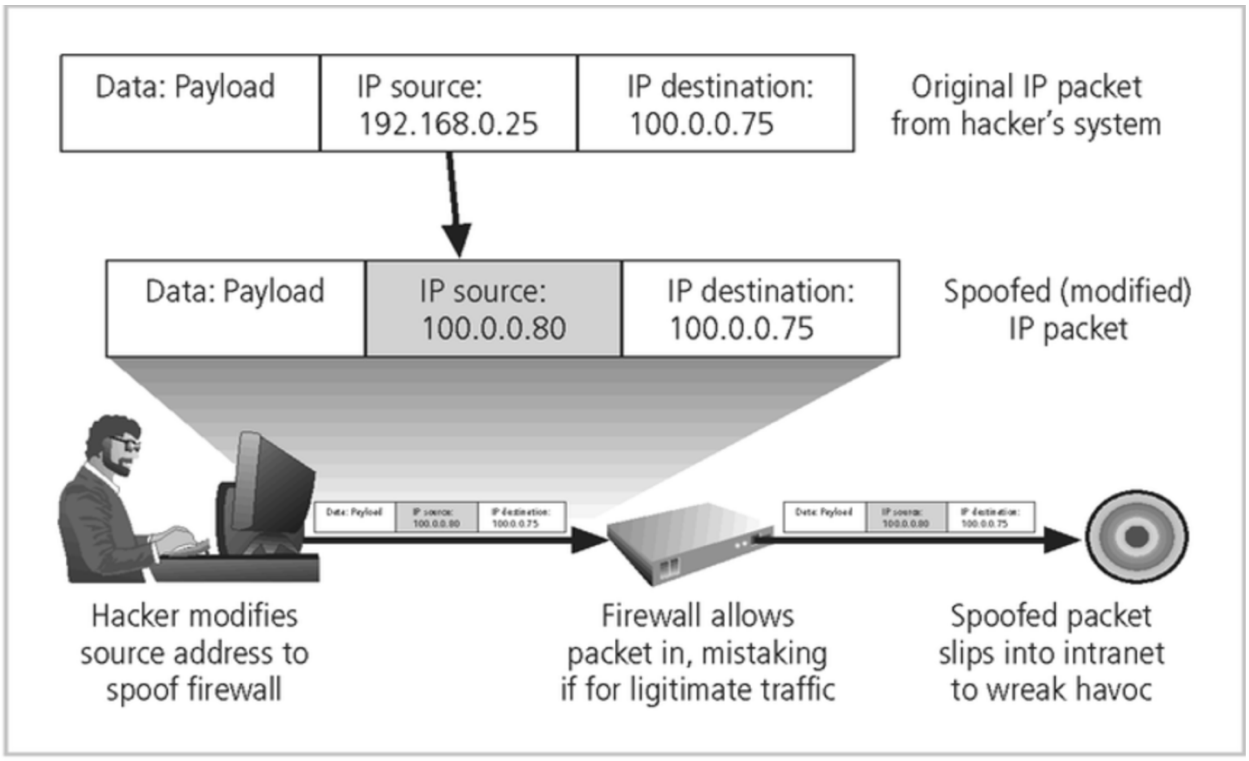


FIGURE 2-10 IP Spoofing

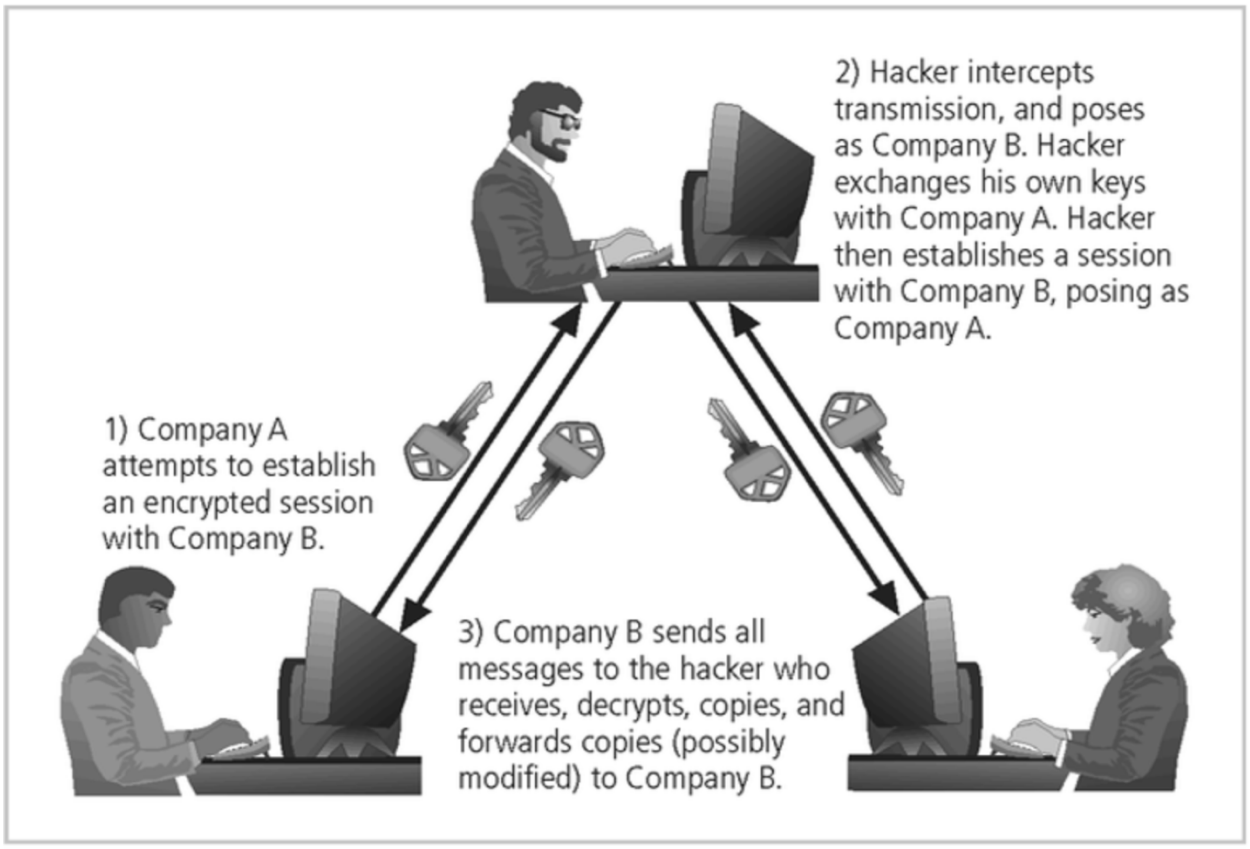


FIGURE 2-11 Man-in-the-Middle Attack

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

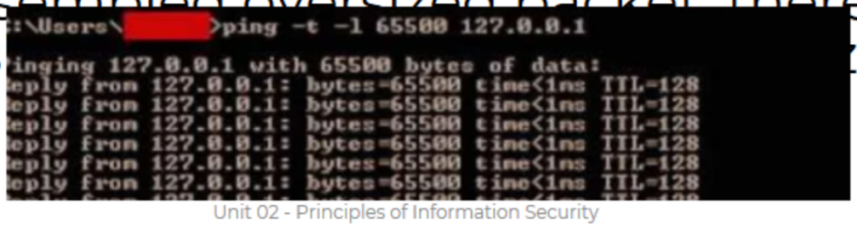
- **Buffer Overflow** –
  - application error occurs when more data is sent to a buffer than it can handle
  - when the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure
  - Usually the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

```
printf ("\n Correct Password \n");
pass = 1;
}
if(pass)
{
/* Now Give root or admin rights to user*/
printf ("\n Root privileges given to the user \n");
}
return 0;
```

```
$ ./bfrovrflw
Enter the password :
hhhhhhhhhhhhhhhhhhhh
Wrong Password
Root privileges given to the user
```

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 caus[redacted]e.



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

Summary

- Unlike any other aspect of IT, information security's primary mission to ensure things stay the way they are
- Information security performs four important functions:
  - Protects organization's ability to function
  - Enables safe operation of applications implemented on organization's IT systems
  - Protects data the organization collects and uses
  - Safeguards the technology assets in use at the organization

Summary

- Threat: object, person, or other entity representing a constant danger to an asset
- Management effectively protects its information through policy, education, training, and technology controls
- Attack: a deliberate act that exploits vulnerability

Summary

• A *hostile environment* for assets is one that has known threats. Example: locating an asset in a war zone or a flood zone, or placing an unprotected machine on the Internet.

• A *benign environment* is a nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural countermeasures.

• An *enclave* is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Summary

A *vulnerability* is a weakness or fault in a system that exposes information to attack.

A bug in a computer program is a very common vulnerability in computer security (e.g. buffer overflow situation).

A procedural failing can subvert technology controls (e.g. a core dump of secure information upon a failure).

A lack of controls can result in vulnerabilities, if controls are subverted (e.g. Enron financials).

An *exploit* is a method for taking advantage of a known vulnerability.

Summary

- A *dangling vulnerability* is one for which there is no known threat (vulnerability is there but not exploitable).
- A *dangling threat* is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).
- *Exposure* is an instance when the system is vulnerable to attack.
- A *compromise* is a situation in which the attacker has succeeded.
- An *indicator* is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

Summary

- A *consequence* is the outcome of an attack. In a purposeful threat, the threat actor has typically chosen a desired consequence for the attack, and selects the IA objective to target to achieve this.
- Disruption: targets availability
- Corruption: targets integrity
- Exploitation: targets confidentiality
- A consequence may cause the information system to lose effectiveness, and may have other costs.
- *Inadvertant disclosure* is a type of consequence, involving accidental exposure of information to an agent not authorized access.