

Introduction to Information Security Chapter 1

*Do not figure on opponents not
attacking; worry about your own
lack of preparation.*

-- Book of the Five Rings

Learning Objectives:

Upon completion of this chapter you should be able to:

- Understand what information security is and how it came to mean what it does today.
- Comprehend the history of computer security and how it evolved into information security.
- Understand the key terms and critical concepts of information security as presented in the chapter.
- Outline the phases of the security systems development life cycle.
- Understand the role professionals involved in information security in an organizational structure.

What Is Information Security?

Information security in today's enterprise is a “well-informed sense of assurance that the information risks and controls are in balance.” –Jim Anderson, Inovant (2002)

The History Of Information Security

- ◆ Computer security began immediately after the first mainframes were developed
- ◆ Groups developing code-breaking computations during World War II created the first modern computers
- ◆ Physical controls were needed to limit access to authorized personnel to sensitive military locations
- ◆ Only rudimentary controls were available to defend against physical theft, espionage, and sabotage



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Courtesy of National Security Agency

FIGURE 1-1 The Enigma²

The 1960s

- ◆ Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant networked communications
- ◆ Larry Roberts developed the project from its inception

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – \$3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan⁴

The 1970s and 80s

- ◆ ARPANET grew in popularity as did its potential for misuse
- ◆ Fundamental problems with ARPANET security were identified
 - No safety procedures for dial-up connections to the ARPANET
 - User identification and authorization to the system were non-existent
- ◆ In the late 1970s the microprocessor expanded computing capabilities and security threats

R-609 – The Start of the Study of Computer Security

- ◆ Information Security began with Rand Report R-609
- ◆ The scope of computer security grew from physical security to include:
 - Safety of the data
 - Limiting unauthorized access to that data
 - Involvement of personnel from multiple levels of the organization

The 1990s

- ◆ Networks of computers became more common, so too did the need to interconnect the networks
- ◆ Resulted in the Internet, the first manifestation of a global network of networks
- ◆ In early Internet deployments, security was treated as a low priority

The Present

- ◆ The Internet has brought millions of computer networks into communication with each other – many of them unsecured
- ◆ Ability to secure each now influenced by the security on every computer to which it is connected

What Is Security?

- ◆ “The quality or state of being secure--to be free from danger”
- ◆ To be protected from adversaries
- ◆ A successful organization should have multiple layers of security in place:
 - Physical security
 - Personal security
 - Operations security
 - Communications security
 - Network security

What Is Information Security?

- ◆ The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information
- ◆ Tools, such as policy, awareness, training, education, and technology are necessary
- ◆ The C.I.A. triangle was the standard based on confidentiality, integrity, and availability
- ◆ The C.I.A. triangle has expanded into a list of critical characteristics of information

Critical Characteristics Of Information

The value of information comes from the characteristics it possesses.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Components of an Information System

- ◆ To fully understand the importance of information security, you need to know the elements of an information system
- ◆ An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization

Securing the Components

- ◆ The computer can be either or both the subject of an attack and/or the object of an attack
- ◆ When a computer is
 - the subject of an attack, it is used as an active tool to conduct the attack
 - the object of an attack, it is the entity being attacked

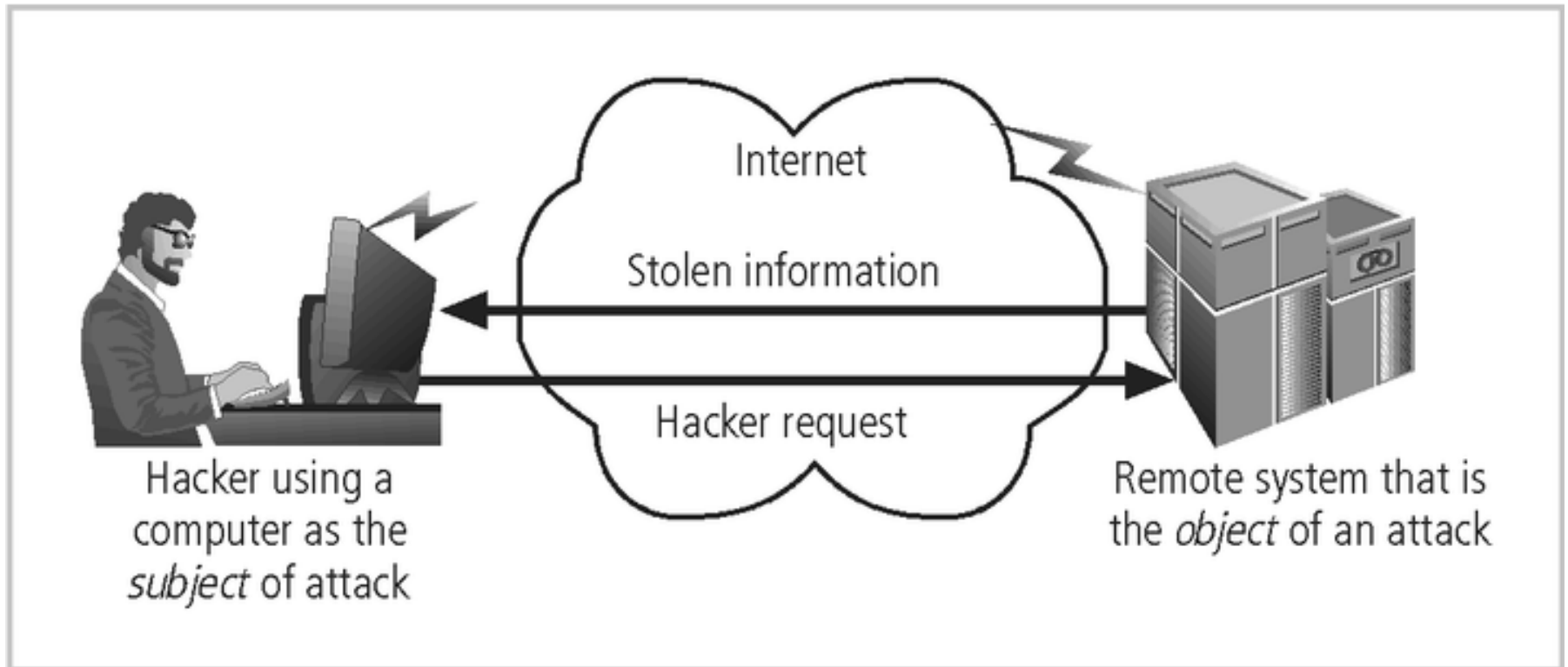


FIGURE 1-5 Computer as the Subject and Object of an Attack

Balancing Security and Access

- ◆ It is impossible to obtain perfect security - it is not an absolute; it is a process
- ◆ Security should be considered a balance between protection and availability
- ◆ To achieve balance, the level of security must allow reasonable access, yet protect against threats

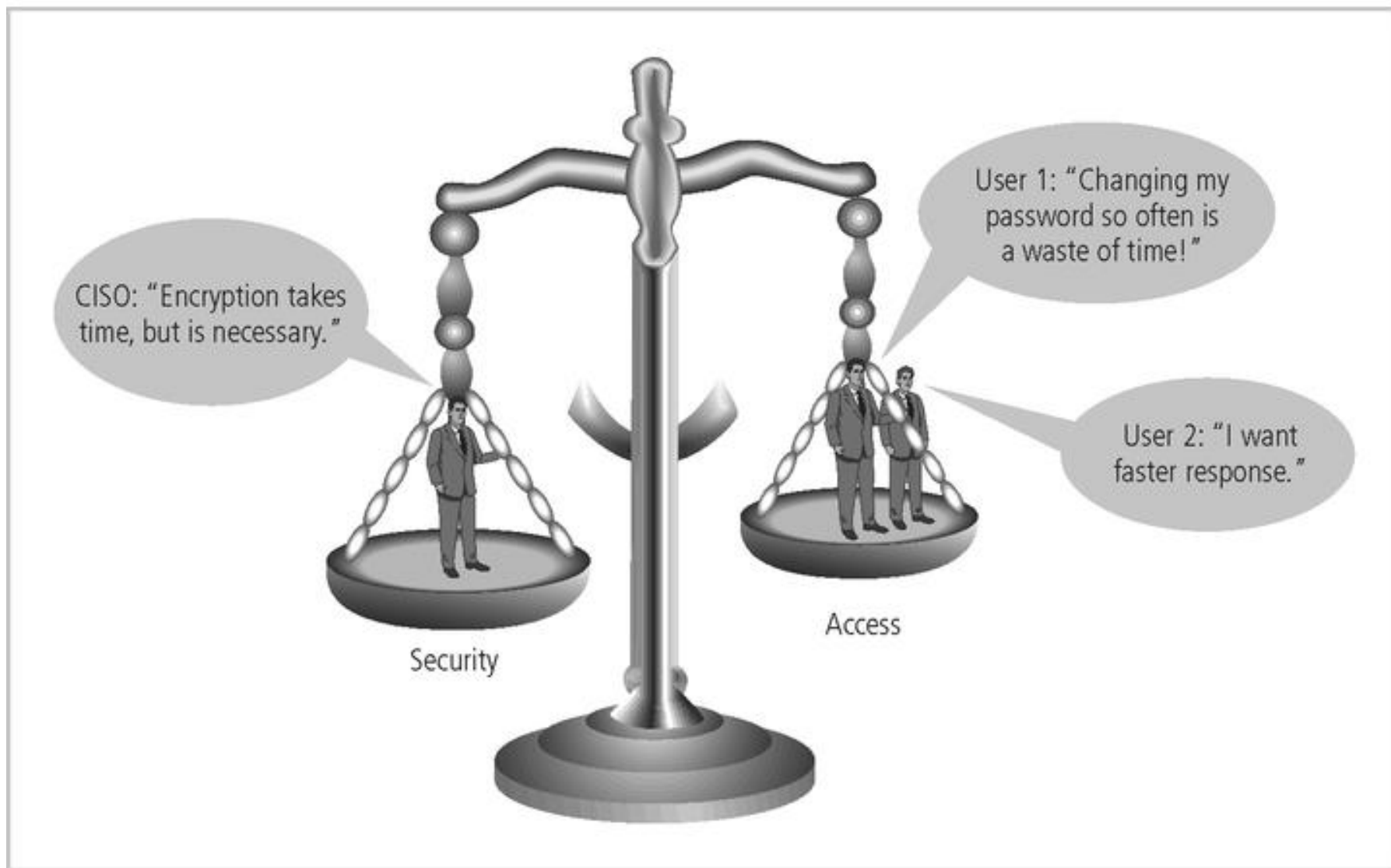


FIGURE 1-6 Balancing Security and Access

Bottom Up Approach

- ◆ Security from a grass-roots effort - systems administrators attempt to improve the security of their systems
- ◆ Key advantage - technical expertise of the individual administrators
- ◆ Seldom works, as it lacks a number of critical features:
 - participant support
 - organizational staying power

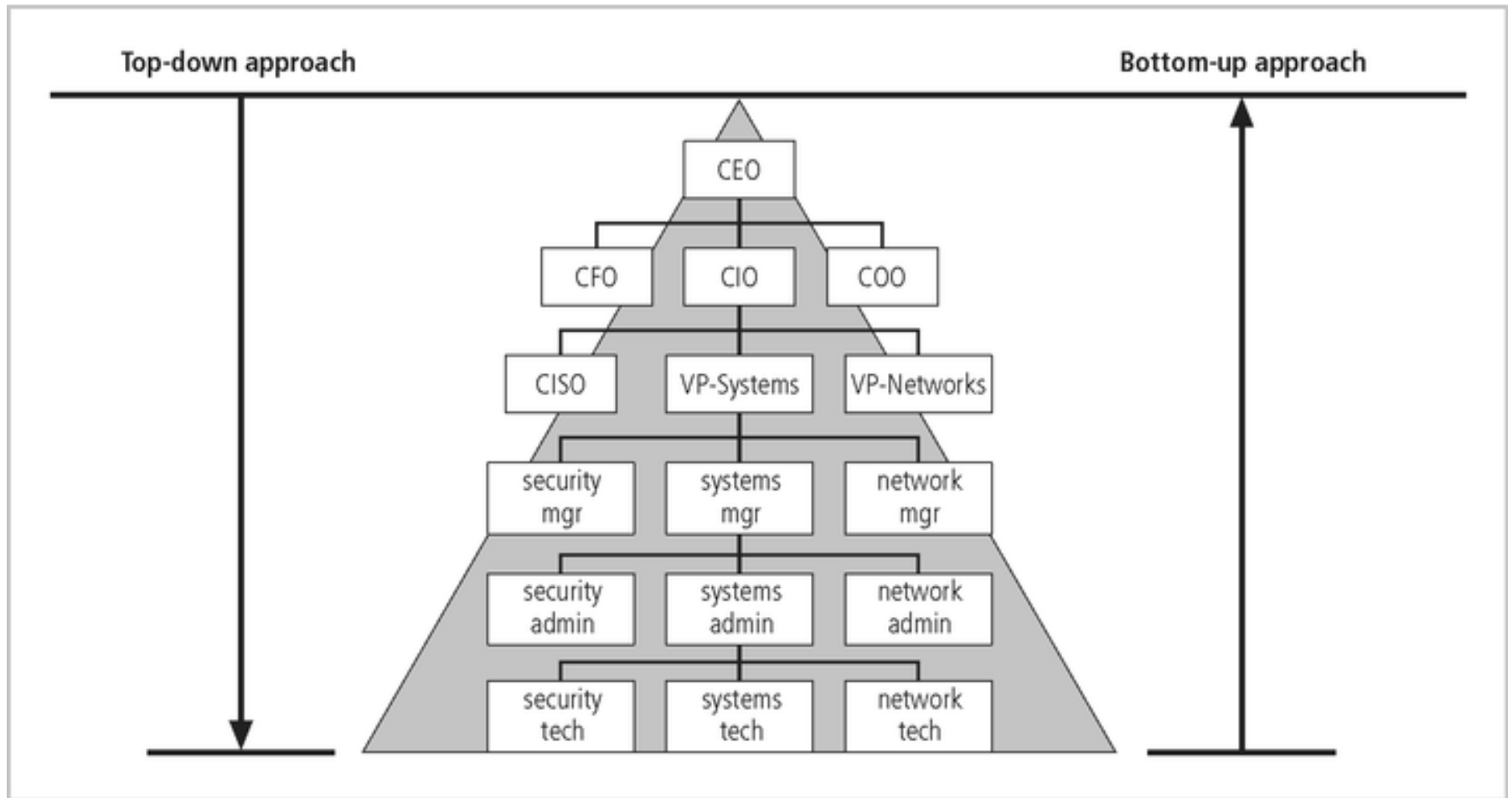


FIGURE 1-7 Approaches to Security Implementation

Top-down Approach

- ◆ **Initiated by upper management:**
 - issue policy, procedures, and processes
 - dictate the goals and expected outcomes of the project
 - determine who is accountable for each of the required actions
- ◆ **This approach has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the chance to influence organizational culture**
- ◆ **May also involve a formal development strategy referred to as a systems development life cycle**
 - Most successful top-down approach

The Systems Development Life Cycle

- ◆ Information security must be managed in a manner similar to any other major system implemented in the organization
- ◆ Using a methodology
 - ensures a rigorous process
 - avoids missing steps
- ◆ The goal is creating a comprehensive security posture/program

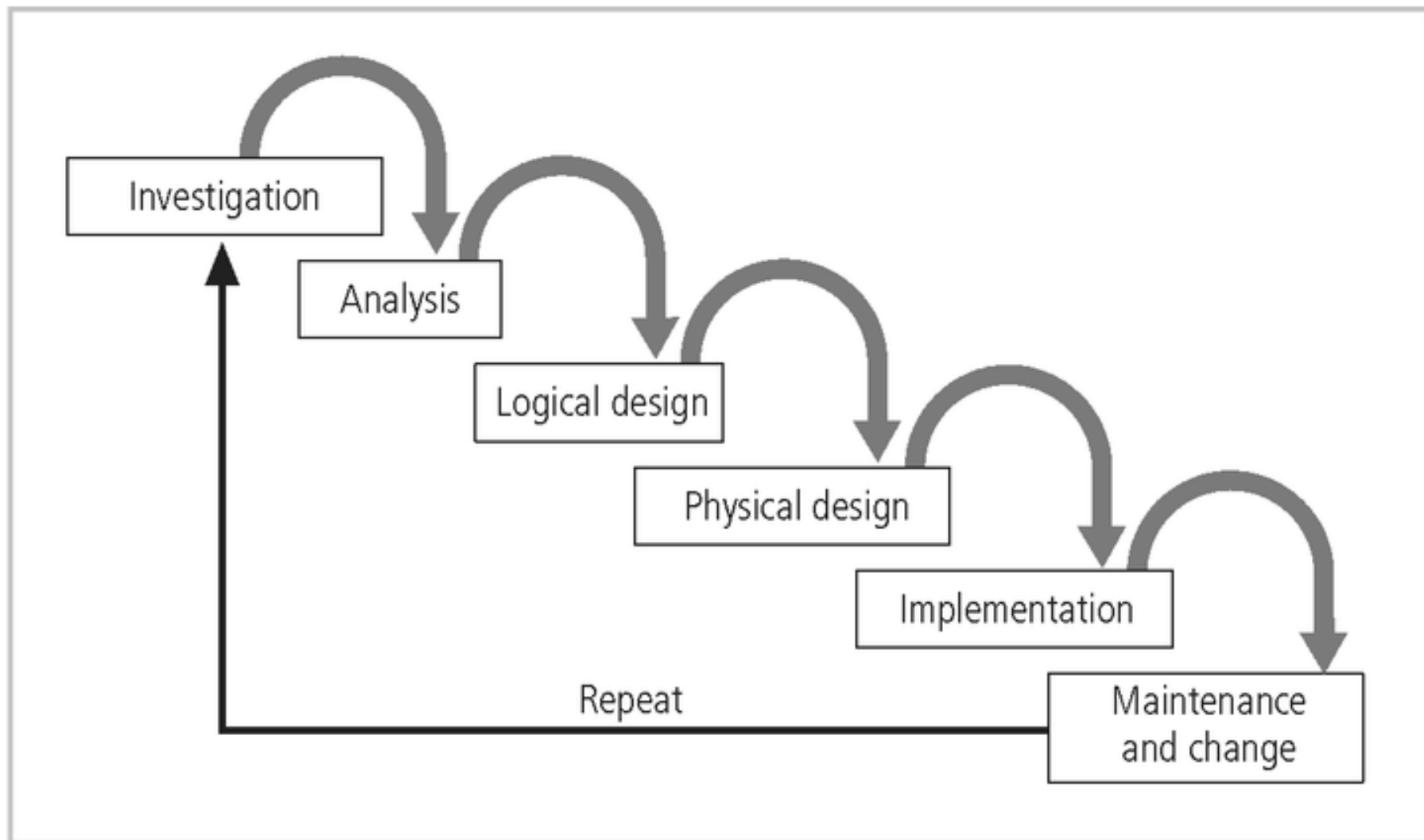


FIGURE 1-8 SDLC Waterfall Methodology

SDLC and the SecSDLC

- ◆ The SecSDLC may be
 - event-driven - started in response to some occurrence or
 - plan-driven - as a result of a carefully developed implementation strategy
- ◆ At the end of each phase comes a structured review

Investigation

- ◆ What is the problem the system is being developed to solve?
 - The objectives, constraints, and scope of the project are specified
 - A preliminary cost/benefit analysis is developed
 - A feasibility analysis is performed to assesses the economic, technical, and behavioral feasibilities of the process

Analysis

- ◆ Consists primarily of
 - assessments of the organization
 - the status of current systems
 - capability to support the proposed systems
- ◆ Analysts begin to determine
 - what the new system is expected to do
 - how the new system will interact with existing systems
- ◆ Ends with the documentation of the findings and a feasibility analysis update

Logical Design

- ◆ Based on business need, applications are selected capable of providing needed services
- ◆ Based on applications needed, data support and structures capable of providing the needed inputs are identified
- ◆ Finally, based on all of the above, select specific ways to implement the physical solution are chosen
- ◆ At the end, another feasibility analysis is performed

Physical Design

- ◆ Specific technologies are selected to support the alternatives identified and evaluated in the logical design
- ◆ Selected components are evaluated based on a make-or-buy decision
- ◆ Entire solution is presented to the end-user representatives for approval

Implementation

- ◆ Components are ordered, received, assembled, and tested
- ◆ Users are trained and documentation created
- ◆ Users are then presented with the system for a performance review and acceptance test

Maintenance and Change

- ◆ Tasks necessary to support and modify the system for the remainder of its useful life
- ◆ The life cycle continues until the process begins again from the investigation phase
- ◆ When the current system can no longer support the mission of the organization, a new project is implemented

Security Systems Development Life Cycle

- ◆ The same phases used in the traditional SDLC adapted to support the specialized implementation of a security project
- ◆ Basic process is identification of threats and controls to counter them
- ◆ The SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

- ◆ Identifies process, outcomes and goals of the project, and constraints
- ◆ Begins with a statement of program security policy
- ◆ Teams are organized, problems analyzed, and scope defined, including objectives, and constraints not covered in the program policy
- ◆ An organizational feasibility analysis is performed

Analysis

- ◆ Analysis of existing security policies or programs, along with documented current threats and associated controls
- ◆ Includes an analysis of relevant legal issues that could impact the design of the security solution
- ◆ The risk management task (identifying, assessing, and evaluating the levels of risk) also begins

Logical & Physical Design

- ◆ Creates blueprints for security
- ◆ Critical planning and feasibility analyses to determine whether or not the project should continue
- ◆ In physical design, security technology is evaluated, alternatives generated, and final design selected
- ◆ At end of phase, feasibility study determines readiness so all parties involved have a chance to approve the project

Implementation

- ◆ The security solutions are acquired (made or bought), tested, and implemented, and tested again
- ◆ Personnel issues are evaluated and specific training and education programs conducted
- ◆ Finally, the entire tested package is presented to upper management for final approval

Maintenance and Change

- ◆ The maintenance and change phase is perhaps most important, given the high level of ingenuity in today's threats
- ◆ The reparation and restoration of information is a constant duel with an often unseen adversary
- ◆ As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation

Security Professionals and the Organization

- ◆ It takes a wide range of professionals to support a diverse information security program
- ◆ To develop and execute specific security policies and procedures, additional administrative support and technical expertise is required

Senior Management

◆ Chief Information Officer

- the senior technology officer
- primarily responsible for advising the senior executive(s) for strategic planning

◆ Chief Information Security Officer

- responsible for the assessment, management, and implementation of securing the information in the organization
- may also be referred to as the Manager for Security, the Security Administrator, or a similar title

Security Project Team

A number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas:

- The champion
- The team leader
- Security policy developers
- Risk assessment specialists
- Security professionals
- Systems administrators
- End users

Data Ownership

- ◆ Data Owner - responsible for the security and use of a particular set of information
- ◆ Data Custodian - responsible for the storage, maintenance, and protection of the information
- ◆ Data Users - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization

Communities Of Interest

- ◆ Each organization develops and maintains its own unique culture and values. Within that corporate culture, there are communities of interest:
 - Information Security Management and Professionals
 - Information Technology Management and Professionals
 - Organizational Management and Professionals

Information Security: Is It an Art or a Science?

- ◆ With the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science

Security as Art

- ◆ No hard and fast rules nor are there many universally accepted complete solutions
- ◆ No magic user's manual for the security of the entire system
- ◆ Complex levels of interaction between users, policy, and technology controls

Security as Science

- ◆ Dealing with technology designed to perform at high levels of performance
- ◆ Specific conditions cause virtually all actions that occur in computer systems
- ◆ Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software
- ◆ If the developers had sufficient time, they could resolve and eliminate these faults

Security as a Social Science

- ◆ Social science examines the behavior of individuals interacting with systems
- ◆ Security begins and ends with the people that interact with the system
- ◆ End users may be the weakest link in the security chain
- ◆ Security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles



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

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



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

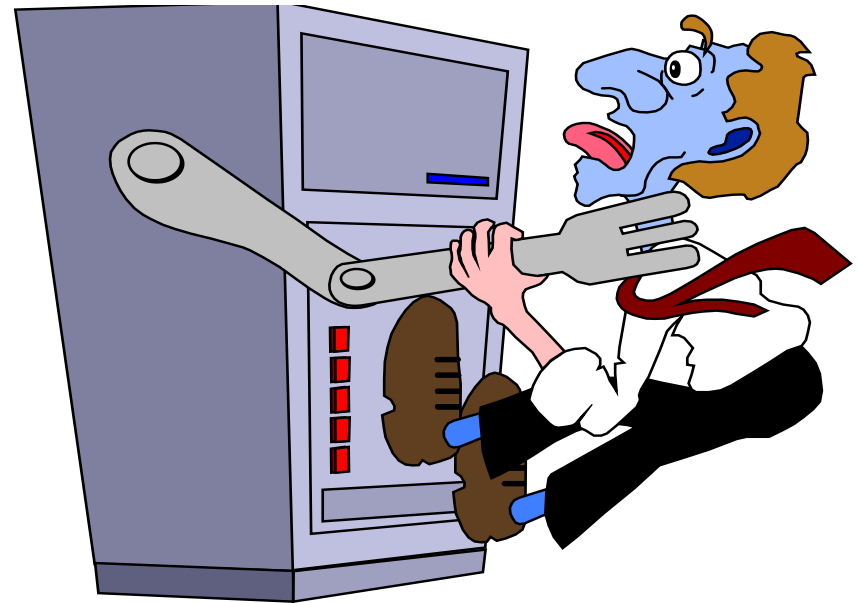
Acts of Human Error or Failure

- 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



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



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

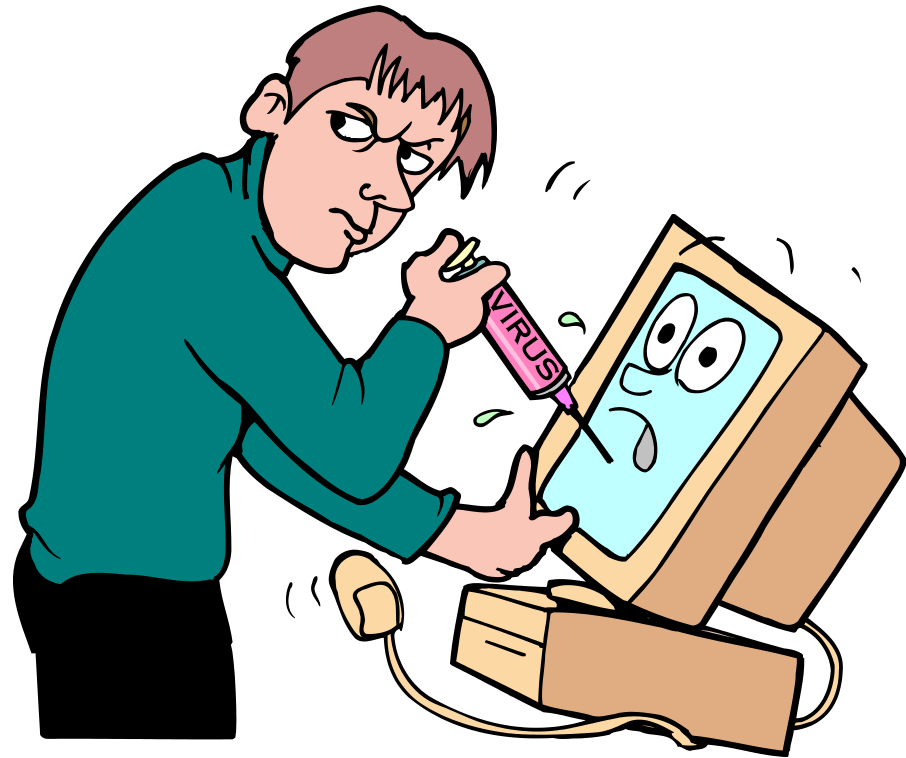
Information Extortion

- 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



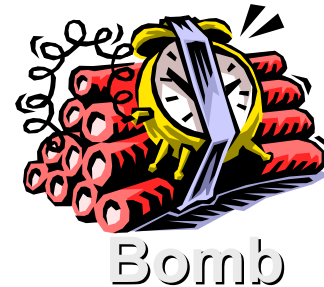
Deliberate Acts of Theft

- 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 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.

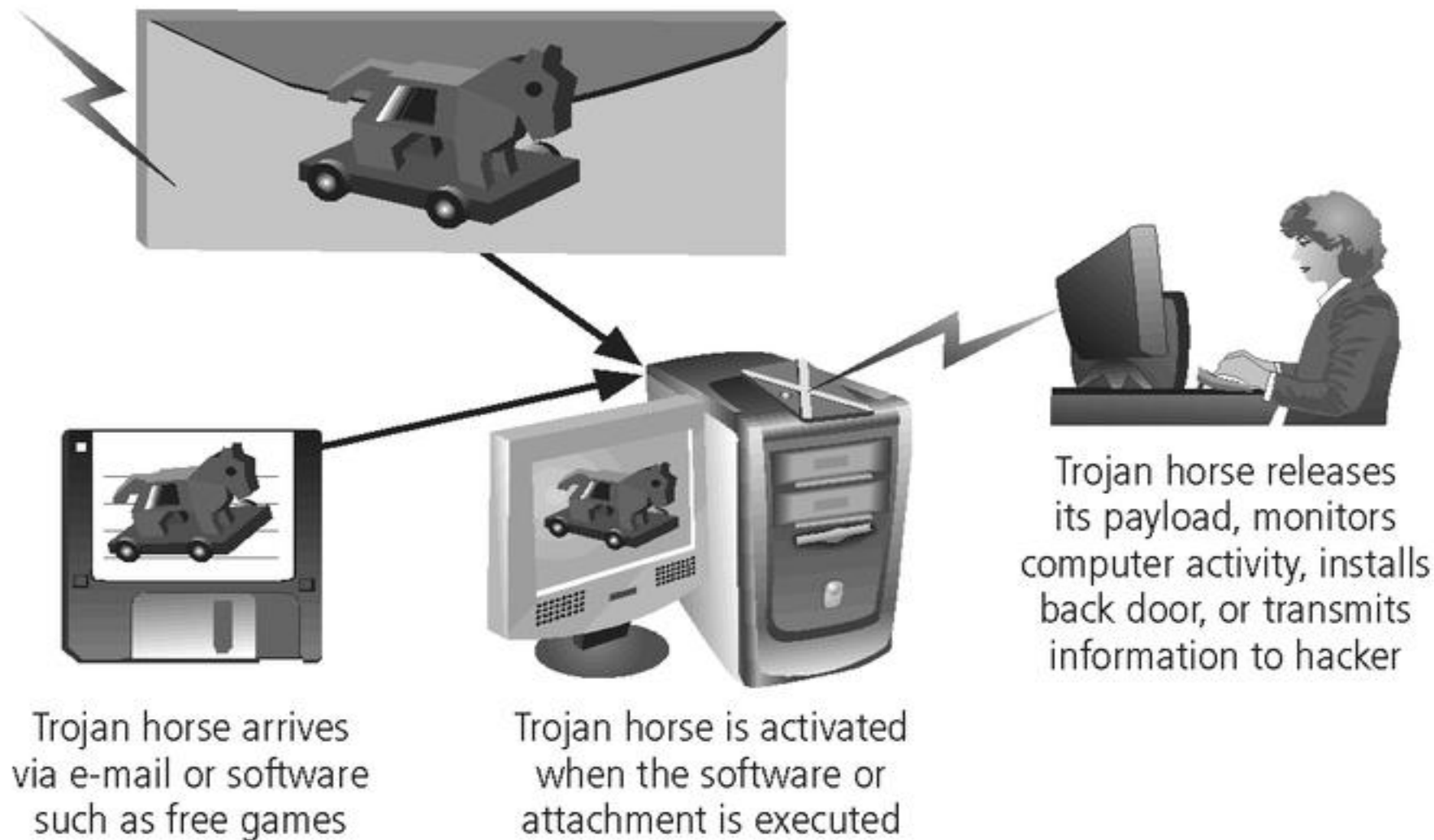



FIGURE 2-8 Trojan Horse Attack

Deliberate Software Attacks

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.

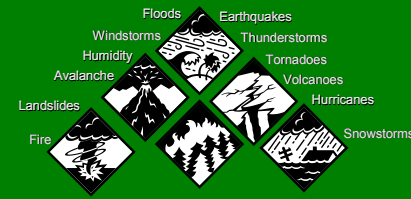
Avoiding Fear Tactics

-  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

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 obsolescence, 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.

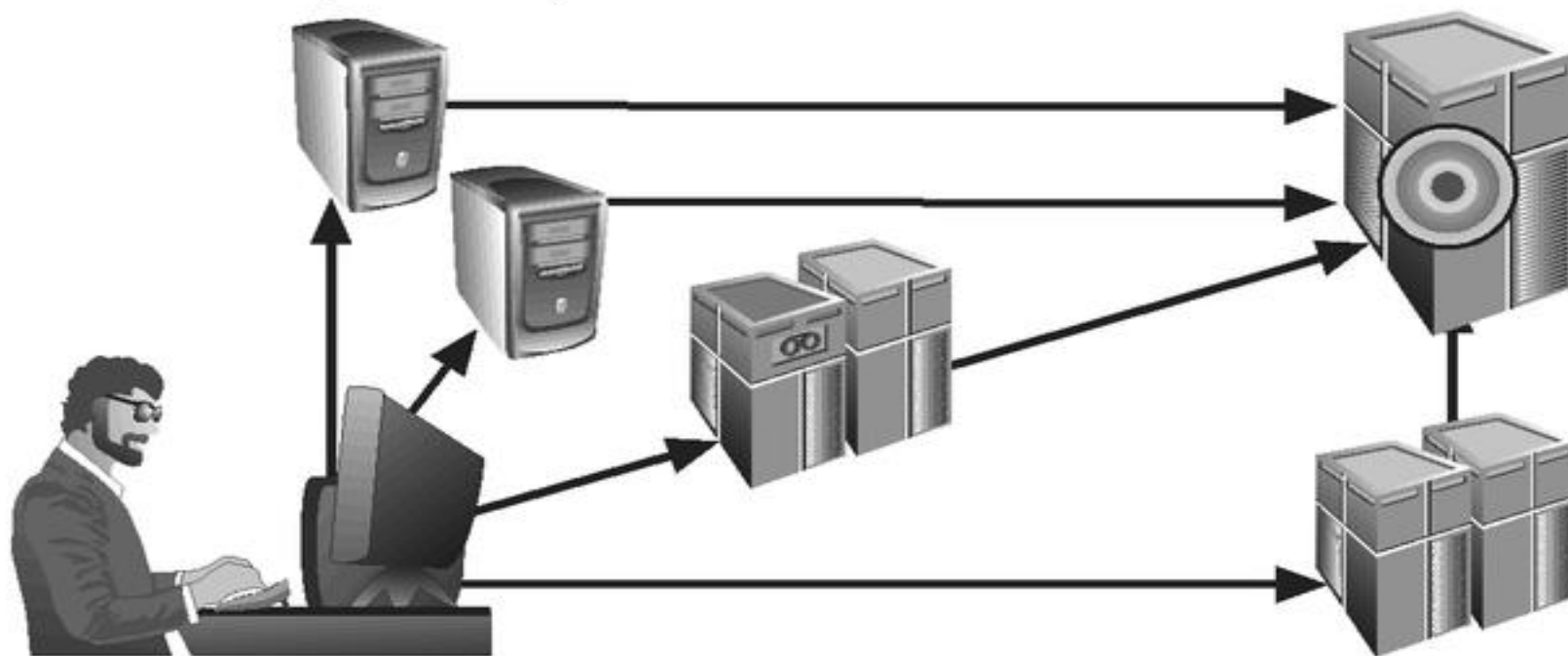


FIGURE 2-9 Denial-of-Service Attacks

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

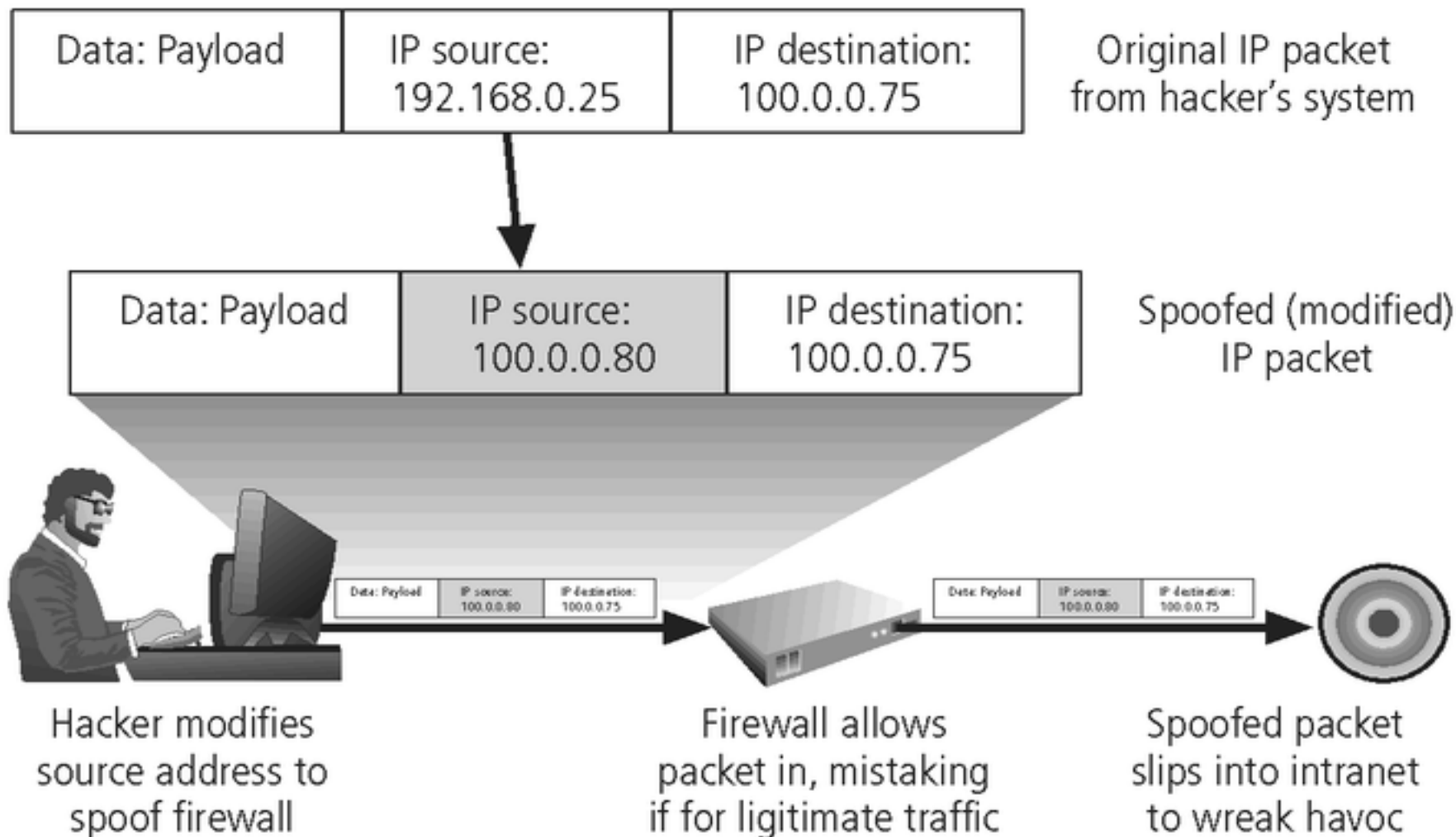


FIGURE 2-10 IP Spoofing

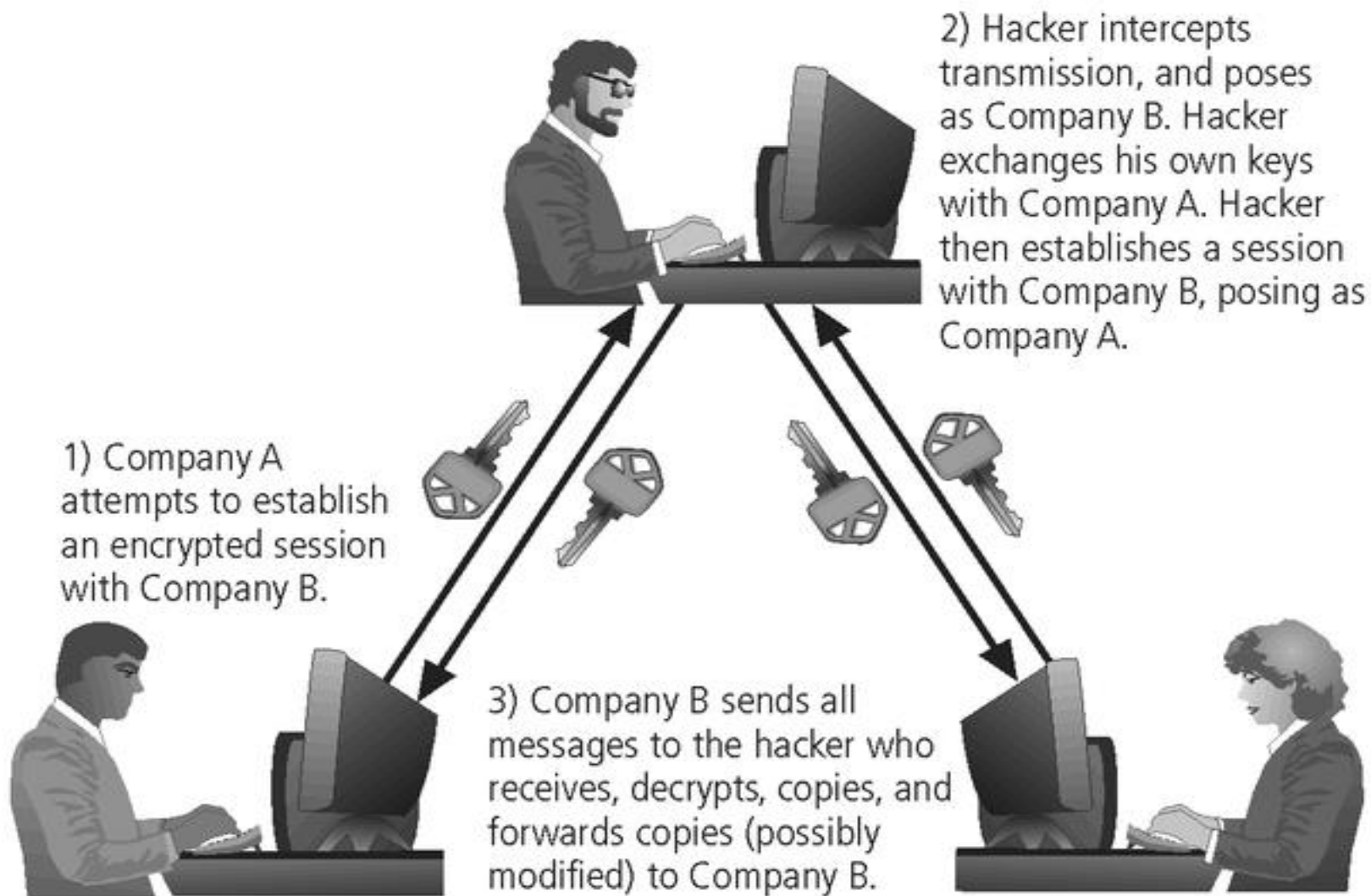





FIGURE 2-11 Man-in-the-Middle Attack

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

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