Information Security

An introduction

What is Security?

Security means protecting any object, computer system, asset from unauthorized access.

Term in Information Security

- **Threat:** It is a potential that can cause harm
- **Vulnerability** is the weakness in the design
- **Attack:** A human who exploits a vulnerability in the computer system perpetrates an attack on the system

Terms cont…

- **Computer Security -** generic name for the collection of tools designed to protect data

- **Network Security -** measures to protect data during their transmission

- **Internet Security -** measures to protect data during their transmission over a collection of interconnected networks

Terms cont…

- Data Security
- Database Security
- OS Security
- Program Security

Protective Measures or Controls

– Control is an action, device, procedure or technique that reduces vulnerability.

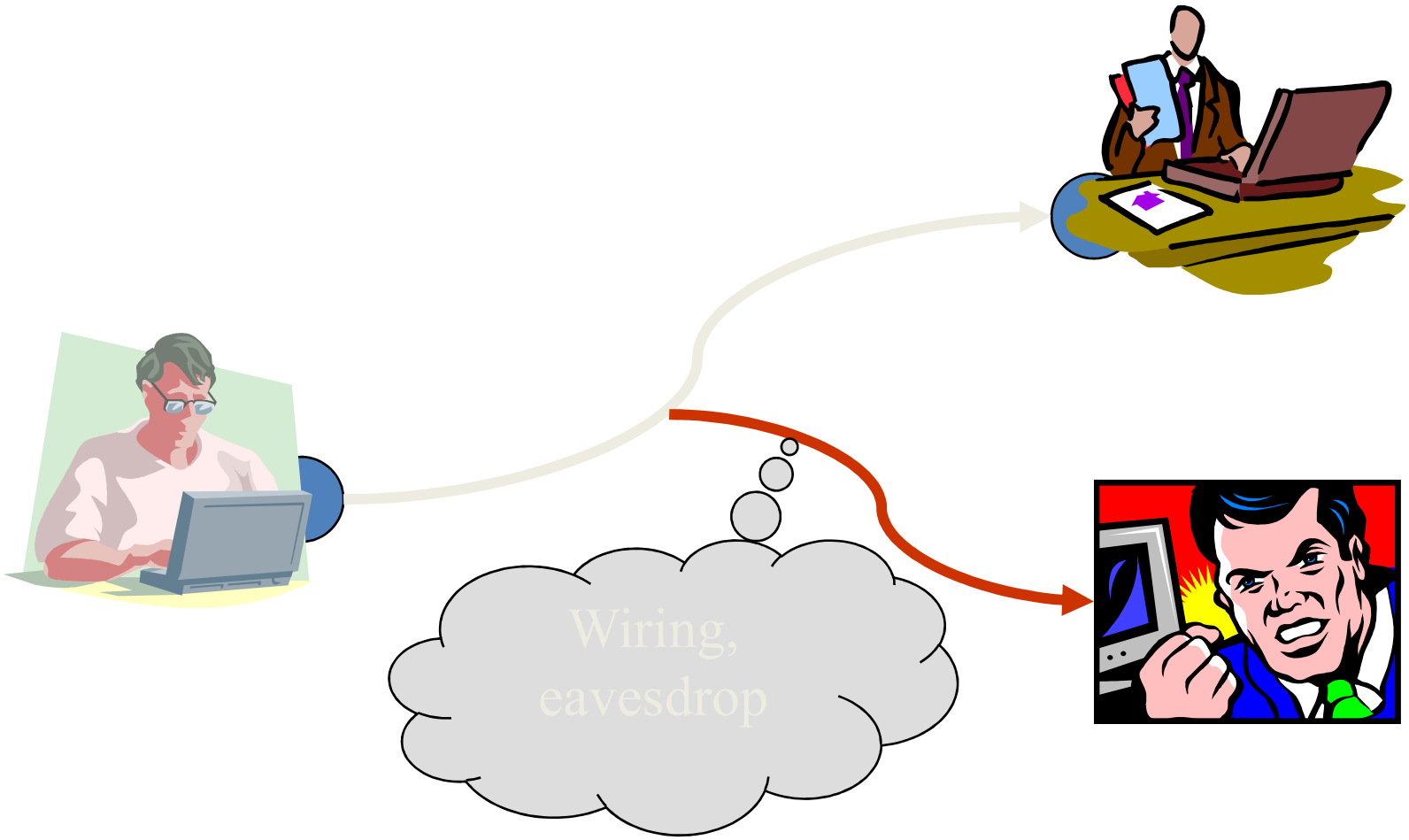
Kinds of Threats

- Interception
  - Release of message contents
  - Traffic analysis
- Interruption
- Modification
- Fabrication
  - To come with something different instead of something existing one.

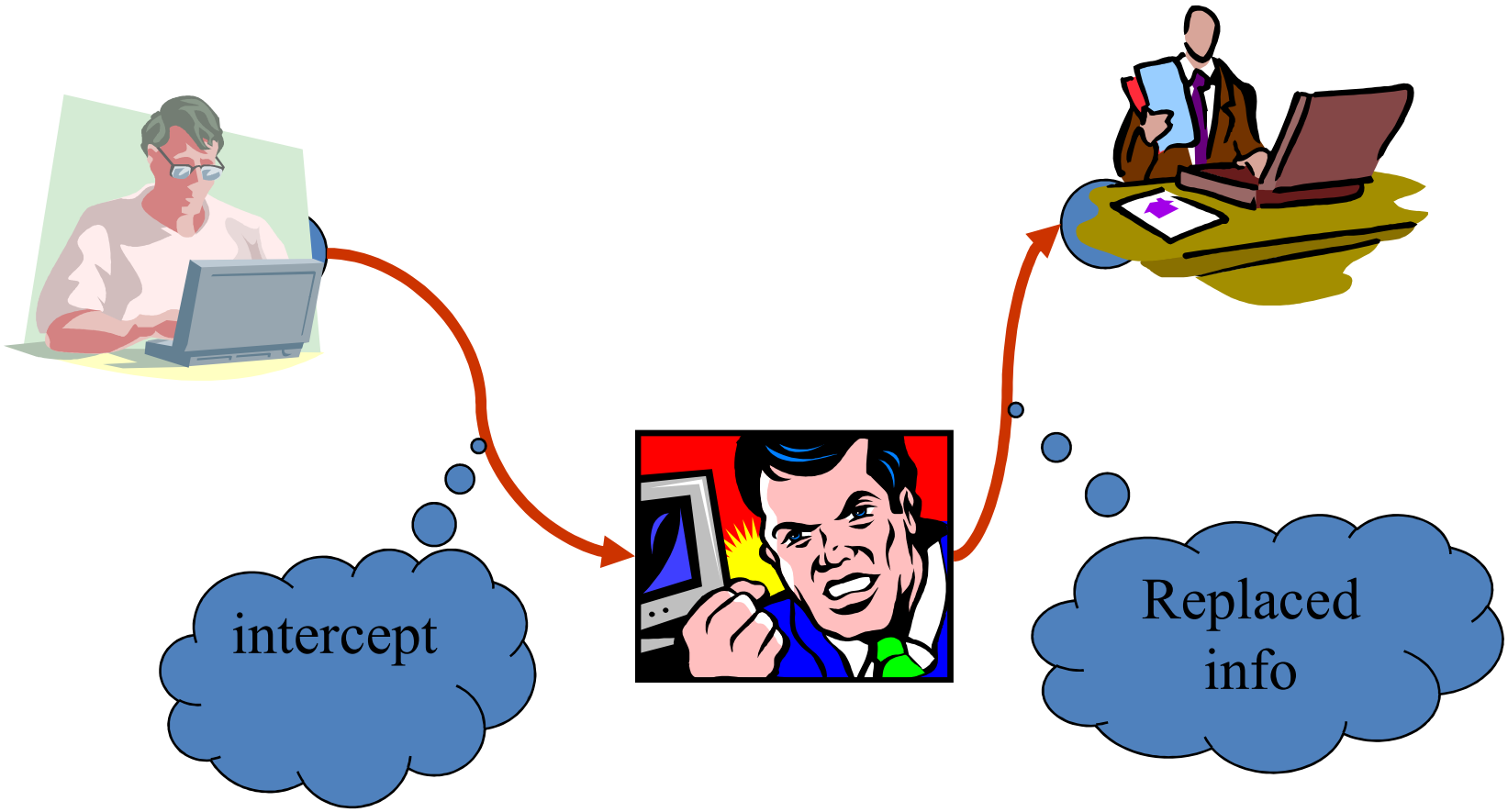
Interruption

Cut wire lines,
Jam wireless
signals,
Drop packets,

Interception



Modification



Fabrication

Also called impersonation

Classify Security Attacks

- **passive attacks** - It attempts to learn or make use of information from the system but does not affect system resources.
- eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
  1. Release of message contents
  2. Traffic analysis

  3. They are very difficult to detect because they do not involve any alteration of the data.

- **active attacks** – Attempts to alter system resources or affect their operation
- modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service
  - It is difficult to prevent active attacks absolutely

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.

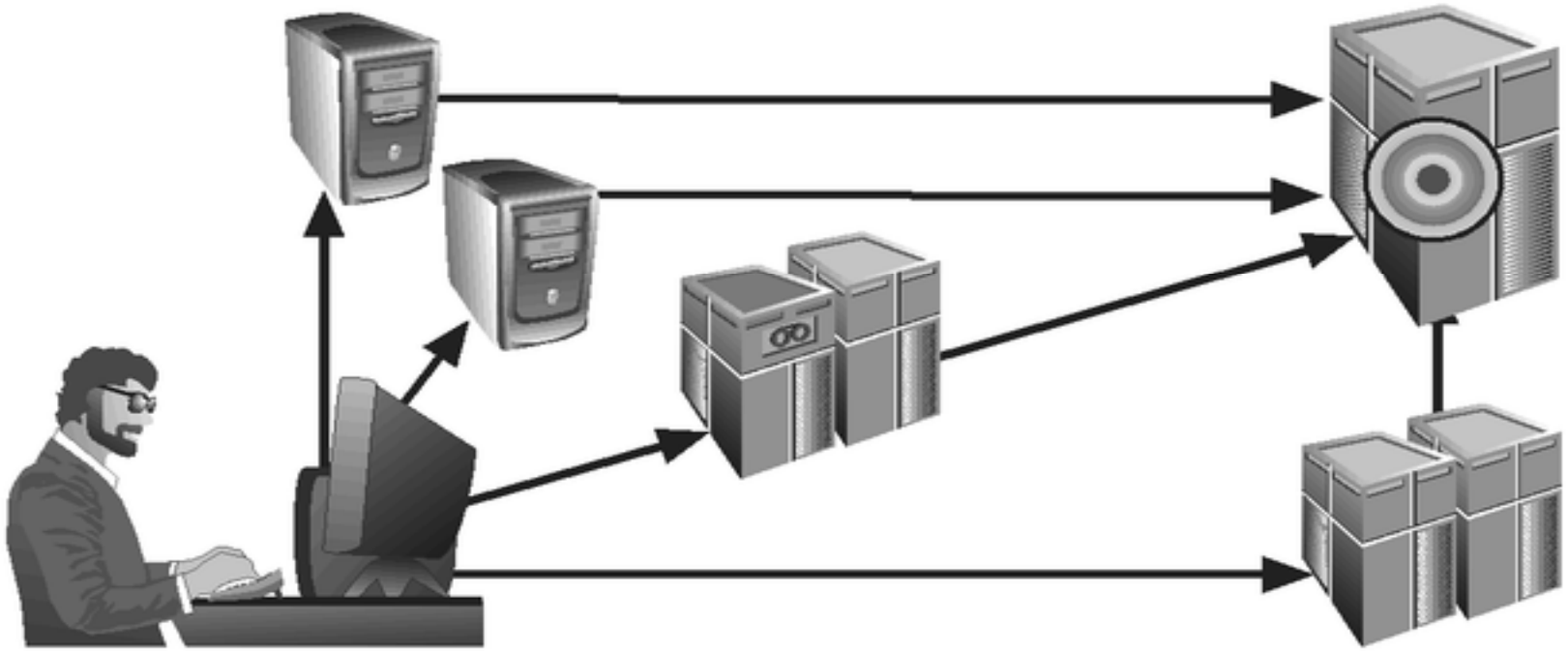


FIGURE 2-9 Denial-of-Service Attacks

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

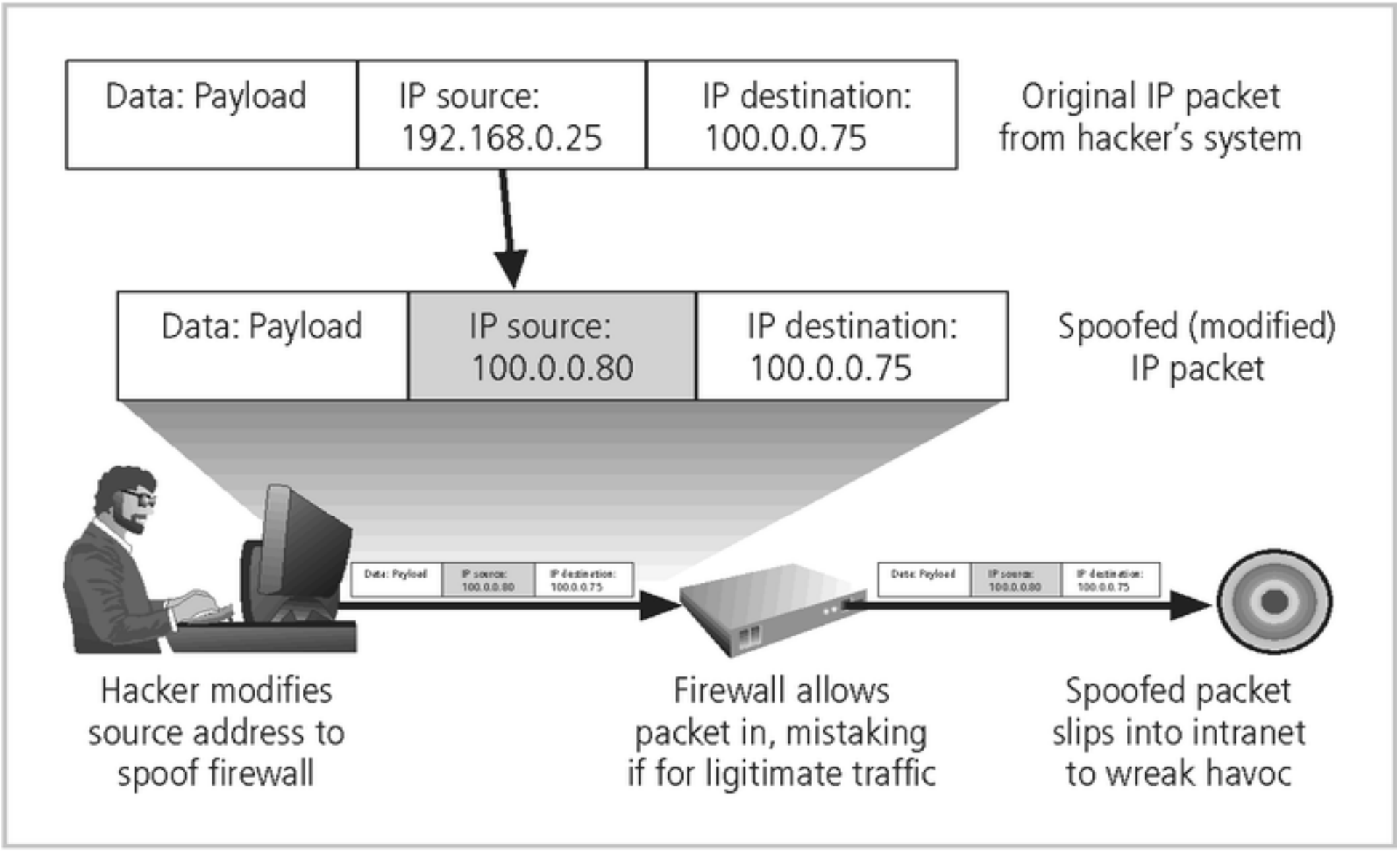


FIGURE 2-10 IP Spoofing

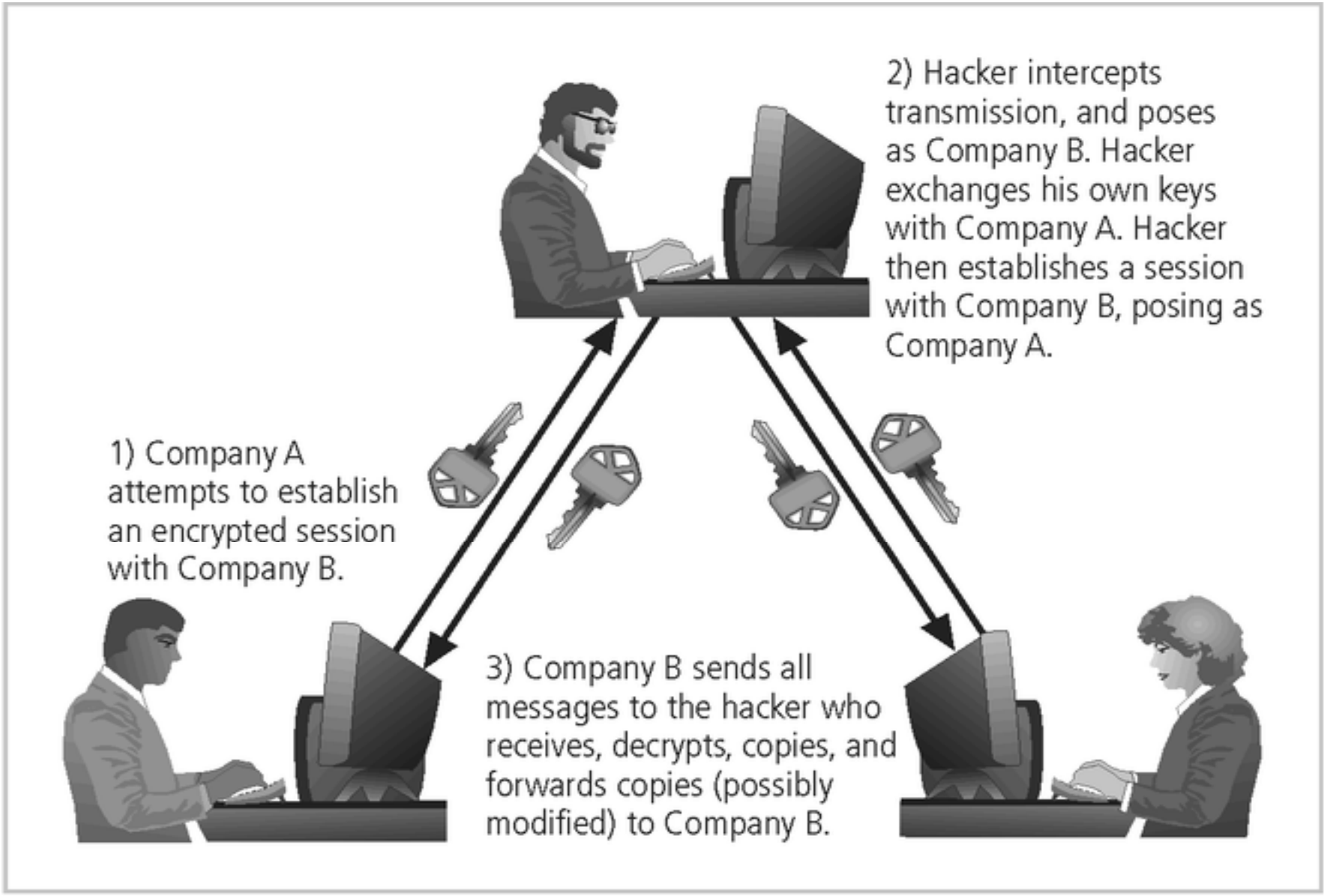


FIGURE 2-11 Man-in-the-Middle Attack

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 papcket, 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

OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Services, Mechanisms, Attacks

- Need systematic way to define requirements

- consider three aspects of information security:
  - **Security attack:** any action that compromises the security information owned by an organization
  - **Security mechanism:** a process that is designed to detect, prevent, or recover from a security attack
  - **Security service:** is something that enhances the security of the data processing systems and the information transfers of an organization

Security Services

- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- **Authentication**
  - the recipient should be able to identify the sender, and verify that the purported sender actually did send the message.
- **Integrity**
  - the recipient should be able to determine if the message has been altered during transmission.
- **Confidentiality**
  - only an authorized recipient should be able to extract the contents of the message from its encrypted form. Otherwise, it should not be possible to obtain any significant information about the message contents.
- **Non-Repudiation**
  - the sender should not be able to deny sending the message.
- **Access Control**
  - Prevention of unauthorized use of a resource.

Security Mechanisms

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
- hence our focus is on this area.

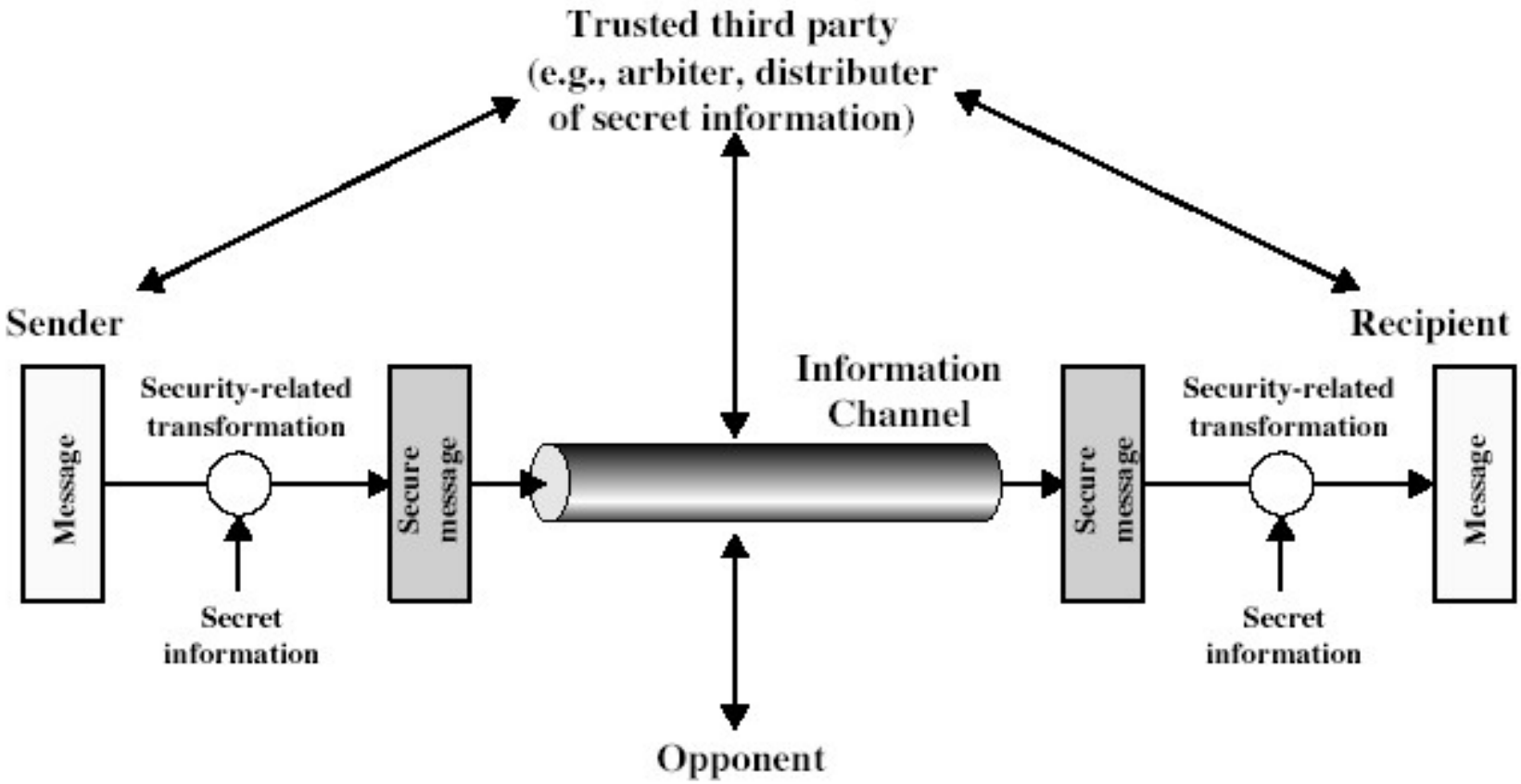
Security Mechanism cont…

- **Encipherment**
- **Digital Signature**
- **Access Control**
  - **Proxy Server**
  - **Firewall**
- **Data Integrity**
- **Authentication Exchange**

Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Model for Network Security



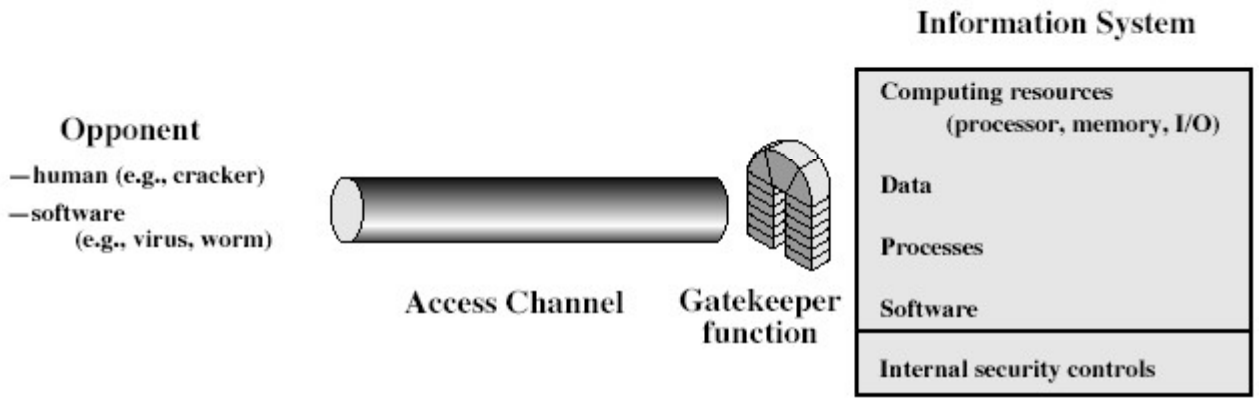
Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

Thank you….