

MS 102

Lecture 1: Introduction to ICT

Course Instructor:
Mr. Gilbert M. G

ICT

- ICT stands for Information Communications Technology.
- ICT refers to any device or system that allows the storage, retrieval, manipulation, transmission and receipt of digital information.
- For example, personal computers, digital television, email, robots.

ICT

- ICT hardware will include:
 - • computers
 - • scanners
 - • digital cameras.

ICT

- ICT covers software will include:
- Standard Office Applications: (Word processor, Spreadsheets, database, graphics etc)
- Accounting packages
- Computer Aided Design

ICT

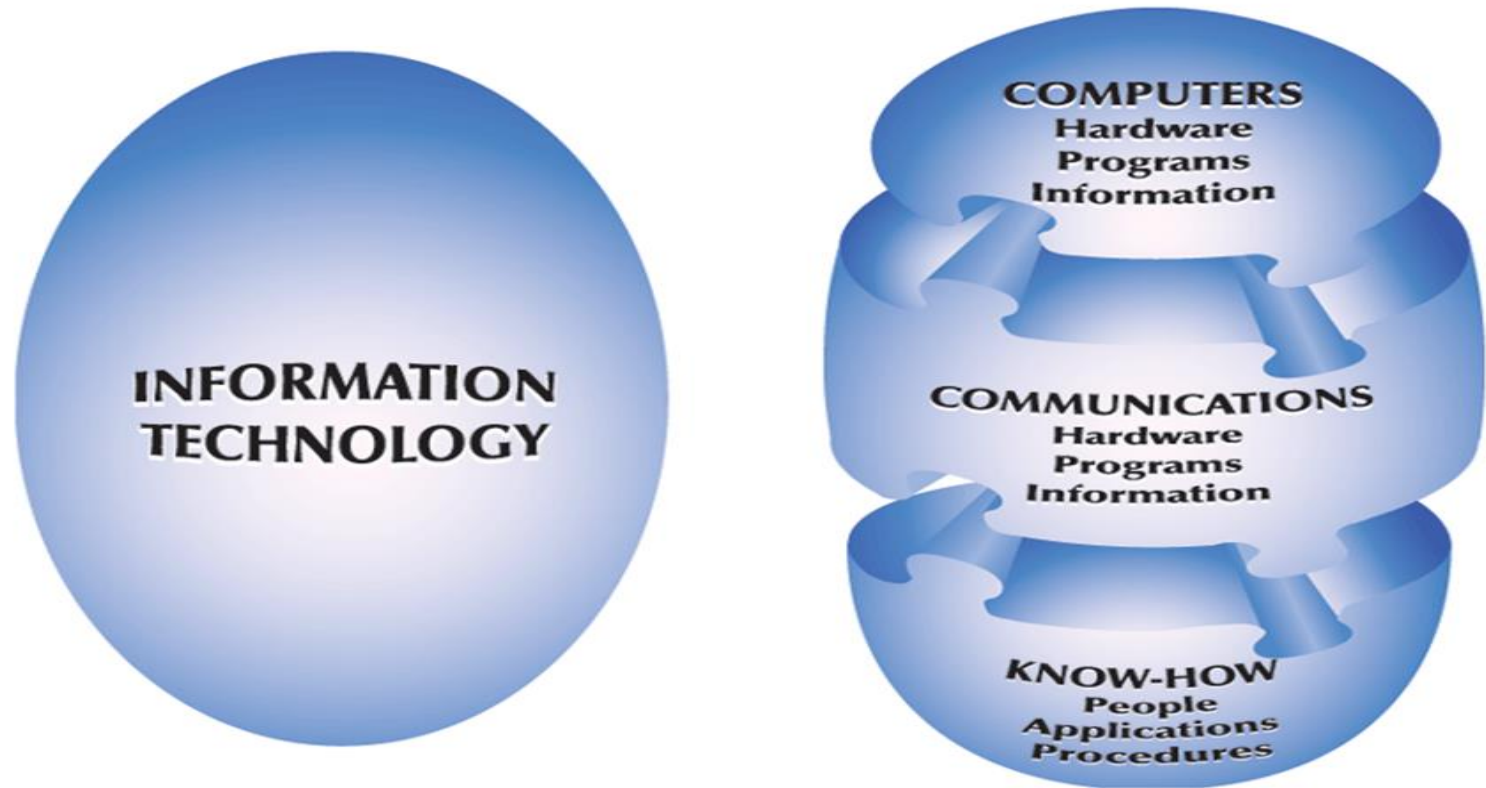
- The 'C' in ICT stands for communications
- Covers all the communications technologies such as:-
 - • digital TV
 - • digital radio
 - • e-mail
 - • Internet
 - • broadband
 - • networks (wired and wireless)
 - • mobile phones
 - • GPS (global positioning systems)
 - • videoconferencing
 - • instant messaging
 - • fax

IT

- Stands for Information Technology
- Refers to a wide variety of items and abilities used in the **creation, storage, and dispersal** of data and information.
- Its three main components are **computers, communications networks, and know-how.**

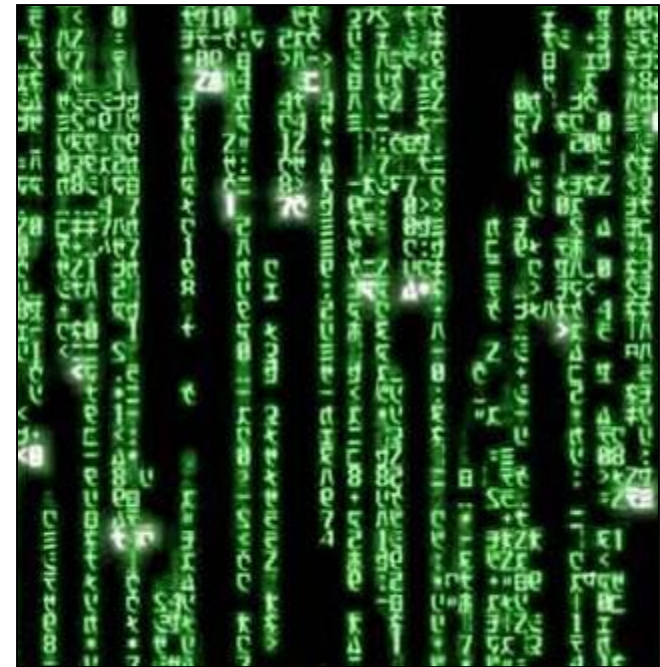
IT

Figure 1.4 The Forces of Information Technology



Data

- Data **are** raw facts and figures that on their own have no meaning
- These can be any alphanumeric characters i.e. text, numbers, symbols



Note the “**are**” bit above? What does this mean?

Data Examples

- Yes, Yes, No, Yes, No, Yes, No, Yes
- 42, 63, 96, 74, 56, 86
- 111192, 111234
- None of the above data sets have any meaning until they are given a **CONTEXT** and **PROCESSED** into a useable form

Data Into Information

- To achieve its aims the organisation will need to **process** data into information.
- Data needs to be turned into meaningful information and presented in its most useful format
- Data must be processed in a **context** in order to give it meaning

Information

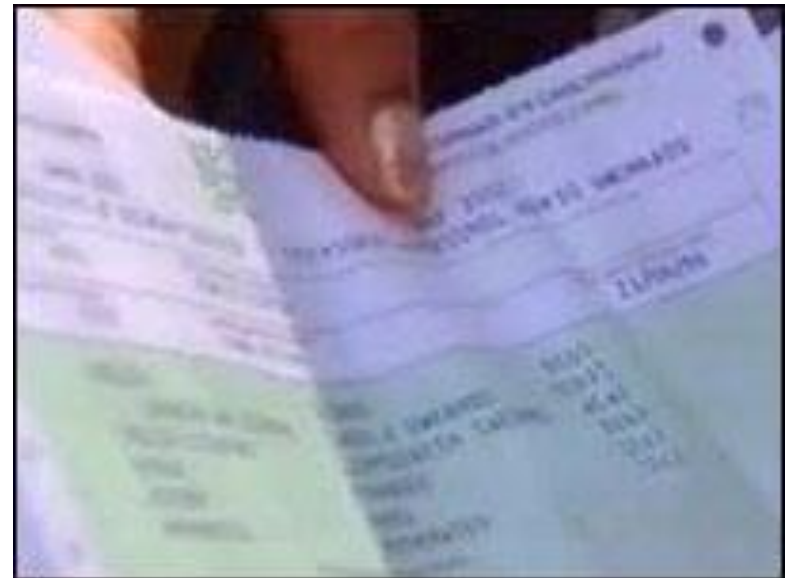
- Data that has been processed within a context to give it meaning

OR

- Data that has been processed into a form that gives it meaning

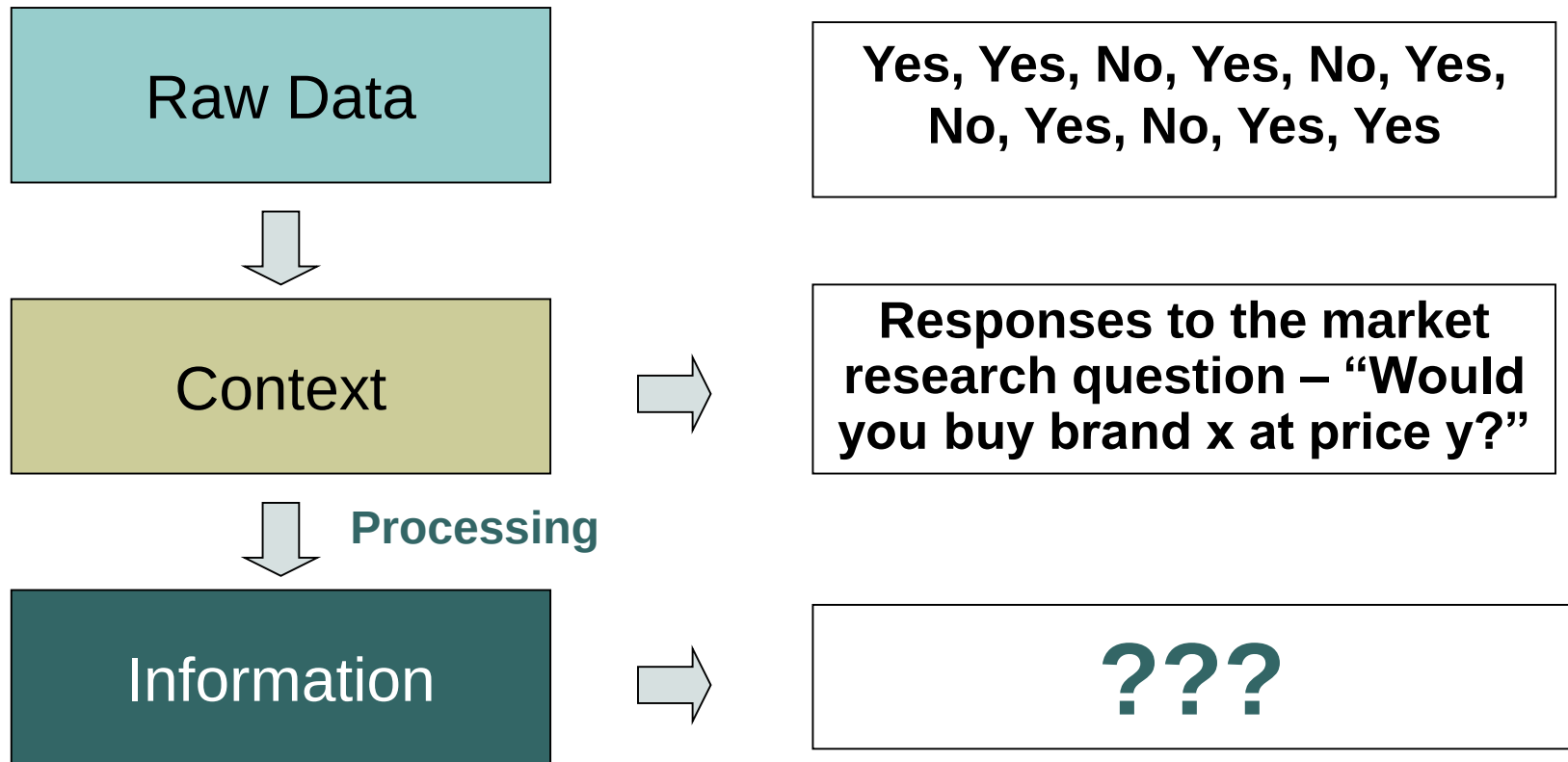
Examples

- In the next 3 examples explain how the data could be processed to give it meaning
- What information can then be derived from the data?

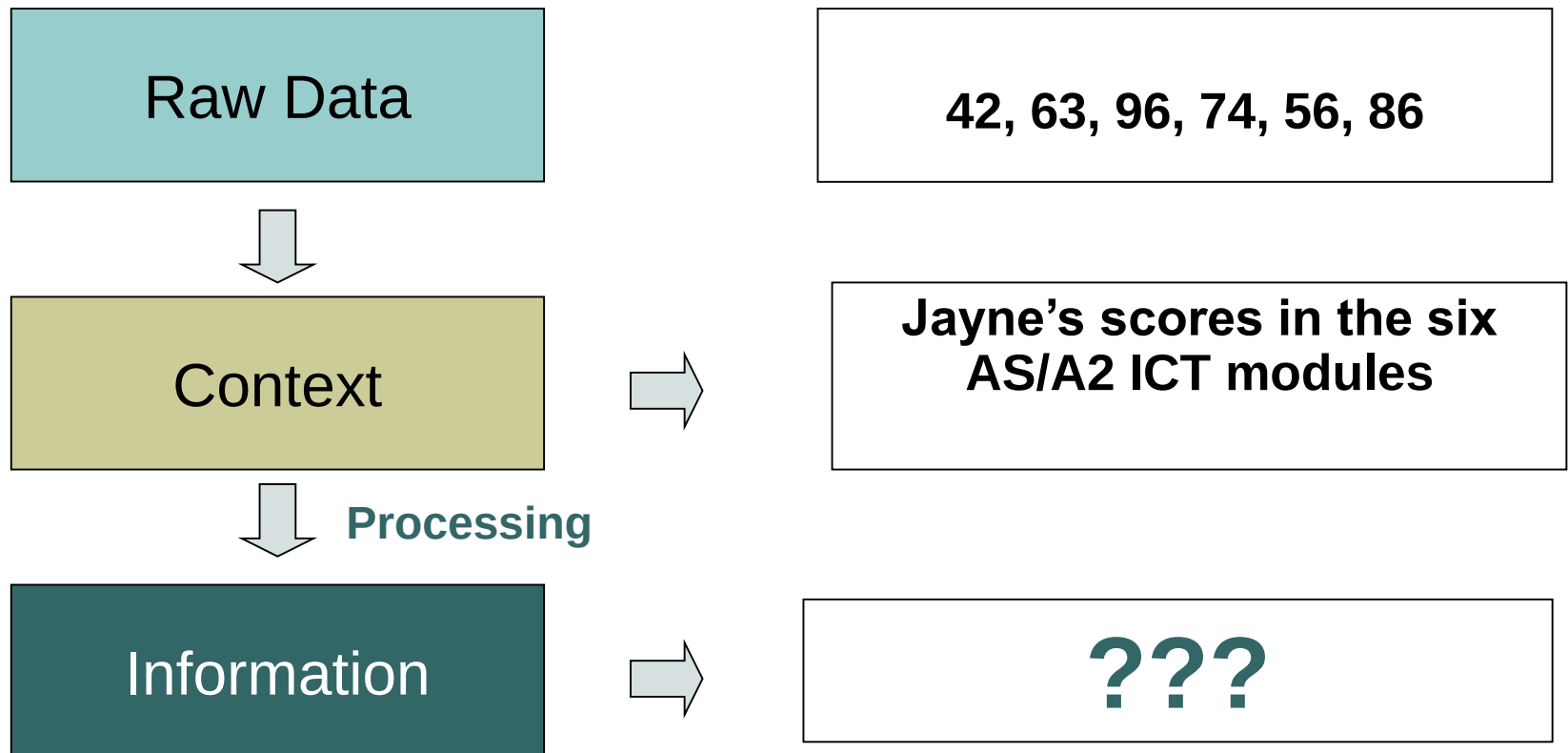


Suggested answers are given at the end of this presentation

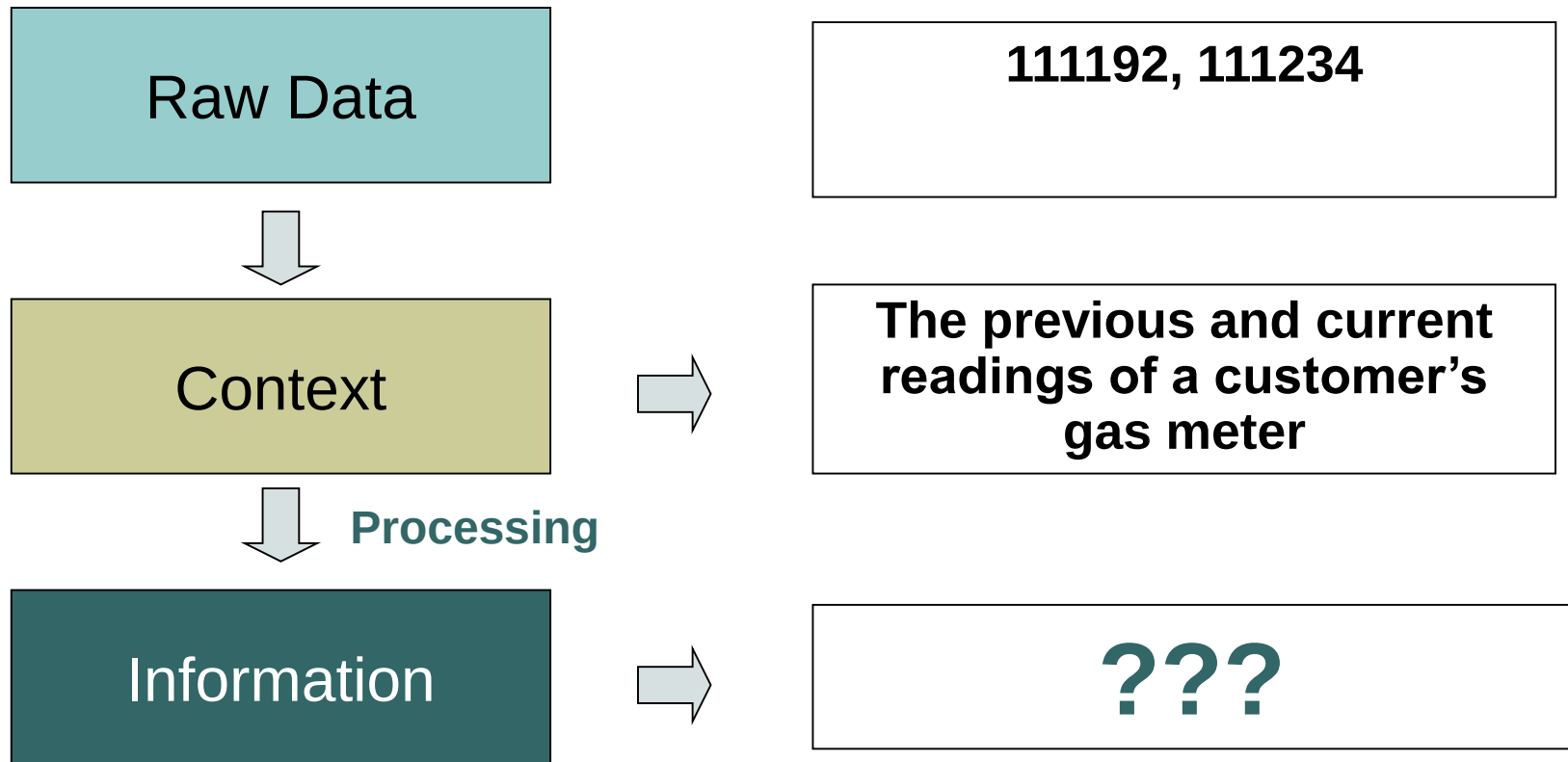
Example 1



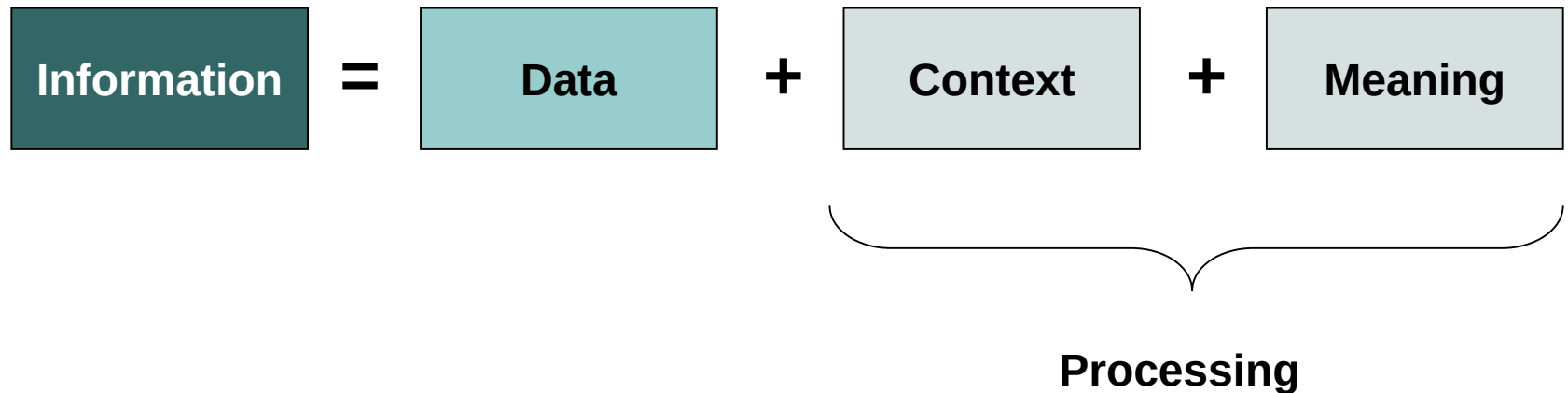
Example 2



Example 3



Summary

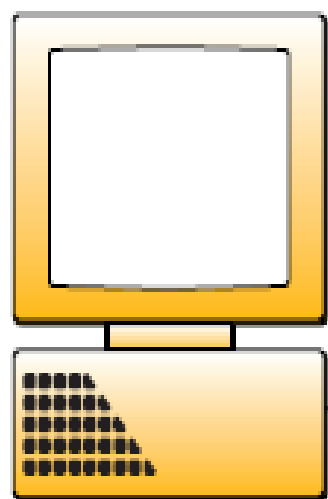


Data – raw facts and figures

Information – data that has been processed (in a context) to give it meaning

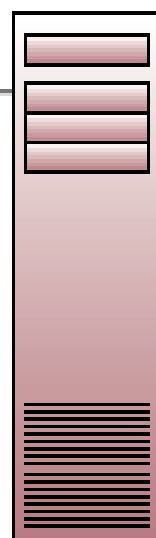
Computer

- An electronic system that can be instructed to accept, process, store, and present data and information.
- Computers come in four sizes:
 - Microcomputers
 - Midrange computers
 - Mainframes
 - Supercomputers



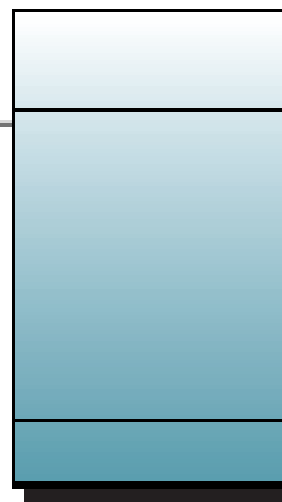
■ **Microcomputer Systems**

Personal computers, network computers, technical workstations, personal digital assistants, information appliances, etc.



■ **Midrange Systems**

Network servers, minicomputers, Web servers, multiuser systems, etc.



■ **Mainframe Systems**

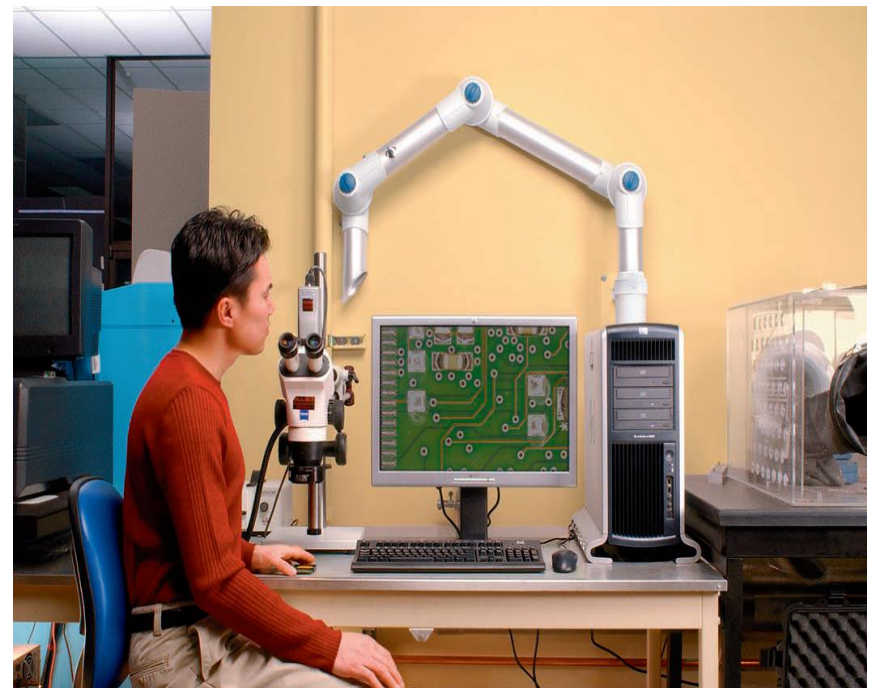
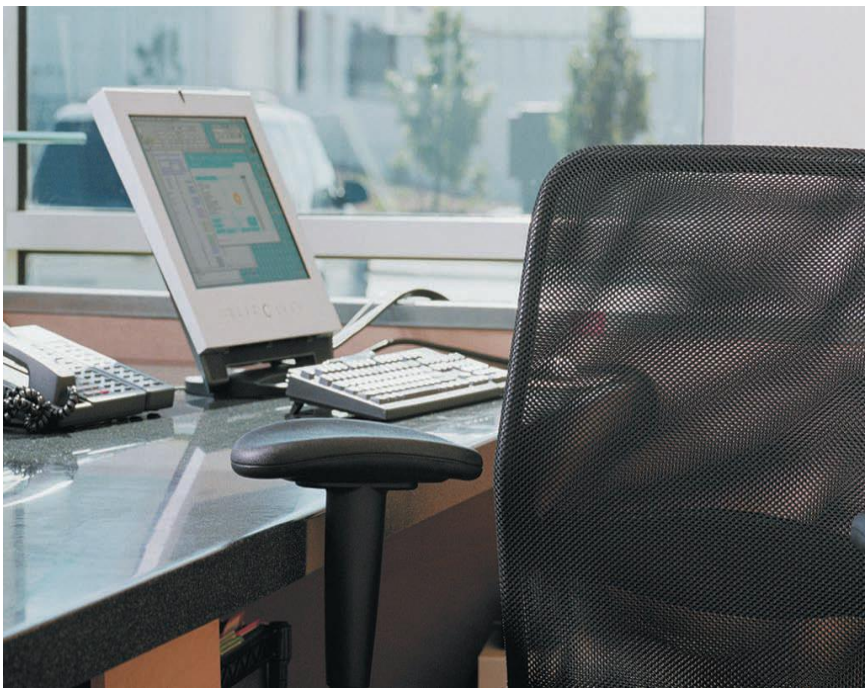
Enterprise systems, superservers, transaction processors, supercomputers, etc.

FIGURE 3.3

Examples of computer system categories.

Computers

- **Microcomputers**: A relatively compact type of computer, the most common of all, easily outsells all other types of computers annually for use in business and at home.
- Five types of Microcomputers:
 - Desktop Computers
 - Notebook Computers/Laptop Computers
 - Tablet PCs
 - Personal Digital Assistants
 - Palm PCs



Microcomputers

Computers

- *Midrange computers and Mainframes*: A computer uses to interconnect people and large sets of information. More powerful than a microcomputer, the minicomputer is usually dedicated to performing specific functions.
- *Supercomputers*: The most powerful of all computers, supercomputers were designed to solve problems consisting of long and difficult calculations.



Supercomputer

Computers

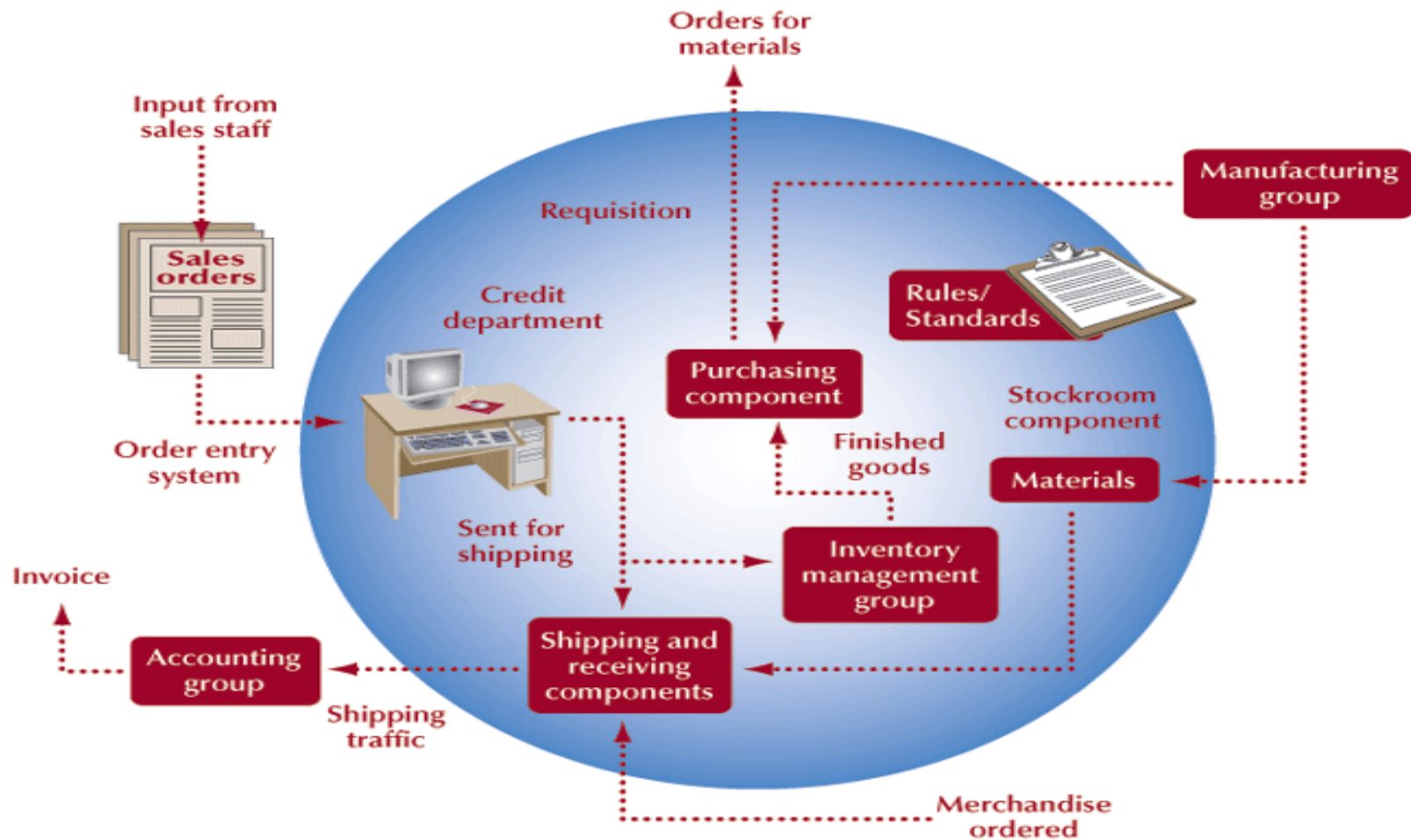
- *Hardware:* The computer and its associated equipment.
- *Program:* A set of instructions that directs a computer to perform certain tasks and produce certain results.
- *Software:* The general term for a set of instructions that controls a computer or a communications network.

Computers

- *System*: A set of components that interact to accomplish a purpose.
- *Information System*: A business information system designed to produce the information needed for successful management of a structured problem, process, department, or business.

Computers

Figure 1.9 A Typical Business System



IT

Communications Networks

- *Communication:* The sending and receiving of data and information over a communications network.
- *Communications Network:* A set of locations, or nodes, consisting of hardware, programs, and information linked together as a system that transmits and receives data and information.
- *Data Communication:* The transmission of data and information through a communications medium.

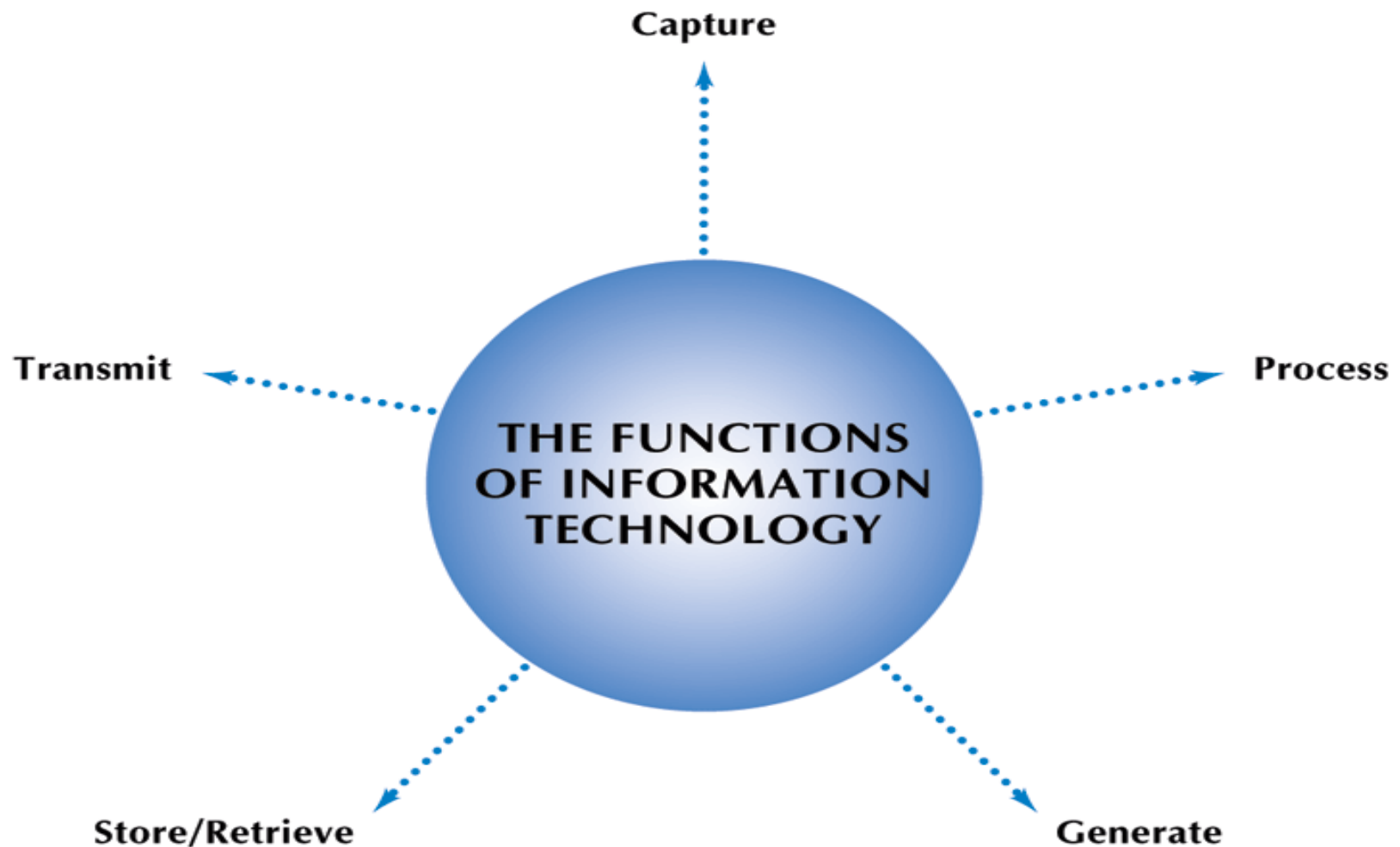
IT

Know-How

- The capability to do something well.
- Information technology know-how consists of:
 - Familiarity with the tools of IT; including the Internet
 - Possession of the skills needed to use these tools
 - An understanding of when to use IT to solve a problem or create an opportunity

The Functions of Information Technology

Figure 1.10 The Six Functions of Information Technology



The Functions of Information Technology (Continued)

- *Capture*: The process of compiling detailed records of activities.
- *Processing*: The process of converting, analyzing, computing, and synthesizing all forms of data or information.
 - Data Processing
 - Information Processing
 - Word Processing
 - Image Processing
 - Voice Processing

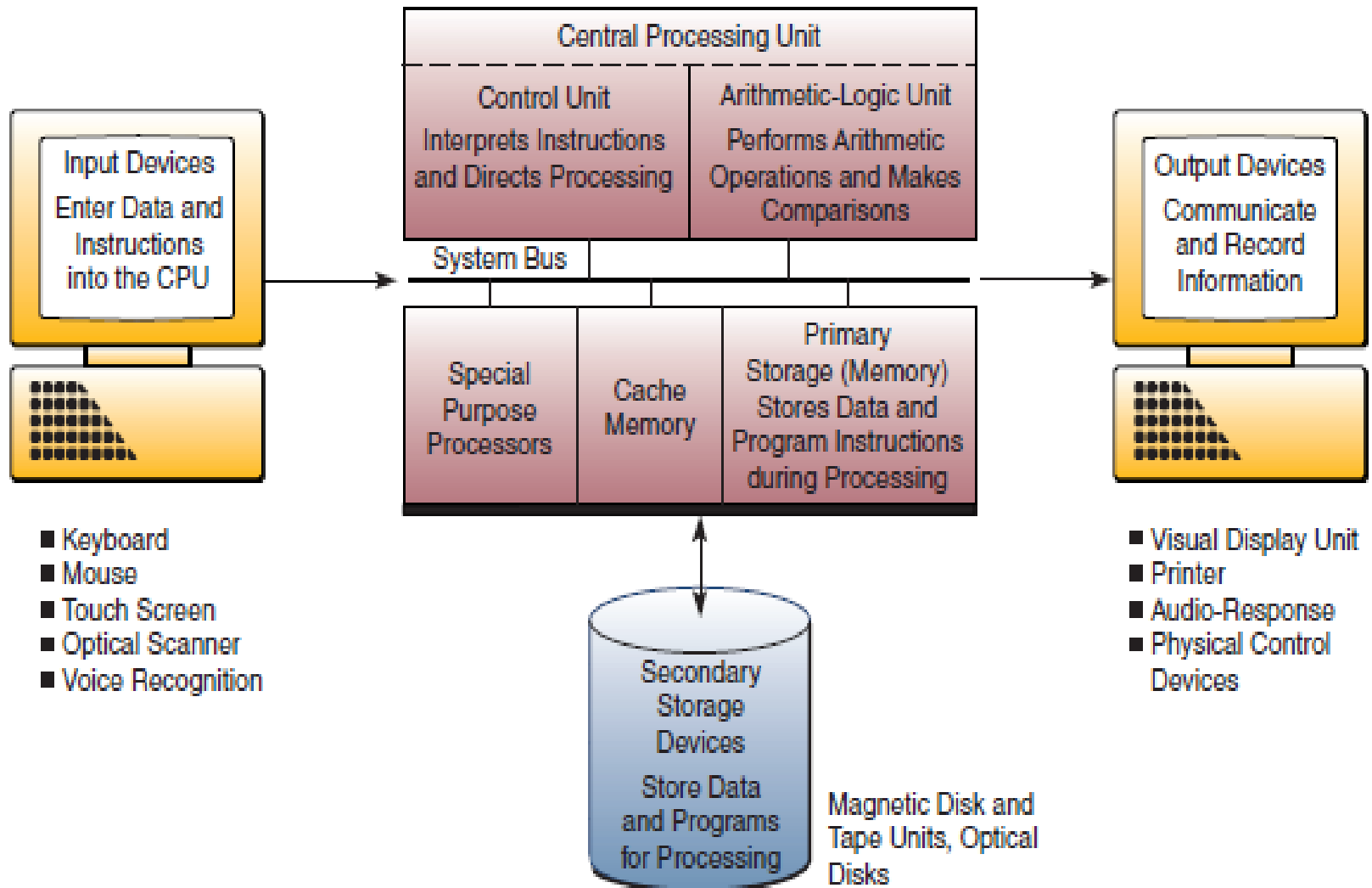
The Functions of Information Technology (Continued)

- *Generation*: The process of organizing information into a useful form, whether as numbers, text, sound, or visual image.
- *Storage and Retrieval*: Storage is the computer process of retaining information for future use. Retrieval is the process by which a computer locates and copies stored data or information for further processing or for transmission to another user.

The Functions of Information Technology (Continued)

- *Transmission:* The computer process of distributing information over a communications network.
 - Electronic Mail, or E-Mail
 - Voice Messaging, or Voice Mail

Computer Parts



Units of Computer Memory Measurements

1 Bit = Binary Digit

8 Bits = 1 Byte

1024 Bytes = 1 KB (Kilo Byte)

1024 KB = 1 MB (Mega Byte)

1024 MB = 1 GB (Giga Byte)

1024 GB = 1 TB (Terra Byte)

1024 TB = 1 PB (Peta Byte)

1024 PB = 1 EB (Exa Byte)

1024 EB = 1 ZB (Zetta Byte)

1024 ZB = 1 YB (Yotta Byte)

1024 YB = 1 (Bronto Byte)

1024 Brontobyte = 1 (Geop Byte)

Geop Byte is The Highest Memory

Information (or computer) Security

- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of **preserving the integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

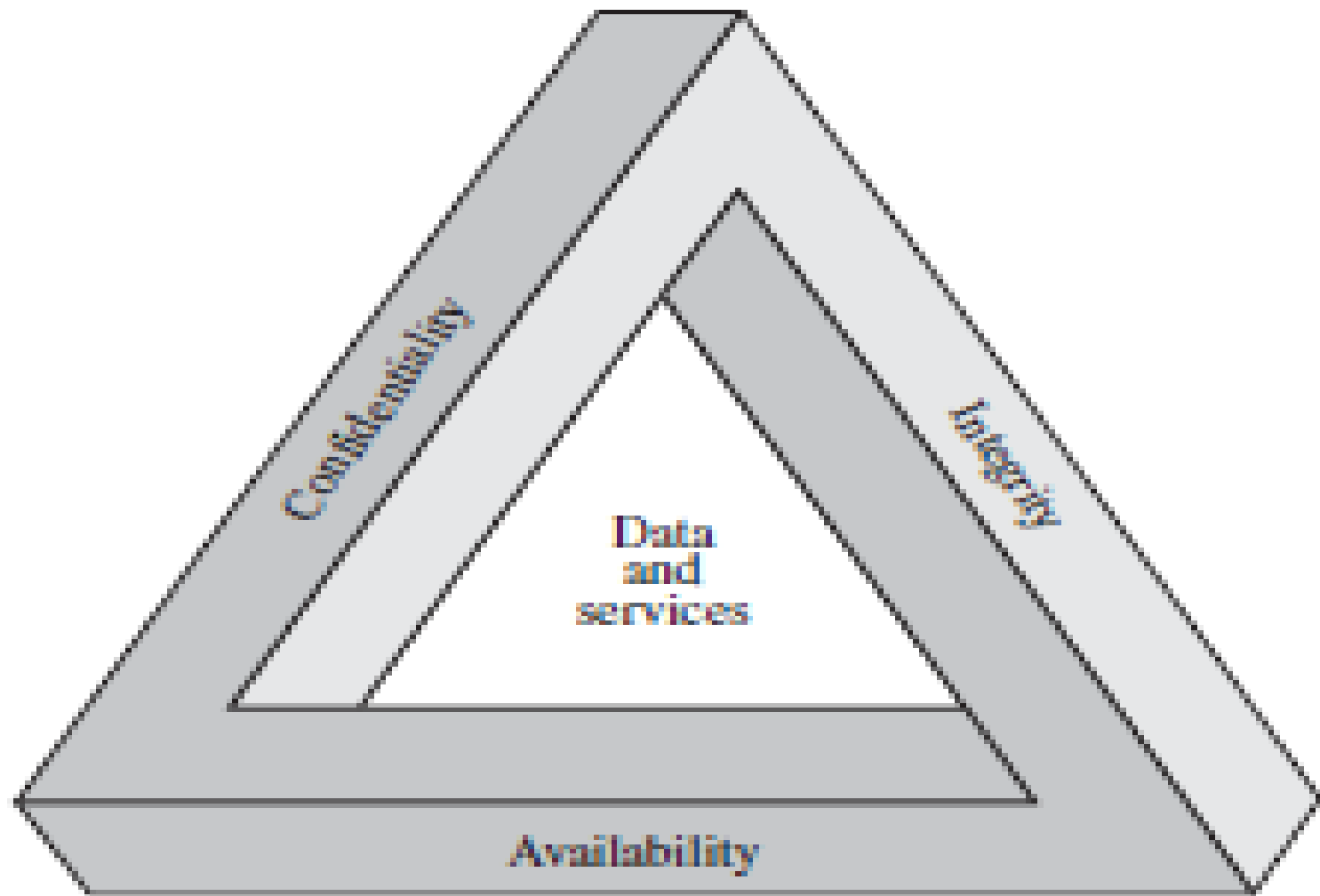


Figure 1.1 The Security Requirements Triad

Security objectives for information and for information systems

- • **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Security objectives for information and for information systems

- • **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

Security objectives for information and for information systems

- • **Availability:** Ensuring timely and reliable access to and use of information.
- A loss of availability is the disruption of access to or use of information or an information system

Computer Security Terminologies

- **Adversary (threat agent)** :An entity that attacks, or is a threat to, a system.
- **Attack:** An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Computer Security Terminologies

- **Countermeasure:** An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- **Risk:** An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Computer Security Terminologies

- **Security Policy:** A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

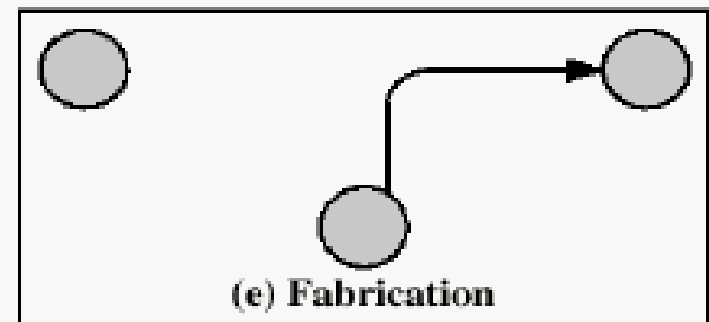
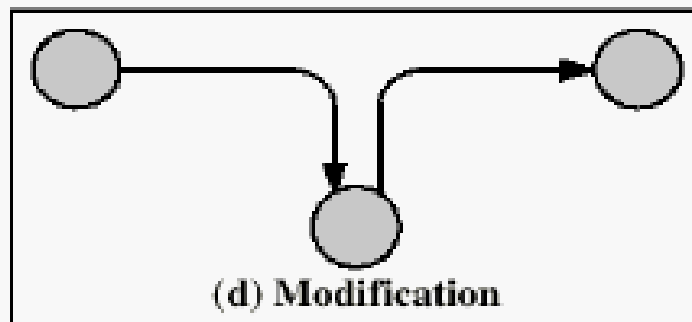
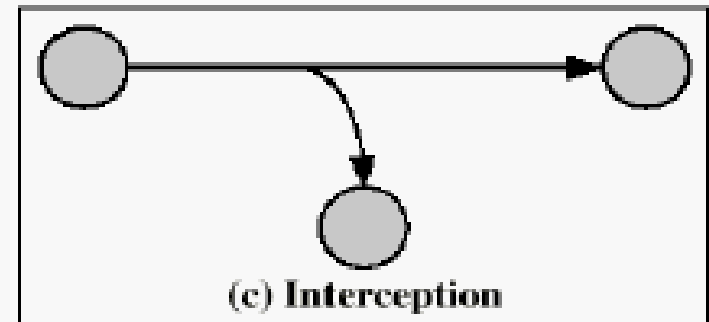
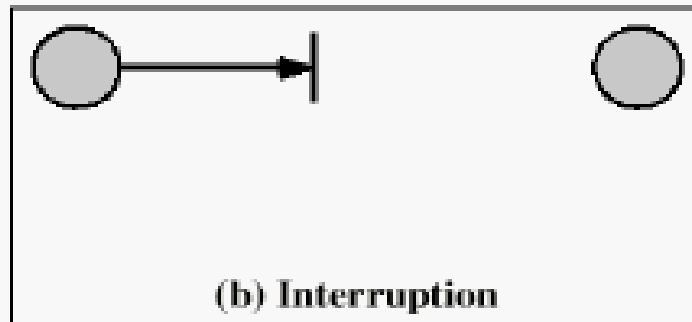
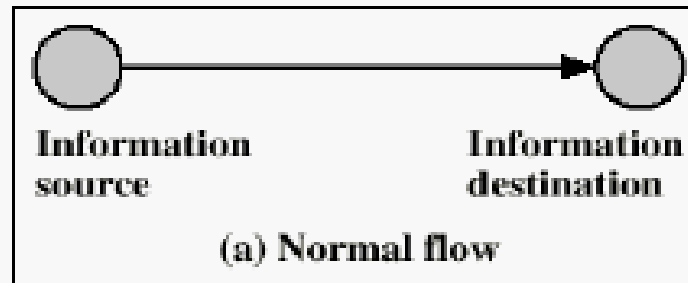
Computer Security Terminologies

- **System Resource (Asset):**Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component—hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Computer Security Terminologies

- **Threat:** is a possible danger that might exploit a vulnerability.
- **Vulnerability:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Security Attacks



Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- Malicious software programs are referred to as **malware** and include a variety of threats, such as computer *viruses*, *worms*, and *Trojan horses*.
- A **computer virus** is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission.
 - Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file
- **Worms** are independent computer programs that copy themselves from one computer to other computers over a network
 - Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer.

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- A **Trojan horse** is a software program that appears to be benign but then does something other than expected
 - The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system.
- **Spyware:** These small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising.

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Viruses:-** can come in the form of instructions such as display a message or image, or it can be highly destructive— destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly.
- **Worms** destroy data and programs as well as disrupt or even halt the operation of computer networks.
- **Worms and viruses** are often spread over the Internet from files of downloaded software, from files attached to e-mail transmissions, or from compromised e-mail messages or instant messaging

Examples of viruses, worm and trojan

NAME	TYPE	DESCRIPTION
Conficker (aka Downadup, Downup)	Worm	First detected in November 2008. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Has more than 5 million computers worldwide under its control. Difficult to eradicate.
Storm	Worm/ Trojan horse	First identified in January 2007. Spreads via e-mail spam with a fake attachment. Infected up to 10 million computers, causing them to join its zombie network of computers engaged in criminal activity.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot, and infected computers to search for more victims. Affected millions of computers worldwide, disrupting British Airways flight check-ins, operations of British coast guard stations, Hong Kong hospitals, Taiwan post office branches, and Australia's Westpac Bank. Sasser and its variants caused an estimated \$14.8 billion to \$18.6 billion in damages worldwide.
MyDoom.A	Worm	First appeared on January 26, 2004. Spreads as an e-mail attachment. Sends e-mail to addresses harvested from infected machines, forging the sender's address. At its peak this worm lowered global Internet performance by 10 percent and Web page loading times by as much as 50 percent. Was programmed to stop spreading after February 12, 2004.
Sobig.F	Worm	First detected on August 19, 2003. Spreads via e-mail attachments and sends massive amounts of mail with forged sender information. Deactivated itself on September 10, 2003, after infecting more than 1 million PCs and doing \$5 to \$10 billion in damage.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated \$10 billion to \$15 billion in damage.
Melissa	Macro virus/ worm	First appeared in March 1999. Word macro script mailing infected Word file to first 50 entries in user's Microsoft Outlook address book. Infected 15 to 29 percent of all business PCs, causing \$300 million to \$600 million in damage.

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- Some **malware** can come in the form of **Keyloggers** to record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers.
- Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory.
- The Zeus Trojan uses keylogging to steal financial information