MANAGEMENT INFORMATION SYSTEM

Dr. Khine Thin Zar
Professor
CEIT Department
YTU

COURSE OUTLINES

- Course Title
  - Management Information Systems
- Grading Policy
  - Exam → 80%
  - Tutorial / Assignment → 20%
- Textbook and Reference Materials
  - Course Manual for Management Information Systems CIS302, University of Ibadan Distance Learning Centre
  - Management Information Systems (Managing The Digital Firm) by Kenneth C. Laudon(New York University), Jane P. Laudon(Azimuth Information Systems), Twelfth Edition
  - Management Information Systems, Sixth Edition, by Effy Oz
- Course Duration
  - 12 Weeks

Securing Information Systems

LEARNING OUTCOMES

When you have studied this session, you should be able to:

- *define* the components of an organizational framework for security and Control
- *describe* the business value of security and control
- *discuss* the most important tools and technologies for safeguarding information resources

CONTENTS

- System Vulnerability and Abuse
- Wireless Security Challenges
- Malicious Software
- Internal Threats
- Establishing a Framework for Security and Control
- Risk Assessment

SYSTEM VULNERABILITY AND ABUSE

What would happen if you tried to link to the Internet without a firewall or antivirus software?

- stole or destroyed valuable data
- make security and control a top priority

Security - the policies, procedures, and technical measures

- used to prevent unauthorized access, alteration, theft, or physical damage to information systems

Controls - methods, policies, and organizational procedures

- ensure the safety of the organization's assets; the accuracy and reliability of its records; and operational adherence to management standards

WHY SYSTEMS ARE VULNERABLE

- Data stored in electronic form are vulnerable to many more kinds of threats than when they existed in manual form
- The potential for unauthorized access, abuse, or fraud can occur at any access point in the network.
- The most common threats can stem from technical, organizational, and environmental factors compounded by poor management decisions.

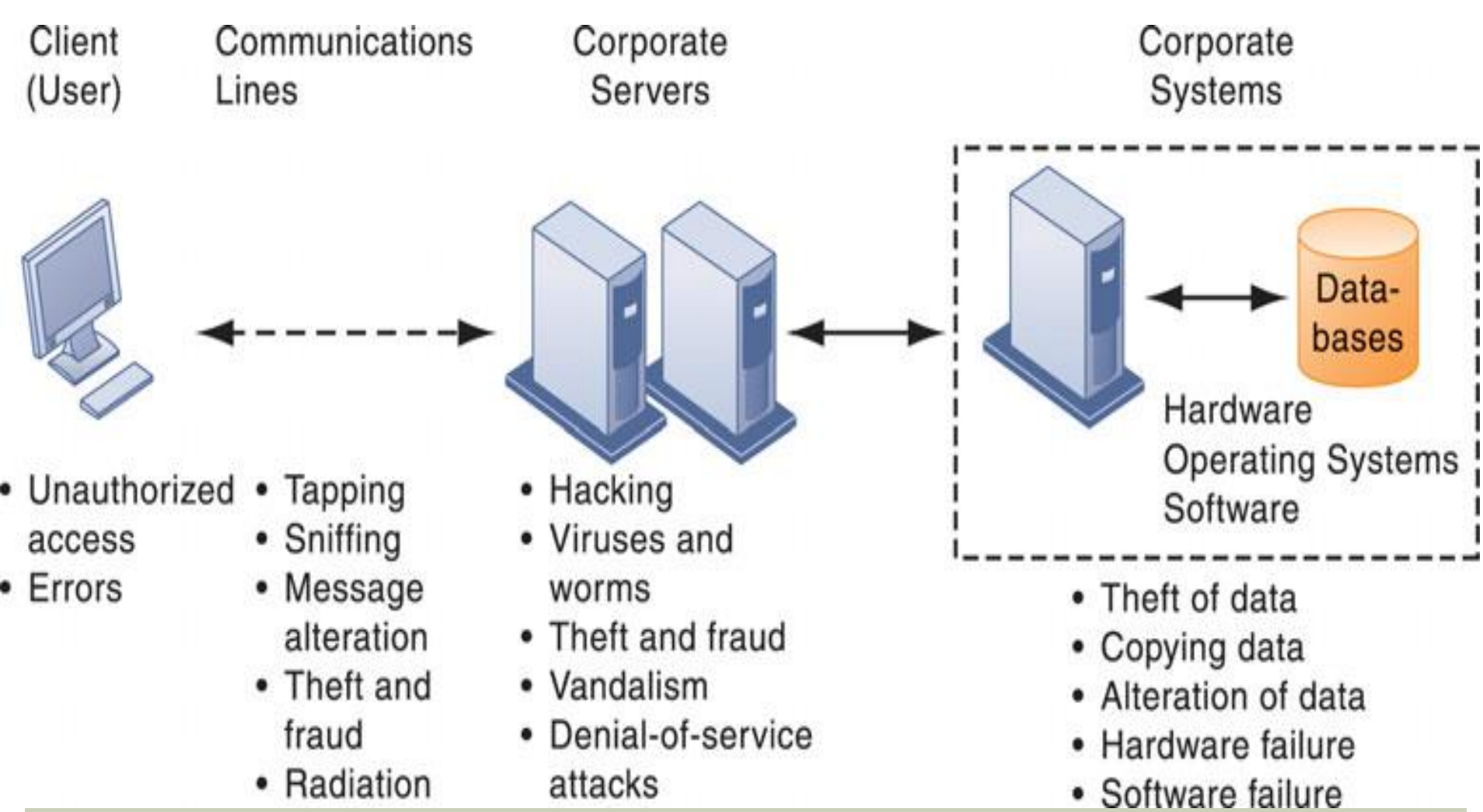

Figure: Contemporary security challenges and vulnerabilities

INTERNET VULNERABILITIES

- Large public networks are more vulnerable than internal networks (virtually open to anyone)
- When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.
- Vulnerability increase from widespread use of
  - e-mail: springboards for malicious software or unauthorized access
  - instant messaging (IM): do not use a secure layer for text messages
  - peer-to-peer file-sharing programs: illegal music sharing

WIRELESS SECURITY CHALLENGES

Is it safe to log onto a wireless network at an airport, library, or other public location?

- Radio frequency bands are easy to scan
- Susceptible to hacking by eavesdroppers
- Local area networks (LANs) using the 802.11 standard can be easily penetrated by outsiders
- Detect unprotected networks, monitor network traffic, and gain access to the Internet or to corporate networks
- The *service set identifiers (SSIDs):* picked up fairly easily by intruders' sniffer programs

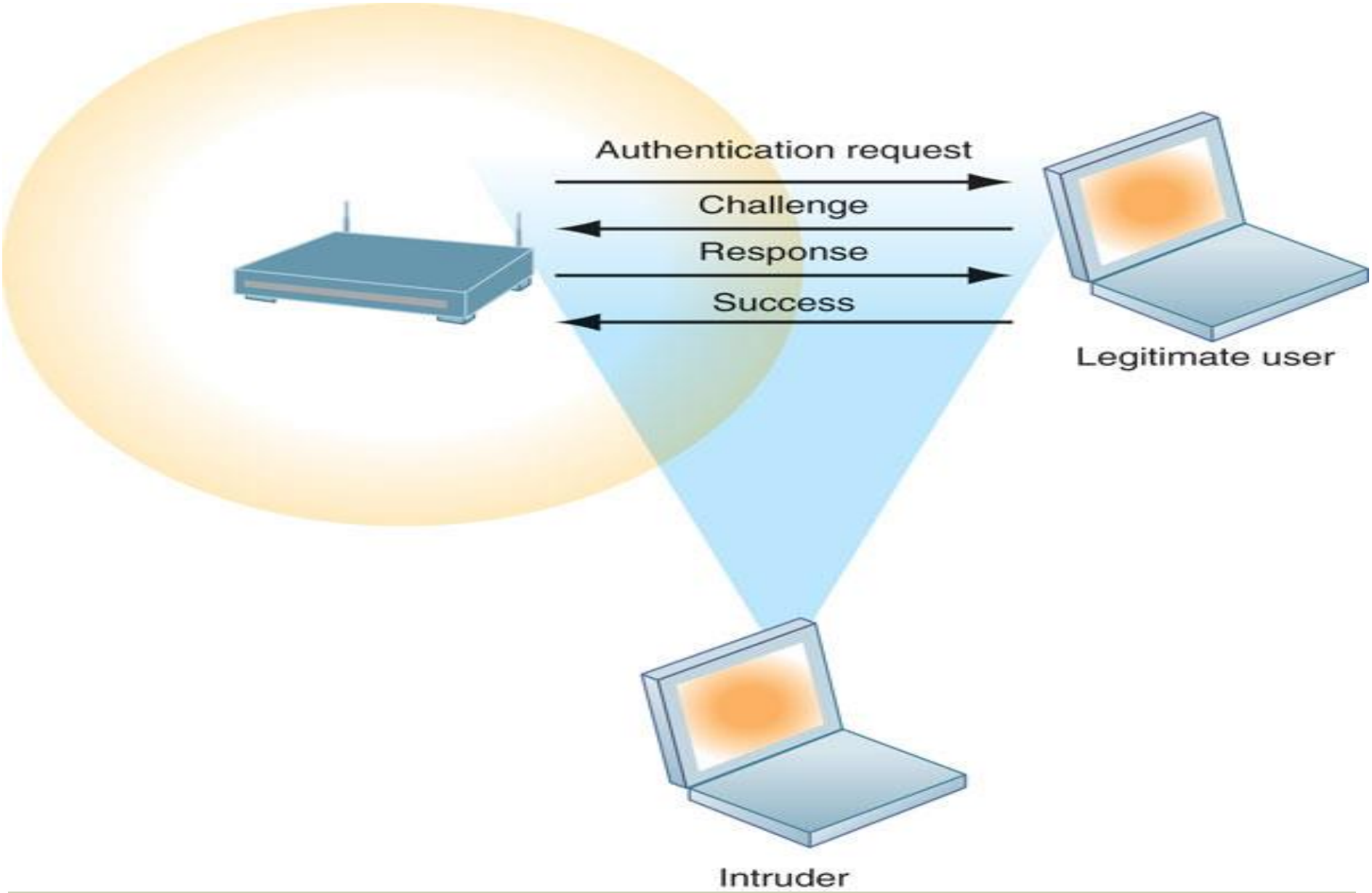

Figure: Wifi security challenges

MALICIOUS SOFTWARE

- **Malware:** include a variety of threats

Computer Virus

- a rogue software program that attaches itself to other software programs or data files in order to be executed
- without user knowledge or permission

Worms

- Independent computer programs that copy themselves from one computer to other computers over a network
- destroy data and programs as well as disrupt or even halt the operation of computer networks

MALICIOUS SOFTWARE (CONT.)

Trojan horse

- a software program that appears to be benign but then does something other than expected
- not itself a virus because it does not replicate
- a way for viruses or other malicious code to be introduced into a computer system

SQL injection attacks

- the largest malware threat
- an attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database

Spyware

- computer users' privacy - nefarious

HACKERS AND COMPUTER CRIME

- A **hacker:** an individual who intends to gain unauthorized access to a computer system
- *Cracker :* denote a hacker with criminal intent
- Unauthorized access by finding weaknesses in the security protections
- Theft of goods and information
- System damage and **cybervandalism**, the intentional disruption, defacement, or even destruction of a Web site or corporate information system

SPOOFING AND SNIFFING

Spoofing

- involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.

Sniffer

- a type of eavesdropping program that monitors information traveling over a network
- enable hackers to steal proprietary information from anywhere on a network

DENIAL-OF-SERVICE ATTACKS

- Hackers flood a network server or Web server with many thousands of false communications
- Requests for services to crash the network
- A **distributed denial-of-service (DDoS)** attack uses numerous computers to inundate and overwhelm the network from numerous launch points
- For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases
- Small and midsize businesses whose networks tend to be less protected than those of large corporations

COMPUTER CRIME

- Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just describe make them targets for other types of **computer crime**
- No one knows the magnitude of the computer crime problem
- How many systems are invaded,
- How many people engage in the practice, or the total economic damage
- The crimes may involve employees, or the company fears that publicizing its vulnerability will hurt its reputation

EXAMPLES OF COMPUTER CRIME

COMPUTERS AS TARGETS OF CRIME
Breaching the confidentiality of protected computerized data
Accessing a computer system without authority
Knowingly accessing a protected computer to commit fraud
Intentionally accessing a protected computer and causing damage, negligently or deliberately
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
Threatening to cause damage to a protected computer
COMPUTERS AS INSTRUMENTS OF CRIME
Theft of trade secrets
Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Schemes to defraud
Using e-mail for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including e-mail and voice mail
Transmitting or possessing child pornography using a computer

IDENTITY THEFT

- A crime in which an imposter obtains key pieces of personal information, (e.g., social security identification numbers, driver's license numbers, or credit card numbers)
- E-commerce sites are wonderful sources of customer personal information—name, address, and phone number.
- Assume new identities and establish new credit for their own purposes

CLICK FRAUD

- When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click
- Direct potential buyers to its products
- **Click fraud** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase
- Become a serious problem at Google and other Web sites that feature pay-per-click online advertising

INTERNAL THREATS

EMPLOYEES

- Company insiders pose serious security problems
- Access to privileged information, and in the presence of sloppy internal security procedures
- User lack of knowledge is the single greatest cause of network security breaches
- A major source of errors: end users and information systems specialists

INTERNAL THREATS (CONT.)

SOFTWARE VULNERABILITY

- A constant threat to information systems
- Growing complexity and size of software programs
- A major problem: the presence of hidden **bugs** or program code defects
- The complexity of decision-making code
- Antivirus products

BUSINESS VALUE OF SECURITY AND CONTROL

- **Protecting information systems** is so critical to the operation of the business
- Companies: individuals' taxes, financial assets, medical records, and job performance reviews
- Government: weapons systems, intelligence operations, and military targets
- Result in serious **legal liability**
- Prevent loss of confidential information, data corruption, or breach of privacy

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

ELECTRONIC EVIDENCE

- Rely on evidence represented as digital data
- E-mail is currently the most common type of electronic evidence
- To respond to a discovery request for access to information that may be used as evidence - required by law to produce those data
- Severe financial and even criminal penalties for improper destruction of electronic documents

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS (CONT.)

COMPUTER FORENSICS

- The scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media
- The information can be used as evidence in a court of law
- It deals with the following problems:
  - Recovering data from computers while preserving evidential integrity
  - Securely storing and handling recovered electronic data
  - Finding significant information in a large volume of electronic data
  - Presenting the information to a court of law

ESTABLISHING A FRAMEWORK FOR SECURITY AND CONTROL

- Won't be reliable and secure unless you know how and where to deploy them
- Need to know where your company is at risk and what controls you must have in place
- Need to develop a security policy and plans for keeping your business

INFORMATION SYSTEMS CONTROLS

- Both manual and automated
- Both general controls and application controls
- **General controls** govern the design, security, and use of computer programs and the security of data files in general
- Apply to all computerized applications and consist of a combination of hardware, software, and manual procedures
- **Application controls** are specific controls unique to each computerized application, such as payroll or order processing
- Can be classified as

  (1) input controls,

  (2) processing controls, and

  (3) output controls

RISK ASSESSMENT

- Determines the level of risk to the firm if a specific activity or process is not properly controlled
- Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage.
- Concentrate on the control points with the greatest vulnerability and potential for loss

SECURITY POLICY

- Consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals
- Drives policies determining acceptable use of the firm's information resources
- An **acceptable use policy (AUP)** defines acceptable uses of the firm's information resources and computing equipment
- **Identity management** consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources

THE ROLE OF AUDITING

How does management know that information systems security and controls are effective?

- Conduct comprehensive and systematic audits
- An **MIS audit** examines the firm's overall security environment as well as controls governing individual information systems
- The auditor should trace the flow of sample transactions through the system
- Security audits review technologies, procedures, documentation, training, and personnel.
- Lists and ranks all control weaknesses
- Assesses the financial and organizational impact of each threat

TECHNOLOGIES AND TOOLS FOR PROTECTING INFORMATION RESOURCES

- An array of technologies for protecting their information resources
- Managing user identities,
- Preventing unauthorized access to systems and data,
- Ensuring system availability, and
- Ensuring software quality

IDENTITY MANAGEMENT AND AUTHENTICATION

- Automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system
- Includes tools for authenticating users, protecting user identities, and controlling access to system resources
- A user must be authorized and authenticated
- **Authentication** refers to the ability to know that a person is who he or she claims to be (using **passwords**)
- New authentication technologies, such as tokens, smart cards, and biometric authentication

FIREWALLS, INTRUSION DETECTION SYSTEMS, AND ANTIVIRUS SOFTWARE

- **Firewalls** prevent unauthorized users from accessing private networks
- **Intrusion detection systems** feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually
- **Antivirus software** is designed to check computer systems and drives for the presence of computer viruses.

ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE

- Use encryption to protect digital information that they store, physically transfer, or send over the Internet.
- **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver
- **public key encryption** uses two keys: one shared (or public) and one totally private
- **Digital certificates** are data files used to establish the identity of users and electronic assets for protection of online transactions

ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE (CONT.)

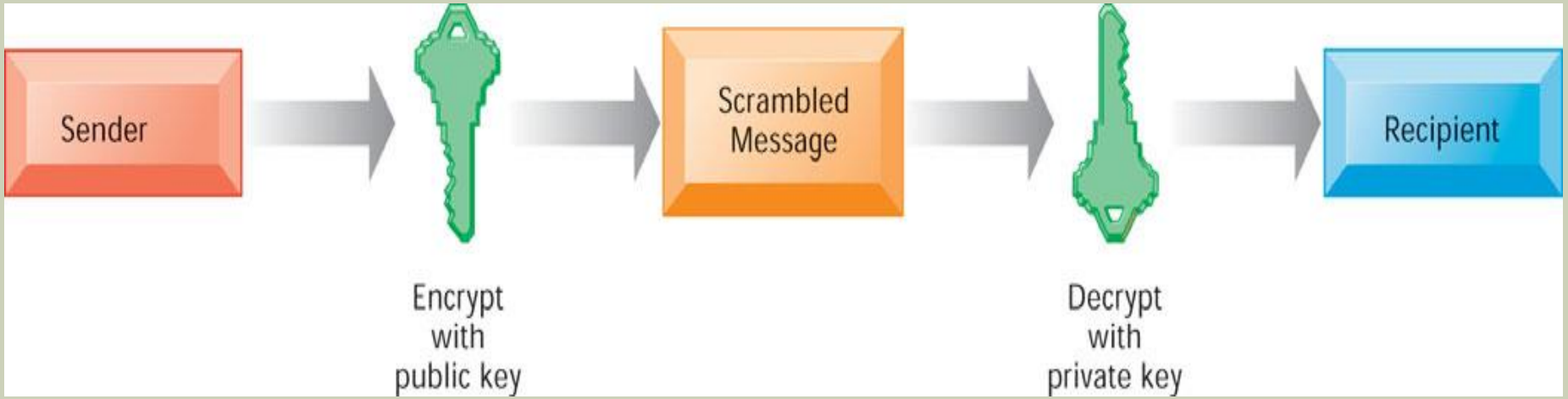

Figure: Public key encryption

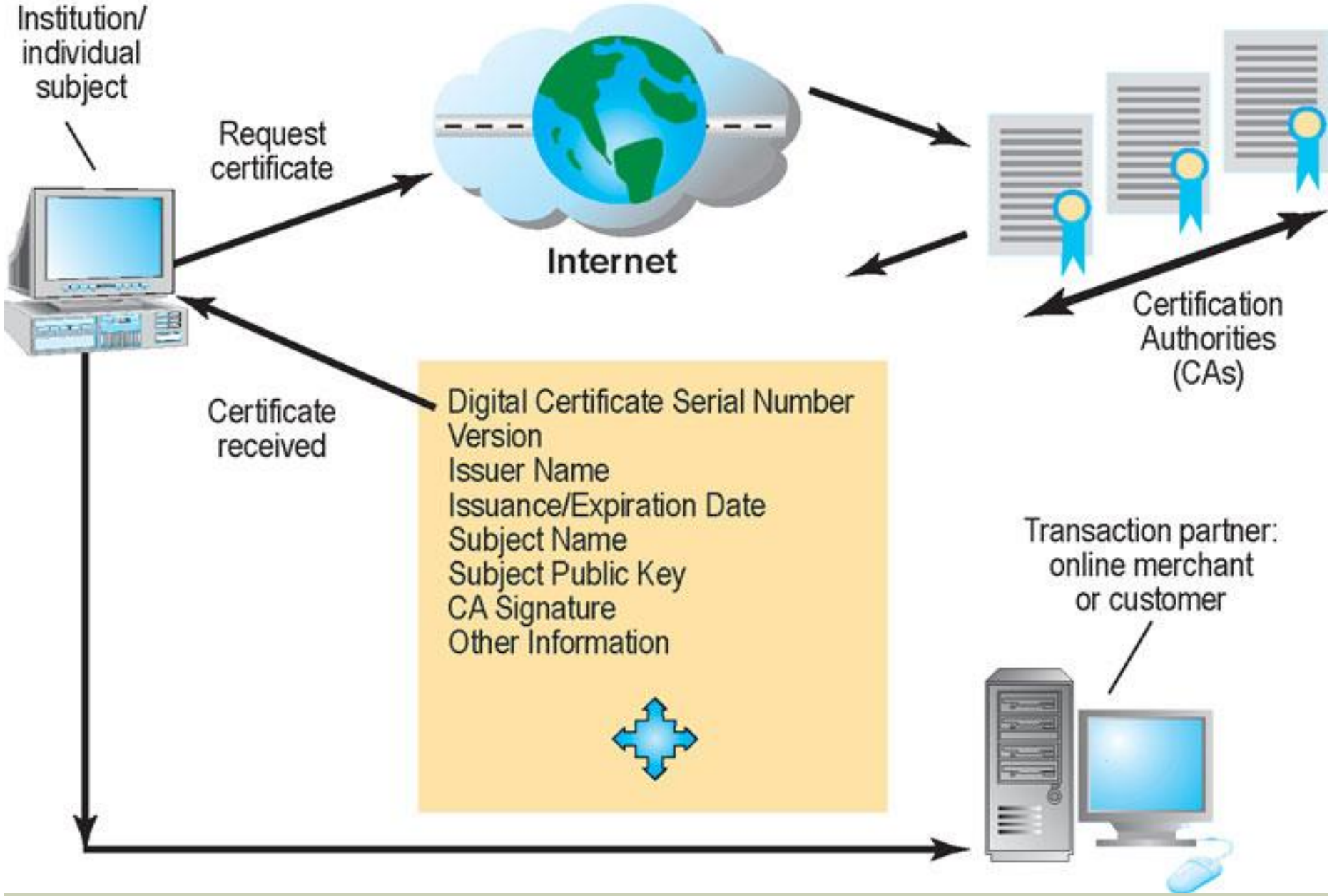

Figure: Digital certificates

ENSURING SYSTEM AVAILABILITY

- Ensure that their systems and applications are always available
- In **online transaction processing**, transactions entered online are immediately processed
- **Fault-tolerant computer systems** contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service.
- **High-availability computing** environments are a minimum requirement for firms with heavy e-commerce processing or for firms that depend on digital networks for their internal operations.
- Both fault tolerance and high-availability computing try to minimize downtime.

SECURITY IN THE CLOUD

- **Accountability and responsibility** for protection of sensitive data still reside with the company owning that data
- Cloud users need to confirm that regardless of where their data are stored or transferred
- Important to know how the cloud provider will respond if a disaster strikes
- **The service level agreement (SLA)**

SECURING MOBILE PLATFORMS

- To be secured like desktops and laptops against malware, theft, accidental loss, unauthorized access, and hacking attempts
- corporate security policy
- To maintain accurate inventory records on all mobile devices, users, and applications;
- To control updates to applications; and
- To lock down lost devices so they can't be compromised.

ENSURING SOFTWARE QUALITY

- Improve system quality and reliability
- Objective assessments of the system in the form of quantified measurements
- Measure the performance of the system and identify problems as they occur
- To prove the correctness of work

THREATS TO INFORMATION

1. Accidents & Disasters
2. Employees & Consultants
3. Business Partnerships
4. Outside Attackers
5. Viruses & Spyware
6. Direct attacks & Scripts

THREATS TO USERS

1. Attacker takes over computer
    i. Virus/Trojan
    ii. Phishing
    iii. Unpatched computer/known holes
    iv. Intercepted wireless data
2. Bad outcomes
    i. Lost passwords, impersonation, lost money
    ii. Stolen credit cards, lost money
    iii. Zombie machine, attacks others
    iv. Commits crimes blamed on you

SECURING E-COMMERCE SERVERS

how can e-commerce server be secured?

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for passwords.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

SECURING E-COMMERCE SERVERS (CONT.)

7. Restrict access to cardholder data by business need to know.

8. Assign a unique id to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security.

ASSESSMENT

1. Why are information systems vulnerable to destruction, error, and abuse?

2. What is the business value of security and control?

3. What are the components of an organizational framework for security and control?

4. What are the most important tools and technologies for safeguarding information resources?

5. List the two categories of threat to a user.

Next Week Lecture: **Transaction Processing System**

THANK YOU.