System Analysis Design

Week-11-Lesson-1

Information Security and Cybercrime

Daffodil International University

Learning Goals

- Computer Applications in the Society
- Security Challenges and Vulnerabilities
- Hackers and Computer Crime
- Proof of Computer Crime
- What are Cyber Crime?
- Technologies and Tools for Protecting Information Resources
- Property Rights: Intellectual Property

Computer Applications in the Society

- Education/Research
- Government
- Science
- Publishing
- Industry
- Enterprise
- Finance
- Healthcare
- Travel
- Personal Communication

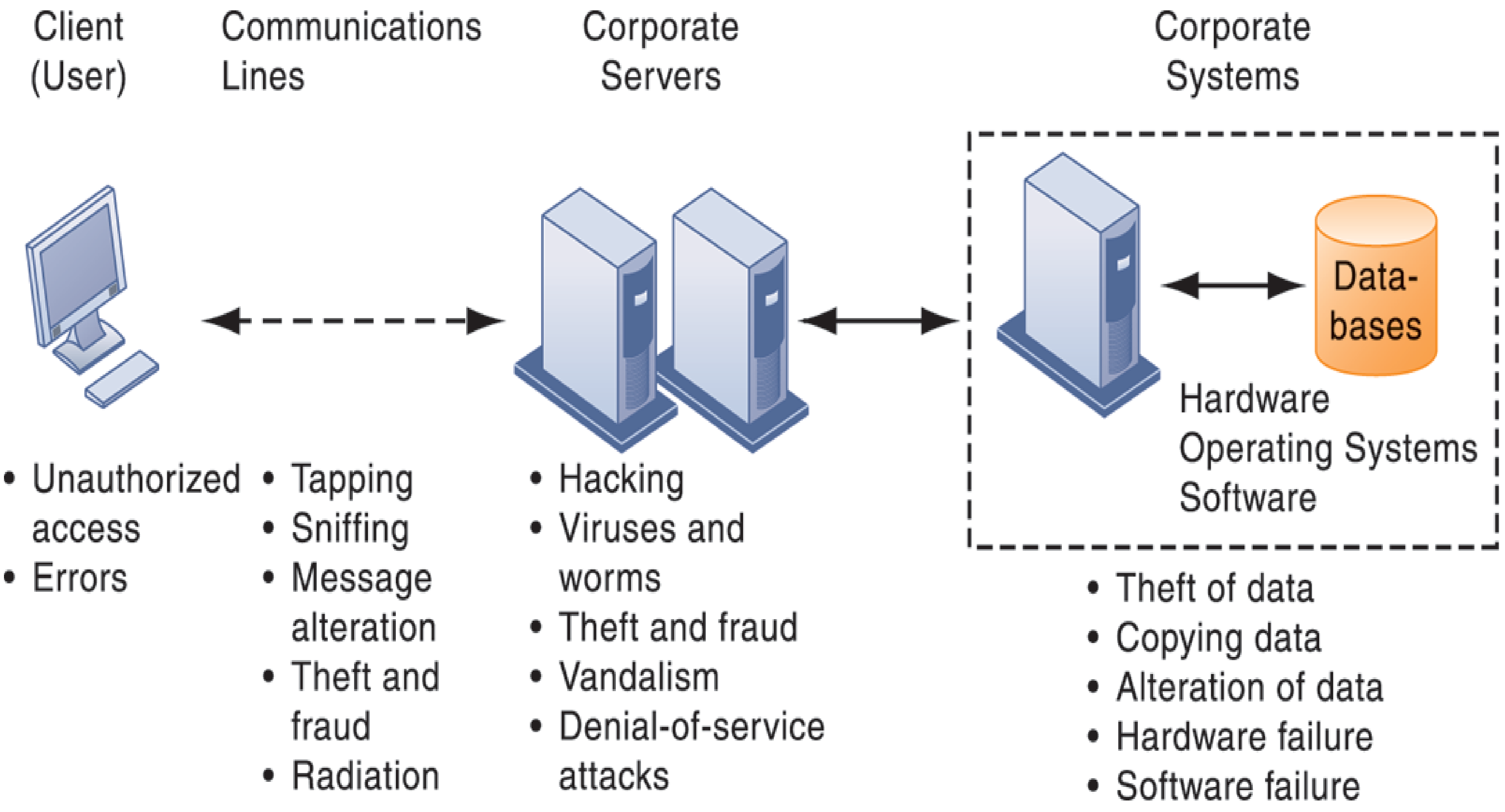
Internet-based Applications in the Society

- **Email-**

- **Social media -**

- **Messenger –**

Security Challenges and Vulnerabilities



Client (User)

- Unauthorized access
- Errors

Communications Lines

- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

Corporate Servers

- Hacking
- Viruses and worms
- Theft and fraud
- Vandalism
- Denial-of-service attacks

Corporate Systems

Databases

Hardware
Operating Systems
Software

- Theft of data
- Copying data
- Alteration of data
- Hardware failure
- Software failure

Malware (malicious software)

- ❑ **Viruses**
  - Rogue software program that attaches itself to other software programs or data files in order to be executed
- ❑ **Worms**
  - Independent computer programs that copy themselves from one computer to other computers over a network.
- ❑ **Trojan horses**
  - A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

Malware (malicious software)

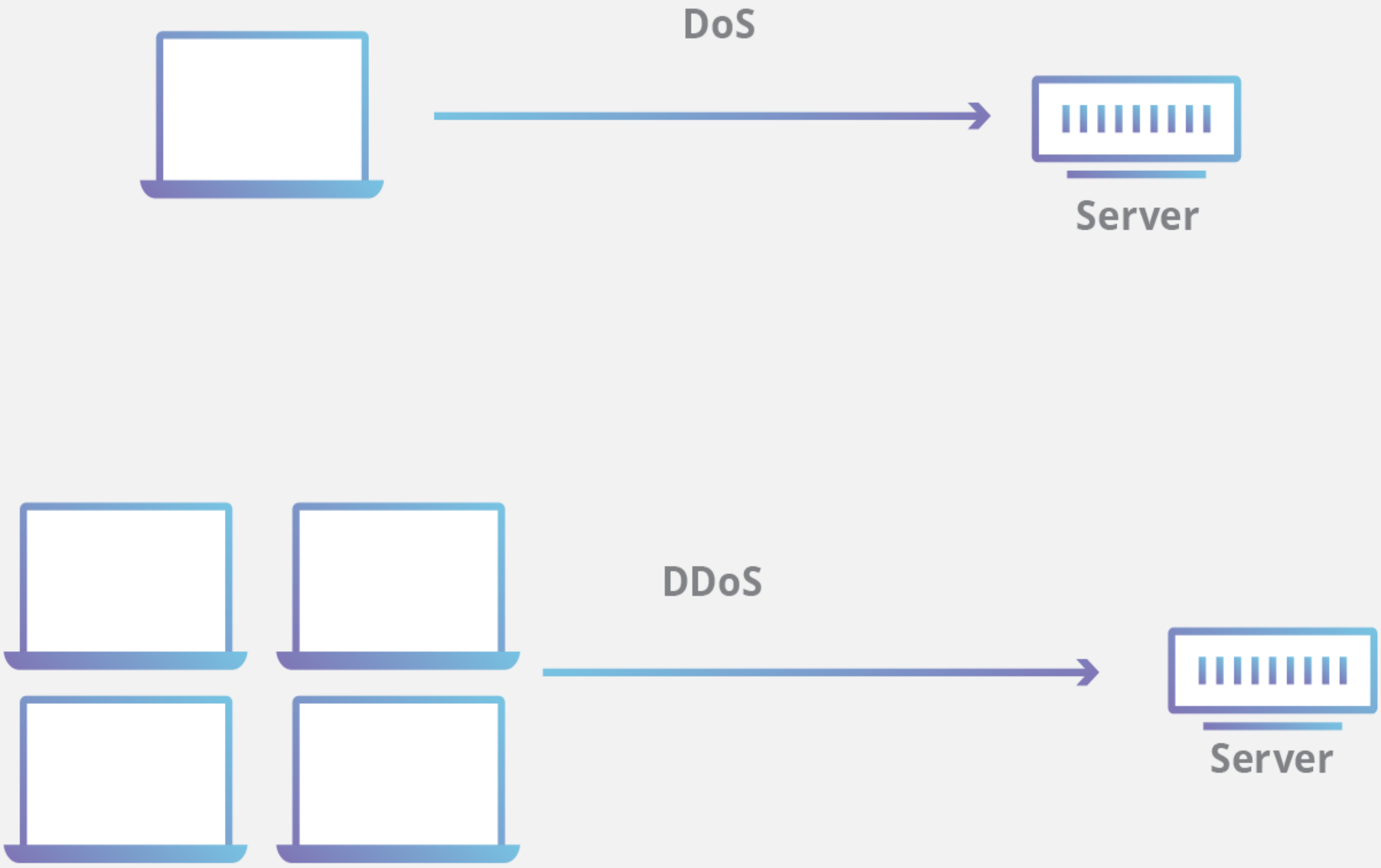
- ❑**SQL injection attacks**
  - Hackers submit data to Web forms that exploits site’s unprotected software and sends rogue SQL query to database
- ❑**Spyware**
  - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
- ❑**Key loggers**
  - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

Computer Crime

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- Sniffer
  - program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, etc.

Computer Crime(Cont..)

- **Denial-of-service attacks (DoS)**
  - Flooding server with thousands of false requests to crash the network.
- **Distributed denial-of-service attacks (DDoS)**
  - Use of numerous computers to launch a DoS



- ❑ DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic

Computer Crime

- Identity theft
  - Theft of personal Information (social security id, driver's license or credit card numbers) to impersonate someone else
- Phishing
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- Evil twins
  - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet

Computer Crime

- **Pharming**
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- **Click fraud**
  - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase

Proof of Computer Crime

- **Electronic evidence**
  - Evidence for white collar crimes often in digital form
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - Proper control of data can save time and money when responding to legal discovery request
- **Computer forensics:**
  - Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
  - Includes recovery of ambient and hidden data

What are Cyber Crime?

- The crime that involves and uses computer devices and Internet, is known as cybercrime.
- Cybercrime can be committed against an individual or a group;
- It can also be committed against government and private organizations. It may be intended to harm someone’s reputation, physical harm, or even mental harm.

What are Cyber Crime(Cont..)

- Offences against computer data and systems
- Misuse of computer devices
- Computer-related forgery
- Computer-related fraud
- Child Pornography
- Offences related to infringements of copyright and related rights

Hacker Targets

Financial data	**Theft, modification or sale, blackmail**
Intellectual Property	**Theft, sale, personal gain**
Personal data	**Modification, sale**
System Access	**Sabotage, backdoors, exploitation**

Information Security

- **Security:** Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems:

  - **Physical Security**
  - **Network Security**
  - **Data Security**

Types of Network Security

- **Access control**
- **Antivirus and antimalware software**
- **Application security**
- **Data loss prevention**
- **Email security**
- **Mobile device security**
- **Security information and event management**

Data Security

- Data security concerns the protection of data from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls, and other safeguards to limit accessibility.

Technologies and Tools for Protecting Information Resources

Firewall:

- Combination of hardware and software that prevents unauthorized users from accessing private networks
- Technologies include:
  - Static packet filtering
  - Network address translation (NAT)
  - Application proxy filtering

Cont…

Intrusion detection systems:

- Monitor hot spots on corporate networks to detect and deter intruders
- Examines events as they are happening to discover attacks in progress

Antivirus and antispyware software:

- Checks computers for presence of malware and can often eliminate it as well
- Require continual updating

Cont…

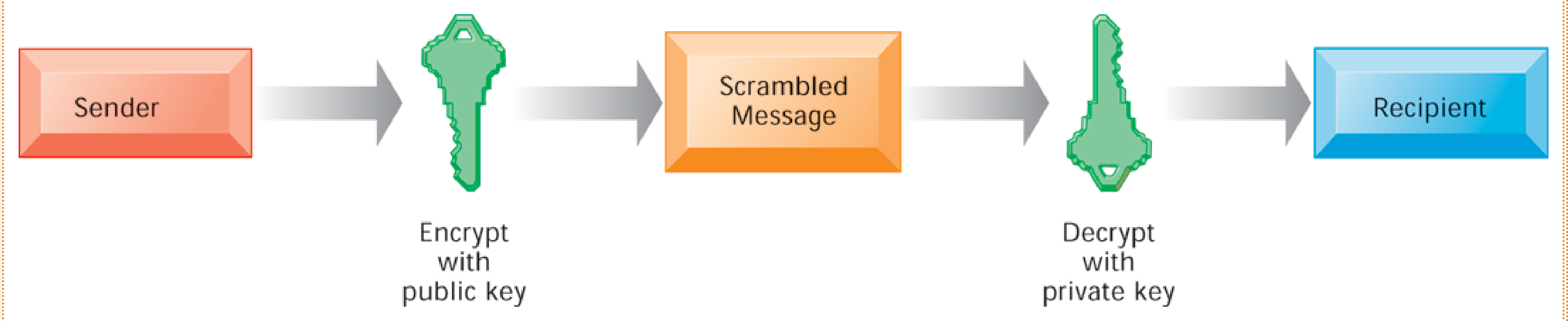
Securing wireless networks

- Continually changing keys
- Encrypted authentication system with central server

Cont…

Encryption:

- Transforming text or data into cipher text that cannot be read by unintended recipients



Cont…

Digital certificate:

- Data file used to establish the identity of users and electronic assets for protection of online transactions
- Uses a trusted third party, certification authority (CA), to validate a user's identity
- CA verifies user's identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner's public key

Safe and Ethical Uses of Computers

- **Ethics**
  - Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors
- **Professional codes of conduct**
  - Promulgated by associations of professionals
    - E.g. AMA, ABA, AITP, ACM
  - Promises by professions to regulate themselves in the general interest of society

Property Rights: Intellectual Property

- **Trade secret:** Intellectual work or product belonging to business, not in the public domain.
- **Copyright:** Statutory grant protecting intellectual property from being copied for the life of the author, plus 70 years.
- **Patents:** Grants creator of invention an exclusive monopoly on ideas behind invention for 20 years

References

1. System Analysis and Design, by Elias M. Awad

2. Systems Analysis and Design, Kendall and Kendall, Fifth Edition