Information System
ITEC-522
First Semester Third Year
Information Technology

Dr. Khalil-ur-Rahmen Khoumbati

Professor

Department of Information Technology

Faculty of Engineering and Technology

University of Sindh, Jamshoro

Khalil.khoumbati@gmail.com

Week #10

SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- Security:
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- Controls:
  - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards

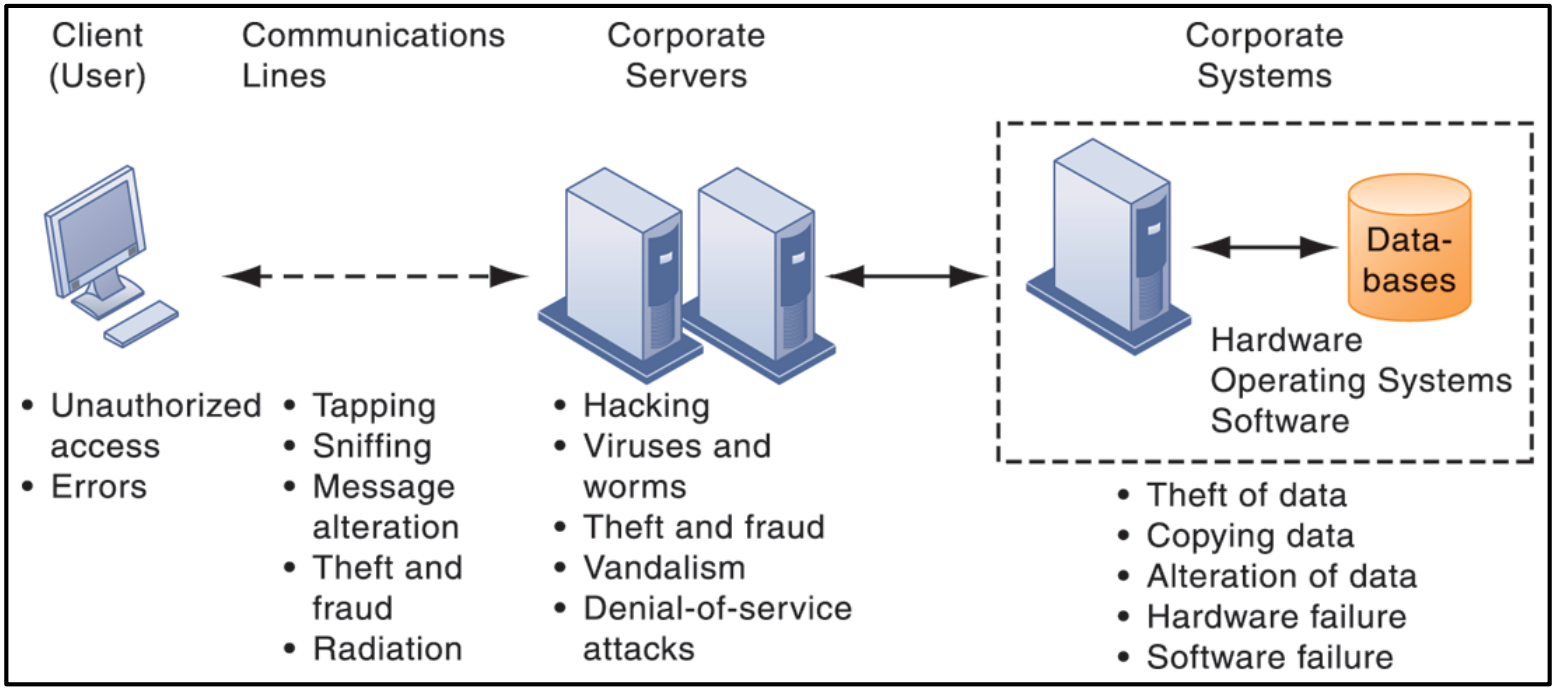
- Why systems are vulnerable
  - Accessibility of networks
  - Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
  - Software problems (programming errors, installation errors, unauthorized changes)
  - Disasters
  - Use of networks/computers outside of firm's control
  - Loss and theft of portable devices

4

Management Information Systems

System Vulnerability and Abuse

CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES



The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

- Internet vulnerabilities
  - Network open to anyone
  - Size of Internet means abuses can have wide impact
  - Use of fixed Internet addresses with cable or DSL modems creates fixed targets hackers
  - Unencrypted VOIP
  - E-mail, P2P, IM
    - Interception
    - Attachments with malicious software
    - Transmitting trade secrets

- Wireless security challenges
  - Radio frequency bands easy to scan
  - SSIDs (service set identifiers)
    - Identify access points
    - Broadcast multiple times
    - **War driving**
      - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
  - WEP (Wired Equivalent Privacy)
    - Security standard for 802.11; use is optional
    - Uses shared password for both users and access point
    - Users often fail to implement WEP or stronger systems

- 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
    - Software program that appears to be benign but then does something other than expected.

- Malware (cont.)
  - 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

9

- Hackers and computer crime
  - System intrusion
  - System damage
  - Cybervandalism
    - Intentional disruption, defacement, destruction of Web site or corporate information system

- 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
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, etc.

11

- Denial-of-service attacks (DoS)
  - Flooding server with thousands of false requests to crash the network.
- Distributed deniaf-service attacks (DDoS)
  - Use of numerous computers to launch a DoS
  - Botnets
    - Networks of “zombie” PCs infiltrated by bot malware
    - Worldwide, 6 - 24 million computers serve as zombie PCs in thousands of botnets

12

- Computer crime
  - Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
  - Computer may be target of crime, e.g.:
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - Computer may be instrument of crime, e.g.:
    - Theft of trade secrets
    - Using e-mail for threats or harassment

13

- 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

14

- 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
- Cyberterrorism and Cyberwarfare

- Internal threats: employees
  - Security threats often originate inside an organization
  - Inside knowledge
  - Sloppy security procedures
    - User lack of knowledge
  - Social engineering:
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

16

- Software vulnerability
  - Commercial software contains flaws that create security vulnerabilities
    - Hidden bugs (program code defects)
      - Zero defects cannot be achieved because complete testing is not possible with large programs
    - Flaws can open networks to intruders
  - Patches
    - Vendors release small pieces of software to repair flaws
    - However exploits often created faster than patches be released and implemented

Discussion

Questions?