Security of Information system

SECURITY OF INFORMATION SYSTEMS

- Security means protection of data from accidental or intentional modification, destruction or disclosure to unauthorized persons
- IS security refers to precaution taken to keep all the aspects of information systems(e.g. H/w, S/w, N/w equip & data)
- Safe from unauthorized use or access

POTENTIAL THREATS TO SECURITY

- ƒNatural disasters such as fire, floods, earthquakes
- ƒAccidents such as disk crashes, file erasure by inexperienced operators
- ƒTheft/erasure of data by disgruntled employees & consultants
- Links to business associates- electronic information can be risky when it travels between or among business affiliates as a part of doing business

POTENTIAL THREATS TO SECURITY (CONTD)

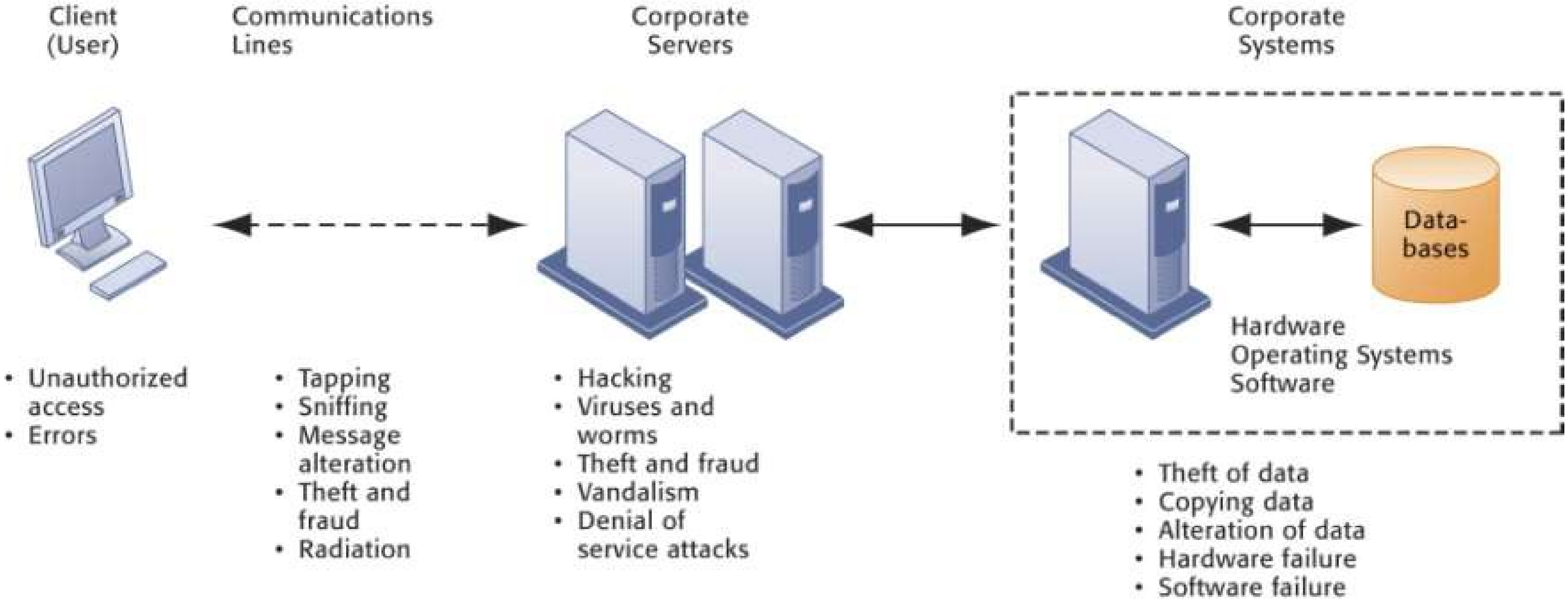
- ƒFrauds by changing programs, data by employees
- With the advent internet & related telecom technologies systems have become more vulnerable
  - ƒ Viruses/Worms as an email attachment
  - ƒ Hackers who break into systems connected to the internet
  - ƒ Denial of service attacks by flooding with mail

POTENTIAL THREATS TO SECURITY (CONTD)

Most IS are compromised through

- Unauthorized access
- Information modification
- Denial of Service & viruses as well as
- Spam
- Spyware &
- Cookies

Contemporary 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

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

System vulnerabilities & abuse-Malicious software (malware)

- **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
- **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

System vulnerabilities & abuse

- **Hackers vs. crackers**

  Activities include

  - **System intrusion**
  - **Theft of goods and information**
  - **System damage**
  - **Cybervandalism**
    - Intentional disruption, defacement, destruction of Web site or corporateinformation system

System vulnerabilities & abuse

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 (spying)program that monitors information traveling over network

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

Botnets: Networks of “zombie” PCs infiltrated by bot malware

Cookies: A message passed to the web browser on a user’s computer by web server.

The browser then stores a message in a text file, and the message is sent back to the server each time the user’s browser request a page from that server.

Cookies are stored on a Hard disk of your computer without your knowledge

System vulnerabilities & abuse

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

System vulnerabilities & abuse

- **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
- **Pharming: Redirects users to a bogus Web page, even when** individual types correct Web page address into his or her browser

System vulnerabilities & abuse

Click fraud

- Individual or computer program clicks online ad

  without any intention of learning more or making a purchase

Global threats - Cyberterrorism and cyberwarfare

- Concern that Internet vulnerabilities and other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups

HOW TO PROTECT DATA/PROGRAMS

- Regular back up of data bases every day/or week depending on the time criticality and size
- ƒIncremental back up at shorter intervals
- Backup copies kept in safe remote location particularly necessary for disaster recovery
- ƒDuplicate systems run and all transactions mirrored if it is a very critical system and cannot tolerate any disruption before storing in disk.
- ƒ Physical locks
- ƒ Password system
- ƒBiometric authentication (Eg: Finger print)

HOW TO PROTECT DATA/PROGRAMS(CONTD)

- Encrypting sensitive data/programs
- ƒIdentification of all persons who read or modify data and logging it in a file
- ƒTraining employees on data care/handling and security
- ƒ Antivirus software
- ƒ Firewall protection when connected to internet
  - Types(can both be hardware & software)
    - Packet filter
    - Application level control: measures security only for certain application such as file transferring
    - Circuit level control: measures security when certain kind of connection(circuit) is made
    - Proxy server
- Audit - control software

DATA SECURITY, PRIVACY AND INTEGRITY

- Data security is concerned with protecting data from

  erasure, theft, unauthorized access and unauthorized

  modifications
- ƒ Data privacy is concerned with protecting data regarding individuals from being accessed and used without the permission/knowledge of concerned individuals
- ƒ Data integrity is concerned with the quality and

  reliability of raw as well as processed data

What is Layered security

- **Layered security**, also known as **layered defense**, describes the practice of combining multiple mitigating security controls to protect resources and data.
- The term bears some similarity to defense in depth,
- A term adopted from a military strategy that involves multiple layers of defense that resist rapid penetration by an attacker but yield rather than exhaust themselves by too-rigid tactics.

What is Layered security(Contd…)

- Because potential Internet security risks can occur at a variety of levels, you need to set up security measures that provide multiple layers of defense against these risks.
- In general, when you connect to the Internet, you should not wonder if you will experience intrusion attempts or denial of service attacks.
- Instead, you should assume that you will experience a security problem.
- Consequently, your best defense is a thoughtful and proactive offense.

What is Layered security(Contd…)

- Using a layered approach when you plan your Internet security strategy ensures that an attacker who penetrates one layer of defense will be stopped by a subsequent layer.
- Your security strategy must include measures that provide protection across the following layers of the traditional network computing model.
- Generally, you need to plan your security from the most basic (system level security) through the most complex (transaction level security).

Customer Layered security

- Consumer(Application) level security measures control how users can interact with specific applications.
- In general, you must configure security settings for each application that you use.
- However, you need to take special care to set up security for those applications and services that you will use from or provide to the Internet.
- These applications and services are vulnerable to misuse by unauthorized users looking for a way to gain access to your network systems.

Various consumer layered security strategies

- Extended validation (EV) SSL certificates
- Multifactor authentication (also sometimes known as versatile or two-factor authentication)
- Single sign-on (SSO)
- Fraud detection and risk-based authentication
- Transaction signing and encryption
- Secure Web and e-mail
- Open fraud intelligence network

Various consumer layered security strategies(contd...)

Extended Validation Certificate (EV)

- It is an X.509 public key certificate issued according to a specific set of identity verification criteria.
- These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued.
- Certificates issued by a CA under the EV guidelines are not structurally different from other certificates (and hence provide no stronger cryptography than other, cheaper certificates), but are designated with a CA-specific policy identifier so that EV-aware software can recognize them.

Various consumer layered security strategies(contd...)

- The criteria for issuing EV certificates are defined by the Guidelines for Extended Validation Certificates, currently (as of May 2012) at version 1.4.
- The guidelines are produced by the CA/Browser Forum, a voluntary organization whose members include leading CAs and vendors of Internet software, as well as representatives from the legal and audit professions.
-