Unit 6

Securing Information Systems

System Vulnerability and Abuse, Business value of security and control, Technology and Tools for protecting Information, Resources, case study

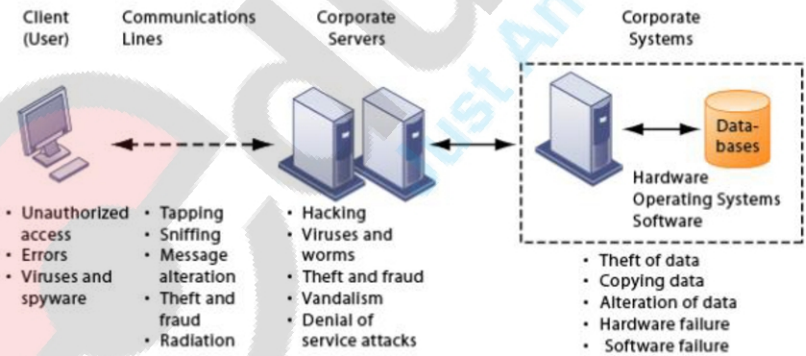
System Vulnerability and Abuse

When data are stored in digital form, they are more vulnerable than when they exist in manual form.

Security refers to the policies, procedures, and technical measures used to prevent Unauthorized access, alteration, theft, or physical damage to information systems.

Controls consist of all the methods, policies, and organizational procedures that ensure the safety of the organizations assets; the accuracy and reliability of its accounting records; and operational adherence to management standards.

Threats to computerized information systems include hardware and software failure user errors physical disasters such as fire or power failure; theft of data, services, and equipment; unauthorized use of data; and telecommunications disruptions. On-line systems and telecommunications are especially vulnerable because data and files can be immediately and directly accessed through computer terminals or at points in the telecommunications network.

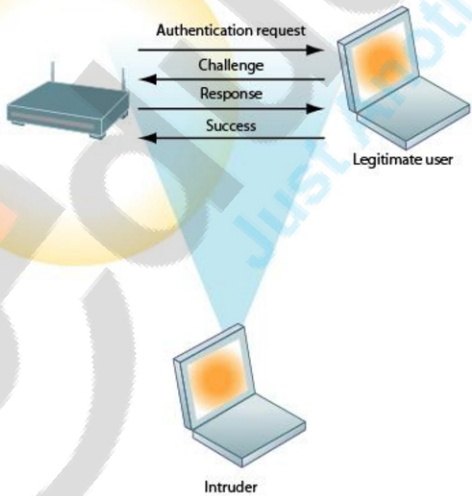


CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES

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.

The Internet poses additional problems because it was explicitly designed to be easily accessed by people on different computer systems. Information traveling over unsecured media can be intercepted and misused. Fixed IP addresses serve as fixed targets for hackers, and Internet software has become a means for introducing viruses and malicious software to otherwise secure networks.
Wireless networks are even more vulnerable because radio frequency bands are easy to scan. LANs that use the Wi-Fi (802.11b) standard can be easily penetrated by outsiders with laptops, wireless cards, external antennae, and freeware hacking software. Service set identifiers (SSID) identifying access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by sniffer programs. In war driving, eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic. The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective. WEP is built into all standard 802.11 products, but users must turn it on, and many neglect to do so, leaving many access points unprotected.



WI-FI SECURITY CHALLENGES

WI-FI SECURITY CHALLENGES

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

Malicious software, or malware, includes threats such as computer viruses and worms, and Trojan horses. A computer virus is rogue software that attaches itself to other programs or data files in order to be executed, and may be highly destructive to files, computer memory, and hard drives. Viruses are typically designed to spread from computer to computer through e-mail attachments or copied files.

Worms are independent computer programs that copy themselves to computers over a network independently from other computer programs or files, and therefore spread more rapidly. A Trojan horse is an apparently benign program that actually performs some hidden action such as installing malicious code or compromising the security of a computer.

Spyware can also act as malicious software by obtaining information about users' buying habits and infringing on privacy. Keyloggers record keystrokes made on a computer to discover steal serial numbers for software and passwords.

A hacker is an individual who intends to gain unauthorized access to a computer system. The term cracker is typically used for hackers with criminal intent. Hackers spoof, or misrepresent themselves, by using fake e-mail addresses or masquerading as someone else. Hacker activities include:

- **Theft of goods and services**
- **System damage**
- **Cyber vandalism:** The intentional disruption, defacement, or even destruction of a Web site or corporate information system.
- **Spoofing:** Hiding of the hackers true identities or email addresses, or redirecting a Web link to a different web site that benefits the hacker.
- **Theft of proprietary information:** A sniffer is an eavesdropping program that monitors network information and can enable hackers to steal proprietary information transmitting over the network.

Denial of service (DoS) attacks: Flooding a network or server with thousands of false communications to crash or disrupt the network. A distributed denial-of-service (DDoS) attack uses hundreds or even thousands of computers to inundate and overwhelm the network from numerous launch points. Hackers can infect thousands of unsuspecting users' computers with malicious software to form a botnet of resources for launching a DDoS.

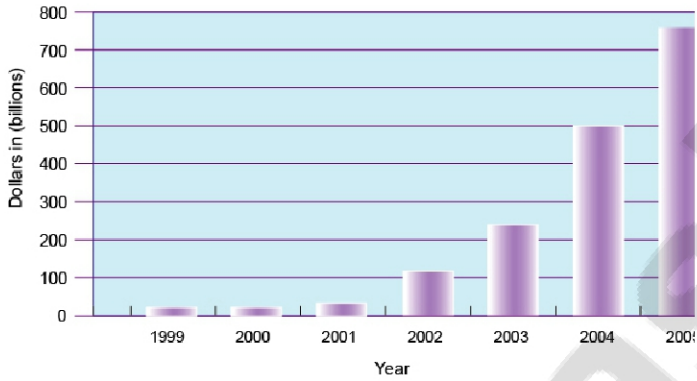


FIGURE WORLDWIDE DAMAGE FROM DIGITAL ATTACKS
This chart shows estimates of the average annual worldwide damage from hacking, malware, and spam

In computer crime, the computer can be either the target of or the instrument of a crime. The most economically damaging kinds of computer crime are DoS attacks, introducing viruses, theft of services, and disruption of computer systems.

Other examples of computer crime include:

• Identity theft: In identity theft, an impostor obtains key pieces of personal information to impersonate someone else and obtain credit, merchandise, or false credentials.

• Phishing: Setting up fake Web sites or sending e-mail messages that appear legitimate in order to coerce users for confidential data. Other phishing techniques include evil twins(wireless networks masquerading as legitimate Internet hotspots, used to capture personal information) and pharming, redirecting users bogus Web sites posing as legitimate Web sites.

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. Click fraud can also be perpetrated with software programs doing the clicking, and bot networks are often used for this purpose.

The U.S. Congress responded to the threat of computer crime in 1986 with the Computer Fraud and Abuse Act. This act makes it illegal to access a computer system without authorization. Most U.S. states and European nations have similar legislation. Congress also passed the National Information Infrastructure Protection Act in 1996 to make virus distribution and hacker attacks to disable Web sites federal crimes.

One concern is that terrorists or foreign intelligence services could exploit network or Internet vulnerabilities to commit cyber terrorism or cyber warfare and cripple networks controlling essential services such as electrical grids and air traffic control systems.

The largest financial threats to businesses actually come from insiders, either through theft and hacking or through lack of knowledge. Malicious intruders may sometimes trick employees into revealing passwords and network access data through social engineering. Employees can also introduce faulty data or improperly process data.

Software errors are also a threat to information systems and cause untold losses in productivity. Hidden bugs or program code defects, unintentionally overlooked by programmers working with thousands of line of programming code, can cause performance issues and security vulnerabilities. Software vendors create lines of code called patches to repair flaws without disrupting the software's operation.

Business value of Security and Control

Security and control have become a critical, although perhaps unappreciated, area of information systems investment. The longer computer systems are down, the more serious the consequences for the firm. With increasing reliance on the Internet and networked systems, firms are more vulnerable than ever to disruption and harm.

Company systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They may contain information on corporate operations, trade secrets, new product development plans, and marketing strategies. Inadequate security and control may also create serious legal liability.

Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Recent U.S. government regulations mandate the protection of data from abuse, exposure, and unauthorized access, and include:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, which requires members of the healthcare industry to retain patient information for six years and ensure the confidentiality of those records

The Gramm-Leach-Bliley Act, which requires financial institutions to ensure the security and confidentiality of customer data

The Sarbanes-Oxley Act, which imposes responsibility on companies and their management to use internal controls to safeguard the accuracy and integrity of financial information

Firms face new legal obligations for electronic records management and document retention as well as for privacy protection. Electronic records management (ERM) consists of policies, procedures, and tools for managing the retention, destruction, and storage of electronic records.

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. Legal cases today increasingly rely on evidence represented as computer data stored on portable floppy disks, CDs, and computer hard disk drives, as well as in e-mail, instant messages, and e-commerce transactions over the Internet. E-mail is currently the most common type of electronic evidence.

An effective electronic document retention policy ensures that electronic documents, e-mail, and other records are well organized, accessible, and neither retained too long nor discarded too soon.

Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. Electronic evidence can reside on computer storage media in the form of computer files and as ambient data, which are not visible to the average user.

Technologies and Tools for Security and Control
Various tools and technologies used to help protect against or monitor intrusion include authentication tools, firewalls, intrusion detection systems, and antivirus and encryption software.

Access control consists of all the policies and procedures a company uses to prevent improper access to systems by unauthorized insiders and outsiders.

Authentication refers to the ability to know that a person is who he or she claims to be. Access control software is designed to allow only authorized persons to use systems or to access data using some method for authentication. New authentication technologies include:

Token: A physical device similar to an identification card that is designed to prove the identity of a single user.

Smart card: A device about the size of a credit card that contains a chip formatted with access permission and other data.

Biometric authentication: Compares a person's unique characteristics, such as fingerprints, face, or retinal image, against a stored set profile.

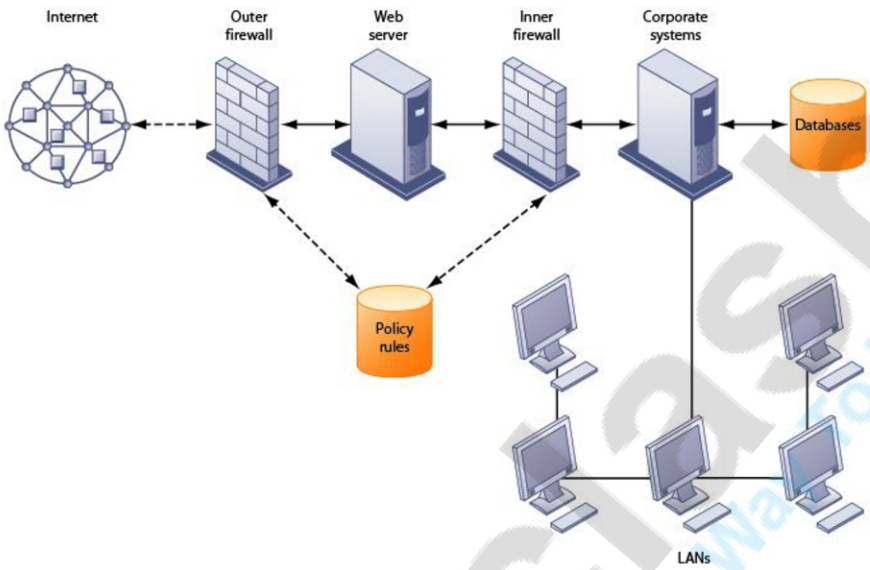
A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic and prevents unauthorized communication into and out of the network. The firewall identifies names, Internet Protocol (IP) addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules programmed into the system by the network administrator. There are a number of firewall screening technologies:

Packet filtering examines fields in the headers of data packets flowing between the network and the Internet, examining individual packets in isolation.

Stateful inspection determines whether packets are part of an ongoing dialogue between a sender and a receiver.

Network Address Translation (NAT) conceals the IP addresses of the organization's internal host computer(s) to protect against sniffer programs outside the firewall.

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate with a user inside the organization, the outside user first "talks" to the proxy application and the proxy application communicates with the firm's internal computer.



A CORPORATE FIREWAL

Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points of corporate networks to detect and deter intruders continually. Scanning software looks for patterns indicative of known methods of computer attacks, such as bad passwords, checks to see if important files have been removed or modified, and sends warnings of vandalism or system administration errors.

Antivirus software is designed to check computer systems and drives for the presence of computer viruses. However, to remain effective, the antivirus software must be continually updated.

Vendors of Wi-Fi equipment have developed stronger security standards. The Wi-Fi Alliance industry trade group's 802.11i specification tightens security for wireless LAN products.

Many organizations use encryption to protect sensitive information transmitted over networks. Encryption is the coding and scrambling of messages to prevent their access by unauthorized individuals.

Two methods for encrypting network traffic on the Web are:

Secure Sockets Layer (SSL): SSL and its successor Transport Layer Security (TLS) enable client and server computers to establish a secure connection session and manage encryption and decryption activities.

Secure Hypertext Transfer Protocol (S-HTTP) is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages.

Data is encrypted by applying a secret numerical code, called an encryption key, so that the data are transmitted as a scrambled set of characters. To be read, the message must be decrypted (unscrambled) with a matching key. There are two alternative methods of encryption:
Symmetric key encryption: The sender and receiver create a single encryption key that is shared.
Public key encryption: A more secure encryption method that uses two different keys, one private and one public.

PUBLIC KEY ENCRYPTION
A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message