CHAPTER 7

NETWORK SECURITY

Security

- Security is about the well-being (*integrity*) of computer systems and data
- Computer security is the protection of data, networks and computing power.
- Computer security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization.

Why Computer Security?

- Computer security is required because most organizations can be damaged by software or intruders.
- The damages include:
  - Damage of computer systems.
  - Damage of internal data.
  - Loss of sensitive information to hostile parties.
  - Use of sensitive information to steal items of monetary value.
  - Use of sensitive information against the organization's customers
  - Damage to the reputation of an organization.
  - Losing the ability to use the system

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK/INTERNET**

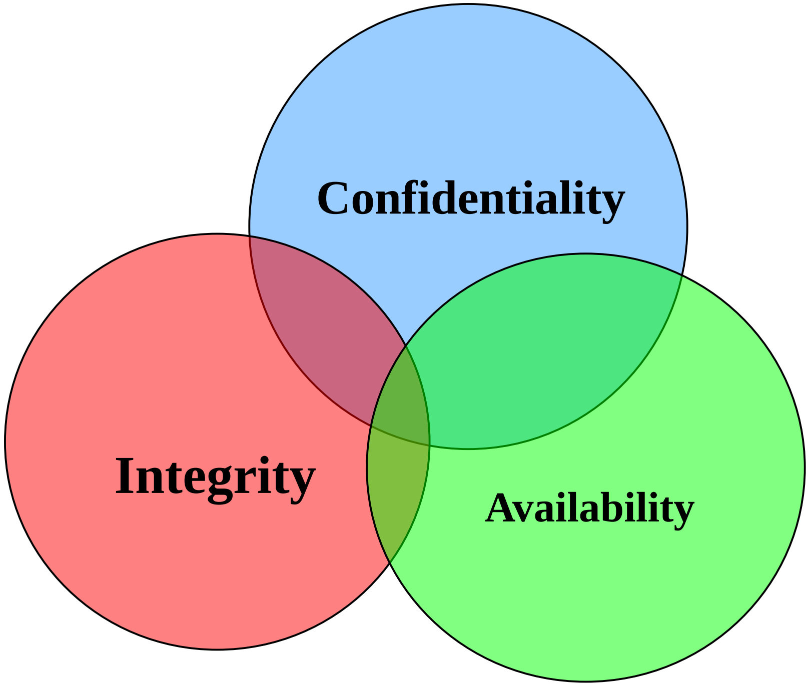
Who is the most secured?

“The most secure computers are those not connected to the Internet and shielded from any interference”

Computer Security Goals

Computer security addresses the following goals:

- *Confidentiality*
- *Integrity*
- *Availability*



Confidentiality

- The requirement that information maintained by a computer system be accessible only by authorized individuals.
- Is the cover-up of information or resources.
- The need for keeping information secret arises from the use of computers in sensitive fields such as government and financial companies.

Integrity

- Refers to the trustworthiness of data or resources
- Integrity is preventing from unauthorized change.
- Guarding against information modifications or destruction.
- Modification occurs when an unauthorized users not only gains access to but changes a resource such as data or the execution of a running process.

Availability

- Availability refers to the ability to use the computer system and information resources at desired times by authorized parties (24/7)
- Availability is an important aspect of reliability
- Unavailable system is at least as bad as no system at all.
- Interruption occurs when an unauthorized party reduces the availability of or to a resource.

Security Threats

- A computer security threat is any person, act, or object that poses a danger to computer security
- A *threat* is a potential violation of security.
- The effects of threats can be an affect on the
  - Confidentiality of data
  - Integrity of data
  - Availability of a system.

Causes of Security Threats

- *Physical threats:*
  - weather, natural disaster, bombs, power failures, terrorism, etc.
- *Human threats:*
  - stealing, fraud, bribery, spying, sabotage, accidents.
- *Software threats:*
  - viruses, worms, Trojan horses, denial of service.

Types of Security Threats/Attacks

- Fraud and Theft
- Loss of Physical and Infrastructure Support
- Intruders
- Malicious Software
- Threats to Personal Privacy
- Denial of Service (DoS)

Fraud and Theft

- An illegal taking of another's physical, electronic, or intellectual property
- Insiders or outsiders can commit computer fraud and theft.
- Insiders (authorized users of a system) are responsible for the majority of fraud.

Loss of Physical and Infrastructure Support

- Power failures
  - Outages
    - a period when a power supply is not available
  - Spikes
    - contain very high voltages
  - Brownouts
    - reduction in the availability of electrical power
- Disasters (natural and man-made)

Intruders

- Intruders are usually trying to gain access to a system, or to increased privileges to which they are not entitled, often by obtaining the password for a legitimate account.
- Hacking: is any attempt to intrude or gain unauthorized access to your system.
  - It can be via some operating system flaw or other means.
  - It may or may not be for malicious purposes.
- Cracking: is hacking conducted for malicious purposes

Malicious Software

- The most sophisticated threats to computer systems are through malicious software, sometimes called malware.
- Malware attempts to cause damage to, or consume the resources of a target system.
- Malicious code can attack personal computers and other platforms.
- Malicious Software refers to
  - Virus
  - Trojan Horse
  - Worm
  - Logic bomb
  - Trap door
  - Zombie

Virus

- A small program that replicates and hides itself inside other programs usually without your knowledge
- A virus is a program that can ”infect” other programs by modification, as well as causing local damage. Such modification includes a copy of the virus, which can then spread further to other programs.
- The new copy of the virus is executed when a user executes the new host program.
  - Similar to biological virus: Replicates and Spreads

Worm

- Worm is an independent program that spreads via network connections, typically using either email, remote execution etc.
- Worm reproduces by copying itself from one computer to another and causes it to execute; no user intervention is required
- It can do as much harm as a virus
- It often creates denial of service (DoS)

Trojan Horse

- Seems to do something good but covertly doing something else.
- Secretly downloading a virus or some other type of mal-ware on to your computers.
- Popular mechanism for hiding a virus or a worm
- Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems

Spy-wares

- A software that literally spies on what you do on your computer.
- Example: Simple Cookies and Key Loggers

Logic Bomb

- **one of oldest types of malicious software**
- **code embedded in legitimate program (Trojan horse)**
- **activated when specified conditions met**
  - **eg presence/absence of some file**
  - **particular date/time**
  - **particular user**
  - **particular series of keystrokes**
- **when triggered typically damage system**
  - **modify/delete files/disks**

Trap door/Backdoor

- Is a mechanism built into a system by its designer
- A trapdoor usually gives the designer away to sneak back into the system
- Gives the original designer a secret route into the system

The effects of malicious software

- Corrupting the systems data
- Increasing file size
- Formatting the hard disk
- Slowing down the system
- Renaming all files with different name
- Display error messages

Denial of Service Attack

DoS Attack:

- Is blocking access of legitimate users to a service.
- It aims to inhibit the normal use of communication facilities
- Make a network service unusable, usually by overloading the server or network

Types of Security

- Physical security
- Logical security

Physical security

- Keeping rooms, computers locked
- A combination of locks and alarms is an excellent theft prevention system for computer
- Surge protectors and uninterruptable power supplies (UPS) are a low cost investment that can save very costly equipment damage.

Logical security

- concerned with security of data stored on devices connected to the network.
- It involves
  - controlling passwords and password policies
  - controlling access to data on servers
  - controlling access to backup tapes
  - preventing sources outside the network from gaining access to the network

Security Solutions

There are a number of basic ways that a computer can be made more secure.

- Backups/disaster recovery
- Encryption
- Authentication
- Validation
- Data Protection
- Anti-Viruses
- Firewall
- Intrusion Detection System (IDS)

Backups (redundancy/disaster recovery)

- The purpose of a backup is to make a copy of data, which is unlikely to be lost or destroyed.
- If we want a backup to be protected from some accidents that would destroy the data, we have to store it in a *different physical location.*
- Backups can be done on tapes, disks and at a different physical location by using network copying.

Backups

There are two kinds of backup

- **Full dump**: copies every file on a source medium to a backup medium.
- **Incremental or differential dump**: copies files according to the level of the dump.
  - A level 0 dump copies everything.
  - A level 1 dump copies everything, which has changed since the last level 0 dump.
  - A level 2 dump copies everything which has changed since the last level 1 dump or level 0 dump and so on.

Encryption

- Process of converting plaintext (readable data) into ciphertext (unreadable characters) to prevent unauthorized parties from viewing or modifying it.
- Encryption key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms
- To read the data, the recipient must decrypt, or decipher the data
- The security of encryption lies in the ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext

Authentication

- Authentication is the process of proving his or her identity using username and password to gain access to a system, network or web site.
- The username and password combination is often referred to as a person’s credentials and it is frequently sent over networks.
- Item that you must carry to gain access to computer or facility are called personal identification number (PIN)

Validation

- Validation describes the ability to provide assurance that a sender's identity is true and that a message, document or file has not been modified.
- Encryption can be used to provide validation by making a digital fingerprint of the information contained within a message.
- A digital fingerprint is a code that uniquely identifies a file or a message by reflecting the content of the file with tremendous specificity.

Antiviruses

To prevent viruses from entering a system there are two options.

- Isolate the machine
  - disconnect it from the Internet or any other network, not using floppy disks, CD-ROMs or any other removable disks.
  - This way one can be sure that no virus enters into the computer.

Antiviruses

- Install an Antivirus program
  - Antivirus programs are designed to keep a watch at all incoming files so that no malicious code can enter the computer.
  - Antivirus is a software utility, which searches the hard disk for viruses and removes which are found.

Antiviruses

- Most Antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.
- AVG, Norton, Kaspersky, AVAST and McAfee are some of the examples of Antivirus programs.

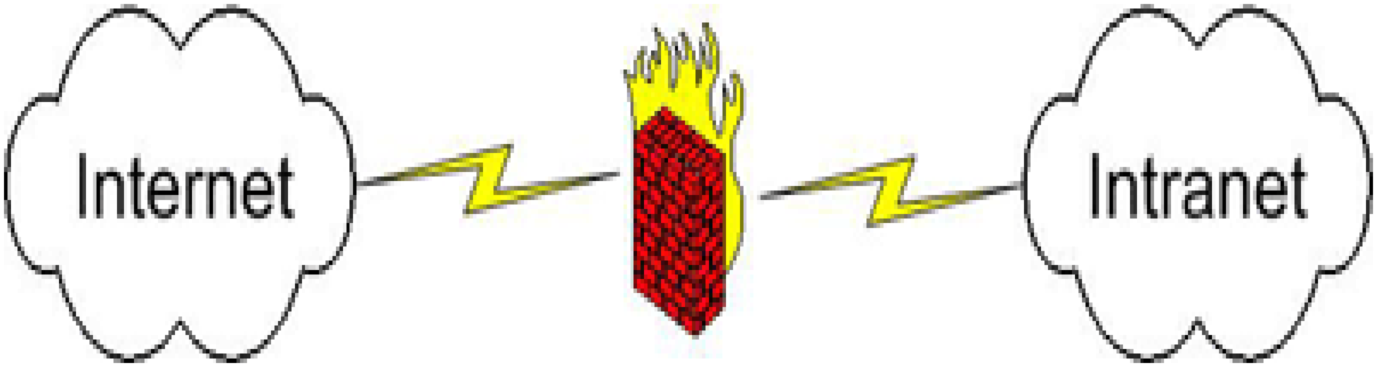
Functions of anti-viruses

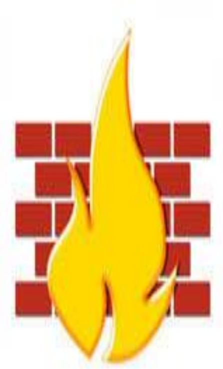
- Identification of known viruses
- Detection of suspected viruses
- Blocking of possible viruses
- Disinfection of infected objects
- Deletion and overwriting of infected objects

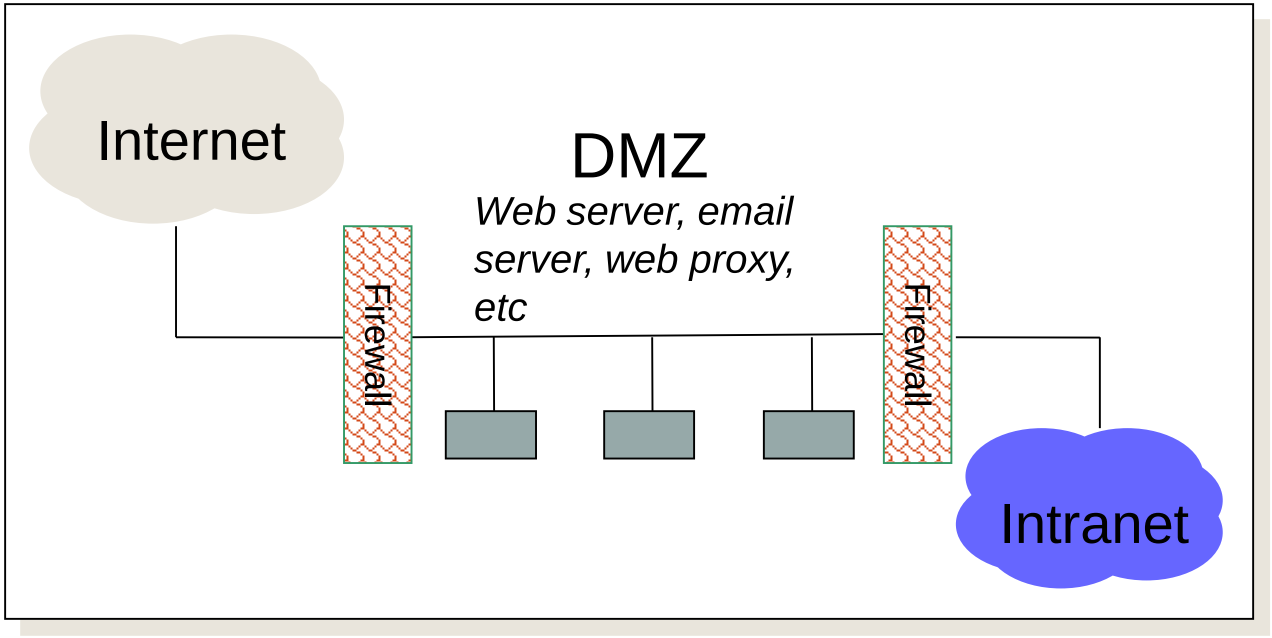
Firewall

- A firewall is a security system consisting of hardware and/or software that prevents unauthorized network access
- A firewall is a network component that provides a security barrier between networks or network segments.
- Firewalls are generally set up to protect a particular network or network component from attack, or unauthorized penetration by outside invaders.

Firewall







Internet

DMZ

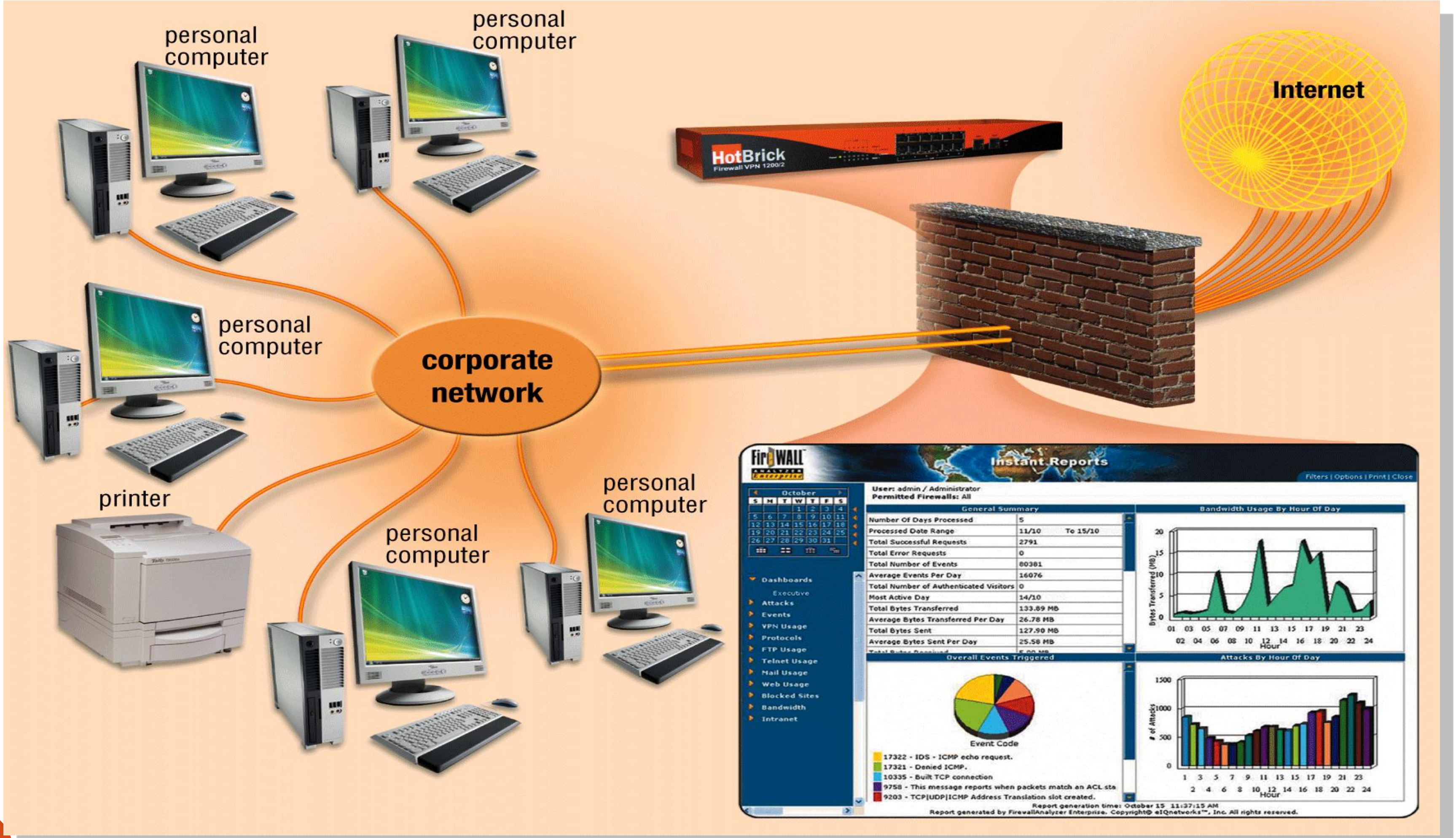
Web server, email server, web proxy, etc

Firewall

Firewall

Intranet

Firewall



User: admin / Administrator
Permitted Firewalls: All

General Summary	
Number Of Days Processed	5
Processed Date Range	11/10 To 15/10
Total Successful Requests	2791
Total Error Requests	0
Total Number of Events	80381
Average Events Per Day	16076
Total Number of Authenticated Visitors	0
Most Active Day	14/10
Total Bytes Transferred	133.89 MB
Average Bytes Transferred Per Day	26.78 MB
Total Bytes Sent	127.90 MB
Average Bytes Sent Per Day	25.58 MB

🟨 17322 - IDS - ICMP echo request.
🟩 17321 - Denied ICMP.
🟦 10335 - Built TCP connection
🟪 9758 - This message reports when packets match an ACL sta
🟥 9203 - TCP|UDP|ICMP Address Translation slot created.

Report generation time: October 15 11:37:15 AM
Report generated by FirewallAnalyzer Enterprise. Copyright© eIQnetworks™, Inc. All rights reserved.

Intrusion Detection System (IDS)

- An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches
- Used to monitor for “suspicious activity” on a network
- It detects both intrusions and misuse
- Freeware IDS exist e.g. snort (www.snort.org)

Intrusion Detection System (IDS)

Intrusion detection functions include

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

Network Security Tools

- ✓ Nessus- vulnerability scanners
- ✓ Wireshark-- packet sniffers
- ✓ Snort (IDS- - intrusion detection system
- ✓ Netcat-- Netcat)
- ✓ Metasploit -Framework (vulnerability exploitation tools)
- ✓ HPing2 -- packet crafting tools
- ✓ Kismet -- wireless tools or packet sniffers
- ✓ TCPDump --- packet sniffers
- ✓ Cain and Abel (password crackers or packet sniffers)
- ✓ John The Ripper (password crackers)