

CHAPTER 5

MAJOR ISSUES IN COMPUTER AND INFORMATION SYSTEM

Compiled by: Tsegaye Berhanu

Outline



- **Effect of ICT**
- **Overview of Computer security and privacy**
- **Legal Issues**
- **Attacks and Threats**
- **Countermeasures**

Effect of ICT on Patterns of Employment

- ❑ **The personal computer (PC) was developed in the early 1980s.**
- ❑ **Before this date, computers were huge, expensive machines that only a few, large businesses owned.**
- ❑ **Now PCs are found on almost every desk in every office, all over the world.**
- ❑ **Because companies now have access to so much cheap, reliable computing power, they have changed the way they are organized and the way they operate. As a result, many people's jobs have changed.**

Areas of Increased Unemployment

- **Manufacturing:**
 - ▣ Many factories now have fully automated production lines.
 - ▣ Instead of using people to build things, computer-controlled robots are used.
- **Secretarial Work:**
 - ▣ Offices used to employ many secretaries to produce the documents required for the business to run.
 - ▣ Now people have personal computers, they tend to type and print their own documents.
- **Accounting Clerks:**
 - ▣ Companies once had large departments full of people whose job was to do calculations (e.g. profit, loss, billing, etc.)
 - ▣ A personal computer running a spreadsheet can now do the same work

Areas of Increased Employment

- **IT Technicians:**
 - **All of the computers in a business need to be maintained: hardware fixed, software installed, etc.**
 - **IT technicians do this work.**
- **Computer Programmers:**
 - **All of the software that is now used by businesses has to be created by computer programmers.**
- **Web Designers:**
 - **Much of modern business is conducted on-line, and company websites are very important.**
 - **Company websites need to be designed and built which is the role of web designers.**
- **Help-Desk Staff:**
 - **People often need help using computers, and software applications.**
 - **Computer and software companies have help-desks staffed by trained operators who can give advice.**

Health Effects of ICT

□ **Eye-Strain:**

- **One health issue that can occur after using computers for a long time is eye-strain (tiredness of the eyes)**
- **This problem can be solved:**
 - **Look away from the monitor at regular intervals.**
 - **Take regular breaks.**
 - **Use an anti-glare filter in front of the monitor to cut down on screen reflections that can also tire the eyes.**

Health Effects of ICT

□ **Back and Neck Ache:**

- **Back and neck pain are caused due to bad sitting posture.**
- **This problem can be solved:**
 - **Use an adjustable, ergonomic chair, and take the time to set it up properly.**
 - **The computer keyboard and monitor should be at the correct height for the seated person (keyboard lower than the elbow, top of monitor at eye level).**
 - **Take regular breaks: get up, walk around, stretch your muscles**

Health Effects of ICT

- **Repetitive Strain Injury (RSI) in Wrists and Hands:**
 - **Any repetitive movement (same movement over and over again) can result in a health problem called repetitive strain injury (RSI).**
 - **In particular, typing and using a mouse for long periods are common causes of RSI in the wrist (it is often called carpal-tunnel syndrome).**
 - **This problem can be solved:**
 - **Use a wrist-rest to support the wrists while typing and when using the mouse.**
 - **Take regular breaks from typing or using the mouse.**

Computer Security and Privacy

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



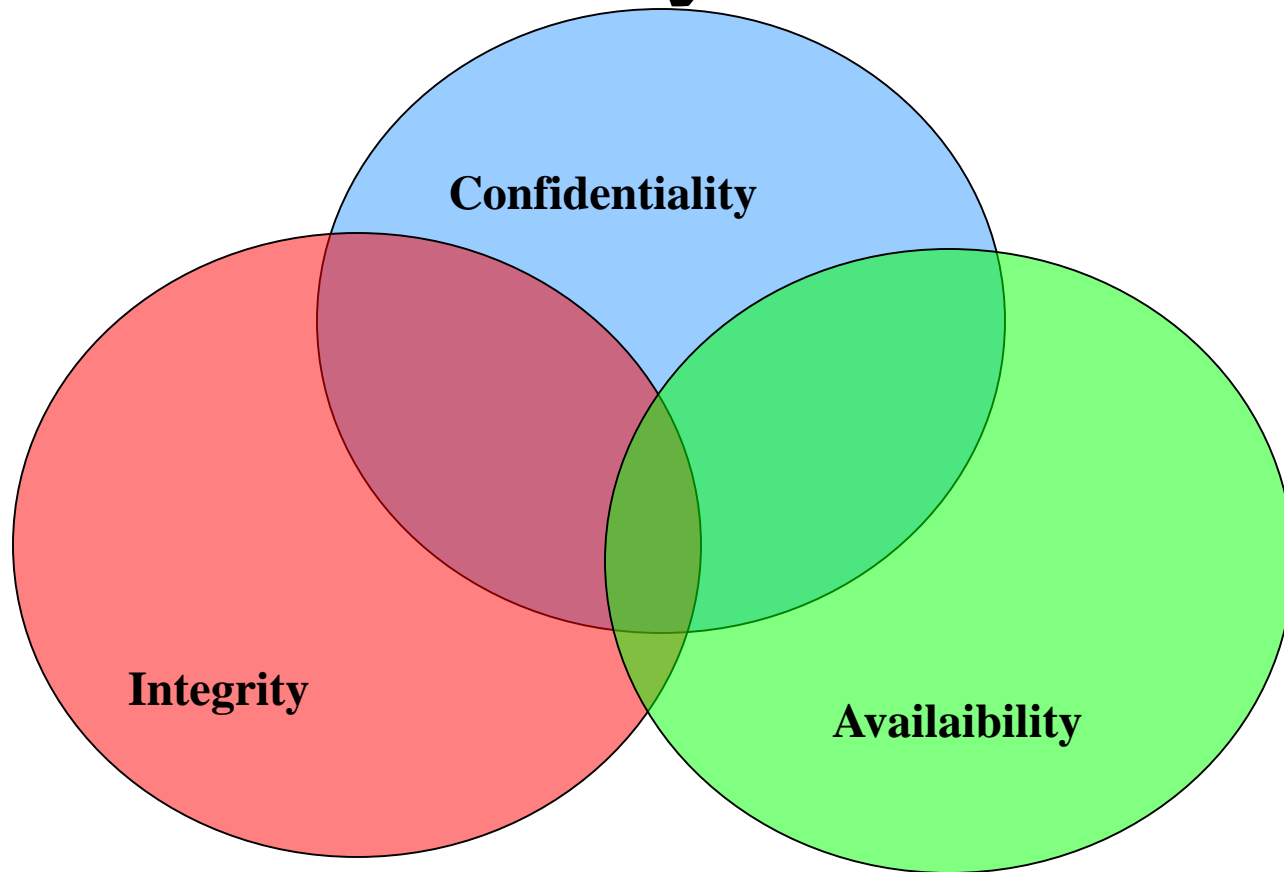
Computer Security and Privacy

Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.




Computer Security and Privacy


Security Goals



Overview

Definitions

 **Security:** The prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction, and other threats.

 **Privacy:** The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.

 **Security/Privacy Threat:** Any person, act, or object that poses a danger to computer security/privacy.

History of Computer Security

- ☰ Until 1960s computer security was limited to physical protection of computers

- ☰ In the 60s and 70s

- **Evolutions**

- Computers became interactive
- Multiuser/Multiprogramming was invented
- More and more data started to be stored in computer databases

- Organizations and individuals **started to worry** about

- What the other persons using computers are doing to their data
- What is happening to their private data stored in large databases

History of Computer Security

☰ In the 80s and 90s

● Evolutions

- Personal computers were popularized
 - LANs and Internet invaded the world
 - Applications such as E-commerce, E-government and E-health started to develop
 - Viruses become major threats
- ### ● Organizations and individuals **started to worry about**
- Who has access to their computers and data
 - Whether they can trust a mail, a website, etc.
 - Whether their privacy is protected in the connected world

History of Computer Security

Famous security problems

- **Morris worm** – Internet Worm
 - November 2, 1988 a worm attacked more than 60,000 computers around the USA
 - The worm attacks computers, and when it has installed itself, it multiplies itself, freezing the computer
 - It exploited UNIX security holes in Sendmail
 - A nationwide effort enabled to solve the problem within 12 hours
- Robert Morris became **the first person** to be indicted under the **Computer Fraud** and Abuse Act.
 - He was sentenced to three years of probation, 400 hours of community service and a fine of \$10,050
- He is currently an **associate professor** at the Massachusetts Institute of Technology (MIT)

History of Computer Security

☰ Famous security problems ...

● NASA shutdown

- In 1990, an Australian **computer science student** was charged for shutting down NASA's computer system for 24 hours

● Airline computers

- In 1998, a major **travel agency** discovered that someone penetrated its ticketing system and has printed airline tickets illegally

● Bank theft

- In 1984, a bank manager was able to steal **\$25 million** through un-audited computer transactions

History of Computer Security

Famous security problems ...

● In **Ethiopia**

- Employees of a company managed to **change their salaries** by fraudulently modifying the company's database
- In 1990s Internet password theft
 - *Hundreds of dial-up passwords were stolen and sold to other users*
 - *Many of the owners lost tens of thousands of Birr each*
- A major company suspended the use of a **remote login** software by technicians who were **looking at** the computer of the General Manager

● In **Africa: Cote d'Ivoire**

- An employee who has been fired by his company deleted all the data in his company's computer

History of Computer Security

Early Efforts

- 1960s: Marked as the **beginning** of true computer security

- 1970s: Tiger teams

- Government and industry sponsored **crackers** who attempted to break down defenses of computer systems in order to uncover vulnerabilities so that patches can be developed

- 1970s: Research and modeling

- Identifying security **requirements**
- Formulating security **policy** models
- Defining recommended **guidelines** and controls
- Development of **secure systems**

Legal Issues

- In the US, **legislation** was enacted with regards to computer security and privacy starting from late 1960s.
- European Council adopted a **convention** on Cyber-crime in 2001.
- The World Summit for Information Society considered computer security and privacy as a **subject of discussion** in 2003 and 2005.
- The **Ethiopian Penal Code** of 2005 has articles on data and computer related crimes.

Attacks & Threats



Computer Security Attacks and Threats

Attacks & Threats



 A computer **security threat** is any person, act, or object that poses a danger to computer security

 Computer world is full of threats!

Attacks & Threats

Types of Threats/Attacks

- Physical Attack
- Hacking Attack
- Denial of Service (DoS) Attack
- Malware Attack

Types of Threats/Attacks

Physical Attack:

- Stealing, breaking or damaging of computing devices

Attacks & Threats

Types of Threats/Attacks

Malware Attack:

- A generic term for software that has malicious purpose
- Examples
 - Viruses
 - Trojan horses
 - Spy-wares
 - New ones: Spam/scam, identity theft, e-payment frauds, etc.

Attacks & Threats

Malware Attack:

Viruses

- “A small program that replicates and hides itself inside other programs usually without your knowledge.”
- Similar to **biological** virus: Replicates and Spreads

Worms

- An independent program that reproduces by copying itself from one computer to another
- It can do as much harm as a virus
- It often creates denial of service

Attacks & Threats

Malware Attack...

Trojan horses


- Secretly downloading a virus or some other type of mal-ware on to your computers.

Spy-wares

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

Attacks & Threats

Hackers/Intrusion Attack:

 **Hacking:** is any attempt to intrude or gain unauthorized access to your system either via some operating system flaw or other means. The purpose may or may not be for malicious purposes.

 **Cracking:** is hacking conducted for malicious purposes.

Attacks & Threats

Denial of Service (DoS) Attack:

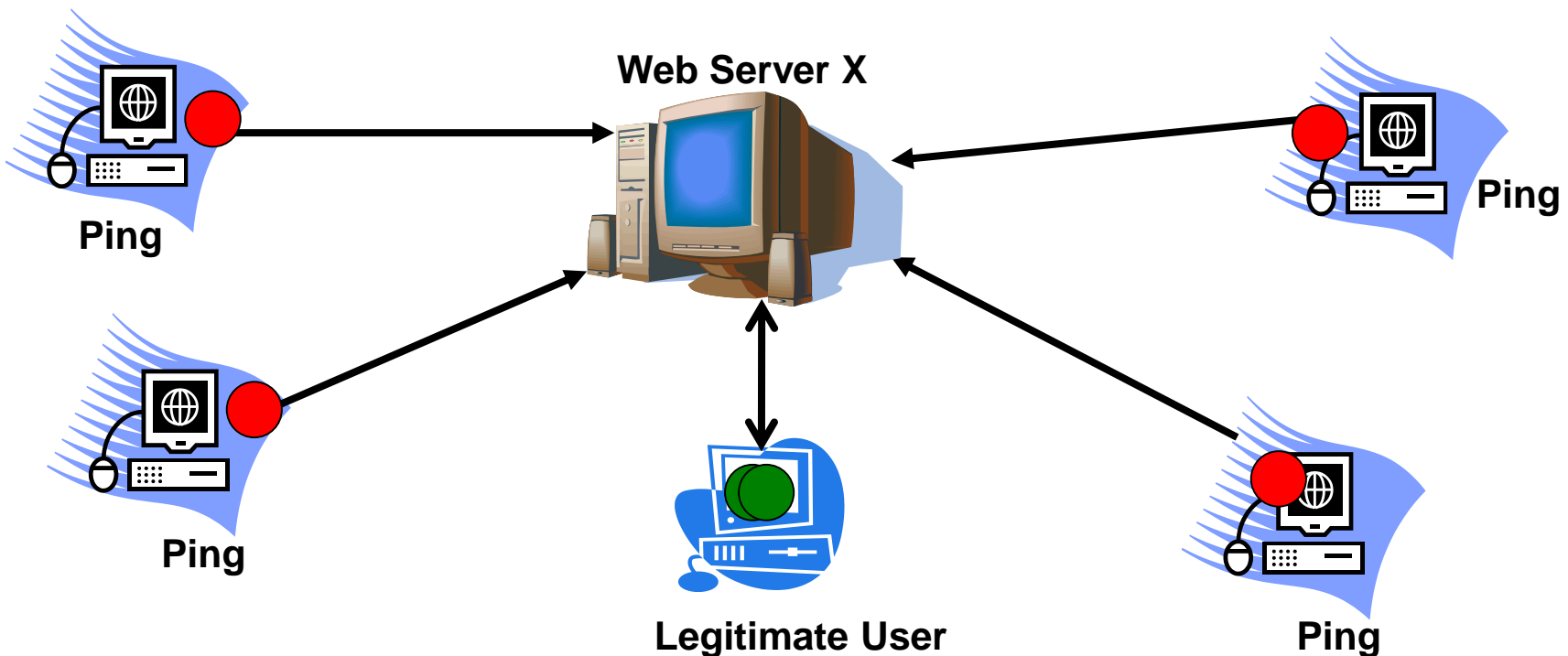
☰ **DoS Attack:** is blocking access of legitimate users to a service.

☰ In computing, a denial-of-service attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Attacks & Threats

Simple illustration of DoS attack

```
C:\>Ping <address of X> -l 65000 -w 0 -t
```



Countermeasures

☰ Computer security controls

- Authentication (Password, Cards, Biometrics)

(What we know, have, are!)

- Encryption

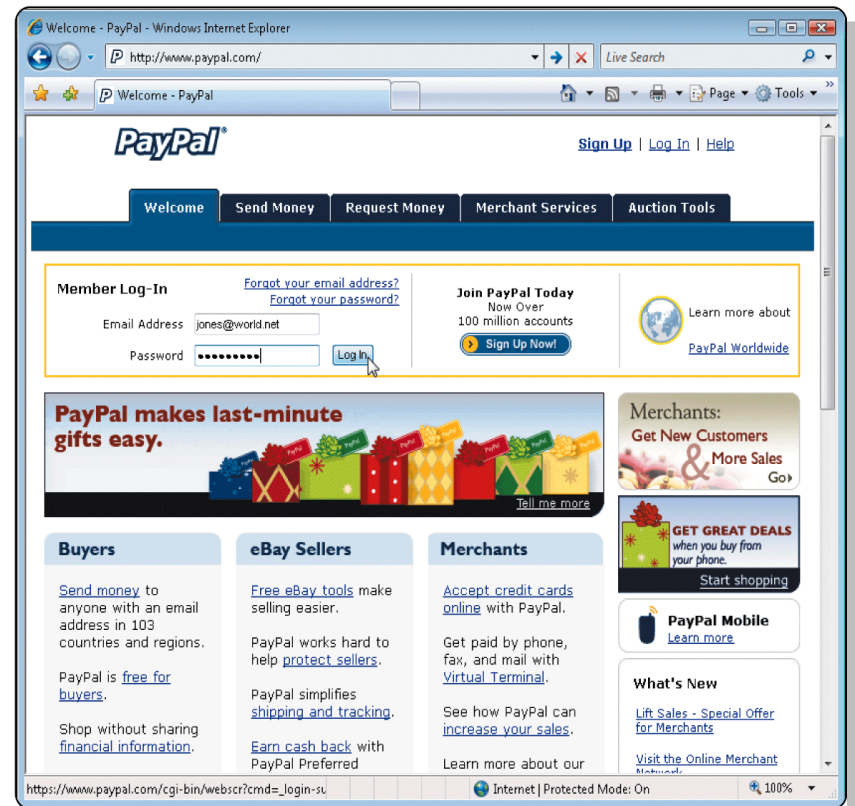
- Anti-virus

- Firewall and Intrusion Detection Software

Countermeasures

Authentication

- ❑ **User name** is a unique combination of characters that identifies user
- ❑ **Password** is private combination of characters associated with the user name that allows access to certain computer resources



Countermeasures

Authentication

How can you make your password more secure?

- Longer passwords provide greater security

PASSWORD PROTECTION		AVERAGE TIME TO DISCOVER	
Number of Characters	Possible Combinations	Human	Computer
1	36	3 minutes	.000018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- Possible characters include the letters A–Z and numbers 0–9
- Human discovery assumes 1 try every 10 seconds
- Computer discovery assumes 1 million tries per second
- Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations

Countermeasures

Authentication

What is a possessed object?

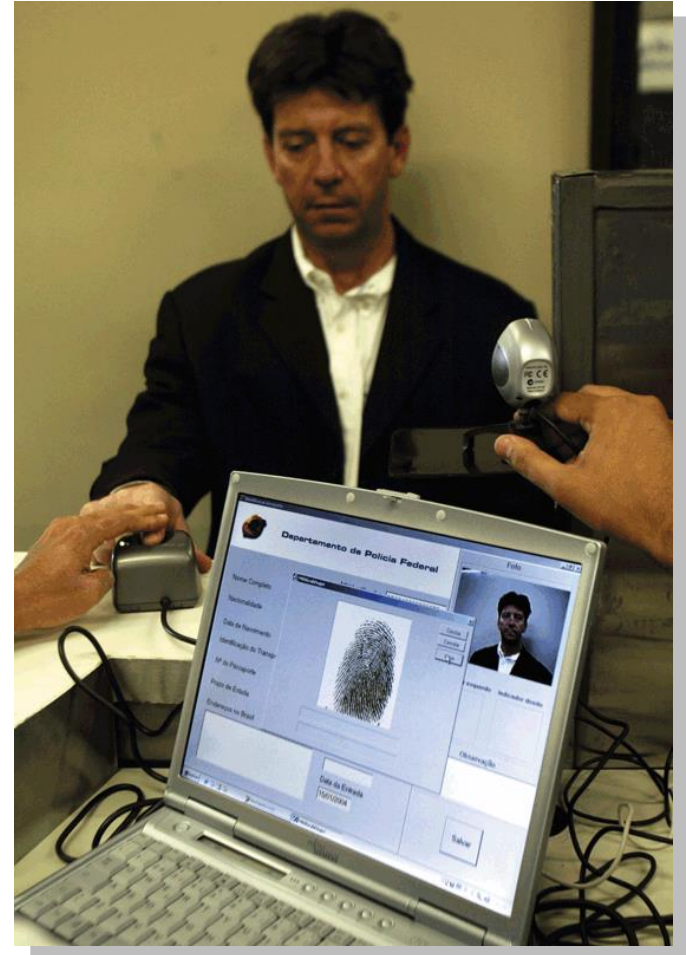
- **Item that you must carry to gain access to computer or facility**
- **Often used with numeric password called **personal identification number (PIN)****

Countermeasures

Authentication

What is a **biometric device**?

- *Biometrics* authentication (or realistic authentication) is used in computer science as a form of identification and access control.
- **Authenticates person's identity using personal characteristic**
 - Fingerprint, hand geometry, voice, signature, and iris



Countermeasures

Encryption

- Safeguards against **information theft**
- Process of converting **plaintext** (readable data) into **ciphertext** (unreadable characters)
- **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

Countermeasures

Anti-Virus

There are

- Generic solutions
 - Ex. Integrity checking
- Virus specific solution
 - Ex. Looking for known viruses

Three categories

- Scanners
- Activity monitors
- Change detection software

Countermeasures

Anti-Virus ...

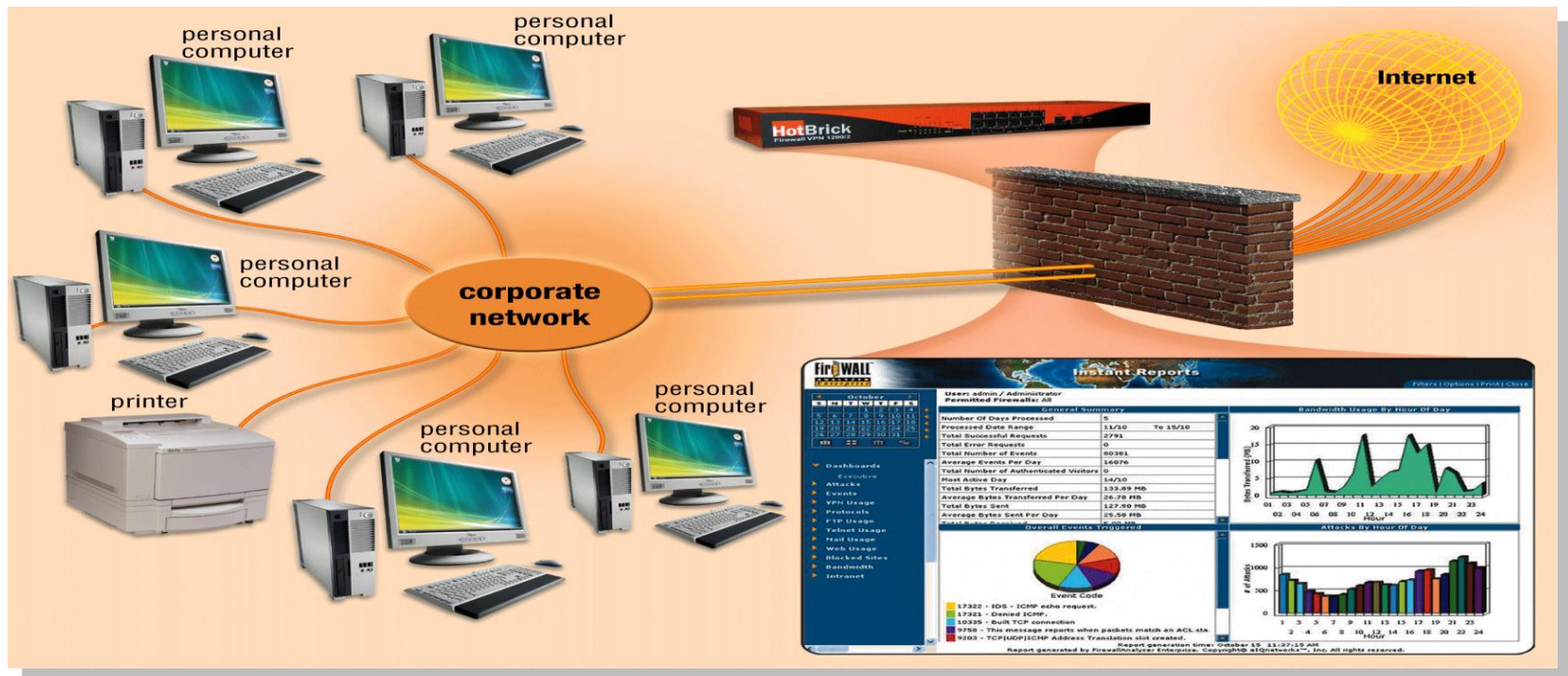
Functions of anti-viruses

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

Countermeasures

Firewall

- Security system consisting of hardware and/or software that prevents unauthorized network access



Countermeasures



Firewall

What is a **personal firewall** utility?

- **Program that protects personal computer and its data from unauthorized intrusions**
- **Monitors transmissions to and from computer**
- **Informs you of attempted intrusion**

Countermeasures

Intrusion Detection Software

- **Analyzes network traffic**
- **Assesses system vulnerabilities, and**
- **Identifies intrusions and suspicious behavior**