EVANGELOS C. ZIOULAS

IT Teacher

VCZ

CHAPTER 7

DATA SAFETY COMPUTER VIRUSES

http://www.zioulas.gr vczioulas@yahoo.com

DATA SAFETY

- In a computer system, the file storage (e.g. hard disk) is not always safe.

- There is always a **chance of loss or destruction** of files and folders. Most of the times, the reason for that is the user himself or some other external factors he cannot control.

POSSIBLE CAUSES OF DESTRUCTION

(A) DAMAGED STORAGE MEDIA

- A possible damage in a peripheral device (e.g. a burnt or demagnetized disk) makes the data access of files and folders sometimes impossible.

(B) COMPUTER VIRUSES

- They are malicious programs created by particular programmers, which cause many problems to computer.

- The **virus** is a piece of software (a program) that acts as an **attachment** of another program which when is activated, the virus **acts silently** and harms computer functions.

- Each year a vast number of new viruses appear.

The first virus appeared in **1986**, though up to our days there have been created almost **150.000.**

- **Possible damages** caused by viruses:
  - **Deleting data** on the hard disk
  - **Causing delay** in data process (deceleration of processing speed)
  - **Displaying** annoying **messages** on the screen
  - **Undue restart** of the system
  - **Problematic function** of Operating System

- A computer virus can penetrate our system usually with two ways:
  - **External storage devices** (floppy disks, cd-roms, dvd, flash memory, external disks)
  - **Computer networks** and **Internet** (Web pages, Instant Messenger, Emails, Ftp)
- Today there are many types of malicious software (**malware**) that can harm our computer.

Computer Worms	They are programs able to **multiply creating many copies** of themselves which transmit through the net from peer to peer causing serious delays. In contrast with viruses, computer **worms do not need to attach themselves to existing programs.** A computer worm is a **self-replicating** malware computer program, which uses a computer network to send copies of it to other computers on the network and it may do so without user awareness.
Trojan Horses	They are **malicious** programs that **deceive the user**. Externally, they **seem to be harmless** making user to believe that he executes an innocent application (e.g. pc-game). However, in the background they install a harmful code which infects the computer. This kind of infection may allow external users to have access to the infected computer, or even more drive to disk format. In contrast with viruses, **Trojan Horses are not transmitted by polluting files.**

Malware	Malicious software which is **harmful** for the security of an information system (viruses, worms, trojans).
Adware	Malicious software, harmless by itself, which fills computer screen with **annoying advertisements** and other announcements.
Spyware	Suspicious software which acts silently and **collects private information** of the user e.g. passwords, credit card numbers.
Crimeware	Software designed to access a user's online account at online shops and other financial services for the purpose of **stealing funds** from those accounts or completing **unauthorized transactions** that enrich the thief controlling the crimeware.
Dialer	Program which creates a connection to the Internet or another computer network over the telephone in order to connect to **premium-rate numbers**. The provider of a dialer searches for security holes on user's computer and makes it dialing up through unauthorized numbers in order to make money.
Dropper	Program designed to **install** some sort of **malware** to a target system. The malware code can be contained within the dropper in such a way as to avoid detection by virus scanners or the dropper **may download the malware** to the target machine once activated.
Rootkits	Techniques that allow malicious programs that are installed to a computer to **stay concealed** and **avoid detection**. They modify the operating system so that the malware is hidden from the user and the security software. Rootkits can prevent a malicious process from being visible in the system's list of processes.
Backdoors	A backdoor is a method of **bypassing** normal **authentication** procedures. Once a system has been infected, one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry.
Hijackers	They **take control** of various parts **of a web browser**, including home page, search pages, and search bar. They may also redirect user to certain sites or prevent him from opening particular websites, such as sites that combat malware. Some will even redirect user to their own search engine when he attempts a search.

(C) MISHANDLING OF THE USER

- The user very often is possible to **delete** or **uninstall accidentally** some programs of the computer.
- The **poor maintenance** is usually another dangerous factor that causes problems:
  - Great exposure to heat, humidity or dust.
  - Unfortunate acts (e.g. dropping water or other liquids to the keyboard)
  - Offensive operations (nervous actions or awkward movements when computer is on)
- Computer is a machine and like all other machines it also requires proper maintenance. Without maintenance, PC may fail. Dust, dirt can lead to serious problem to PC like low speed, freeze, random error message, and rebooting automatically.

- People may don't understand this and hire technicians. But the basic problem is poor maintenance. To avoid these and many like problems, people must have to give attention to the PC.
- Check the computer regularly to ensure it works well. For proper maintenance of computer, the user must know about the processor used, installed RAM, the hard drive capacity, the version of the operating system because these are the terms which help to troubleshoot the problem.

(D) INTRUSION OF UNWANTED USERS

- When computers are connected to the Internet, their data become vulnerable to **attacks of unwanted and unauthorized programmers** best known as **Hackers** (or **Crackers** if they are malicious).
- Hackers having access to a computer, can easily change, deteriorate, delete or even copy its data. These actions considered as **cybercrimes** and the users are prosecuted.

BACK-UP FILES

Copying user's data in an alternative storage device (e.g. cd-rom, dvd, external disk) protects user from any possible loss.

A user should frequently use the **appropriate system utility** in order to create back-up files and store the **latest version** of system files. This can be done as follows:

Win XP *Start → Programs → Accessories → System tools → Back-Up Files*
Win 7 *Start → All Programs → Maintenance → Back-Up & Restore*

PROTECTION MEASURES AGAINST VIRUSES

1. **Be careful of the applications you execute** especially when they are not authentic (that means they don't come straight from their manufacturer or they are not bought from a commercial store).
2. **Install Antivirus** and **Internet Security** applications that can fully protect you against the most common and offensive malware (e.g. Norton, Panda, McAfee, Kaspersky, Zone Alarm, AVG etc).
3. Renew your programs' shield **updating frequently** the antivirus programs through the internet, so the computer to be updated against all the new viruses.
4. **Activate computer's Firewall** every time you connect to the Internet, so that you deter all the unwanted users to invade at your computer. This can be done as follows:

Win XP *Start → Settings → Control Panel → Windows Firewall*
Win 7 *Start → Control Panel → System & Security → Windows Firewall*