 

“AZƏRBAYCAN HAVA YOLLARI” CJSC NATIONAL AVIATION ACADEMY”

**Topic:** Operating System Security (OS Security)

**Subject:** Operating system

**Teacher:** Sahmaliyev Memmed

**Student:** Aliyeva Qumru

**Group:** 2450-I

**Date:** 19.11.22

**Signature:**

**Baku 2022**

***Operating System Security (OS Security)*** ***Antiviruses.***

What Does Operating System Security (OS Security) Mean?

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.

OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

Techopedia Explains Operating System Security (OS Security)

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.

OS security may be approached in many ways, including adherence to the following:

Performing regular OS patch updates

Installing updated antivirus engines and software

Scrutinizing all incoming and outgoing network traffic through a firewall

Creating secure accounts with required privileges only (i.e., user management)

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to discuss following topics in this chapter.

Authentication

One Time passwords

Program Threats

System Threats

Computer Security Classifications

Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

Username / Password − User need to enter a registered username and password with Operating system to login into the system.

User card/key − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

User attribute - fingerprint/ eye retina pattern/ signature − User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

Random numbers − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.

Secret key − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.

Network password − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as Program Threats. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

Trojan Horse − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.

Trap Door − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.

Logic Bomb − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.

Virus − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

Worm − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.

Port Scanning − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.

Denial of Service − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them. Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website.

Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely. For this reason it's important that you always use antivirus software, and keep it up to date to protect your data and devices.

How do antivirus products work?

Antivirus products work by detecting, quarantining and/or deleting malicious code, to prevent malware from causing damage to your device. Modern antivirus products update themselves automatically, to provide protection against the latest viruses and other types of malware.

Which antivirus product should I use?

Antivirus software is often included for free within the operating systems that run Windows and Apple computers. If you make sure that this built-in antivirus is switched on, you'll instantly be safer.

New computers often come with a trial version of a separate antivirus product installed (such as McAfee, Norton and Avast). You should note that:

when the trial version expires, you'll have to pay (or register) to continue using it

separate antivirus products won't always work alongside the built-in antivirus software and could even stop it from working completely

with so many products available you may want to carry out your own research to find out which is right for you

How do I use my antivirus product?

When you first install (or switch on) your antivirus product, run a full scan to make sure your computer is free of all known malware.

Make sure your antivirus software is set to automatically scan all new files, such as those downloaded from the internet or stored on a USB stick, external hard drive, SD card, or other type of removable media.

Make sure your antivirus software is set to receive updates automatically.

We've also created more detailed advice on protecting your PCs and laptops from viruses and other kinds of malicious software.

Do I need antivirus products on my smartphone and tablet?

No, provided that you only install apps and software from official stores such as Google Play and the Apple App Store. You should also set your apps (and the tablet/smartphone itself) to update automatically. For more information, read our blog covering antivirus for mobile phones.