****

**“AZƏRBAYCAN HAVA YOLLARI” CJSC**

**NATIONAL AVIATION ACADEMY**

**Topic**: Operating system security. Antiviruses.

**Subject**: Operating Systems

**Teacher**: Mammad Sahmaliyev

**Group**: 2450i

**Student**: Alakbarova Rahimakhanim

**Date**: 14.11.22

**Signature**: Alakbarova Rahimakhanim

**Baku 2022**

Operating system (OS) security is a means to protect one’s OS from all kinds of threats. The OS, of course, is the user interface (UI) that allows a user to interact with his or her computer. He or she types in commands for the system to execute.

Operating system security includes all of the preventive and control measures one puts on his or her computer to safeguard it and other connected devices (e.g., printer, etc.) that contain confidential information that hackers would likely steal, modify, or delete if the system is compromised.

Think of operating system security as all of the procedures (e.g., going through a security check at a building entrance, etc.) and measures (e.g., locking out all unauthorized personnel from internal staff-only rooms, etc.) that building managers and staff employ to keep thieves and other unwanted people out of office premises.



**What Cyber Threats Can Operating System Security Protect Against?**

Operating system security can safeguard computers from threats like:

**Trojans:** These gather user login credentials and send them to malicious users or hackers so they can take control of the infected computer.

**Trap doors:** These do not interrupt how a program is designed to work but get in through gaping security holes in its code so their controllers can control it without alerting the legitimate user.

**Logic bombs:** These cause a program to misbehave only when specific conditions specified by the hackers are met, making them much harder to detect than other threats.

**Worms:** These generate multiple copies on a system and can infect connected devices. Each copy uses system resources, thus preventing all other processes from getting the resources necessary to run. As a result, they can shut down the infected computer or even the entire network it is connected to.

**Port scanning:** This is a means employed by hackers to detect system vulnerabilities to attack the system.

**Denial-of-service (DoS) attacks:** These usually prevent users from using their computers by using up all their resources, thus slowing or even shutting them down.

**How Can You Ensure Operating System Security?**

Various ways to employ operating system security exist, including beefing up authentication measures and using one-time passwords, which we discussed in more detail below.

**Beefing Up Authentication**

Authentication simply matches an identified computer user with the programs installed on a particular system. In this case, the OS is programmed to ensure that the current user is running a program that he or she is authorized to. OSs typically authenticates users via:

**Username-password combinations:** Users need to enter an OS-registered username and matching password to log in to a computer.

**User cards or keys:** Users need to punch a card into a slot or enter a key generated by a key generator (e.g., a dongle, etc.) that works with the OS to log in to a system.

**User attributes:** These can include a fingerprint, an eye retina pattern, or other biometric signature that a user needs for an input device connected to the OS to log in to a computer.

**Using One-Time Passwords**

One-time passwords give additional security when used alongside standard authentication. One-time password systems require users to input a unique password each time they log in to a system. Once a one-time password is used, it cannot be used again. One-time passwords can come in various forms such as:

**Random numbers:** Users can, for instance, get cards that have numbers printed on them. Each number has a matching letter. When they log in to a computer, it will ask them for the numbers corresponding to randomly chosen letters.

**Secret keys:** Users are given a piece of hardware that creates secret IDs mapped to their user credentials. The system will ask them for the secret ID that the device generates.

**Network passwords:** Some applications send one-time passwords to users via their registered mobile phone numbers or email addresses. They need to enter this password before they can log in to a computer.

**Antiviruses**

Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems.

Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety of threats, including other types of malicious software, such as keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets and ransomware.

**How antivirus software works**

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.

**Antivirus software usually performs these basic functions:**

Scanning directories or specific files for known malicious patterns indicating the presence of malicious software;

Allowing users to schedule scans so they run automatically;

Allowing users to initiate new scans at any time; and

Removing any malicious software it detects. Some antivirus software programs do this automatically in the background, while others notify users of infections and ask them if they want to clean the files.

In order to scan systems comprehensively, antivirus software must generally be given privileged access to the entire system. This makes antivirus software itself a common target for attackers, and researchers have discovered remote code execution and other serious vulnerabilities in antivirus software products in recent years.

**Types of antivirus programs**

Antivirus software is distributed in a number of forms, including stand-alone antivirus scanners and internet security suites that offer antivirus protection, along with firewalls, privacy controls and other security protections.

Some antivirus software vendors offer basic versions of their products at no charge. These free versions generally offer basic antivirus and spyware protection, but more advanced features and protections are usually available only to paying customers.

While some operating systems are targeted more frequently by virus developers, antivirus software is available for most OSes:

**Windows antivirus software.**

Most antivirus software vendors offer several levels of Windows products at different price points, starting with free versions offering only basic protection. Users must start scans and updates manually and typically free versions of antivirus software won't protect against links to malicious websites or malicious attachments in emails. Premium versions of antivirus software often include suites of endpoint security tools that may provide secure online storage, ad blockers and file encryption. Since 2004, Microsoft has been offering some kind of free antivirus software as part of the Windows operating system itself, generally under the name Windows Defender, though the software was mostly limited to detecting spyware prior to 2006.

**macOS antivirus software.**

Although macOS viruses exist, they're less common than Windows viruses, so antivirus products for macOS are less standardized than those for Windows. There are a number of free and paid products  available, providing  on-demand tools to protect against potential malware threats through full-system malware scans and the ability to sift through specific email threads, attachments and various web activities.

**Android antivirus software.**

Android is the world's most popular mobile operating system and is installed on more mobile devices than any other OS. Because most mobile malware targets Android, experts recommend all Android device users install antivirus software on their devices. Vendors offer a variety of basic free and paid premium versions of their Android antivirus software including anti-theft and remote-locating features. Some run automatic scans and actively try to stop malicious web pages and files from being opened or downloaded.

**Virus detection techniques**

Antivirus software uses a variety of virus detection techniques.

Originally, antivirus software depended on signature-based detection to flag malicious software. Antivirus programs depend on stored virus signatures -- unique strings of data that are characteristic of known malware. The antivirus software uses these signatures to identify when it encounters viruses that have already been identified and analyzed by security experts.

Signature-based malware cannot detect new malware, including variants of existing malware. Signature-based detection can only detect new viruses when the definition file is updated with information about the new virus. With the number of new malware signatures increasing at around 10 million per year as long ago as 2011, modern signature databases may contain hundreds of millions, or even billions, of entries, making antivirus software based solely on signatures impractical. However, signature-based detection does not usually produce false positive matches.

Heuristic-based detection uses an algorithm to compare the signatures of known viruses against potential threats. With heuristic-based detection, antivirus software can detect viruses that haven't been discovered yet, as well as already existing viruses that have been disguised or modified and released as new viruses. However, this method can also generate false-positive matches when antivirus software detects a program behaving similarly to a malicious program and incorrectly identifies it as a virus.

Antivirus software may also use behavior-based detection to analyze an object's behavior or potential behavior for suspicious activities and infers malicious intent based on those observations. For example, code that attempts to perform unauthorized or abnormal actions would indicate the object is malicious, or at least suspicious. Some examples of behaviors that potentially signal danger include modifying or deleting large numbers of files, monitoring keystrokes, changing settings of other programs and remotely connecting to computers.