CS 222 Project:

Cyber-Attacks in modern OS

Course Title:	Operating System
Course Code:	CS 222
Instructor:	Dr.Alaa Aldin
Semester:	1st.2023
Due Date:	10-28-2023

Abdulrahman Abanmi	439012760
Abdullah Aljasser	442016153
Abdulrahman Alafif	443015728
Omar Alhozimi	443014015

Abstract:

In today's interconnected digital realm, operating systems (OS) bridge the intricate world of hardware to the evolving landscape of application software. Consequently, they are central to digital operations. This paper delves into OS vulnerabilities, threats they face, and subsequent cyberattacks that exploit these vulnerabilities. The paper concludes with recommended strategies for enhancing OS security, emphasizing the need for robust cybersecurity practices to preserve the broader digital infrastructure.

Table of Contents

Table of Figure

Introduction:

Cyber-attacks on modern operating systems represent a critical and pervasive challenge in the realm of cybersecurity. Operating systems (OS) serve as the foundational software that manages computer hardware and facilitates communication between applications and the underlying hardware components. Due to their integral role, operating systems have become prime targets for cybercriminals seeking unauthorized access, data compromise, or system disruption.

As technology advances, modern operating systems have evolved to incorporate sophisticated features, extensive functionalities, and intricate network connections. While these advancements enhance user experience and system capabilities, they also introduce vulnerabilities that cyber attackers exploit for malicious purposes.

Operating Systems Vulnerabilities:

An operating system vulnerability is a loophole or flaw in your operating system that makes it easier for cybercriminals to break in. An operating system is the main software that runs your computer or device – common examples include Windows, MacOS, Android, and Linux.

It's likely you've heard the weird rumor that Macs are impervious to operating system vulnerabilities. Don't believe the stories: all operating systems are vulnerable to cyber-attack. This is because all operating systems are:

- **extremely popular:** which makes the attack more powerful and resourceful to the attackers.
- **extremely complex:** when you have such complex operating system you must encounter a big number of bugs that are not easily detectable.

Operating system vulnerabilities are usually caused by unpatched software, malware, and phishing attacks. Because operating system patching is so important, Microsoft has set up a clever way to address each new Windows operating system vulnerability with their weekly "Patch Tuesday" updates.

Types of an Operating Systems Vulnerabilities

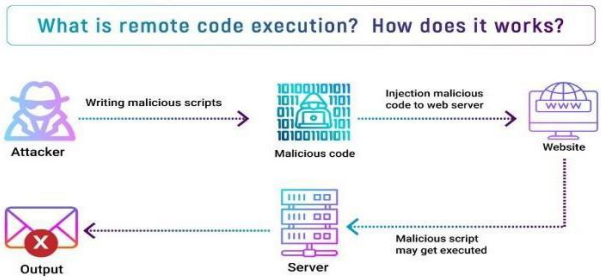
Here we're going to mention some of the most popular types of an attack, starting with,

- **Buffer Overflow**: Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems. It is one of the best-known software security vulnerabilities yet remains fairly common. This is partly because buffer overflows can occur in various ways and the techniques used to prevent them are often error prone.

  Also known as a buffer overrun, buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

- **Remote Code Execution (RCE)**: RCE attackers scan the internet for vulnerable applications. Once they spot a remote code vulnerability, they attack it over a network. Attackers often create a remote command shell that lets them control some aspect of the target system remotely.

  Remote code security vulnerabilities provide attackers with the ability to execute malicious code, or malware, and take over an affected system. After gaining access to the system, attackers will often attempt to elevate their privileges from user to admin.



- **Memory corruption**: Memory corruption can be described as the vulnerability that may occur in a computer system when its memory is altered without an explicit assignment. The contents of a memory location are modified due to programming errors which enable attackers to execute an arbitrary code.

- **Denial of Service**: A DoS attack floods a system and a network with traffic. It exhausts the system resources and bandwidth so it's unable to process real users' requests. When multiple systems are used for the attack, we talk about Distributed Denial of Service. DoS attacks are sometimes a diversion for other attacks. While you focus on the DoS attack, another attack can penetrate your system.

- **Privilege escalation**: is the act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Finally, we can say that operating systems vulnerabilities are an open door for attackers. It can lead to other attacks, computers compromised and information disclosure. It is important to patch your environment to limit the risk.

Types of attacks on a system

Unfortunately, there is an increasing number of types of attacks made by the attackers to benefit from anyone they target, from users to big companies, and governments.

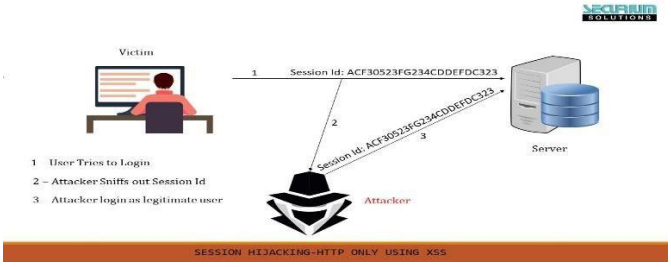
We collected the most interesting and dangerous types to make the reader more aware of them:

- **Man-in-the-middle (MITM) attack**

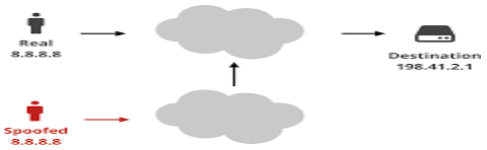
  A Man-in-the-Middle (MITM) attack occurs when an outsider intercepts and distributes communications that appear to be engaging between two parties. Assailants can filter, alter, and steal important information while in the conversation, Here is some

  examples using the type of attack:

  i. **Session hijacking**: Session hijacking is a type of MITM attack in which the attacker waits for a victim to log in to an application, such as for banking or email, and then steals the session cookie. The attacker then uses the cookie to log in to the same account owned by the victim but instead from the attacker's browser.



ii. **IP Spoofing**: IP spoofing is used by an attacker to convince a system that it's communicating with a known, trusted entity and provide the attacker with access to the system. The attacker sends a packet with the IP source address of a known, trusted host rather than its own IP source address to a target host. The target host might accept the packet and act upon it.

iii. 

Unfortunately, currently there's no single technology or configuration to stop all Man-in the-Middle attacks. Generally, encryption and digital certificates provide an efficient safeguard against MitM attacks, assuring both the confidentiality and integrity of communications. But a man-in-the-middle attack are often injected into the center of communications in such how that encryption won't help.

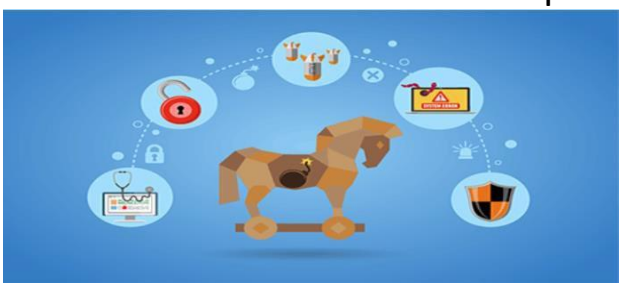
- **Malware Attack**

  Malicious software is often described as unwanted software that's installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the web. Here are some of the most common sorts of malware:

  Macro Viruses: These viruses infect applications like Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code within the computer system.

i. **Stealth Viruses**: Stealth viruses take over system functions to conceal or hide themselves. they are doing this by compromising malware detection software in order that the software will report an infected area as being uninfected. These viruses conceal any increase within the size of an infected file or changes to the file's date and time of last modification.

ii. **Trojans**: A Trojan or a trojan horse may be a program that hides during a useful program and typically has a malicious function. a major difference between viruses and Trojans is that Trojans don't self-replicate. additionally, to launching attacks on a system, a Trojan can establish a back door which will be exploited by attackers. for instance, a Trojan are often programmed to open a high-numbered port therefore the hacker can use it to listen then perform an attack.



iii. **Logic Bombs**: A logic bomb is a set of instructions in a program carrying a malicious payload that can attack an operating system, program, or network. It only goes off after certain conditions are met. A simple example of these conditions is a specific date or time. A more complex example is when an organization fires an employee and logs their dismissal in their system.

iv. **Worms**: A worm malware refers to a malicious program that replicates itself, automatically spreading through a network. The worm malware exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.

v. **Ransomware**: Ransomware may be a sort of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system during a way that's not difficult for a knowledgeable person to reverse, more advanced malware uses a way called cryptoviral extortion, which encrypts the victim's files during a way that creates them nearly impossible to recover without the decryption key.

- ## Phishing attack

Phishing attack is that the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could even be a link to an illegitimate website which will trick you into downloading malware or handing over your personal information.

Spear phishing may be a very targeted sort of phishing activity. Attackers take the time to conduct research into targets and make messages that are personal and relevant. due to this, spear phishing are often very hard to spot and even harder to defend against. one among the only ways in which a hacker can conduct a spear phishing attack is email spoofing, which is when the information within the "From" section of the e-mail is falsified, making it appear as if it's coming from someone you recognize , like your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning, they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

- **Zero-day Exploits**

  There is a window after a network vulnerability is disclosed before a patch or other fix is applied. Attackers using the internet will use the vulnerability during that period. To defend against this kind of cyber-attack, continuous monitoring is required. Before online criminals do, infrastructure penetration testing can find flaws in your network.

Ways to Prevent Cyber Attacks

1. **Train your staff**

   One of the most common ways cyber criminals get access to your data is through your employees. They'll send fraudulent emails impersonating someone in your organization and will either ask for personal details or for access to certain files. Links often seem legitimate to an untrained eye and it's easy to fall into the trap. This is why employee awareness is vital.

2. **Keep your software and systems fully up to date**

   Often cyber attacks happen because your systems or software aren't fully up to date, leaving weaknesses. So cybercriminals exploit these weaknesses to gain access to your network. Once they are in – it's often too late to take preventative action.

3. **Install a Firewall**

   There are so many-different types of sophisticated data breaches and new ones surface every day and even make comebacks.

   Putting your network behind a firewall is one of the most effective ways to defend yourself from any cyber attack. A firewall system will block any brute force attacks made on your network and/or systems before it can do any damage, something we can help you with.

4. **Backup your data**

In the event of a disaster (often a cyber attack) you must have your data backed up to avoid serious downtime, loss of data and serious financial loss.

5. **Control access to your systems**

one of the attacks that you can receive on your systems can be physical, having control over who can access your network is really important. Somebody can simply walk into your office or enterprise and plug in a USB key containing infected files into one of your computers allowing them access to your entire network or infect it.

6. **WIFI Security**

any device can get infected by connecting to a network, if this infected device then connects to your business network your entire system is at serious risk.

7. Passwords

Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have access to everything in your system and any application you use.

-The impact of cyber-attacks on modern OS:

Operating system cyberattacks can have a serious effect on people and businesses,resulting in financial losses, reputational harm, and data breaches.

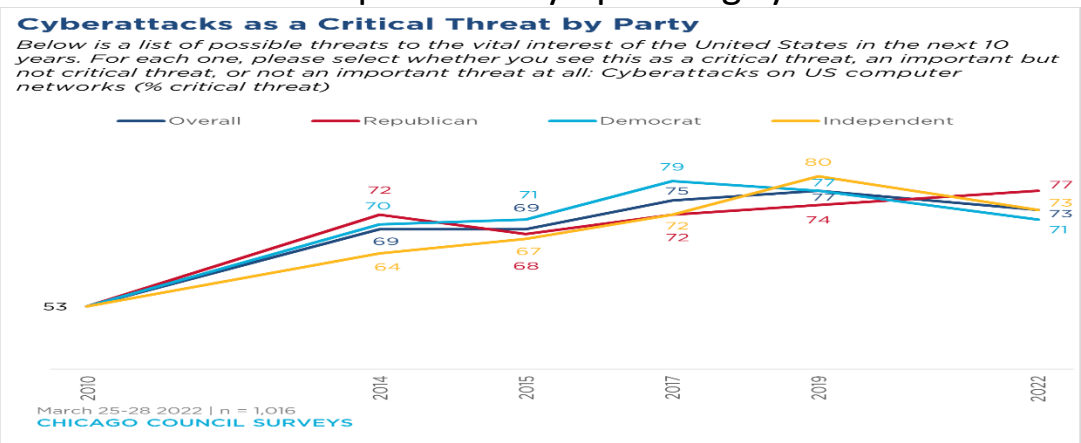
Data breaches: are among the most frequent effects of cyberattacks on operating systems. Attackers can obtain sensitive data, including trade secrets, financial information, and personal information, when an operating system is compromised.

Subsequently, this information may be exploited for nefarious activities including fraud, identity theft, and extortion.

Financial losses: Cyberattacks have the potential to cause large financial losses as well. Ransomware attacks, for instance, have the ability to encrypt the data of an organization and demand payment in ransom for the decryption key. Additionally, organizations may have to pay for incident response teams and other expenses while responding to cyberattacks.

- **Key infrastructure:** can be severely impacted by cyberattacks. Critical infrastructure systems, including electricity grids, water treatment plants, and transportation networks, are managed and **controlled by operating systems**. Blackouts, water shortages, and interruptions to transportation could result from a successful cyberattack on a key infrastructure system. It is possible to disseminate propaganda and false information using cyberattacks. Devices that are used to access the internet and social media, such as computers, smartphones, and tablets, are powered by operating systems. Cyberattacks have the ability to take advantage of holes in operating systems to disseminate propaganda and false information widely.

It is possible to influence elections and other democratic processes through cyberattacks. Voting machines and electronic devices are powered by operating systems.



-Implementing security Defenses:

1-**Security Polices:**

A security policy ought to be thoroughly considered, decided upon, and included in an ongoing document that all parties sign and updates as necessary.

The frequency of port scans, password requirements, virus detectors and other items are examples of contents.

2- **Instruction Detection:**

Attack detection attempts to detect attacks whether they succeed or fail.

The different techniques differ in several aspects:

The time at which detection occurs**:**

during the attack or after the fact. types of information reviewed to detect attacks**.** Some attacks can only be detected by analyzing multiple sources of information.

Response to an attack, which may include notifying the administrator or automatically stopping the attack **(**e.g.G. kill the attacking process) until the attack can be traced to identify the attacker.

Another approach is to direct the **attacker to the honeypot on the honeynet:**

attacker to the honeypot on the honeynet. The idea behind a honeypot is a computer that runs normal services but that no one uses for real work. Such a system should not normally log network traffic**,** so any traffic entering or leaving such a system is by definition suspicious.

Honeypots are typically stored on a honeynet protected by a reverse firewall that allows potential attackers to access the honeypot but does not allow outbound traffic. **(**So if a honeypot is compromised, an attacker cannot use it as a base of operations to attack other systems**.)** Honeypots are

carefully monitored and any suspicious activity is carefully logged and investigated.

3-**Virus Protection(Optional)**:

Modern antivirus programs are essentially signature-based detection systems that (in some cases) also have the ability to disinfect and restore vulnerable files to their original state.

Viruses and antivirus programs are increasing rapidly.

For example, viruses today typically mutate as they spread, so antivirus programs look for families of related signatures rather than specific signatures. Some antivirus programs check for anomalies, e.g. B. opening an executable program for writing (not by the compiler). Avoiding illegal, free, and shared software can help reduce the risk of contracting a virus, but even official software has sometimes been infected by disgruntled employees.

Some virus scanners run suspicious programs in a sandbox, an isolated, secure area of the system that mimics the real system. Rich Text Format, RTF, files cannot contain macros and therefore cannot contain Word macro viruses.

Conclusion:

As digitization propels us forward, the responsibilities and vulnerabilities of operating systems intensify. While threats are pervasive, we can combat these challenges with proactive measures, continuous learning, and innovation. It's vital to understand, adapt, and fortify our systems, contributing to a secure digital future.

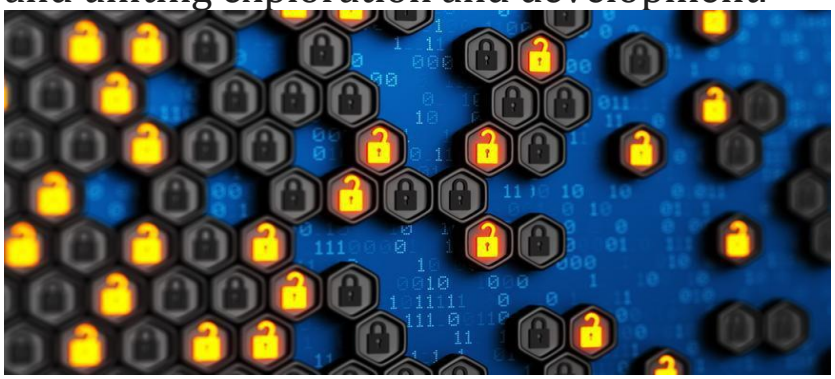
Data breaches, fiscal losses, reputational damage, and dislocation of operations are just some of the implicit impacts of cyber-attacks on operating systems. In addition,cyber-attacks can be used to achieve other vicious pretensions, such as spreading intimation and propaganda, manipulating choices, and dismembering critical structures. cyber-attacks on ultramodern operating systems are serious trouble, but there are several effects that individualities and associations can do to alleviate the threat. By taking these ways, we can help to protect ourselves from the negative consequences of cyber-attacks.

In addition to the conclusion, there are some fresh studies on cyber-attacks on ultramodern operating systems and what we can do to cover ourselves Cyber-attacks are a global problem.
Cyber-attacks can be carried out from anywhere in the world, and they can target associations of all sizes, anyhow of assiduity or position. This means that it's important for individuals and associations to take a way to cover themselves, regardless of where they're located. Cyber-attacks are getting more sophisticated and complex. bushwhackers are constantly developing new ways to exploit vulnerabilities in operating systems and other software. This means that it's **important to stay over-to-date on the rearmost security pitfalls** and to find ways to alleviate them. Cyber-attacks are a growing trouble for critical structures. Operating systems are used to control and manage critical structure systems, similar to power

grids, water treatment installations, and transportation networks. **A successful cyber-attack on a critical structure system** could have ruinous consequences for society as a whole. In light of these challenges, it's more important than ever for individuals and associations to find a way to protect themselves from cyber-attacks on operating systems.

Then are some fresh effects we can do Support exploration into new security technologies. Experimenters are constantly developing new ways to protect operating systems and other software from cyber-attacks. **By supporting this exploration**, we can help to develop new and effective security measures. Educate the public about cyber-attacks.

One of the stylish ways to protect ourselves from cyber-attacks is to **be apprehensive of the pitfalls and to know how to avoid them**. We can educate the public about cyber-attacks through public mindfulness juggernauts, academy programs, and other enterprise. Work together to address the trouble of cyber-attacks. Governments, assiduity, and academia need to work together to address the trouble of cyber-attacks on operating systems. This includes participating in information about security pitfalls, developing new security norms, and uniting exploration and development.



References:

- Info-Savvy. "What are Different Types of Attacks on a System?"
- Leaf IT. "10 Ways to Prevent Cyber Attacks."
- IP Specialist. "Types of Attacks on an Operating System."