**Seminar 3**

The operating system is the brains of the machine, acting as a gateway between the human and the computer's hardware and software. Using loopholes in the OS's code, hackers can access sensitive information, destroy files, or even crash the device. Protecting a computer's operating system is essential as it serves as the machine's brain.

**Operating system Security**

When we talk about protecting the privacy, reliability, and availability (CIA) of an OS, we're referring to what we call "operating system security."

Operating system security works to keep the OS safe from things like worms, trojans, and other infections, as well as configuration errors and outside intrusions (Wepman, n.d.).

**OS Security Threats**

We'll look at some of the most typical ways in which an OS can be compromised.

1. **Malware**

Viruses, worms, trojans, and rootkits are only some of the forms of malware that exist. Malicious software, or malware, is code designed to steal information, damage a device, or corrupt data without the owner's knowledge or permission. Malware, short for malicious software, is software designed to do harm by tricking a computer into carrying out an attacker's instructions.

1. **Buffer Overflow**

A buffer's primary purpose is to hold information while it is being transferred or processed. The amount of data that can be stored in each buffer varies. The buffer or equivalent temporary storage space is stuffed to its capacity during a buffer overflow attack. It's possible that the application trying to write the data will accidentally overwrite other regions in memory if the buffer overflows.

1. **Denial of Service**

DoS attacks are launched when a system is flooded with bogus requests until it can no longer handle its legitimate users' requests. In contrast to exhausting a system's resources, some types of DoS assaults can actually harm the system's fundamental infrastructure. (Hysolate, n.d.).

1. **Poor Performance**

It's common knowledge that operating systems that are several versions old have poor performance. Without proper support, the performance drops even further. Doubling the difficulty of the problem, in54qwin it raises the question, and opening the door to massive financial losses, is typical of the results of this type of issue. That equipment loses its dependability as time passes. (Wattlecorp, 2020).

1. **Software Vulnerabilities**

In general, operating systems have hundreds of thousands of lines of code. Hundreds of security flaws are injected into the code during developing each operating system since people must write the code and then test and debug it. Patches are often released by Microsoft and Apple to address security flaws and improve the reliability of their respective operating systems.

1. **Physical Security**

The best way to protect an OS is with solid physical protections. Operating system code and configuration files are typically stored on a system's hard disc, making them vulnerable to tampering, deletion, or theft by anybody with physical access to the machine. Therefore most business servers are kept in secure locations under constant watch by personnel carrying weapons. (Wepman, n.d.).

**Techniques and Methods to overcome OS Risks:**

Antivirus and other endpoints security mechanisms, operating system patch updates, firewall protection, and the enforcement of secure access via least privileges and user controls are the most often employed methods for protecting operating systems (roy, 2018).

**Ensuring OS Security:**

1. **Authentication Measures**

When a user logs in, their credentials are checked against a database or set of programmes to see which ones they have access to. Every OS has its own set of permissions and security measures to make sure only authorized users can launch specific applications.

For operating system-level authentication, you can employ the following methods:

1. Security keys
2. Password-username combinations
3. Digital fingerprinting and other biometric signature technologies
4. Authentication with multiple factors
5. **Using one time password**

When added to other authentication methods, one-time passwords further tighten security. Each time a user logs in, a new password is generated for them. To prevent unauthorized access, a one-time password should be unique.

1. **Virtualization**

When you use virtualization, you may effectively separate software from hardware. The primary benefit of virtualization is the increased efficiency, adaptability, and security it brings. Virtualizations come in various forms, from the desktop to the application to the network to the server to the storage to the operating system. (Hysolate, n.d.).

**Refactoring:**

Through a process known as refactoring, functionality is preserved as code is reorganized. Refactoring is a technique used to enhance the internal workings of a program by making numerous incremental changes to it without affecting its outward appearance or behavior.

Software engineers and developers refactor code to enhance the program's architecture, functionality, and performance. By simplifying and organizing code, refactoring makes programmes easier to understand. In addition to revealing previously unseen flaws, refactoring can help engineers secure their code (S. Gillis, n.d.).

**Implementing Code refactoring techniques:**

Gathering the bare minimum of requirements is the first step in the feature implementation process. A project's codebase grows and evolves over time as its creator gains experience and insight. Afterward, you make adjustments to the code to address the issue and any special circumstances. However, after a few weeks, it will become tough for you to comprehend your own code. Therefore, this is where refactoring comes into play with computer code. Code refactoring refers to the process of improving or upgrading the code without altering the software's functionality or the exterior behaviour of the programme.

It's safe to say that when it comes to refactoring code using an Agile methodology, Red-Green has won hands down as the preferred strategy. This method is grounded in the "test-first" philosophy of design and development, which is the cornerstone of every refactoring process. Developers lead the refactoring of the test-driven development cycle, which is broken down into three distinct phases.

RED: Creating the failed "red-test" is the first step. Then, you pause to assess what features still need refinement.

Green: In the second stage, you create "green" builds by writing code that is just simple enough to work.

Refactor: In the third and final stage, you polish your code to keep your tests passing.

Accordingly, there are essentially two stages to this method: First, you'll need to write some code to implement a new feature in your system, and then you'll need to rework that code. Remember that you shouldn't perform both tasks simultaneously while in the pipeline (GeeksforGeeks, 2020).

In the year 2020, working in a virtual or geographically distributed team was the standard. In 2020, many of us were compelled to take part in the largest work-from-home experiment ever conducted, and the way we work was irrevocably altered as a result.

**What are Virtual Teams?**

A remote team is a group of people who normally work together in person but who now do it virtually, using online collaboration and communication technologies. Global virtual teams consist of remote professionals from all around the world.

Managing remote teams presents its own set of difficulties. As a virtual team leader, you can keep your team happy, efficient, and productive by following these seven steps. (Ciapponi, 2019).

**Skills required to be effective member of development team:**

1. **Maintain effective communication**

Schedule periodic updates, such as a weekly online chat. The members of the remote team will be able to communicate more effectively as a result.

1. **Ensure that you are utilizing appropriate resources**

Every remote group needs a reliable means of immediate communication, and Slack is the ideal platform for this. Think about spending money on a programmed that will help you organize your projects. Your team's conversations, files, and collaboration can all be found in one convenient location.

1. **Gain credibility**

To succeed as a virtual team leader, you must earn the respect and confidence of your team members. You accomplish this by speaking openly, honestly, and with genuineness.

1. **Plan Ahead**

Contribute to the team's goals while also encouraging individual growth and development. By doing so, they will feel more invested in their work.

1. **Maintain a steady feedback loop**

A great way to keep your remote workers motivated is to provide frequent feedback on their performance.

1. **Do your best to encourage your remote workers.**

Remote work can be isolating, so it's important to make your virtual staff feel appreciated (Waters, 2021).

**References:**

Ciapponi, G. (2019). *Three strategies to build successful virtual teams*. [online] Ideas. Available at: <https://www.wework.com/ideas/professional-development/management-leadership/three-strategies-to-build-successful-virtual-teams>.

GeeksforGeeks. (2020). *7 Code Refactoring Techniques in Software Engineering*. [online] Available at: <https://www.geeksforgeeks.org/7-code-refactoring-techniques-in-software-engineering/>.

Hysolate (n.d.). *Understanding OS Security: Threats and Security Controls*. [online] Hysolate. Available at: <https://www.hysolate.com/learn/sandboxing/understanding-os-security-threats-and-security-controls/>.

roy (2018). *Discuss operating system design issues*. [online] www.ques10.com. Available at: <https://www.ques10.com/p/25212/discuss-operating-system-design-issues-1/>?.

S. Gillis, A. (n.d.). *What is Refactoring (Code Refactoring)?* [online] SearchAppArchitecture. Available at: <https://www.techtarget.com/searchapparchitecture/definition/refactoring>.

Waters, S. (2021). *The success behind virtual teams: the ultimate guide | BetterUp*. [online] www.betterup.com. Available at: https://www.betterup.com/blog/virtual-teams.

Wattlecorp, T. (2020). *Security Issues with Unsupported Operating System (OS)*. [online] Wattlecorp. Available at: https://www.wattlecorp.com/risks-of-unsupported-os/ [Accessed 30 Aug. 2022].

Wepman, J. (n.d.). *What Is Password Hacking?* [online] It Still Works. Available at: <https://itstillworks.com/password-hacking-7273695.html>.