AMMAR

BSCS_F19_M63

15-01-2023

ERROR PREVENTION TECHNIQUES

Two-Factor (2-Step) Authentication	Two-Factor Authentication (2FA) is a security measure that requires users to provide two forms of identification to access an application or system. The first form of identification is typically a **password**, while the second is a **code** sent to the user's mobile device or email. This technique is commonly used in the software engineering and networking domains to prevent unauthorized access to sensitive data. For example, a bank might use 2FA to protect online banking accounts, requiring customers to enter a password and a code sent to their mobile phone before they can access their account.
Code Reviews	One of the most effective ways to prevent errors in software development is through code reviews. This is a process where one or more team members review and provide feedback on the code written by others. This allows for **multiple perspectives** to be applied to the code, which can help to identify and fix errors before they are deployed. For example, a software development team might hire a code reviewing expert to ensure that the code is free of (logical) errors and meets certain standards before it is released to the public.
Network Segmentation	Network segmentation is a technique used to **divide** a network into smaller, more secure segments. This technique is commonly used in the networking domain to prevent unauthorized access to sensitive data. For example, a company might use network segmentation to separate its internal network from the Internet, preventing hackers from accessing sensitive data.
Backup and Recovery	Backup and recovery is a technique used to create and maintain **copies** of data in case of a disaster or data loss. This technique is commonly used in the software engineering and networking domains to prevent data loss caused by hardware failures or other disasters. For example, a company might use backup and recovery to create and maintain copies of its data in case of a power outage or other disaster.
Firewall	Firewalls are a security measure used to protect computer networks from unauthorized access. Firewalls act as a **barrier** between a private internal network and the Internet, filtering incoming and outgoing traffic based on predefined rules. They are commonly used in the networking domain to prevent hackers from accessing sensitive data. For example, a company might use a firewall to prevent unauthorized access to its internal network from the Internet.
Penetration Testing	Penetration testing is a technique used to identify **vulnerabilities** in a system or network. This technique is commonly used in the security domain to prevent attacks on systems and networks. For example, a company might hire Professional or Ethical hackers to try to hack the systems, and exploit any possible vulnerability, to identify vulnerabilities in its website or network and then take steps to fix them.
Compliance Testing	Compliance testing is a technique used to ensure that a system or application meets certain **regulatory requirements**. This technique is commonly used in the security domain to prevent violations of **laws** and regulations. For example, a company might use compliance testing to ensure that its systems comply with data protection regulations such as GDPR.
	Virtualization is a technique used to create **virtual versions** of computer systems and networks. This technique is commonly used in the software engineering and networking domains to improve the security

Virtualization	and reliability of systems while also maintaining a great user experience. For example, a company might use virtualization to create a virtual version of its internal network. Which will eventually allow its users to access the network from any location while also ensuring that the network is reliable, and secure from any kind of intrusion.
Fuzzing	Fuzz Testing, also known as fuzzing, is a technique used to test the security and reliability of software applications and systems by providing them with **unexpected** or **abnormal** inputs. The goal of fuzz testing is to identify vulnerabilities and defects in the software by providing it with inputs that it was not designed to handle. This technique is commonly used in the software engineering domain to identify and prevent defects in the software. The test can be done on different parts of the software such as file formats, network protocols, and APIs. For example, a software developer might use fuzz testing to identify vulnerabilities in a web application by providing it with unexpected inputs, such as large file uploads or unexpected data formats. This technique can help identify and prevent defects in the software that could be exploited by hackers.
Instruction Set Randomization	ISR is a technique used to **randomize** the instructions of a program to make it harder for attackers to reverse engineer or exploit the program, as they would need to identify and understand the randomization in order to understand the program's behavior. This technique is commonly used to protect the firmware of graphics cards, GPUs, and CPUs from attacks. This technique is often overlooked in the field of graphics, GPUs, and CPUs, but it is an important tool for protecting these systems from attackers. For example, a GPU manufacturer might use ISR to protect the firmware of their GPUs from attacks. By randomizing the instruction set of the firmware, the manufacturer makes it more difficult for attackers to identify and exploit vulnerabilities in the firmware. This helps to improve the security and reliability of the GPU, as well as the systems that use the GPU.

By, TheMR