Question & Answers

SECURITY

Sercan Külcü | Operating Systems | 10.04.2023

Contents

Why is security a critical concern in modern computing environments, and what are some common types of security threats?

Security is a critical concern in modern computing environments because computers are increasingly interconnected and accessible through various networks, making them more vulnerable to security threats. Some common types of security threats include viruses, worms, Trojans, ransomware, phishing, and social engineering attacks.

What is an operating system, and how does it play a central role in providing security mechanisms and policies?

An operating system is a software system that manages computer hardware and software resources and provides common services for computer programs. It plays a central role in providing security mechanisms and policies by providing a secure execution environment for applications, controlling access to system resources, enforcing security policies, and providing security features such as firewalls, antivirus software, and encryption.

What is authentication, and how does it help to protect system resources and data?

Authentication is the process of verifying the identity of a user or device to gain access to system resources or data. Authentication helps to

protect system resources and data by ensuring that only authorized users or devices are granted access, and that unauthorized users or devices are prevented from accessing the system.

What is access control, and how does it help to prevent unauthorized access to system resources and data?

Access control is the process of controlling access to system resources and data based on the identity and privileges of the user or device. Access control helps to prevent unauthorized access to system resources and data by enforcing security policies and restricting access to authorized users or devices.

What is encryption, and how does it help to protect data from unauthorized access and modification?

Encryption is the process of converting data into a secret code to prevent unauthorized access and modification. Encryption helps to protect data from unauthorized access and modification by ensuring that only authorized users with the correct decryption key can access and modify the data. It also provides a secure method of transmitting data over insecure networks, such as the Internet.

What is a firewall, and how does it help to protect computer networks from external attacks?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, such as the Internet. Firewalls can be implemented using hardware or software, or a combination of both. They help to prevent unauthorized access to network resources and can block malicious traffic such as viruses, worms, and other types of malware.

What is a virtual private network (VPN), and how does it help to protect network communications from eavesdropping and other forms of interception?

A virtual private network (VPN) is a secure and encrypted network connection that allows remote users to access a private network over the Internet. It helps to protect network communications from eavesdropping and other forms of interception by encrypting the data that is transmitted between the user and the network. VPNs use various protocols such as OpenVPN, IPsec, and SSL/TLS to provide secure and encrypted communication.

What is a rootkit, and how does it enable attackers to gain unauthorized access to a computer system?

A rootkit is a type of malicious software that is designed to hide its presence on a computer system and provide privileged access to an attacker. Rootkits can be installed through various means such as exploiting vulnerabilities in software or through social engineering attacks. Once installed, a rootkit can allow an attacker to access and control the affected system without the user's knowledge. Rootkits can be used to steal sensitive information, launch other types of attacks, and maintain persistence on the system.

What is a buffer overflow attack, and how does it exploit vulnerabilities in software to gain unauthorized access to system resources and data?

A buffer overflow attack is a type of software vulnerability that occurs when a program attempts to store more data in a buffer than it was designed to hold. This can cause the extra data to overflow into adjacent memory locations, which can be exploited by an attacker to execute malicious code or to gain unauthorized access to system resources and data. Buffer overflow attacks can be prevented through proper input validation and bounds checking, as well as other security measures such as data execution prevention (DEP).

What is a denial-of-service (DoS) attack, and how does it disrupt the normal functioning of computer systems and networks?

A denial-of-service (DoS) attack is a type of attack that attempts to disrupt the normal functioning of computer systems and networks by overwhelming them with a flood of traffic or requests. This can cause legitimate users to be unable to access the system or network, leading to a loss of service. DoS attacks can be launched using various techniques such as flooding the target with traffic, exploiting vulnerabilities in the system or network, or using a botnet to coordinate the attack. Defending against DoS attacks typically involves implementing measures such as rate limiting, traffic filtering, and using specialized hardware or services to absorb and mitigate the attack.

What are some emerging trends and technologies in computer security, and how are they likely to impact the design and implementation of operating systems in the future?

Some emerging trends and technologies in computer security include:

- Artificial intelligence (AI) and machine learning (ML) for threat detection and response

- Blockchain for secure data storage and transmission

- Quantum computing for cryptographic applications

- Hardware-based security mechanisms such as Trusted Platform Modules (TPMs) and Secure Enclaves

- Cloud-based security services and solutions

These emerging technologies are likely to impact the design and implementation of operating systems in the future by requiring new security mechanisms and policies to address their unique characteristics and requirements.

How do modern operating systems protect against attacks that exploit hardware vulnerabilities, such as Meltdown and Spectre?

Modern operating systems protect against attacks that exploit hardware vulnerabilities such as Meltdown and Spectre by implementing software-based mitigations such as kernel page-table isolation, Retpoline, and indirect branch prediction barriers. These mitigations prevent malicious software from accessing sensitive kernel memory and prevent speculative execution attacks that exploit speculative execution in modern processors.

What is a sandbox, and how does it help to prevent malicious software from accessing sensitive system resources and data?

A sandbox is a security mechanism that provides a controlled environment for executing untrusted or unknown software. Sandboxing helps to prevent malicious software from accessing sensitive system resources and data by limiting the software's access to only the resources and data that are necessary for its execution. Sandboxing can be

implemented at the application level, where each application is executed within its own sandbox, or at the system level, where all applications are executed within a single sandbox.

What is a security policy, and how does it help to ensure that computer systems and networks are used in accordance with organizational goals and values?

A security policy is a set of rules and procedures that govern the use of computer systems and networks within an organization. A security policy helps to ensure that computer systems and networks are used in accordance with organizational goals and values by defining acceptable use, access control, data protection, and other security-related requirements. Security policies also help to ensure compliance with laws, regulations, and industry standards.

What is a security audit, and how does it help to identify vulnerabilities and risks in computer systems and networks?

A security audit is a systematic evaluation of a computer system or network's security posture. A security audit helps to identify vulnerabilities and risks in computer systems and networks by reviewing security policies, procedures, and controls, testing system configurations and settings, and identifying potential attack vectors. A security audit can be conducted internally by an organization's own security team or externally by a third-party security service provider. The results of a security audit can be used to prioritize security

investments and improvements, and to ensure ongoing compliance with security policies and standards.