2024-03-18
Zandra Hedlund
zandra.hedlund0004@stud.hkr.se

HKR – Introduction to Computer Security

Final Exam, March 2024.

Notice: The total number of points is 30. To pass with grade 3, you need to acquire at least 16 points. To pass with grade 4, you need at least 21 points. To pass with grade 5, you need at least 26 points.

Question 1. Think about a regular PC with internet connection. List different resource types and services that need to be protected on this PC. (2p)

- Protect the operating system against malware and viruses while ensuring regular security updates.
- Utilize firewall protection to regulate incoming and outgoing network traffic, preventing unauthorized access.
- Maintain secure configurations for services like Remote Desktop Protocol (RDP) and File Sharing to limit potential attack surfaces.
- Safeguard web browsers against malicious websites, phishing attempts, and browser-based exploits, updating them regularly.
- Employ protection measures for email, including spam filtering, phishing detection, and encryption for sensitive communications.
- Ensure all installed applications receive regular updates to patch security vulnerabilities and avoid malware infections.
- Encrypt sensitive data and perform regular backups to prevent unauthorized access and protect against data loss.
- Enforce strong passwords and multi-factor authentication for user accounts, along with limited user privileges to minimize security breaches.
- Implement physical security measures to prevent theft or unauthorized access to the computer.
- Install and update antivirus and antimalware software to detect and remove malicious software.
- Keep up-to-date with security updates and patches for the operating system and installed software to address known vulnerabilities.
- Educate users on safe computing practices to avoid clicking on suspicious links or downloading files from unknown sources.

Question 2. What kind of harm does a denial-of-service (DoS) attack cause? Does a DoS attack affect data confidentiality? (2p)

A denial-of-service (DoS) attack disrupts services, causing downtime, financial losses, and reputation damage. While it primarily targets availability, it can indirectly impact data confidentiality if it prevents access to sensitive data. However, its main goal is to overwhelm systems with excessive traffic or requests, rather than directly compromising data confidentiality.

A denial-of-service (DoS) attack aims to disrupt the normal functioning of a computer system, network, or service by overwhelming it with a flood of illegitimate requests or traffic. While a DoS attack primarily targets the availability of a system or service rather than data confidentiality, it can still cause significant harm.

Organizations should implement robust defense mechanisms, such as network traffic monitoring, rate limiting, and DoS mitigation solutions, to mitigate the impact of DoS attacks and ensure the continuity of their operations.

Question 3. What factors affect the strength of a password? (2p)

Several factors influence the strength of a password:

- **Length**: Longer passwords are generally stronger as they provide more possible combinations and are harder to crack through brute-force attacks.

- **Complexity**: Including a mix of different character types such as uppercase letters, lowercase letters, numbers, and special characters increases password complexity and strength.

- **Unpredictability**: Avoiding easily guessable patterns, common words, or personal information makes passwords more resistant to dictionary attacks and guessing.

- **Variety of Characters**: Using a diverse range of characters in a password increases its strength. Incorporating letters, numbers, and special characters adds complexity.

- **Avoidance of Patterns**: Avoiding sequential characters, repeated characters, or easily identifiable patterns makes passwords harder to crack.

- **Unique to Each Account**: Using unique passwords for each account prevents a single compromised password from affecting multiple accounts.

- **Regular Updates**: Changing passwords periodically reduces the risk of compromise, especially after security incidents or data breaches.

- **Avoidance of Personal Information**: Avoiding passwords based on personal information like birthdays, names, or addresses reduces the risk of easy guessing by attackers.

By considering these factors and creating strong, unique passwords for each account, individuals can significantly enhance the security of their online accounts and protect against unauthorized access.

Question 4. What is a symmetric cipher? And what is an asymmetric cipher? (2p)

A symmetric cipher is a cryptographic algorithm that uses the same key for both encryption and decryption of data. It operates on plaintext data using a shared secret key to produce ciphertext, which can then be decrypted back to plaintext using the same key. Symmetric ciphers are typically faster and more efficient than asymmetric ciphers but require secure key distribution mechanisms.

An asymmetric cipher, also known as public-key cryptography, uses a pair of keys for encryption and decryption: a public key and a private key. The public key is freely distributed to anyone, while the private key is kept secret by the owner. Messages encrypted with the public key can only be decrypted by the corresponding private key, providing secure communication channels without the need for a shared secret. Asymmetric ciphers are slower but offer advantages like secure key exchange and digital signatures.

Question 5. What is the least privilege principle in security design? Is the least privilege principle followed if the root (or administrator) privilege is shared among all users of an operating system? (2p)

The least privilege principle in security design states that users, processes, or systems should have only the minimum level of access or permissions necessary to perform their tasks. This principle aims to minimize the potential impact of security breaches or errors by limiting access to only essential resources.

Sharing root (or administrator) privileges among all users of an operating system violates the least privilege principle. Granting all users unrestricted access to system-level privileges increases the risk of accidental or intentional misuse, as any user can perform critical administrative tasks and potentially compromise system integrity or security. Instead, adhering to the least privilege principle involves granting root privileges only to trusted administrators or privileged users who require elevated access for specific tasks, while regular users are granted limited privileges appropriate to their roles and responsibilities.

Question 6. What are the drawbacks of using a memory card (e.g. a magnetic stripe card) as a authentication method? State at least two different drawbacks. (2p)

Using a memory card, such as a magnetic stripe card, for authentication has several drawbacks. Firstly, magnetic stripe cards are susceptible to skimming, where attackers can covertly capture card data using illegal card readers, leading to unauthorized access or identity theft. Secondly, magnetic stripe cards typically rely on static data stored on the card, making them vulnerable to cloning or duplication, allowing attackers to create counterfeit cards and impersonate legitimate users. These weaknesses undermine the security of magnetic stripe cards and highlight the need for more secure authentication methods, such as chip-based smart cards or biometric authentication.

Question 7. Explain the similarities between a virus and a worm. Also explain the difference between a virus and a worm. (2p)

Similarities

Both viruses and worms are types of malicious software (malware) designed to infect and spread to other systems.

- They can both cause damage to computer systems, compromise data integrity, and disrupt normal operations.
- Both viruses and worms can exploit security vulnerabilities in software or networks to propagate and infect new systems.
- They can both be spread through various means, including email attachments, infected files, network connections, or removable storage devices.

Differences

- Viruses typically attach themselves to executable files or documents and require user interaction or execution to spread, whereas worms are standalone programs that can spread independently without requiring a host file.
- Viruses rely on human actions, such as opening infected files or running infected programs, to propagate, whereas worms can self-replicate and spread automatically over networks by exploiting vulnerabilities in network services or software.
- Viruses may include payload components to modify or corrupt files, delete data, or perform other destructive actions, whereas worms may focus primarily on propagation and spreading, with less emphasis on payload functionality.
- Viruses can be easier to detect and remove since they typically infect specific files or locations, whereas worms may spread more rapidly and discreetly across networks, making detection and containment more challenging.

Question 8. You are asked to configure a firewall for your home network. The purpose is to only allow web traffic (on both directions), while blocking all the other types of traffic. A potential problem is a malicious packet might be disguised as incoming web traffic by using source port 80. Explain how a stateful packet filter firewall can be used to block fake web traffic which are usually unsolicited. (2p)

A stateful packet filter firewall can effectively block fake web traffic disguised as incoming web traffic by maintaining the state of active network connections. It does this by verifying whether incoming packets with destination port 80 (HTTP) are part of established or related connections initiated from within the network.

Unsolicited packets that do not match established connections are considered potentially fake web traffic and can be blocked to prevent unauthorized access or exploitation attempts. This approach helps ensure that only legitimate web traffic is allowed to pass through the firewall, enhancing the security of the home network.

Question 9. What is IPSec and what are its major functionalities? Is IPSec transparent to applications? (2p)

IPSec (Internet Protocol Security) is a suite of protocols that secures communication over IP networks by providing encryption, authentication, and integrity protection for IP packets. Its major functionalities include confidentiality, authentication, integrity, key management, and tunneling for VPNs.

While IPSec operates at the network layer and is generally transparent to most applications, some network configurations may require adjustments for compatibility.

Question 10. Explain the SQL injection attack. Why controlling user inputs can reduce the risks of SQL injection attack? (2p)

SQL injection is a cyberattack where attackers exploit vulnerabilities in web applications by injecting malicious SQL code through user inputs. Controlling user inputs involves validating, sanitizing, and escaping special characters to prevent attackers from executing unauthorized SQL commands. Implementing measures like input validation, parameterized queries, and least privilege access helps reduce the risks of SQL injection attacks and protects against unauthorized access, data manipulation, or server compromise.

By controlling and sanitizing user inputs effectively, web applications can mitigate the risks associated with SQL injection attacks and protect the confidentiality, integrity, and availability of their data and resources.

Question 11. Why do web sites use cookies? Describe an example where a Cross-Site Scripting (XSS) attack is used to steal a victim user’s cookie information. (2p)

Websites use cookies to enhance user experience by storing user preferences, session information, and authentication tokens. Cookies help websites remember users' login status, personalize content, track user interactions, and provide targeted advertising. They play a crucial role in improving website functionality, maintaining user sessions, and enabling features like shopping carts and personalized recommendations.

In a Cross-Site Scripting (XSS) attack, an attacker injects malicious scripts into a vulnerable website, which, when executed in a victim's browser, can steal their cookie information. For instance, an attacker may inject malicious code into a website's comment section. When a victim user views the comment, the script executes, allowing the attacker to steal their cookie information and potentially hijack their session or access sensitive data.

Question 12. Digital signature is a use of asymmetric cryptography. Suppose there are two users Alice and Bob. Alice creates a message and sends it to Bob. In together with this message, Alice also appends her digital signature. What key material can be used by Alice to create (sign) her digital signature? Alice's key or Bob's key? A public key or a private key? (2p)

To create (sign) her digital signature, Alice would use her private key. Digital signatures are created using the sender's private key and can be verified using the corresponding public key. This ensures that the signature can only be created by the owner of the private key and can be verified by anyone with access to the corresponding public key. Therefore, Alice would use her private key to sign the message, and Bob would use Alice's public key to verify the signature.

Question 13.

Imagine a smart home alarm system. In such a system, there are different types of sensors, such as camera, motion sensor, smoke sensor, etc. Collected data may be transferred to a central station for data storage and real-time response. The service of data storage and real-time response can be provided by a commercial company. The purpose is to detect theft, robbery, fire, water damage, etc.

(1) There is apparently a confidentiality and privacy issue here. Analyze the infringement to privacy brought by the sensor installation and data collection. Make suggestions to the system design that can minimize the worries on privacy infringement. (2p)
(2) Who should be given access to the system and data? How can effective access control be implemented to protect accesses to local and centralized data storage, and to system-user interfaces? (2p)
(3) Data encryption methods can have an important role here to protect both data in storage and data on transmission. Imagine a few different attack scenarios where data can be stolen or be modified/deleted if there is no proper encryption and authentication? (2p)

1. The installation of sensors in a smart home alarm system raises privacy concerns as it involves monitoring activities within the home. Suggestions to minimize privacy infringement include implementing transparent data collection policies, obtaining explicit consent from users before collecting data, anonymizing or pseudonymizing collected data to reduce the risk of identifying individuals, and providing users with control over their data, such as the ability to opt-out of certain data collection activities or delete collected data.

2. Access to the system and data should be granted only to authorized individuals, such as homeowners, security personnel, and trusted service providers. Effective access control mechanisms can be implemented by enforcing strong authentication methods, such as passwords, biometric authentication, or multi-factor authentication, to verify the identity of users accessing the system or data. Role-based access control (RBAC) can be employed to define and enforce access privileges based on users' roles and responsibilities, limiting access to sensitive data to only those who need it.

3. Without proper encryption and authentication, data in storage and transmission is vulnerable to various attack scenarios. For instance, in a scenario where data transmission

is not encrypted, an attacker could eavesdrop on network traffic and intercept sensitive information, such as alarm activation signals or video feeds from cameras. In another scenario, if data stored in centralized storage is not encrypted, an attacker who gains unauthorized access to the storage system could steal or tamper with sensitive data, such as footage from security cameras or logs of alarm events. Additionally, without authentication mechanisms in place, attackers could impersonate legitimate users and gain unauthorized access to the system or data, potentially causing disruption or misuse of the smart home alarm system. Implementing encryption methods such as SSL/TLS for data transmission and AES encryption for data storage, along with strong authentication mechanisms, can help mitigate these risks and protect sensitive information from unauthorized access or tampering.