Examen de CEG 4399 Preparation QCM generer

Lecture 1-2 : Introduction

Q1: What is the primary goal of computer security?

A) To improve system performance
B) To safeguard data, hardware, and communication networks from unauthorized access
C) To enhance user experience
D) To reduce the cost of software development
Correct answer: B) To safeguard data, hardware, and communication networks from unauthorized access

Q2: What are the three main objectives of computer security, often referred to as the CIA triad?

A) Confidentiality, Integrity, Accountability
B) Confidentiality, Integrity, Availability
C) Confidentiality, Identification, Authentication
D) Confidentiality, Accessibility, Integrity
Correct answer: B) Confidentiality, Integrity, Availability

Q3: Which of the following refers to the assurance that information is not altered except in an authorized way?

A) Availability
B) Privacy
C) Integrity
D) Confidentiality
Correct answer: C) Integrity

Q4: What is a passive attack in computer security?

A) An attack where the attacker modifies the data stream
B) An attack that involves unauthorized monitoring or eavesdropping
C) An attack that blocks legitimate access to services
D) An attack that uses a virus to damage the system
Correct answer: B) An attack that involves unauthorized monitoring or eavesdropping

Q5: What is the purpose of security policies in an organization?

A) To increase software performance
B) To define rules and practices for protecting assets and systems
C) To reduce hardware costs
D) To monitor employee productivity
Correct answer: B) To define rules and practices for protecting assets and systems

Q6: Which term refers to any situation or entity that could potentially harm computer system assets?

A) Risk
B) Threat
C) Attack
D) Vulnerability
Correct answer: B) Threat

Q7: What is a vulnerability in the context of computer security?

A) A measure used to prevent unauthorized access
B) A potential flaw or weakness in a system that can be exploited
C) A device used to monitor network traffic
D) A cryptographic method to secure data
Correct answer: B) A potential flaw or weakness in a system that can be exploited

Q8: Which of the following is a type of active attack?

A) Eavesdropping
B) Replay attack
C) Traffic analysis
D) Scanning
Correct answer: B) Replay attack

Q9: What does the term "risk" refer to in computer security?

A) The likelihood that an attack will occur and the damage it may cause
B) The process of encrypting data for security
C) A legal framework for data protection
D) The prevention of unauthorized access
Correct answer: A) The likelihood that an attack will occur and the damage it may cause

Q10: In the context of threat modeling, what does the STRIDE technique refer to?

A) A cryptographic algorithm
B) A method for identifying threats like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
C) A risk assessment tool used to calculate vulnerabilities
D) A programming language used in secure software development
Correct answer: B) A method for identifying threats like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

—----------

Lecture 3 : Review of Cryptography

Q1: What is the main purpose of encryption?

A) To increase data transfer speed
B) To encode a message so its meaning is hidden
C) To store data securely on the cloud
D) To perform mathematical calculations
Correct answer: B) To encode a message so its meaning is hidden

Q2: In symmetric encryption, which of the following is true?

A) The encryption and decryption keys are the same
B) The encryption and decryption keys are different
C) It only uses a public key for encryption
D) It is not possible to decrypt the message
Correct answer: A) The encryption and decryption keys are the same

Q3: Which type of cipher uses multiple alphabets for encryption?

A) Mono-alphabetic cipher
B) Caesar cipher
C) Poly-alphabetic cipher
D) One-time pad cipher
Correct answer: C) Poly-alphabetic cipher

Q4: What is a "one-time pad" in cryptography?

A) A type of block cipher
B) A method of encryption where the key is the same length as the message and used only once
C) A cipher that shifts the alphabet by three letters
D) An algorithm used for key generation in RSA
Correct answer: B) A method of encryption where the key is the same length as the message and used only once

Q5: What is the main objective of transposition ciphers?

A) To change the characters of the plaintext
B) To rearrange the characters of the plaintext
C) To substitute each character with another
D) To use different keys for each letter
Correct answer: B) To rearrange the characters of the plaintext

Q6: What does AES stand for in cryptography?

A) Advanced Encryption Standard
B) Asymmetric Encryption System
C) Algorithm for Encrypted Security
D) Adaptive Encryption Scheme
Correct answer: A) Advanced Encryption Standard

Q7: In a cryptographic system, what is meant by the "avalanche effect"?

A) A small change in the key causes minimal changes in the ciphertext
B) A small change in the plaintext causes a significant change in the ciphertext
C) It refers to the failure of an encryption algorithm
D) A method of breaking a cipher through statistical analysis
Correct answer: B) A small change in the plaintext causes a significant change in the ciphertext

Q8: Which encryption algorithm uses both public and private keys?

A) DES
B) AES
C) RSA
D) Caesar cipher
Correct answer: C) RSA

Q9: What is the primary weakness of the Data Encryption Standard (DES)?

A) It is too slow for practical use
B) It is not based on mathematical principles
C) It uses a short key length, making it vulnerable to brute-force attacks
D) It uses a public key for both encryption and decryption
Correct answer: C) It uses a short key length, making it vulnerable to brute-force attacks

Q10: What is the key difference between stream ciphers and block ciphers?

A) Stream ciphers encrypt one symbol at a time, while block ciphers encrypt groups of symbols
B) Stream ciphers use asymmetric keys, and block ciphers use symmetric keys
C) Block ciphers are used for faster encryption
D) Stream ciphers are more secure than block ciphers
Correct answer: A) Stream ciphers encrypt one symbol at a time, while block ciphers encrypt groups of symbols

Q11: What does RSA encryption rely on for its security?

A) The difficulty of factoring large numbers
B) The use of random keys
C) The substitution of characters
D) The speed of modern processors
Correct answer: A) The difficulty of factoring large numbers

Q12: In the context of secret sharing, what is a (t, n)-threshold scheme?

A) A system where t participants must agree to change the encryption key
B) A system where any t participants out of n can reconstruct the secret
C) A system where t shares are needed to distribute the secret to n participants

D) A system where n participants must agree to a new encryption standard
Correct answer: B) A system where any t participants out of n can reconstruct the secret

---

Lecture 4 : Security in the Software Development Life Cycle

Q1: What is the main goal of integrating security into the Software Development Life Cycle (SDLC)?

A) To reduce software development costs
B) To prevent vulnerabilities and create secure software
C) To speed up software delivery
D) To test software performance
Correct answer: B) To prevent vulnerabilities and create secure software

Q2: At which phase of the SDLC should threat modeling be conducted to identify potential security issues?

A) Design phase
B) Implementation phase
C) Testing phase
D) Deployment phase
Correct answer: A) Design phase

Q3: Which of the following is a common software vulnerability that can lead to security breaches?

A) Inadequate documentation
B) Buffer overflow
C) Code redundancy
D) Lack of user interface testing
Correct answer: B) Buffer overflow

Q4: What is the primary goal of secure coding practices during the implementation phase?

A) To minimize code size
B) To prevent common flaws like input validation issues
C) To reduce development time
D) To improve the user interface design
Correct answer: B) To prevent common flaws like input validation issues

Q5: Which of the following tools can be used for static code analysis to detect vulnerabilities before deployment?

A) OWASP ZAP
B) Burp Suite
C) SonarQube
D) Penetration testing tools

Correct answer: C) SonarQube

Q6: What is the purpose of the "disposal" phase in the SDLC?

A) To deploy the software to the production environment
B) To remove or archive data securely and perform media sanitization
C) To add new features to the software
D) To perform software performance testing
Correct answer: B) To remove or archive data securely and perform media sanitization

Q7: Which SDLC model involves overlapping steps to ensure flexibility and minimize risks?

A) Waterfall model
B) Sashimi model
C) Spiral model
D) Agile model
Correct answer: B) Sashimi model

Q8: What is the main purpose of a Configuration Management Plan (CMP) according to NIST guidelines?

A) To manage system performance
B) To control changes and ensure they don’t affect security
C) To improve software usability
D) To track software sales and licenses
Correct answer: B) To control changes and ensure they don’t affect security

Q9: Which of the following is a common attack that exploits vulnerabilities in SQL databases?

A) Cross-Site Scripting (XSS)
B) Buffer overflow
C) SQL injection
D) Cross-Site Request Forgery (CSRF)
Correct answer: C) SQL injection

Q10: What is a key benefit of using dynamic code analysis tools?

A) They detect vulnerabilities without executing the code
B) They analyze code in real-time during execution to find vulnerabilities
C) They reduce the size of the codebase
D) They improve software usability testing
Correct answer: B) They analyze code in real-time during execution to find vulnerabilities

Q11: In the context of API security, what is a common threat associated with improper use of APIs?

A) SQL injection

B) Server-Side Request Forgery (SSRF)
C) Buffer overflow
D) Code redundancy
Correct answer: B) Server-Side Request Forgery (SSRF)

Q12: Which level of the Software Capability Maturity Model (CMM) involves a controlled and measured process?

A) Initial
B) Repeatable
C) Defined
D) Managed
Correct answer: D) Managed

Lecture 5 : Access Control and Management

Q1: What is the main function of access control?

A) To monitor network traffic
B) To allow or deny permission to specific resources
C) To encrypt all data in a system
D) To control user passwords
Correct answer: B) To allow or deny permission to specific resources

Q2: Which of the following is a type of physical access control?

A) Password authentication
B) Firewalls
C) Hardware-based door locks
D) Data encryption
Correct answer: C) Hardware-based door locks

Q3: In access control, what is the process of verifying a user's identity called?

A) Authorization
B) Authentication
C) Accounting
D) Identification
Correct answer: B) Authentication

Q4: What does RBAC stand for in access control?

A) Role-Based Access Control
B) Rule-Based Access Control
C) Resource-Based Access Control
D) Risk-Based Access Control
Correct answer: A) Role-Based Access Control

Q5: Which of the following models is considered the least restrictive in terms of access control?

A) Discretionary Access Control (DAC)
B) Mandatory Access Control (MAC)
C) Role-Based Access Control (RBAC)
D) Attribute-Based Access Control (ABAC)
Correct answer: A) Discretionary Access Control (DAC)

Q6: What is the primary characteristic of Mandatory Access Control (MAC)?

A) Users have full control over access permissions
B) Permissions are set based on system policies, not user discretion
C) Users can assign their permissions to others
D) It uses attributes like user location for access decisions
Correct answer: B) Permissions are set based on system policies, not user discretion

Q7: What are labels in the context of MAC (Mandatory Access Control)?

A) A form of encryption used to secure data
B) Classification levels assigned to objects and subjects
C) Access tokens distributed to users
D) Temporary permissions assigned to a user
Correct answer: B) Classification levels assigned to objects and subjects

Q8: Which access control model dynamically assigns roles to users based on predefined rules?

A) Attribute-Based Access Control (ABAC)
B) Rule-Based Role-Based Access Control (RB-RBAC)
C) Discretionary Access Control (DAC)
D) Mandatory Access Control (MAC)
Correct answer: B) Rule-Based Role-Based Access Control (RB-RBAC)

Q9: What is the purpose of the principle of least privilege in access control?

A) To grant users the maximum access rights possible
B) To restrict users to only the permissions necessary for their tasks
C) To allow users to change their own access permissions
D) To revoke all user access privileges automatically
Correct answer: B) To restrict users to only the permissions necessary for their tasks

Q10: Which of the following services provides centralized authentication and authorization in a network environment?

A) LDAP
B) RADIUS

C) Kerberos
D) TACACS+
Correct answer: B) RADIUS

Q11: What is the main purpose of Access Control Lists (ACLs)?

A) To track user login times
B) To specify which users or processes are allowed to access specific resources
C) To encrypt data on the network
D) To prevent unauthorized software installations
Correct answer: B) To specify which users or processes are allowed to access specific resources

Q12: Which protocol is commonly used to maintain distributed directory information services over a network?

A) RADIUS
B) LDAP
C) Kerberos
D) SAML
Correct answer: B) LDAP

—----------

Lecture 6 : Security in the Network and Internet

Q1: Which of the following is NOT a typical characteristic of networks?

A) Anonymity
B) Automation
C) Transparency
D) Routing diversity
Correct answer: C) Transparency

Q2: What does TCP/IP stand for?

A) Transmission Control Protocol/Internet Protocol
B) Transfer Communication Protocol/Internet Process
C) Technical Communication Process/Internet Program
D) Transmission Communication Protocol/Internal Process
Correct answer: A) Transmission Control Protocol/Internet Protocol

Q3: Which of the following is a vulnerability specific to networks?

A) Single user
B) Centralized control
C) Shared resources
D) No need for security policies
Correct answer: C) Shared resources

Q4: What is a typical characteristic of a Local Area Network (LAN)?

A) Covers a wide geographic area
B) Shared by multiple organizations
C) Locally controlled and physically protected
D) Exposed to the general public
Correct answer: C) Locally controlled and physically protected

Q5: Which of the following describes a "Man-in-the-Middle" attack?

A) An attacker intercepts communication between two parties and pretends to be one of them.
B) An attacker installs malware on a target system.
C) A legitimate user is blocked from accessing a network resource.
D) Sensitive information is encrypted before being transmitted.
Correct answer: A) An attacker intercepts communication between two parties and pretends to be one of them.

Q6: What is the purpose of a firewall in a network?

A) To enhance network speed
B) To prevent unauthorized access to or from a private network
C) To distribute data between different systems
D) To monitor internet usage
Correct answer: B) To prevent unauthorized access to or from a private network

Q7: Which of the following is NOT a type of firewall?

A) Stateful inspection
B) Application proxy
C) Intrusion Detection System (IDS)
D) Packet filtering gateway
Correct answer: C) Intrusion Detection System (IDS)

Q8: Which of the following is a characteristic of a Denial of Service (DoS) attack?

A) Flooding a server with excessive requests to exhaust its resources
B) Hacking into a server to steal data
C) Encrypting sensitive files on a server
D) Installing malware on multiple systems
Correct answer: A) Flooding a server with excessive requests to exhaust its resources

Q9: What is the primary function of encryption in network security?

A) To increase the speed of data transmission
B) To protect data by converting it into a format that is unreadable without a key
C) To allow easy sharing of sensitive information

D) To prevent data from being backed up
Correct answer: B) To protect data by converting it into a format that is unreadable without a key

Q10: What does a VPN (Virtual Private Network) do?

A) Blocks harmful websites
B) Provides anonymous browsing
C) Establishes a secure connection over a public network
D) Encrypts data at rest
Correct answer: C) Establishes a secure connection over a public network

—----------

bonus

Q1: What is the primary focus of the course CEG4399 - Design of Secure Computer Systems?

A) Software development practices
B) Fundamentals of secure system design and cybersecurity
C) Hardware optimization
D) Cloud infrastructure management
Correct answer: B) Fundamentals of secure system design and cybersecurity

Q2: Which of the following security principles are covered in the first week of the course?

A) Cryptography, PKI, and SSL
B) Confidentiality, Integrity, Availability (CIA)
C) Malware detection, Firewalls, VPNs
D) Software licensing and open-source tools
Correct answer: B) Confidentiality, Integrity, Availability (CIA)

Q3: What is a key goal of secure system design mentioned in the document?

A) Maximizing performance
B) Balancing security with risk
C) Reducing operational costs
D) Improving user interface design
Correct answer: B) Balancing security with risk

Q4: What is the significance of CrowdStrike in the context of this course?

A) It's a case study on software development best practices
B) It represents a real-world example of a major cybersecurity incident
C) It is a tool used for secure coding
D) It's an example of a new encryption standard
Correct answer: B) It represents a real-world example of a major cybersecurity incident

Q5: Which of the following is NOT mentioned as a focus area in the course structure?

A) Web Application Security
B) Mobile and IoT Security
C) Database performance optimization
D) Cloud Security
Correct answer: C) Database performance optimization

Q6: What is the importance of network security according to the course?

A) It prevents software crashes
B) It protects against vulnerabilities in communication protocols
C) It reduces hardware costs
D) It improves website design
Correct answer: B) It protects against vulnerabilities in communication protocols

Q7: Which type of assessment contributes the most to the overall grade in CEG4399?

A) Class activities
B) Midterm exam
C) Assignments
D) Final exam
Correct answer: D) Final exam (30%)

Q8: What is a recommended security practice for web application development, as mentioned in the course outline?

A) Use of deprecated libraries
B) Implementing firewalls and DDoS protection
C) Following OWASP Top 10 guidelines
D) Avoiding encryption for performance reasons
Correct answer: C) Following OWASP Top 10 guidelines

Q9: What is a key takeaway regarding the role of information in modern life according to the document?
A) Information is no longer as important in global transactions
B) Information flows are critical, and computing security is a high priority
C) Modern life can function without computerized systems
D) Data privacy is not a primary concern anymore
Correct answer: B) Information flows are critical, and computing security is a high priority

Q10: Which methodology is introduced in the course to address threats in software development?
A) Waterfall model
B) DevSecOps
C) Agile development
D) SCRUM
Correct answer: B) DevSecOps