CSE 4380 Exam 1 Review
Fall 2024

1. A nonce is
    A. A random number
    B. A one-time password
    C. A single use-token
    D. A challenge negation

Solution: A random number

2. How long would it take to break 128-bit AES assuming 10^6 (1 million) decryptions per microsecond on average?
    A. 5.4×10^{18}seconds
    B. 5.4×10^{18}days
    C. 5.4×10^{18}years
    D. 5.4×10^{18}millennia

Solution: 5.4×10^{18} years

3. Which is not true about DES?
    A. It is a symmetric key algorithm
    B. It is an asymmetric key algorithm
    C. It is no longer secure
    D. It is no longer the current NIST recommended standard

Solution: It is an asymmetric key algorithm

4. Ensuring timely and reliable access to and use of information.
    A. Contigency planning
    B. Integrity
    C. Disaster recovery plan
    D. Availability

Solution: Availability

5. Which of the following is a not a phase in the virus lifetime
    A. Infection Phase
    B. Dormant Phase
    C. Triggering Phase
    D. Execution Phase

Solution: Infection Phase

6. The security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.
    A. Least priviledge
    B. Isolation
    C. Psychological acceptability
    D. Least astonishment

Solution: Psychological acceptability

7. Shoulder surfing is a type of what attack?
    A. Replay
    B. Eavesdropping
    C. Reconnaisance
    D. Cross-site scripting

Solution: Eavesdropping

8. What is an example of a moderate impact loss of confidentiality?
    A. Student enrollment information is exposed
    B. Entries in an online discussion forum are falsified
    C. Access to an online telephone directory is blocked
    D. A personal health record is exposed

Solution: A personal health record is exposed

9. How much more security do you get against brute force when you go from a 64-bit key to an 80-bit key?
   A. 25% more
   B. 16 times as much
   C. $2^8 = 256$ times as much
   D. $2^{16} = 65,536$ times as much

Solution: $2^{16} = 65,536$ times as much

10. What property does Alices signature on a message NOT provide?
    A. Authentication: The message came from Alice
    B. Non-repudiation: The receiver can prove that Alice signed it
    C. Data integrity: The message has not been altered since it left Alice
    D. Confidentiality: The message has not been read by anyone except Alice

Solution: Confidentiality: The message has not been read by anyone except Alice

11. A secure hash function has which of these properties?
    A. It is impossible to undo the hash to find original input X
    B. It is computationally infeasible to compute the hash of X
    C. It is impossible to find inputs X and Y with the same hash value
    D. It is computationally infeasible to find inputs X and Y with the same hash value

Solution: It is computationally infeasible to find inputs X and Y with the same hash value

12. A program or user interface should always respond in the way that is least likely to surprise the user.
    A. Least priviledge
    B. Isolation
    C. Psychological acceptability
    D. Least astonishment

Solution: Least astonishment

13. Which security principle dictates that you should use multiple, diverse, and complementary defense mechanisms?
    A. Least privilege
    B. Accountability
    C. Defense in Depth
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Defense in Depth

14. What is the purpose of a certificate?
    A. To encrypt the secret key
    B. To keep the private key secret
    C. To prove that an identity and a public key are linked
    D. To prove that a certificate authority trusts a given user

Solution: To prove that an identity and a public key are linked

15. A brute force attack on a hash function with n-bit outputs requires about how many hash operations?
    A. 2^n
    B. $(2^n)^{1/2} (the square root of 2^n)$
    C. n
    D. n^2

Solution: $(2^n)^{1/2} (the square root of 2^n)$

16. Which is true about AES?
    A. It is a symmetric key algorithm
    B. It is an asymmetric key algorithm
    C. It is no longer secure
    D. It replaced the MD5 algorithm

Solution: It is a symmetric key algorithm

17. This is the original message or data that is fed into the algorithm as input.
    A. Plaintext
    B. Ciphertext
    C. Plain key
    D. Message digest

Solution: Plaintext

18. Which of the following terms isn't equivalent
    A. Policy
    B. Rights
    C. Authorizations
    D. Privileges
    E. Entitlements

Solution: Policy

19. When checking the digital signature of Bobs message, how is a hash function used?
    A. It is used to hash the input to the encryption function
    B. It is used to hash the output of the decryption function
    C. It is used to hash Bobs public key before decryption; the key is long otherwise
    D. It is used to hash the message; the hash is compared with the decrypted hash value

Solution: It is used to hash the message; the hash is compared with the decrypted hash value

20. APT
    A. Advanced Persistant Threat
    B. Advanced Persistant Trojan
    C. Asynchronous Partition Table
    D. Advanced Persistant Thread

Solution: Advanced Persistant Threat

21. A downside to the Access Control Matrix
    A. It's sparse
    B. Its one to one relationship
    C. Its one to many relationship
    D. It follows the rule of least privilege

Solution: It's sparse

22. This is an attack on system availability
    A. Incapacitation
    B. Corruption
    C. Misappropriation
    D. Usurpation

Solution: Incapacitation

23. The design of security measures embodied in both hardware and software should be as simple and small as possible.
    A. KISS method
    B. Encapsulation
    C. Economy of mechanism
    D. Complete mediation

Solution: KISS method

24. Role-Based Access Control
    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).
    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

25. Which of these is NOT a requirement for secure use of symmetric encryption?
    A. Sender and receiver keep the key secure
    B. Hiding the details of the encryption algorithm from the attacker
    C. Sender and receiver have obtained the secret key in a secure fashion
    D. Keys are long and random enough to prevent brute force attacks

Solution: Hiding the details of the encryption algorithm from the attacker

26. Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated
    A. Computer Security
    B. Information Systems
    C. Auditing
    D. Security controls

Solution: Security controls

27. Cryptanalysis is
    A. The study of cryptography
    B. A symmetric encryption attack
    C. The analysis of a cryptographic algorithm
    D. The study of codes

Solution: The analysis of a cryptographic algorithm

28. Which of these is considered a secure cryptographic hash function?
    A. MD5

B. SHA (the Secure Hash Algorithm)

C. SHA-384

D. SHA-1024

Solution: SHA-384

29. Which of these systems has a high availability requirement (just choose the best answer)?

    A. A university Website

    B. A system to process financial transactions

    C. An online telephone directory

    D. Anti-virus software running on a PC

Solution: A system to process financial transactions

30. What type of plaintext is hardest to perform brute force on (starting from the ciphertext)?

    A. English text

    B. Chinese text

    C. A Windows 7 executable

    D. A compressed spreadsheet of numerical data

Solution: A compressed spreadsheet of numerical data

31. A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

    A. Attack surface

    B. Attack vector

    C. Attack tree

    D. Attack pattern

Solution: Attack tree

32. What verifies the user can access what they are requesting?

A. Authentication
B. Authorization
C. Audit
D. Access control

Solution: Authorization

33. Keeping the trusted code base very small in trusted computing is an example of which security property?
    A. Least privilege
    B. Default Security
    C. Defense in Depth
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Minimize the variety, size, and complexity of trusted components (KISS)

34. An attempt by an unauthorized user to gain access to a system by posing as an authorized user
    A. Deauthentication
    B. Masquerading
    C. Repudiation
    D. Man-in-the-middle

Solution: Masquerading

35. Traffic analysis is what type of attack?
    A. Inference
    B. Interference
    C. Interception
    D. Intrusion

Solution: Interception

36. Using a public encryption scheme which key would Alice use to send an ecrypted message to Bob?

A. Alice's private key
B. Bob's private key
C. Alice's public key
D. Bob's public key

Solution: Bob's public key

37. What is the BEST reason to be concerned about the insider threat?
    A. Insiders can plant malware on the system
    B. Insiders have some degree of authorized access to the system
    C. Insiders like disgruntled employees have greater motivation to cause harm
    D. Insiders are harder to prosecute than external hackers

Solution: Insiders have some degree of authorized access to the system

38. Which virus creates copies during replication that are functionally equivalent but have distinctly different bit patterns, in order to vary its signature
    A. Metamorphic virus
    B. Polymorphic virus
    C. Stealth virus
    D. Cryptographic virus

Solution: Metamorphic virus

39. What is the first step in devising security services and mechanisms?
    A. Developing a security policy
    B. Deciding between prevention and detection/reaction
    C. Designing assurance metrics
    D. Locking down unnecessary services

Solution: Developing a security policy

40. In which application area is integrity typically valued higher than confidentiality?
    A. Military documents
    B. Financial transactions
    C. Health care records
    D. Video rental records

Solution: Financial transactions

41. A practice in which multiple privilege attributes are required to achieve access to a restricted resource.
    A. Least priviledge
    B. Separation of priveledge
    C. Authorization
    D. Least common mechanism

Solution: Separation of priveledge

42. Random numbers for cryptography should have which of these features?
    A. Uniform distribution, Independence, and Unbreakability
    B. Uniform distribution, Independence, and Unpredictability
    C. Non-uniform distribution, Independence, and Unbreakability
    D. Non-uniform distribution, Independence, and Unpredictability

Solution: Uniform distribution, Independence, and Unpredictability

43. Creating a digital envelope includes which of these steps?
    A. Encrypt the symmetric key with the senders public key
    B. Encrypt the symmetric key with the receivers public key
    C. Encrypt the senders private key with the receivers public key
    D. Encrypt the receivers private key with the senders public key

Solution: Encrypt the symmetric key with the receivers public key

44. Why do attackers have a significant advantage over defenders?

    A. Security mechanisms are complex and it is not obvious that such measures are needed

    B. Computer security has complex requirements that are hard to describe

    C. The attacker only needs to find one hole; defenders must attempt to close all holes

    D. Finding successful attacks is straightforward exercise once the system is understood

Solution: The attacker only needs to find one hole; defenders must attempt to close all holes

45. Attribute-based Access Control

    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

46. Why is security a weak-link property?

    A. One weakness in the system leads to more weaknesses later

    B. The security of the whole system is only as good as the security of each (exposed) part

    C. The link between typical users and the system security goals is weak

    D. Weak links in a defense can be overcome with stronger links through security design

Solution: The security of the whole system is only as good as the security of each (exposed) part

47. Role Based Access Control

    A. Is based on the roles that users assume in a system rather than the users identity

    B. Is based on the roles the resources assume in a system rather than the resources type

    C. Is based on the roles the processes assumes in a system rather than the user's identity

D. Is based on the roles the access conrtol matrix assumes in a system rather than the role's identity

Solution: Is based on the roles that users assume in a system rather than the users identity

48. An attempt to learn or make use of information from the system that does not affect system resources.
    A. Passive Attack
    B. Port Scanning
    C. nmap
    D. Exfiltration

Solution: Passive Attack

49. Why is it difficult to simply ban the use of mobile code in a strictly controlled environment (e.g. military)?
    A. Mobile code makes Flash animations possible
    B. Mobile code runs more efficiently than static code
    C. Virus scanners use mobile code to distribute and install patches
    D. Virus scanners would fail to detect the use of mobile code, making enforcement hard

Solution: Virus scanners use mobile code to distribute and install patches

50. Encryption of a plaintext using ones private key is .
    A. insecure, because anyone with the public key can decrypt it
    B. useful for providing authentication but not confidentiality
    C. useful for providing confidentiality but not authentication
    D. useful for providing both authentication and confidentiality

Solution: useful for providing authentication but not confidentiality

51. Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

A. Risk Management
B. Risk Management Framework
C. Incident Response
D. Contingency Planning

Solution: Contingency Planning

52. Which is not an example of mult-factor authentication?
    A. A key and a PIN
    B. Your eyeball and a key
    C. Credit card and an authenticator app
    D. The way you walk and a password

Solution: Credit card and an authenticator app

53. Assures that information is not made available or disclosed to unauthorized individuals.
    A. Data integrity
    B. Confidentiality
    C. Encryption
    D. Authentication

Solution: Confidentiality

54. Why do people use 3DES?
    A. AES is not yet a federal standard
    B. It is three times as secure as DES
    C. It is almost three times faster than DES
    D. It retains the security of DES against cryptanalysis

Solution: It retains the security of DES against cryptanalysis

55. What is the advantage of a digital envelope over encrypting the message with the public key?

A. The digital envelope method uses less bandwidth

B. Public key encryption is less secure than symmetric key encryption

C. Public key encryption is slow, so it saves computation time in most cases

D. Public key encryption can only be made to work on small amounts of data at a time

Solution: Public key encryption is slow, so it saves computation time in most cases

56. Discretionary Access Control

    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

57. What verifies the use is who they say they are?

    A. Authentication

    B. Authorization

    C. Audit

    D. Access control

Solution: Authentication

58. Lowering the decision threshold on a biometric measure results in

    A. More false positives

    B. More false negatives

Solution: More false negatives

59. Authentication, authorization, and audit (AAA) are all part of which security property?
    A. Least privilege
    B. Accountability
    C. Default security
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Accountability

60. A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm.
    A. Weakness
    B. Threat
    C. Vulnerability
    D. Breach

Solution: Threat

61. A misconfigured rule enforced by a firewall is an example of which of these?
    A. Risk
    B. Threat
    C. Attack
    D. Vulnerability

Solution: Vulnerability

62. Why is the DES algorithm considered unacceptable today?
    A. It is too slow
    B. It is vulnerable to brute force
    C. It is vulnerable to cryptanalysis
    D. It is vulnerable to rainbow tables

Solution: It is vulnerable to brute force

63. A flaw or weakness in a systems design, implementation, or operation and management that could be exploited to violate the systems security policy.
    A. Weakness
    B. Threat
    C. Vulnerability
    D. Breach

Solution: Vulnerability

64. Which of these involves backup systems?
    A. Prevention
    B. Detection
    C. Response
    D. Recovery

Solution: Recovery

65. Which of these statements is true?
    A. Public key encryption is commonly used to share secret keys
    B. Public key encryption is likely to supplant symmetric key encryption in the next decade
    C. Public key encryption is more secure against brute force than symmetric key encryption
    D. Public key encryption is more secure against cryptanalysis than symmetric key encryption

Solution: Public key encryption is commonly used to share secret keys

66. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
    A. Access Control
    B. Identity Management
    C. Authentication

D. Service Acquisition

Solution: Access Control

67. Which of the following biometric schemes is the most accurate?
    A. Retina
    B. Iris
    C. Hand
    D. Finger

Solution: Iris

68. Mandatory Access Control
    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).
    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.
    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

69. What doesn't a digital signature provide?
    A. Integrity
    B. Confidentiality
    C. Non-repudiation
    D. Authenticity

Solution: Confidentiality

70. Which of these is NOT a part of what needs to be considered when developing a security policy?
    A. The value of the assets being protected
    B. The effect on ease of use of the system of various decisions
    C. The degree to which the security system implementation meets its specifications
    D. The cost of failure and recovery

Solution: The degree to which the security system implementation meets its specifications

71. An attempt to alter system resources or affect their operation.
    A. Breach
    B. Exploit
    C. Active Attack
    D. Denial of Service

Solution: Active Attack

72. Which of these is the best for encrypting secret keys when speed is critical?
    A. RSA
    B. Diffie-Hellman
    C. DSS
    D. ECC

Solution: ECC

73. What is the main advantage of risk management over risk avoidance?
    A. It leads to greater focus on defending against more dangerous threats
    B. It leads to removal of a greater number of vulnerabilities from the system
    C. It leads to defending against a larger variety of threats
    D. It is more effective against insider threats

Solution: It leads to defending against a larger variety of threats

74. What is an attack against hashed passwords?
    A. Dictionary attack
    B. Rainbow Table
    C. Salting
    D. Reactive password checking

Solution: Rainbow Table

75. Asymmetric encryption requires
    A. Alice and Bob have the same key
    B. Alice has 1 key and Bob has 2
    C. Alice has two keys and Bob has two keys
    D. A way to securely transmit keys

Solution: Alice has two keys and Bob has two keys

76. Attribute-Based Access Control
    A. Defines authorizations that express conditions on properties of both the resource and the subject
    B. Defines authorizations that express conditions on properties of both the user and the subject
    C. Defines authorizations that express conditions on properties of both the resource and the system
    D. Defines authorizations that express conditions on properties of both the system and the subject

Solution: Defines authorizations that express conditions on properties of both the resource and the subject

77. Symmetric encryption provides
    A. Confidentiality
    B. Integrity
    C. Availability

Solution: Confidentiality

78. The degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes
    A. Level of assurance
    B. Assurance
    C. Risk level
    D. Mitigation factor

Solution: Assurance

79. Trying every possible combination is what type of attack?
    A. Brute-force attack
    B. Man-in-the-middle
    C. Monte Carlo
    D. Combo attack

Solution: Brute-force attack

80. Manufacturers setting a strong password on wireless routers is an example of which security property?
    A. Least privilege
    B. Accountability
    C. Default security
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Default security

81. Any means taken to deal with a security attack.
    A. Countermeasure
    B. Mitigation
    C. Risk
    D. Patch

Solution: Countermeasure

82. Multi-factor authentication doesn't involve
    A. Something you have
    B. Something you are
    C. Something you know
    D. Something you prove

Solution: Something you prove

83. Which of these crypto tools does a certificate NOT need?
    A. Hashing
    B. Symmetric key encryption
    C. Decryption using the public key
    D. Encryption using the private key

Solution: Symmetric key encryption

84. A threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence.
    A. Attack
    B. Exploit
    C. Threat
    D. Vulnerability

Solution: Attack

85. Which of these is the best example of why administration of systems is so important to security?
    A. Administrators have more privilege than other users
    B. Administrators are responsible for password creation
    C. The bulk of attacks can be blocked by a properly administered firewall
    D. The bulk of attacks are against vulnerabilities for which there are patches available

Solution: The bulk of attacks are against vulnerabilities for which there are patches available

86. For a bank website, what kind of checking of identity should the certificate authority do (ideally)?
    A. Go to the banks website to validate their information
    B. Make a phone call to the head of the banks Website division
    C. Go to a bank branch in person and get bank details from a manager
    D. Go to the bank headquarters and verify details in person with the CEO and the top Website people

Solution: Go to the bank headquarters and verify details in person with the CEO and the top Website people

87. A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
    A. System security plan
    B. Security policy
    C. Rules based enforcement
    D. Authentication and Authorization

Solution: Security policy

88. If our main concern is confidentiality of data from a hostile countrys hackers, we should be most concerned about what type of attack?
    A. Active insider attack
    B. Passive insider attack
    C. Active outsider attack
    D. Passive outsider attack

Solution: Active outsider attack

89. Asymmetric encryption does not provide
    A. Confidentiality
    B. Integrity

C. Availability

Solution: Availability