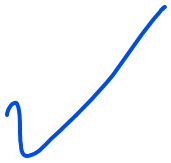
QUIZ 1

Question 1

To mitigate the security risk to your system, you need to

- Increase the surface of defense
- Use the layering architecture
- Increase the surface of defense
- Use the defense in depth strategy and reduce the attack surfaces.



Question 2

The confidentiality of the asset involves

- The correct working of the system
- Only the privacy of the legitimate users.
- Only the encryption of the data.
- Data confidentiality and Privacy

Question 3

Which statement is false?

- Computer security is protection of the integrity, availability, and confidentiality of information system resources
- The more critical a component or service the higher the level of availability required
- Assurance is the process of examining a computer product or system with respect to certain criteria
- The first step in devising security services and mechanisms is to develop a security policy

Question 4

The main principle of security system design is

- Use of multiple overlapping protection approaches
- All of the other options
- Every user should operate with the least set of privileges necessary to perform the task.
- Access decisions based on permissions rather than exclusions

Question 5

When there is a security breach an impact of moderate level result in

- All of the other options
- Significant financial loss
- Significant harm to individuals that does not involve loss of life or serious, life-threatening injuries
- Significant damage to organizational assets

Question 6

The attack that causes unauthorized disclosure of the asset is

- M Masquerade attack
- Misuse attack
- Inference attack
- Corruption attack

– exposure
– interception
– intrusion

other answers

Question 7

which statement is true?

- Security mechanisms typically do not involve more than one particular algorithm or protocol.
- In the context of security our concern is with the vulnerabilities of system resources
- Threats are attacks carried out
- Assurance is the process of examining a computer product or system with respect to certain criteria

Question 8

The system integrity means that

- The stem is available to legitimate users
- The data encrypted
- Only authorized users are allowed to work on the
- The system is working as it should be and the data not tampered with

Question 9

What are the main objectives of any security system?

- To allow users to access the asset
- To ensure the confidentiality, integrity, and the availability of the asset.
- To prevent all users to access the data
- To find a way to distribute the security keys

Question 10

An active attack can be in the form of

- Traffic analysis
- Reply attack
- Inference attack
- All the other options

QUIZ 2

Question 1

For general-purpose block-oriented transmission you would typically use

- CBC
- CTR
- CFB
- OFB

Question 2

Which statement is false?

- SHA-1 is considered to be very secure.
- The one-way hash function is important not only in message authentication but also in digital signatures,
- SHAIS perhaps the most widely used family of hash function
- SH-2 shares the same structure and mathematical operations as its predecessors, and this is a cause for concern

Question 3

If the only form of attack that could be made on an encryption algorithm is brute force, then the way to counter such attacks would be to

- use less keys
- one more keys
- use shorter keys
- use longer key

Question 4

attacks have several approaches, all equivalent in effort to factoring the product of two primer

- Brute force
- Mathematical
- Chosen cipher text
- Timing

Question 5

The ____ scheme has reigned supreme as the most widely accepted and implemented approach to public key encryption

- SHA-1
- HMAC
- RSA
- MDS

Question 6

___ Is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n

- SHA
- RSA
- MES
- AES

Question 7

Which statement is true?

- AES uses a Feistel structure
- Stream ciphers are far more common than block ciphers
- The ciphertext only attack is the easiest to defend again.
- “Each block of 64 plaintext bits is encoded independently using the same key” is a description of the CBC mode of operation

Question 8

____ is a procedure that allows communicating parties to verify that received or stored messages are authentic

- Collision resistance
- Cryptanalysis
- Message authentication
- Decryption

Question 9

The exact substitutions and transformations performed by the algorithm depend on the

- secret key
- ciphertext
- decryption algorithm
- encryption algorithm

Question 10

Cryptographic systems are generically classified by

- the way in which the plaintext is processed
- All of the other options
- the type of operations used for transforming plaintext to cipher text
- the number of keys used

QUIZ 3

A ___ attack involves an adversary repeating a previously captured user response

- Trojan horse
- Denial-of-service
- replay
- eavesdropping

Question 2

A loss of ____ is the unauthorized disclosure of information

- Integrity
- Availability
- confidentiality
- authenticity

Question 3

control access based on comparing security labels with security clearances

- DAC
- MAC
- RBAC
- ABAC

Question 4

is the traditional method of implementing access control.

- DAC ← correct!
- ABAC
- MAC

Question 5

A ____is when an adversary attempts to achieve user authentication without access to the remote host or to the intervening communications path

- Trojan horse attack
- host attack
- eavesdropping attack
- client attack

Question 6

implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

- Resource control
- Audit control
- System control
- Access control

Question 7

strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords

- computer-generated password
- proactive password checking
- reactive password checking
- user education

Question 8

is based on the roles the users assume in a system rather than the user's identity

- RBAC
- MAC
- ADAC
- DAC

Question 9

To counter threats to remote user authentication systems generally rely on some form of protocol

- Trojan horse
- challenge-response
- denial-of-service
- eaves drooping

Question 10

The purpose of a ____ Is to produce a "fingerprint of a file message, or other block of data.

- hash function
- digital signature
- secret key
- keystream

Midterm Review Questions

Multiple Choice

_____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- Availability
- System Integrity
- Privacy
- Data Integrity

A _____ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- low
- normal
- moderate
- high

A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources

- passive attack
- inside attack
- outside attack
- active attack

The _____ prevents or inhibits the normal use or management of communications facilities.

- passive attack
- traffic encryption
- denial of service
- masquerade

The assurance that data received are exactly as sent by an authorized entity is _____

- authentication
- data confidentiality

- Access control
- data integrity

The _____ is the encryption algorithm run in reverse.

- decryption algorithm
- plaintext
- ciphertext
- encryption algorithm

The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the _____.

- SHA
- RSA
- AES
- DSS

Digital signatures and key management are the two most important applications of _____ encryption.

- private-key
- public-key
- preimage resistant
- advanced

Each individual who is to be included in the database of authorized users must first be _____ in the system.

- verified
- authenticated
- identified
- enrolled

True or False – ALL FALSE

1.The “A” in the CIA triad stands for “authenticity”.

2.Security mechanisms typically do not involve more than one particular algorithm or protocol.

3.The advantage of a stream cipher is that you can reuse keys.

4.User authentication is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.

5.An individual’s signature is not unique enough to use in biometric applications.

True or False – ALL TRUE

1.The first step in devising security services and mechanisms is to develop a security policy.

2.Symmetric encryption is used primarily to provide confidentiality.

3.The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

4.An important element in many computer security services and applications is the use of cryptographic algorithms.

5.A good technique for choosing a password is to use the first letter of each word of a phrase.

6.Depending on the application, user authentication on a biometric system involves either verification or identification.

Chapter 1 – Computer Systems Overview

TRUE/FALSE QUESTIONS:

T F 1. Threats are attacks carried out.

T F 2. Computer security is protection of the integrity, availability, and confidentiality of information system resources.

T F 3. Data integrity assures that information and programs are changed only in a specified and authorized manner.

T F 4. Availability assures that systems works promptly and service is not denied to authorized users.

T F 5. The "A" in the CIA triad stands for "authenticity".

T F 6. The more critical a component or service, the higher the level of availability required.

T F 7. Computer security is essentially a battle of wits between a perpetrator who tries to find holes and the administrator who tries to close them.

T F 8. Security mechanisms typically do not involve more than one particular algorithm or protocol.

T F 9. Many security administrators view strong security as an impediment to efficient and user-friendly operation of an information system.

T F 10. In the context of security our concern is with the vulnerabilities of system resources.

T F 11. Hardware is the most vulnerable to attack and the least susceptible to automated controls.

T F 12. Contingency planning is a functional area that primarily requires computer security technical measures.

T F 13. X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.

T F 14. The first step in devising security services and mechanisms is to develop a security policy.

T F 15. Assurance is the process of examining a computer product or system with respect to certain criteria.

MULTIPLE CHOICE QUESTIONS:

1. Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

   A. Availability
   B. System Integrity
   C. Privacy
   D. Data Integrity

2. _____ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

   A. System Integrity
   B. Data Integrity
   C. Availability
   D. Confidentiality

3. A loss of _____ is the unauthorized disclosure of information.

   A. confidentiality
   B. integrity
   C. authenticity
   D. availability

4. A _____ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

   A. low
   B. normal
   C. moderate
   D. high

5. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy is a(n) _____.

   A. countermeasure
   B. vulnerability
   C. adversary
   D. risk

6. An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n) _____.

   A. risk
   B. asset
   C. attack
   D. vulnerability

7. A(n) _____ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action can be taken.

A. attack B. countermeasure

C. adversary D. protocol

8. A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources.

A. passive attack B. inside attack

C. outside attack D. active attack

9. Masquerade, falsification, and repudiation are threat actions that cause _____ threat consequences.

A. unauthorized disclosure B. deception

C. disruption D. usurpation

10. A threat action in which sensitive data are directly released to an unauthorized entity is _____.

A. corruption B. disruption

C. intrusion D. exposure

11. An example of _____ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.

A. masquerade B. interception

C. repudiation D. inference

12. The _____ prevents or inhibits the normal use or management of communications facilities.

A. passive attack B. traffic encryption

C. denial of service D. masquerade

13. A _____ is any action that compromises the security of information owned by an organization.

A. security mechanism B. security attack

C. security policy D. security service

14. The assurance that data received are exactly as sent by an authorized entity is _____.

A. authentication B. data confidentiality

C. access control D. data integrity

15. _____ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

A. Traffic padding B. Traffic routing

C. Traffic control D. Traffic integrity

SHORT ANSWER QUESTIONS:

1. _____ is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

2. Confidentiality, Integrity, and Availability form what is often referred to as the _____.

3. A loss of _____ is the disruption of access to or use of information or an information system.

4. In the United States, student grade information is an asset whose confidentiality is regulated by the _____.

5. A(n) _____ is a threat that is carried out and, if successful, leads to an undesirable violation of security, or threat consequence.

6. A(n) _____ is any means taken to deal with a security attack.

7. Misappropriation and misuse are attacks that result in _____ threat consequences.

8. The assets of a computer system can be categorized as hardware, software, communication lines and networks, and _____.

9. Release of message contents and traffic analysis are two types of _____ attacks.

10. Replay, masquerade, modification of messages, and denial of service are example of _____ attacks.

11. Establishing, maintaining, and implementing plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations is a _____ plan.

12. A(n) _____ assessment is periodically assessing the risk to organizational operations, organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission or organizational information.

13. The OSI security architecture focuses on security attacks, _____, and services.

14. A _____ is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

15. Security implementation involves four complementary courses of action: prevention, detection, response, and _____.

Chapter 1 – Computer Systems Overview

Answer Key

TRUE/FALSE QUESTIONS:

1. F
2. T
3. T
4. T
5. F
6. T
7. T
8. F
9. T
10. T
11. T
12. F
13. T
14. T
15. F

MULTIPLE CHOICE QUESTIONS:

1. C
2. A
3. A
4. D
5. B
6. C
7. B
8. A
9. B
10. D
11. A
12. C
13. B
14. D
15. A

SHORT ANSWER QUESTIONS:

1. Computer Security
2. CIA triad
3. availability
4. FERPA (Family Educational Rights and Privacy Act)
5. attack
6. countermeasure
7. usurpation
8. data
9. passive
10. active
11. contingency
12. risk
13. mechanisms
14. digital signature
15. recovery

Chapter 2 – Cryptographic Tools

TRUE/FALSE QUESTIONS:

T F 1. Symmetric encryption is used primarily to provide confidentiality.

T F 2. Two of the most important applications of public-key encryption are digital signatures and key management.

T F 3. Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

T F 4. The secret key is input to the encryption algorithm.

T F 5. Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits.

T F 6. Modes of operation are the alternative techniques that have been developed to increase the security of symmetric block encryption for large sequences of data.

T F 7. The advantage of a stream cipher is that you can reuse keys.

T F 8. A message authentication code is a small block of data generated by a secret key and appended to a message.

T F 9. Like the MAC, a hash function also takes a secret key as input.

T F 10. The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

T F 11. Public-key cryptography is asymmetric.

T F 12. Public-key algorithms are based on simple operations on bit patterns.

T F 13. The purpose of the DSS algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

T F 14. An important element in many computer security services and applications is the use of cryptographic algorithms.

T F 15. Some form of protocol is needed for public-key distribution.

MULTIPLE CHOICE QUESTIONS:

1. The original message or data that is fed into the algorithm is _____.

   A. encryption algorithm B. secret key

   C. decryption algorithm D. plaintext

2. The _____ is the encryption algorithm run in reverse.

   A. decryption algorithm B. plaintext

   C. ciphertext D. encryption algorithm

3. _____ is the scrambled message produced as output.

   A. Plaintext B. Ciphertext

   C. Secret key D. Cryptanalysis

4. On average, _____ of all possible keys must be tried in order to achieve success with a brute-force attack.

   A. one-fourth B. half

   C. two-thirds D. three-fourths

5. The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the _____.

   A. SHA B. RSA

   C. AES D. DSS

6. If the only form of attack that could be made on an encryption algorithm is brute-force, then the way to counter such attacks would be to _____ .

   A. use longer keys B. use shorter keys

   C. use more keys D. use less keys

7. _____ is a procedure that allows communicating parties to verify that received or stored messages are authentic.

A. Cryptanalysis B. Decryption

C. Message authentication D. Collision resistance

8. The purpose of a _____ is to produce a "fingerprint" of a file, message, or other block of data.

A. secret key B. digital signature

C. keystream D. hash function

9. _____ is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.

A. DSS B. RSA

C. SHA D. AES

10. A _____ is created by using a secure hash function to generate a hash value for a message and then encrypting the hash code with a private key.

A. digital signature B. keystream

C. one way hash function D. secret key

11. Transmitted data stored locally are referred to as _____ .

A. ciphertext B. DES

C. data at rest D. ECC – elliptic curve cryptography

12. Digital signatures and key management are the two most important applications of _____ encryption.

A. private-key B. public-key

C. preimage resistant D. advanced

13. A _____ is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

A. mode of operation
B. hash function
C. cryptanalysis
D. brute-force attack

14. Combined one byte at a time with the plaintext stream using the XOR operation, a _____ is the output of the pseudorandom bit generator.

A. keystream
B. digital signature
C. secure hash
D. message authentication code

15. A _____ protects against an attack in which one party generates a message for another party to sign.

A. data authenticator
B. strong hash function
C. weak hash function
D. digital signature

SHORT ANSWER QUESTIONS:

1. Also referred to as single-key encryption, the universal technique for providing confidentiality for transmitted or stored data is _____ .

2. There are two general approaches to attacking a symmetric encryption scheme: cryptanalytic attacks and _____ attacks.

3. The _____ algorithm takes the ciphertext and the secret key and produces the original plaintext.

4. A _____ attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

5. A _____ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.

6. A _____ processes the input elements continuously, producing output one element at a time.

7. Public-key encryption was first publicly proposed by _____ in 1976.

8. The two criteria used to validate that a sequence of numbers is random are independence and _____ .

9. A _____ is a hardware device that sits between servers and storage systems and encrypts all data going from the server to the storage system and decrypts data going in the opposite direction.

10. In July 1998 the _____ announced that it had broken a DES encryption using a special purpose "DES cracker" machine.

11. The simplest approach to multiple block encryption is known as _____ mode, in which plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key.

12. A _____ stream is one that is unpredictable without knowledge of the input key and which has an apparently random character.

13. The _____ is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.

14. _____ is provided by means of a co-processor board embedded in the tape drive and tape library hardware.

15. The purpose of the _____ algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

Terms in this set (22)

T	Access control is the central element of computer security.
T	An auditing function monitors and keeps a record of user accesses to system resources.
T	The principal objectives of computer security are to prevent unauthorized users from gaining access to resources, to prevent legitimate users from accessing resources in an unauthorized manner, and to enable legitimate users to access resources in an authorized manner.
T	A user may belong to multiple groups.
T	An access right describes the way in which a subject may access an object.
F	Traditional RBAC systems define the access rights of individual users and groups of users.
Access control	1. _____ implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

Authentication	_____ is verification that the credentials of a user or other system entity are valid.	★
Authorization	_____ is the granting of a right or permission to a system entity to access a system resource.	★
DAC	_____ is the traditional method of implementing access control.	★
MAC	_____ controls access based on comparing security labels with security clearances.	★
mandatory access control	A concept that evolved out of requirements for military information security is ____ .	★
subject	A _____ is an entity capable of accessing objects.	★
object	A(n) _____ is a resource to which access is controlled.	★
RBAC	_____ is based on the roles the users assume in a system rather than the user's identity.	★
role	A _____ is a named job function within the organization that controls this computer system	★

Constraints	_____ provide a means of adapting RBAC to the specifics of administrative and security policies in an organization.
Cardinality	_____ refers to setting a maximum number with respect to roles.
ABAC	Subject attributes, object attributes and environment attributes are the three types of attributes in the _____ model.
access management	The _____ component deals with the management and control of the ways entities are granted access to resources.
Object	The basic elements of access control are: subject, _____, and access right.
Environment	The three types of attributes in the ABAC model are subject attributes, object attributes, and _____ attributes.

THIS SET IS OFTEN IN FOLDERS WITH...

Chapter 4 - Access Control (Computer Security...

39 terms

Computer Security: Principles and Practice (4...

34 terms