UCLA CCLE

Winter 2021 - COM SCI136-1 - REIHER

Started on	Tuesday, 9 February 2021, 7:57 AM PST
State	Finished
Completed on	Tuesday, 9 February 2021, 9:06 AM PST
Time taken	1 hour 8 mins
Grade	**88.00** out of 100.00

Question **1**

Incorrect

0.00 points out of 4.00

Let P be the set of all states of a system, R be the set of states a particular security mechanism allows the system enter, and Q be the set of all secure states in the system as defined by the system's security policy. If there is a state r that is a member of P and R, and r is not a member of Q, which of the following describes the security mechanism?

a. The security mechanism is secure

b. The security mechanism matches the security policy

c. The security mechanism is narrow ✖

d. The security mechanism is broad

e. The security mechanism is precise

Your answer is incorrect.

The correct answer is:
The security mechanism is broad

Correct

4.00 points out of 4.00

What is the purpose of a shadow password file?

- a. To prevent non-privileged users from accessing some password-related information ✔
- b. To allow the use of salting in password storage
- c. To allow the system to send users plaintext versions of passwords they have forgotten
- d. To permit storage of passwords in encrypted forms
- e. To deceive attackers into trying to crack fake passwords

Your answer is correct.

The correct answer is:

To prevent non-privileged users from accessing some password-related information

Question **3**

Correct

4.00 points out of 4.00

Which of the following is an example of a covert channel?

- a. Sending data between two machines encrypted with the receiver's public key
- b. A tamper-resistant hardware link between two computers that is only usable by the computers' trusted processes
- c. Sending data between two machines encrypted with the sender's private key
- d. Diffie-Hellman key exchange
- e. Sending information between two processes by adjusting the time slice behavior of the sender ✔

Your answer is correct.

The correct answer is:
Sending information between two processes by adjusting the time slice behavior of the sender

Correct

4.00 points out of 4.00

For a commercial system trying to provide separation of function, which of the following is likely to be true?

a. Different security mechanisms will be used in each part of the system

b. The system will use the Bell-LaPadula security model

c. Strong barriers will be placed between users working for different clients who are competitors

d. Critical security functions will require at least two different users to take action

e. New software will not be developed on production systems ✔

Your answer is correct.

The correct answer is:

New software will not be developed on production systems

Question **5**

Correct

4.00 points out of 4.00

Which of the following is the best example of transitive trust?

a. Using cipher block chaining to protect a data transmission containing multiple packets

b. Using virtual memory techniques to prevent a process from accessing another process' memory

c. TPM used by the OS to sign the validity of a particular version of an application ✔

d. The Biba integrity security model

e. Using nonces to defeat a replay attack

Your answer is correct.

The correct answer is:
TPM used by the OS to sign the validity of a particular version of an application

Correct

4.00 points out of 4.00

Which of the following is the best example of a phishing attack?

a. Using a buffer overflow to take over a web server

b. A forged email saying that you need use a particular web site to reset your password ✔

c. Leaving a flash drive infected with malware lying in a parking lot

d. Performing a man-in-the-middle attack on Internet commerce

e. An email message trying to sell you a product you don't want

Your answer is correct.

The correct answer is:
A forged email saying that you need use a particular web site to reset your password

Question **7**

Correct

4.00 points out of 4.00

Which of the following is the best example of fail safe design?

a. A reverse firewall that only permits outgoing packets to a set of trusted IP addresses ✔

b. Data execution prevention

c. Exclusively using open source libraries in one's software products

d. Using timestamps in a cryptographic protocol

e. SYN cookies

Your answer is correct.

The correct answer is:
A reverse firewall that only permits outgoing packets to a set of trusted IP addresses

Correct

4.00 points out of 4.00

Which of the following is an important element of PGP?

a. Use of symmetric cryptography for authentication

b. Reliance on a limited set of well known signing authorities

c. Freedom from chains of trust

d. Embedding trust information in a digital signature ✔

e. Protection against denial of service attacks

Your answer is correct.

The correct answer is:
Embedding trust information in a digital signature

Question 9

Correct

4.00 points out of 4.00

Which of the following approaches would be helpful in detecting that a piece of ciphertext was encrypted using only permutation techniques?

a. Attacking the random number generator used to create the key

b. The Kasiski method

c. The Index of coincidence method

d. Finding repeated patterns of symbols in the cipher text

e. Examining the frequency distributions of the encrypted data ✔ Permutation ciphers do not change the frequency distribution of the plaintext symbols

Your answer is correct.

The correct answer is:
Examining the frequency distributions of the encrypted data

Correct

4.00 points out of 4.00

What kind of security system does a type flaw attack typically operate against?

a. A system for defending against DDoS attacks
b. A randomization method for key selection
c. An ASLR system combating buffer overflows
d. A capability-based access control system
e. A cryptographic protocol ✔

Your answer is correct.

The correct answer is:
A cryptographic protocol

Question **11**

Correct

4.00 points out of 4.00

What aspect of TCP does a SYN flood attack try to misuse?

a. Interfaces between TCP and IP
b. Limited size of open connection tables at a server ✔
c. TCP's use of sequence numbers
d. TCP slow start
e. TCP's exponential backoff feature

Your answer is correct.

The correct answer is:
Limited size of open connection tables at a server

Correct

4.00 points out of 4.00

What kind of attack does padding typical help defeat?

- a. An attack on Diffie-Hellman key exchange
- b. A replay attack
- c. A DDoS attack
- d. A traffic analysis attack ✔
- e. A man-in-the-middle attack

Your answer is correct.

The correct answer is:
A traffic analysis attack

Question 13

Incorrect

0.00 points out of 4.00

Deep packet inspection is likely to be used in which of the following defenses?

- a. An ingress filtering system
- b. An onion routing system
- c. A filtering gateway ✖
- d. A proxy gateway
- e. A SYN cookie system

Your answer is incorrect.

The correct answer is:
A proxy gateway

Correct

4.00 points out of 4.00

Which of the following approaches helps a security protocol avoid the suppress-replay attack when timestamps are used in the protocol?

a. Including multiple timestamps in all messages
b. Using asymmetric cryptography in the protocol
c. Using symmetric cryptography in the protocol
d. Ensuring all parties in the protocol are authenticated
e. Always using timestamps from a single clock ✔

Your answer is correct.

The correct answer is:
Always using timestamps from a single clock

Question **15**

Correct

4.00 points out of 4.00

Why have modern GPUs caused problems with the use of passwords for authentication?

a. They make dictionary attacks easier ✔
b. They make password salting impossible
c. GPUs cannot authenticate users via passwords
d. They can intercept and divulge passwords when they are created
e. They limit possible choices of passwords

Your answer is correct.

The correct answer is:
They make dictionary attacks easier

Correct

4.00 points out of 4.00

Node A is sending a large quantity of data to node B over the network. They are encrypting the data with AES, using ECB mode. A network error flips one bit in the encrypted version of block N. Which blocks will be improperly deciphered at B due to the bit flip?

a. Block N-1, block N, and block N+1

b. All blocks in the same packet as block N

c. Block N and block N+1

d. Block N and all subsequent blocks

e. Block N ✔

Your answer is correct.

The correct answer is:
Block N

Question **17**

Correct

4.00 points out of 4.00

Which of the following changes to the basic Chinese Wall policy does the aggressive Chinese Wall policy add?

a. Adding integrity controls to confidentiality controls

b. Ability to apply the model in a distributed environment

c. A generalization of the conflict of interest classes ✔

d. More precise inspection of operations on objects controlled by the policy

e. Applicability to system objects, in addition to user level objects

Your answer is correct.

The correct answer is:
A generalization of the conflict of interest classes

Correct

4.00 points out of 4.00

In the context of computer security, what is OCTAVE?

- a. A framework to self-assess security of a system ✔
- b. A DDoS defense tool
- c. An access control policy
- d. A mechanism for reporting security flaws in software
- e. A firewall

Your answer is correct.

The correct answer is:
A framework to self-assess security of a system

Question **19**

Correct

4.00 points out of 4.00

Your company backs up its critical data on tapes, which are stored in a remote facility. Which of the following is the best technology to protect the data on the backup tapes?

- a. DES
- b. AES ✔
- c. RSA
- d. SHA 256
- e. Elliptic curve cryptography

Your answer is correct.

The correct answer is:
AES

Correct

4.00 points out of 4.00

Which of the following is an advantage polyalphabetic substitution ciphers have over monoalphabetic substitution ciphers?

- a. Polyalphabetic ciphers make frequency analysis harder ✔
- b. Polyalphabetic ciphers offer better diffusion properties
- c. Polyalphabetic ciphers are safe against use of index of coincidence cryptanalytic methods
- d. Polyalphabetic ciphers offer better perfect forward secrecy
- e. Polyalphabetic ciphers use simpler key creation methods

Your answer is correct.

The correct answer is:
Polyalphabetic ciphers make frequency analysis harder

Question **21**

Correct

4.00 points out of 4.00

In the context of use of cryptography, what is meant by a round?

- a. The period after which a new key must be established
- b. The period over which feedback is applied in use of a cryptographic mode
- c. One of several repeated operations as part of a cipher ✔
- d. An exchange of messages in a cryptographic protocol
- e. The steps in negotiating the cipher and other properties of an encrypted session

Your answer is correct.

The correct answer is:
One of several repeated operations as part of a cipher

Correct

4.00 points out of 4.00

In the context of computer security, what is the difference between a weakness and a vulnerability?

a. A weakness is a more serious security problem than a vulnerability

b. There is no meaningful difference between these terms

c. A weakness is a system flaw with no security implications, while a vulnerability is a flaw with security implications

d. A weakness is a vulnerability that can be exploited

e. A vulnerability is a weakness that can be exploited ✔

Your answer is correct.

The correct answer is:

A vulnerability is a weakness that can be exploited

Question **23**

Incorrect

0.00 points out of 4.00

Which of the following is true of identity-based encryption?

a. The only secrets required by such a system are the secret keys ✖ Another secret is used to derive the keys

b. It uses symmetric cryptography

c. It does not require trusted third parties

d. It can provide key escrow services

e. It can be based on RSA

Your answer is incorrect.

The correct answer is:

It can provide key escrow services

Correct

4.00 points out of 4.00

Which of the following operations is easy to perform in a capability-based access control system?

a. Determining the entire set of subjects that can access an object

b. Taking access permissions away from a user in a distributed system

c. Determining the entire set of objects that a subject can access ✔ Just examine the subject's capabilities

d. Ensuring proper access control when subjects and objects are located in different nodes of a network

e. Changing a remote user's ability to access a local resource

Your answer is correct.

The correct answer is:
Determining the entire set of objects that a subject can access

Question **25**

Correct

4.00 points out of 4.00

Which of the following is true of IPSec?

a. It includes procedures for key distribution

b. It can only be used to provide message confidentiality

c. It only works with IPv4

d. Its transport mode encrypts only the payload of an IP packet ✔

e. It can be used to provide availability

Your answer is correct.

The correct answer is:
Its transport mode encrypts only the payload of an IP packet

◄ Sample midterm exam answer ...

Jump to...

Lecture 11: Intrusion ... ►