Winter 2021 - COM SCI136-1 - REIHER

Started on	Wednesday, 17 March 2021, 11:07 AM PDT
State	Finished
Completed on	Wednesday, 17 March 2021, 12:23 PM PDT
Time taken	1 hour 15 mins
Grade	**81.00** out of 99.00 (**82**%)

Question **1**

Incorrect

0.00 points out of 3.00

In which of the following cases would link level encryption be a better solution than end-to-end encryption, where the endpoints are the originating client and destination server?

a. When communicating to sites that use HSTS

b. When using wireless networks

✖ While also worthwhile to use link encryption across the wireless network, also encrypting end-to-end offers better protection

c. When crossing a DMZ boundary

d. In distributed caching systems in an ISP

e. When using IPSec

Your answer is incorrect.

The correct answer is:
In distributed caching systems in an ISP

Question **2**

Correct

3.00 points out of 3.00

Which of the following is an example of the use of confinement in system security?

- a. Password salting
- b. AES
- c. A biometric authentication mechanism
- d. A compiler for a type safe programming language ✔
- e. SYN cookies

Your answer is correct.

The correct answer is:
A compiler for a type safe programming language

Question **3**

Correct

3.00 points out of 3.00

Which of the following pairs of desirable cipher characteristics are most likely to conflict with each other?

- a. Non-propagation of errors and diffusion ✔ Diffusion spreads information through the encrypted text, making an error more likely to propagate
- b. Ciphertext size matching plaintext size and simplicity of implementation
- c. Confusion and non-propagation of errors
- d. Confusion and ciphertext size matching plaintext size
- e. Simplicity of implementation and diffusion

Your answer is correct.

The correct answer is:
Non-propagation of errors and diffusion

Question **4**

Correct

3.00 points out of 3.00

What is the security relationship to the concept of variable synchronization?

- a. Mis-synchronized variables can lead to exploitable inconsistencies ✔
- b. Variable synchronization is necessary to ensure proper use of ASLR
- c. Variable synchronization allows attackers to predict cryptographic key selection
- d. Variable synchronization is used to control fuzz testing of computer systems
- e. Variable synchronization prevents CSRF attacks

Your answer is correct.

The correct answer is:
Mis-synchronized variables can lead to exploitable inconsistencies

Question **5**

Incorrect

0.00 points out of 3.00

Which of the following is necessary for a persistent cross-site scripting attack to succeed?

- a. The attacker must intercept a user request for a legitimate web site and redirect it to a malicious site
- b. A third party web site must store the attacker's script and make it available for download
- c. A user must click on a link crafted by the attacker that contains a malicious script
- d. The attacker must be able to inject malicious content into a query being built by a web site ✖
- e. A user must be deceived into visiting a malicious web site

Your answer is incorrect.

The correct answer is:
A third party web site must store the attacker's script and make it available for download

Question 6

Correct

3.00 points out of 3.00

What benefit do users gain from Tor that they do not get from simple anonymizers?

a. None of the Tor machines know who the senders and receivers are ✔ Traditional anonymizers know who sent and received things

b. Eavesdroppers cannot detect that an end user is working with Tor, while they could detect use of simpler anonymizes

c. Tor does not require the extra overheads of cryptography

d. Tor uses more efficient routing than the triangle routing implicit in simpler anonymizes

e. Tor uses much less total bandwidth to send messages than simpler anonymizers do

Your answer is correct.

The correct answer is:
None of the Tor machines know who the senders and receivers are

Question 7

Correct

3.00 points out of 3.00

In the context of computer security, what is meant by the term fast flux?

a. Frequently reconfiguring botnets to change their peering relationships

b. Quickly changing the characteristics of a DDoS attack to keep ahead of defenses

c. Designing code to perform rapid attempts to exploit a race condition

d. Frequent updates to an intrusion detection system to keep up with new attacks

e. Rapidly changing a DNS translation for one name to one of several IP addresses ✔

Your answer is correct.

The correct answer is:
Rapidly changing a DNS translation for one name to one of several IP addresses

Question 8

Correct

3.00 points out of 3.00

What's strict about HTTP Strict Transport Security?

- a. A web site running it will require browsers to use HTTPS ✔
- b. No third party cookies may be downloaded to users
- c. No scripts may be downloaded
- d. Only AES can be used for encryption
- e. A browser running it will require web sites to use HTTPS

Your answer is correct.

The correct answer is:
A web site running it will require browsers to use HTTPS

Question 9

Correct

3.00 points out of 3.00

What is the generation effect as relates to passwords?

- a. If permitted, people tend to reuse the same password for multiple purposes
- b. Systems requiring periodic changes of passwords result in users cycling through a small number of different passwords
- c. Passwords that have been used for a particular purpose for a long period of time are less safe
- d. Passwords users choose for themselves are easier for attackers to guess than those generated by algorithms
- e. Passwords users choose for themselves are more memorable than those generated by algorithms ✔

Your answer is correct.

The correct answer is:
Passwords users choose for themselves are more memorable than those generated by algorithms

Question **10**

Correct

3.00 points out of 3.00

If I wish to conceal the volume and patterns of my network traffic from eavesdroppers, which of the following approaches will be most effective?

- a. Source address filtering
- b. Padding ✔
- c. IPSec in transport mode
- d. Firewalls
- e. TLS

Your answer is correct.

The correct answer is:
Padding

Question **11**

Correct

3.00 points out of 3.00

What is the core element that so-called "trusted computing systems," such as the Trusted Platform Module, rely on?

- a. Hardware designed to ensure trust ✔
- b. Formal analysis of a security design
- c. Extensive testing of the system in question
- d. Careful operating system design
- e. Use of high quality cryptography

Your answer is correct.

The correct answer is:
Hardware designed to ensure trust

Question **12**

Correct

3.00 points out of 3.00

What special benefit is gained from an autonomous agent model of IDS systems that traditional models may not have?

a. Ability to consider both network and host events

b. Easy ability to evolve to meet changing conditions

c. Ability to combine anomaly detection and misuse detection techniques

d. Clearer explanations of the reasons an attack was signaled

e. Fault tolerance ✔ Failure of any single component does not cripple this kind of IDS.

Your answer is correct.

The correct answer is:
Fault tolerance

Question **13**

Correct

3.00 points out of 3.00

Which of the following security issues is related to pseudo-random number generators?

a. TCP sequence number initialization ✔ For example, Numberjack

b. DEP

c. Proper choice of cryptographic mode

d. Signature-based malware detection

e. Egress filtering

Your answer is correct.

The correct answer is:
TCP sequence number initialization

Question **14**

Incorrect

0.00 points out of 3.00

Which of the following is an example of complete mediation?

- a. A network design that incorporates a DMZ ✖
- b. Using a fuzz testing tool to detect unsafe input handling
- c. A one time pad encryption algorithm
- d. An intrusion detection system tuned to cause zero false negatives
- e. A firewall checking all entering packets against a white list of IP addresses

Your answer is incorrect.

The correct answer is:
A firewall checking all entering packets against a white list of IP addresses

Question **15**

Correct

3.00 points out of 3.00

Which of the following best describes a stealth virus?

- a. A virus that changes its internal representation to avoid signature detection
- b. A virus that is introduced into systems in stealthy ways
- c. A virus that moves to a new computer before it can be detected on its previous host
- d. A virus that is hidden in a seemingly benign email attachment
- e. A virus that takes active measures to conceal its presence in a system ✔

Your answer is correct.

The correct answer is:
A virus that takes active measures to conceal its presence in a system

Question **16**

Correct

3.00 points out of 3.00

What kind of malware requires use of a C&C channel?

- a. Trojan horses
- b. Logic bombs
- c. Worms
- d. Botnets ✔
- e. Viruses

Your answer is correct.

The correct answer is:
Botnets

Question **17**

Correct

3.00 points out of 3.00

Which of the following is a reason why we do not arbitrarily increase key length in public key algorithms?

- a. Longer key lengths increase the ease of attackers deriving the private key from the public key
- b. Only a maximum number of key bits can be embedded in a public key certificate
- c. Well regarded public key algorithms only work for certain defined key lengths
- d. Longer public keys typically incur greater performance costs for encryption and decryption ✔ Usually the mathematical operations underlying PK take an amount of time dependent on key length
- e. Users cannot be expected to remember very long private keys

Your answer is correct.

The correct answer is:
Longer public keys typically incur greater performance costs for encryption and decryption

Question **18**

Correct

3.00 points out of 3.00

Which of the following defensive technologies will face challenges if the local users visit web sites using HTTPS?

a. Ingress filtering based on IP addresses

b. SYN cookies

c. Secure boot services

d. Diffie-Hellman key exchange

e. Proxy-based firewalls ✔ They won't be able to see into the packets

Your answer is correct.

The correct answer is:
Proxy-based firewalls

Question **19**

Correct

3.00 points out of 3.00

Which of the following reasons describes why the C programming language is regarded as especially dangerous from a computer security perspective?

a. C is slow, making it easier to exploit race conditions

b. C does not bounds check variables ✔

c. C is inherently susceptible to SQL injection attacks

d. C allows use of functions like gets() and scans()

e. C does not support error checking of functions

Your answer is correct.

The correct answer is:
C does not bounds check variables

Question **20**

Incorrect

0.00 points out of 3.00

Why aren't certificates carried in the S-BGP updates?

a. Including certificates would exceed the allowable size of a BGP message

b. S-BGP certificates are only created when checking is required, which might not be when a message is created

c. Those creating S-BGP messages may not be aware of the certificates they should include

d. S-BGP does not require certificates

e. Certificates are not included in standard BGP, so they cannot be included in S-BGP ✖ They could be included as an option without affecting the protocol

Your answer is incorrect.

The correct answer is:
Including certificates would exceed the allowable size of a BGP message

Question **21**

Correct

3.00 points out of 3.00

If a client asks a DNSSEC resolver to provide a lookup for a name that has no assigned IP address, what will the resolver return to the client?

a. A record indicating that a range of names are unassigned, with a signature from the authoritative server ✔

b. An unsigned response indicating that the name in question is unassigned

c. A record indicating that the name in question is unassigned, with a signature from the authoritative server

d. A record indicating that the name in question is unassigned, with a signature from the DNSSEC resolver

e. A record indicating that a range of names are unassigned, with a signature from the DNSSEC resolver

Your answer is correct.

The correct answer is:
A record indicating that a range of names are unassigned, with a signature from the authoritative server

Question **22**

Correct

3.00 points out of 3.00

Anagramming is a technique that is helpful in which of the following security-related operations?

- a. DDoS defense
- b. Voice recognition-based biometric authentication
- c. Analyzing source code for buffer overflows
- d. Attacking transposition ciphers ✔
- e. Performing a brute force attack on salted password files

Your answer is correct.

The correct answer is:
Attacking transposition ciphers

Question **23**

Incorrect

0.00 points out of 3.00

In a typical intrusion detection system architecture, which of the following statements is true of the IDS' director component?

- a. The director obtains logs directly from a data source
- b. The director decides whether to signal an attack
- c. The director presents information to the system administrator in a human-readable format.
- d. The director chooses the type of model to be used in anomaly detection ✖ That's a choice of the designer of the IDS, not of the director.
- e. The director sniffs the network to obtain information about packets being sent and received

Your answer is incorrect.

The correct answer is:
The director decides whether to signal an attack

Question **24**

Correct

3.00 points out of 3.00

Which of the following are true of Kerberos?

- a. Kerberos tickets distribute session keys ✔
- b. Kerberos runs an adjudicated protocol
- c. Kerberos depends on public key cryptography
- d. Kerberos authenticates, but does not distribute keys
- e. Kerberos does not depend on clocks

Your answer is correct.

The correct answer is:
Kerberos tickets distribute session keys

Question **25**

Incorrect

0.00 points out of 3.00

Which of the following problems would a firewall that performs deep packet inspection be likely to detect that a firewall not doing such inspection would not?

- a. Spoofing of local source addresses
- b. Port scanning
- c. Attempts to deliver spam to a mail server ✖ Often handled by IP blacklisting, which does not require deep packet inspection
- d. Exploitation of the Heartbleed bug
- e. Packets coming from a known botnet member

Your answer is incorrect.

The correct answer is:
Exploitation of the Heartbleed bug

Question **26**

Correct

3.00 points out of 3.00

Which of the following types of machines is an enterprise most likely to put in its DMZ, assuming proper use of that network organization?

a. Workstation machines used by employees

b. Laptop computers used by employees

c. A web server ✔ Typically much more accessible by outsiders than other machines

d. The sysadmin's console machine

e. Backup servers

Your answer is correct.

The correct answer is:
A web server

Question **27**

Correct

3.00 points out of 3.00

What do reconstruction attacks target?

a. Reverse firewalls

b. 802.11 encryption methods

c. The privacy of data used by a machine learning system ✔

d. Anomaly-based IDSes

e. Systems using ASLR to prevent buffer overflows

Your answer is correct.

The correct answer is:
The privacy of data used by a machine learning system

Question **28**

Correct

3.00 points out of 3.00

Which of the following statements about Diffie-Hellman key exchange is **incorrect**?

a. Diffie-Hellman is based on properties of exponentiation

b. Diffie-Hellman requires pre-arrangement of some quantities between the partners

c. Diffie-Hellman is used to distribute public keys ✔

d. Diffie-Hellman can exchange a key across an insecure channel with reasonable security

e. Diffie-Hellman is widely used in setting up TLS sessions

Your answer is correct.

The correct answer is:
Diffie-Hellman is used to distribute public keys

Question **29**

Correct

3.00 points out of 3.00

What benefit do we typically hope to obtain by choosing the right cryptographic mode for a communication?

a. Improved uniqueness of the cryptography ✔

b. Greater resilience to timing attacks

c. Effective increase in the key length

d. Concealing the identity of the sender and receiver

e. Easier key distribution

Your answer is correct.

The correct answer is:
Improved uniqueness of the cryptography

Question **30**

Correct

3.00 points out of 3.00

If a web site wants to protect its clients against CSRF attacks, which of the following approaches will be helpful?

a. Not downloading any scripts to its users

b. Using HTTPS for all communications with its users

c. Ensuring that all critical operations require a confirmation from the user ✔ The attacker does not see the confirmation request

d. Encrypting any cookies it provides to its users

e. Using parameterized variables in its SQL queries

Your answer is correct.

The correct answer is:
Ensuring that all critical operations require a confirmation from the user

Question **31**

Correct

3.00 points out of 3.00

Which of the following is helpful in running specification intrusion detection on a computer system?

a. Ongoing observation of changes in behavior of the system

b. Knowledge of a set of discovered vulnerabilities in the system

c. Well defined state transitions in the system ✔ Tells you when to look for problems in the specification

d. Complete logging of all external interactions with the system

e. Statistical models of the behavior of the system

Your answer is correct.

The correct answer is:
Well defined state transitions in the system

Question **32**

Correct

3.00 points out of 3.00

For a biometric authentication system, what is the implication of a false negative reading?

a. A packet was improperly dropped

b. A user who should have been authenticated was not ✔

c. Denial of service on the authentication system

d. Possibility of a buffer overflow in the authentication system

e. A user who should not have been authenticated was.

Your answer is correct.

The correct answer is:
A user who should have been authenticated was not

Question **33**

Correct

3.00 points out of 3.00

What is an attack surface?

a. A description of the set of points from which a DDoS attack has been launched

b. A formalization of the lowest level of an attack tree

c. A description of the methods an attacker uses to attempt to compromise a system or application

d. A description of the ways an attacker can attempt to compromise a system or application ✔

e. The output of a formal security analysis tool applied to a piece of software

Your answer is correct.

The correct answer is:
A description of the ways an attacker can attempt to compromise a system or application

◄ Answer sheet for sample ...

Jump to...