UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2020

Lab Quiz 7

Quiz relates to Lectures 17 and 18. Questions might have been seen in a different order on LEARN.

QUESTION 1

The purpose of the record protocol in TLS is to:

(a) change the cryptographic algorithms from previously used ones

(b) signal events such as failures

(c) set up sessions with the correct keys and algorithms

(d) provide confidentiality and integrity for messages

---

provide confidentiality and integrity for messages

QUESTION 2

The purpose of the handshake protocol in TLS is to:

(a) change the cryptographic algorithms from previously used ones

(b) signal events such as failures

(c) set up sessions with the correct keys and algorithms

(d) provide confidentiality and integrity for application messages

---

set up sessions with the correct keys and algorithms

---

cont/. . .

QUESTION 3

When TLS is used to protect web browser communications with HTTPS, a man-in-the-middle (MITM) attack is possible if an attacker is able to:

(a) masquerade as a network node

(b) add root certificates into the browser

(c) obtain a valid server certificate

(d) alter the hello messages in the TLS handshake

---

add root certificates into the browser

QUESTION 4

Let us consider the following TLS cipher suite: `TLS_RSA_WITH_AES_128_CBC_SHA`. When this cipher suite is chosen, RSA is used:

(a) to sign the server's ephemeral Diffie-Hellman value

(b) to sign the client's ephemeral Diffie-Hellman value

(c) to encrypt the pre-master secret with the server's long-term key

(d) to encrypt the pre-master secret with the client's long-term key

---

to encrypt the pre-master secret with the server's long-term key

---

QUESTION 5

Galois counter mode (GCM) is often used in TLS to provide:

(a) data confidentiality

(b) data integrity

(c) error checking

(d) authenticated encryption

---

authenticated encryption

---

cont/...

QUESTION 6

How is the ciphersuite used in a run of the TLS protocol decided?

(a) It is chosen by the server

(b) It is chosen by the client

(c) It is negotiated between client and server

(d) It is defined by the latest version of TLS

It is negotiated between client and server

QUESTION 7

Which of the following features is not available in TLS 1.3?

(a) Authenticated encryption with associated data

(b) Forward secrecy

(c) Stream ciphersuite

(d) Data compression

Data compression

QUESTION 8

The TLS 1.3 handshake protocol is NOT concerned with:

(a) Session key renewal

(b) Session key confirmation

(c) Public key certificates

(d) Cipher suite renegotiation

Cipher suite renegotiation

---

cont/...

QUESTION 9

When TLS uses authenticated encryption modes, such as CCM or GCM, the additional authenticated data includes:

(a) the session key

(b) the pre-master secret

(c) the peer certificate

(d) the sequence number and header data

---

the sequence number and header data

QUESTION 10

A construction for a message authentication code from any hash function, often used in TLS, is known as:

(a) CMAC

(b) HMAC

(c) SHA-1

(d) GCM

HMAC
