UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 8

Quiz relates to Lectures 19 and 20. Questions might have been seen in a different order on LEARN.

QUESTION 1

A difference between the public key infrastructure used by TLS for web browsers, and that provided by PGP for email security, is:

(a) PGP keys can be signed by any other user

(b) PGP keys are certified in a hierarchical manner

(c) PGP keys have no expiry date

(d) PGP keys can use any type of public key algorithm

PGP keys can be signed by any other user

QUESTION 2

PGP is a security protocol to protect emails in transit. Which of the following statements about PGP is true:

(a) it provides confidentiality of metadata such as email headers

(b) it provides end-to-end security between the sender and recipient

(c) it requires special processing by email servers during email transit

(d) it uses hierarchical digital certificates as also used in HTTPS

---

it provides end-to-end security between the sender and recipient

---

cont/...

QUESTION 3

STARTTLS is a security protocol often used to protect emails in transit. For this purpose:

(a) STARTTLS can provide only client-server security

(b) STARTTLS can provide client privacy

(c) STARTTLS can provide only link-by-link security

(d) STARTTLS can provide client end-to-end security

STARTTLS can provide only link-by-link security

QUESTION 4

STARTTLS is a security protocol often used to protect emails in transit. When used for email protection, STARTTLS:

(a) can protect confidentiality of email contents from malicious mail servers

(b) can provide end-to-end security between the sender and recipient

(c) requires special processing by email clients

(d) can apply cryptographic protection to metadata such as email headers

---

can apply cryptographic protection to metadata such as email headers

---

QUESTION 5

One common way to apply the IPsec protocol uses a gateway-to-gateway architecture. Which of the following statements about this architecture is true?

(a) It is typically used to provide secure remote access from a single host

(b) It is typically used for secure remote management of a single server

(c) It provides protection for data throughout its transit (end-to-end)

(d) It is typically used with IPsec in tunnel mode

It is typically used with IPsec in tunnel mode

---

cont/...

QUESTION 6

One common way to apply the IPsec protocol uses a host-to-host architecture. Which of the following statements about this architecture is true?

(a) It is often used to connect hosts on unsecured networks to resources on secured networks

(b) A typical application is to securely connect two separate secure networks

(c) It provides protection for data throughout its transit (end-to-end)

(d) It is typically used with IPsec in tunnel mode

It provides protection for data throughout its transit (end-to-end)

QUESTION 7

Like TLS, IPSec can be used to set up secure communication between nodes. Which of the following applies to IPSec, but not to TLS?

(a) Different suites of cryptographic algorithms can be used.

(b) Traffic flow confidentiality may be provided.

(c) Forward secrecy may be provided using Diffie-Hellman key exchange.

(d) The protocol specification defines both key establishment and security of user data.

Traffic flow confidentiality may be provided.

QUESTION 8

Transport mode is generally used in:

(a) host-to-host architectures

(b) gateway-to-gateway architectures

(c) host-to-gateway architectures

(d) gateway-to-host architectures

---

host-to-host architectures

---

cont/...

QUESTION 9

POP and IMAP are mail access protocols to let:

(a) a MUA download an email from a MTA.

(b) a MUA upload an email to a MTA.

(c) a MTA download an email from a MUA.

(d) a MTA upload an email to a MUA.

---

a MUA download an email from a MTA.

QUESTION 10

DKIM is:

(a) a specification for cryptographically signing email messages.

(b) a policy-based specification describing how emails should be handled.

(c) a protocol to allow X.509 certificates to be bound to DNS names.

(d) a directory lookup service providing a maaping between host name and IP address.

---

a specification for cryptographically signing email messages.
