CSS 322 – QUIZ 6 ANSWERS

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

Question 1 [5 marks]

Multiple choice. Select the most accurate answer. Choose only one. You receive 1 mark for a correct answer. You lose 0.5 marks for an incorrect answer. 0 marks for an unanswered question.

a) If Transport Layer Security is used to secure data (e.g. web pages) between a client and server, TLS uses:

   a. Public key algorithms for data confidentiality and MD5 or SHA1 for data integrity

   b. Message authentication codes for data integrity and symmetric key algorithms for data confidentiality

   c. Symmetric key algorithms for key exchange and message authentication codes for authentication

   d. Public key algorithms for key exchange and Diffie-Hellman for data integrity

Correct answer: (b)

Option (a) is incorrect because public key algorithms are not used for confidentiality (only for the key exchange and certificates)

Option (b) is correct – MAC and symmetric key are used in TLS.

Option (c) is incorrect because symmetric key is not used for key exchange (you need to exchange a key before you do symmetric key)

Option (d) is incorrect because Diffie Hellman is not used for integrity (its used for key exchange).

b) When using the Authentication Header (AH) in IPsec (transport mode) and sending a FTP message, which of the following pieces of information are authenticated:

   a. The source and destination fields in the IP header

   b. The entire IP, TCP and FTP headers

   c. The entire IP and TCP headers (not FTP)

   d. The Authentication Data field in the AH

   e. The mutable fields in the IP header

Correct answer: (a)

See Quiz 5 answers for similar discussion.

c) SSL/TLS:

a. Can provide confidentiality for any Internet application

b. Can provide data integrity for any Internet application

c. Is used by HTTPS to provide web security

d. Is used by IPsec to provide network security

Correct answer: (c)

Options (a) and (b) are incorrect because TLS is only for TCP based applications, not UDP based Internet applications

Option (c) is correct – HTTPS is HTTP over TLS

Option (d) is incorrect – IPsec is independent of TLS.

d) In the SSL Handshake Protocol:

a. RSA must be used for the client and server to exchange keys

b. The key length used by the client and server is always 256-bits

c. The server can be authenticated from its X.509 certificate

d. A HELLO message from the client to server contains the secret key to be used for the symmetric key encryption

Correct answer: (c)

Option (a) is incorrect because algorithms other than RSA can be used for key exchange, e.g. Diffie Hellman

Option (b) is incorrect because the client and server can choose a key length.

Option (c) is correct because the server does authenticate by sending its certificate (i.e. its signed public key).

Option (d) is incorrect because the HELLO message does not contain the secret key – the secret key is contained in the key exchange.

e) If you had access (e.g. login as an administrator) to the SIIT gateway router, for all messages passing through that router, you could:

a. Read the contents of the messages if they were encrypted only with TLS

b. Read the contents of the messages if they were encrypted only with IPsec (transport mode)

c. Read the contents of the messages if they were encrypted with any encryption algorithm/protocol.

d. Not read the contents of the messages if they were all encrypted with IPsec (transport mode)

Correct answer: (d)

Option (a), (b) and (c) are incorrect because even at a router, if the packet is encrypted, although you can see the packet, you cannot see the message.

Question 2 [5 marks]

A PC1 is sending HTTP data to PC2. It travels through routers R1, R2, R3 and R4, in that order. You can identify the IP address of a node as its name, e.g. IP address of R1 is “R1”.

a) If IPsec Encapsulating Security Payload (including Authentication) is used in transport mode from PC1 to PC2, in the IP packet structure below, identify each header or field (that is, fill in the boxes).

IP			HTTP	Data		

Answers:

IP ESP Header TCP HTTP Data ESP Trailer ESP Auth

ENCRYPTENCRYPTENCRYPTENCRYPT

b) Indicate the fields which have some or partial encryption applied on them.

c) For the scenario in part (a), what network node does the destination address in the IP header refer to?

Answer: PC2 (the eventual destination)

d) If in part (a) instead of transport mode, tunnelling mode is used where a tunnel is created from PC1 to R4, there is protection provided against traffic analysis (although the protection is limited). How is this protection provided?

Answer: the inner IP packet header containing the original source and destination is encrypted – anyone on the tunnel cannot see how the original source or destination is. (It is limited protection because outside the tunnels the source/destination can be seen).

e) For the scenario in part (d), what is the destination IP address of the packet seen by router R2?

Answer: R4 (the destination of the tunnelled packet)