CSS 322 – QUIZ 8 ANSWERS

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

Question 1 [3 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) 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.

c) 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 [4 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). [1.5 marks]

IP				Data	ESP Trailer	ESP Auth

Answers:

I did not include this question in the marks (that is, the quiz was out of 8.5, not 10). This is because it is not always true that a HTTP packet is split between a HTTP header and Data. If you look closely at a HTTP message such as a GET request, there is no clear difference between Header and Data, and hence it is technically wrong to draw them separately as my diagram below.

The intended answer was:

IP ESP Header TCP HTTP Data ESP Trailer ESP Auth

b) For the scenario in part (a), what network node does the destination address in the IP header refer to? [0.5 mark]

Answer: PC2 (the eventual destination)

c) 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). Explain how this protection is provided. [1.5 marks]

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).

d) For the scenario in part (d), what is the destination IP address of the packet seen by router R2? [0.5 mark]

Answer: R4 (the destination of the tunnelled packet)

Question 3 [3 marks]

Fill in the tables to create firewall rules that perform the following actions on a local network with address 203.131.209.0 (subnet mask 255.255.255.0). You can assume that by default, all traffic will be accepted. You can refer to entire networks by their network address, e.g. 203.131.209.0 refers to all computers on the local network. You can use * to many ‘any’.

a) Block all traffic to any server on the local network.

Rule	Source IP	Source Port	Dest IP	Dest Port
1 DROP	*	*	203.131.209.0	1 to 1024

b) Block traffic from client 203.131.209.3 on the local network to web servers on the network 64.233.189.0 (with subnet mask 255.255.255.0).

Rule	Source IP	Source Port	Dest IP	Dest Port
2 DROP	203.131.209.3	*	64.233.189.0	80