CSS 322 – QUIZ 8A 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.

1. The Diffie-Hellman exchange in Transport Layer Security (TLS/SSL) is used for exchanging:
   a) Secret values between two users
   b) Certificates between two users
   c) Nonce values between two users
   d) Sequence numbers between two users
   e) Encrypted files between two users

Correct answer: (a)

Diffie-Hellman is used to exchange secret values (whether or not used in TLS/SSL or other protocols).

2. Stateful packet inspection:
   a) Allows a firewall to reject (drop) packets based on the content of emails (e.g. spam, viruses)
   b) Allows a firewall to reject (drop) packets that contain malicious HTTP GET requests
   c) Allows a firewall to reject (drop) packets that do not belong to an open TCP connection
   d) Requires a dual homed bastion host
   e) Requires a screened subnet with demilitarized zone (DMZ)

Correct answer: (c)

Stateful packet inspection involves the firewall keeping a record of the open TCP connections, and therefore blocking traffic based on this.

3. 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 [2 marks]

If ESP in transport mode is used in IPsec when sending a HTTP request, select which pieces of information are authenticated (you may select more than one – you must get all correct to receive full marks):

a) Mutable fields (those that may change) in the IP header
b) The headers from Physical and Data Link/MAC layers
c) The Authentication Data field in the header
d) The first 96-bits of the payload
e) The TCP header
f) The entire IP header
g) The HTTP request

Correct answers: (e) and (g)

The structure of an IPsec packet when using ESP is:

Physical | MAC | IP | ESP | TCP | HTTP Data | ESP Trailer

The authentication covers the entire payload of the original IP packet, that is, TCP, FTP and Data.

Option (a) is false because if we calculate the MAC across mutable fields (those that will change), then the authenticated data sent will be different from the authenticated data received. Therefore, the MAC (authentication) will fail, when it should pass.

Option (b) is false because IPsec doesn't provide any coverage of the lower layer (Physical, MAC/Data link) headers.

Option (c) is false because the Authentication Data field carries the actual MAC – hence it is impossible to achieve. That is, the input to the MAC function cannot include the output of the MAC function!

Option (d) is false because the scheme would be almost useless. If only 96 bits of the payload were considered, then it would be possible for the remaining bits of the payload to be changed, without the receiver detecting it.

Option (e) is true – the authentication does cover the TCP header.

Option (f) is false because of answer to option (a).

Option (g) is true – the authentication does cover the application layer header.

Marks: selecting (e) or (g) gave 1 mark each. Selecting an incorrect option resulted in loss of 0.5 mark. Hence, if you selected (d) and (e) you received 0.5 out of 2. If you selected (d), (e) and (g) you received 1.5 out of 2.

Question 3 [2 marks]

Assume SIIT Bangkadi network is connected to SIIT Rangsit network via the public Internet. Explain an advantage and disadvantage of using IPsec in tunnelling mode (versus transport mode) to secure traffic between the two networks.

Advantage of tunnelling mode

Answers: easy to configure and manage (only at routers), do not need IPsec on all hosts, adding a new host can have automatic protection

Disadvantage of tunnelling mode

Answers: no security over internal network, routers (tunnel end points) are single point of failure, possible performance bottleneck

Question 4 [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 - 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