

CSE 497B/Spring 2007 - Quiz 2  
Thursday, March 1, 2007 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. You have 20 minutes to complete this quiz, so focus on those questions whose subject matter you know well. Write legibly and check your answers before handing it in.

**Short Answer - some will be one or two words – no more than 3 sentences**

1. (3pts) List *three* differences between the IPsec protocols *authentication header* (AH) and *encapsulated security payload*.

*answer:* (1) ESP does encryption where AH does not; (2) AH MACs the IP header where ESP does not; (3) AH stores the MAC in the AH header where ESP stores it on the end of the payload; (4) others...

2. (5pts) What is the purpose of the *tickets* in the Needham-Schroeder protocol? Why are *timestamps* rather than nonces used in the Kerberos implementation of tickets?

*answer:* Tickets are statements from the trusted third party that provide the session key to Alice and Bob. Timestamps are used so that the freshness values used for verifying the recency of messages from the TTP and Alice need not be retained indefinitely.

**Word Problems - take your time and answer clearly and completely.**

4. (10pts) Suppose you have a network as defined above. Create stateless firewall policies for the following network firewalls FW1 and FW2. Create only as many rules as you need (use the minimum) in the order they should be evaluated.

- (a) Unless otherwise specified, all traffic should be denied.
- (b) The satellite networks should be able to communicate with any DMZ host over http (port 80).
- (c) Nobody outside the DMZ should be able to contact the internal network.
- (d) All the hosts inside the internal network 128.168.12 must be able to contact the internal SMTP server 128.168.12.5 (port 25).
- (e) The internal (128.168.12.5) and DMZ (128.168.11.5) SMTP servers must be able to exchange SMTP messages (port 25).
- (f) Any internet SMTP server can exchange SMTP messages with the DMZ SMTP server 128.168.11.5 (port 25).



FW1				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
129.168.0.*	*	128.168.11.*	80	A
129.168.1.*	*	128.168.11.*	80	A
11.14.*	*	128.168.11.*	80	A
12.*	*	128.168.11.*	80	A
128.168.11.*	80	129.168.0.*	*	A
128.168.11.*	80	129.168.1.*	*	A
128.168.11.*	80	11.14.*	*	A
128.168.11.*	80	12.*	*	A
*	*	128.168.11.5	25	A
128.168.11.5	25	*	*	A
*	25	128.168.11.5	*	A
128.168.11.5	*	*	25	A
*	*	*	*	D
FW2				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
128.168.12.5	*	128.168.11.5	25	A
128.168.11.5	25	128.168.11.5	*	A
128.168.11.5	*	128.168.12.5	25	A
128.168.12.5	25	128.168.11.5	*	A
*	*	*	*	D