T-110.6220 Network security

Practice examination

Answer at most 5 of the 6 parts below. (If you answer all, part 6 will not be graded.)

Part I: Authentication protocols

1. Consider the following key-exchange protocol:

1.	$A \rightarrow B$:	$A, B, N_A, \text{Certificate}_A$
2.	$B \rightarrow A$:	$A, B, N_A, N_B, E_A(SK), S_B(A,B, N_A,N_B, E_A(SK)), \text{Certficate}_B$

The session key is SK.

(a) What are the E, S and MAC?

(b) Is the session key fresh? Justify your answer.

(c) Does this protocol provide entity authentication? Justify your answer.

(d) Does this protocol provide forward secrecy? Justify your answer.

(e) Does this protocol provide identity protection? Justify your answer.

(f) Add a third message to the protocol to achieve for mutual key confirmation.

Part II: IPsec and firewalls

(a). What are SPD, SAD, PAD in IPsec? Explain briefly the contents and purpose of each.

A host with the IP address 205.33.144.10 is configured with the following IPsec policy:

Local IP	Local port	Remote IP	Remote port	Protocol	Action
205.33.144.10	*	*	80	TCP	Bypass
205.33.144.10	7733	205.34.11.4	7734	TCP	ESP
*	*	*	*	*	Discard

(b) What does this policy aim to achieve?

(c) What weakness is there in this configuration?

(d) Write a better policy that provides the intended protection. What non-standard features does your solution require from the IPsec implementation?

Part III: Wireless security

(a) If users access the web over TLS/SSL, do they benefit at all from WLAN security?

Explain briefly the purpose and limitations of the following security measures on wireless LANs:

(b) Disabling SSID broadcast

(c) Aluminum foil in walls

(d) TKIP

Part IV: Kerberos and TLS

(a) Compare the trust models in Kerberos and TLS.

(b) Kerberos is use almost exclusively on intranets while TLS is used on the Internet. Why?

Part V: Cellular authentication
Here are two authenticated key-exchange protocols:

1. X → Y: RAND
2. Y → X: A3 (Ki, RAND)

Kc = A8 (Ki, RAND)

1. X → Y: RAND, SQN⊕AK, f1 (K, RAND, SQN)
2. Y → X: f2 (K, RAND)

CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

(a) Where are the protocols used, and what are X and Y?
(b) What differences are there in the protocol properties?
(c) How would the other protocol change if we simplify it by replacing SQN⊕AK with SQN?

Part VI Multicast security

Explain how the TESLA authentication works and why it is good for broadcast streams.