T-110.5240 Network security
Lecturer: Tuomas Aura
Examination 2010-12-22

Answer at most 5 of the 6 parts. (If you answer too many, Part 6 will not be marked.)

Part 1: Authentication protocols

Consider the following key-exchange protocol:

1.	$A \rightarrow B$:	A, B, N_A, Certificate_A
2.	$B \rightarrow A$:	A, B, N_A, N_B, $E_A(SK)$, $Sign_B(A, B, N_A, N_B, E_A(SK))$, Certificate_B
3.	$A \rightarrow B$:	A, B, $MAC_{SK}(A,B)$
The session key is SK.		

(a) What security properties are lost if the nonce N_A is removed from all messages of the protocol?
(b) What security properties are lost if the signature $Sign_B(...)$ is removed from the second message?
(c) What security properties are lost if the third message is removed from the protocol?

Part 2: Threat analysis

Oodi is an online service at Aalto University which the stores university student records i.e. student personal data and course grades.

(a) What security threats are there against this service? Number the threats in approximate priority order.
(b) Which of these threats can be mitigated by using TLS?

Part 3: IPsec

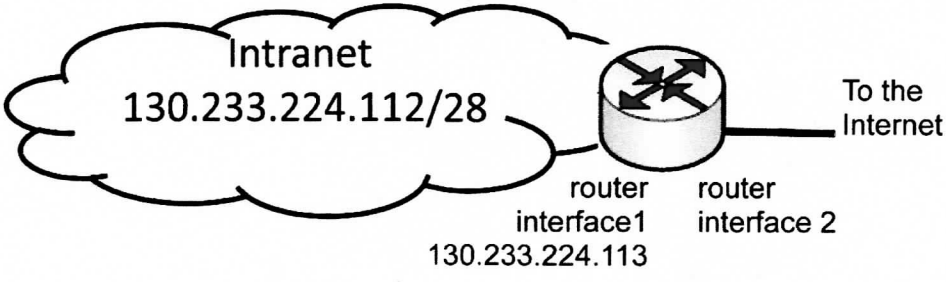
(a) What are SPD, SAD and PAD in IPsec, and what is their purpose?

(b) What kinds of security associations are there in IPsec, and what is their purpose?

(c) What headers are there on an IPsec data packet when it is used for VPN?

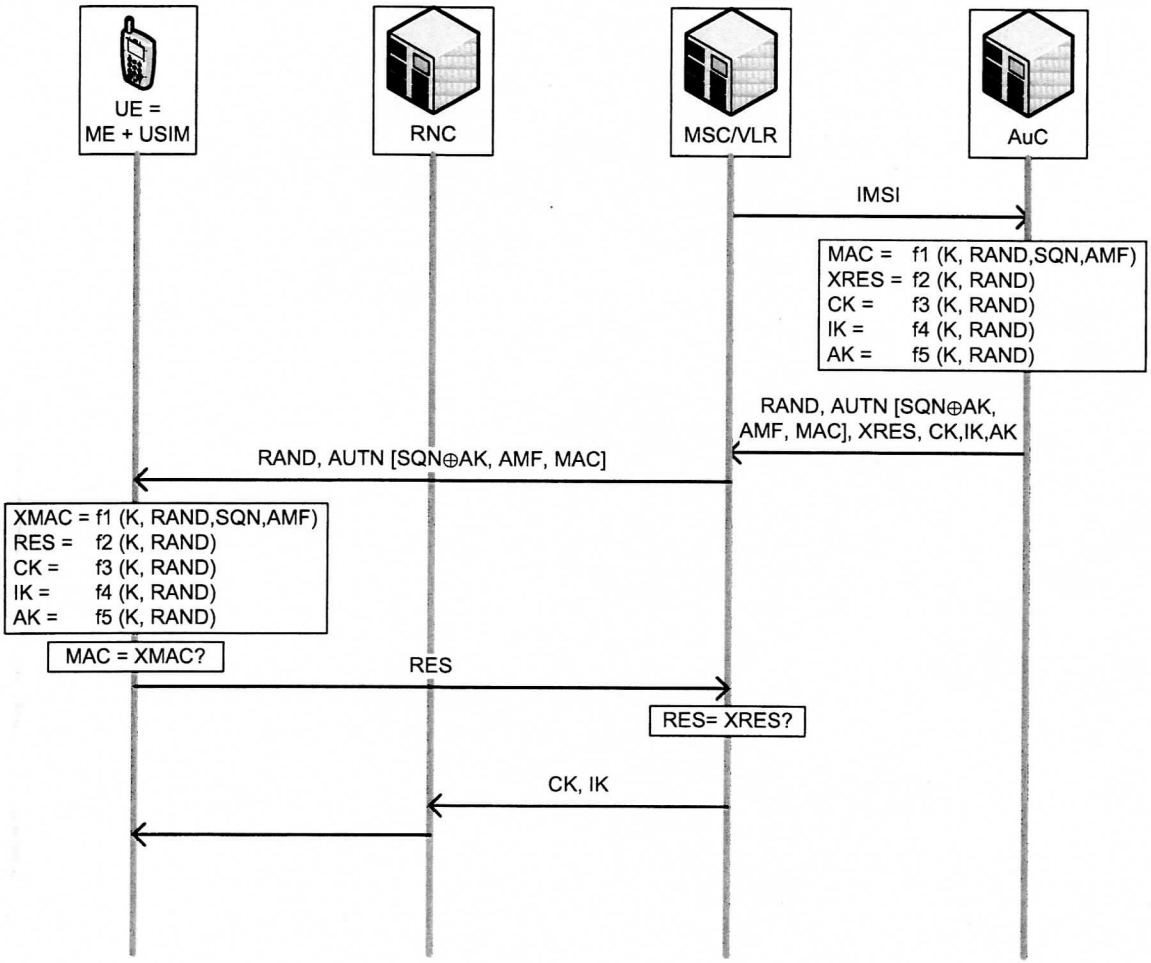
Part 4: Firewalls

Define stateless firewall rules that implement ingress and egress filtering for the gateway router below. (Use some easily understandable notation for the firewall rules, or provide an explanation of your notation.)



Part 5: Cellular network security

Explain the security and privacy properties of the UMTS AKA protocol and how they arise from the protocol messages. Include also the performance optimizations made in the protocol design. (You can use the picture below as a partial reference. You do not need to explain the implementation details of the cryptographic algorithms.)



Part 6: DoS

How could the Internet architecture and protocols be modified to prevent packet flooding denial-of-service attacks? Base your answer on an analysis of the current Internet architecture and its vulnerabilities.