T-110.6220 Special course in network security
Lecturer: Tuomas Aura
Examination 2008-12-15

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

Part 1: Authentication protocols

Consider the following key-exchange protocol:

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

The session key is SK.

(a) How does B obtain the values of N_B, SK?
(b) How does B obtain the value of Certficate_B?
(c) Is this protocol contributory? Explain why.
(d) Does this protocol provide entity authentication? Explain why.
(e) Does this protocol provide forward secrecy? Explain why.
(f) What security properties are lost if the third message is removed from the protocol?

Part 2: TLS/SSL

(a) What security threats are there for a free online email service?
(b) Which of them are solved by using TLS and how? Which are not and why?
(c) How is TLS positioned in the protocol stack?

Part 3: Wireless security

(a) If you use an IPsec tunnel to connect to your intranet services, do you need WLAN security at the wireless access link? Explain why or why not.
(b) When might it be necessary to revoke a WLAN client certificate that is used for EAP-TLS authentication in WPA2?
(c) When you walk around with your mobile phone, can observers around you find out your SIM card's unique identifier IMSI? Why or why not?

Part 4: Kerberos:

Kerberos authentication can take up to 6 messages:

1. A → AS:	Preauthentication, A, TGS, N_{A1}, $Addr_A$
2. AS → A:	A, TGT, E (K_A ; $K_{A\text{-}TGS}$, N_{A1}, TGS, $Addr_A$)
3. A → TGS:	TGT, $Authenticator_{A\text{-}TGS}$, B, N_{A2}, $Addr_A$
4. TGS → A:	A, Ticket, E($K_{A\text{-}TGS}$; K_{AB}, N_{A2}, B, $Addr_A$)
5. A → B:	Ticket, $Authenticator_{AB}$
6. B → A:	AP_REP
E(X ; Y) denotes encryption and integrity protection of message Y with key X.	

(a) What is the purpose of Kerberos?
(b) What are A, AS, TGS and B?
(c) What are TGT and Ticket?
(d) What is the purpose of Preauthentication?
(e) Messages 2 and 4 have similar structure. So have TGT and Ticket. How does Kerberos prevent replay attacks where the attacker substitutes one of these for the other?
(f) What is identity delegation in Kerberos?

Part 5: Firewalls

Consider the following firewall rules:

Protocol	Src IP	Src port	Dst IP	Dst port	Action
TCP	223.20.13.0/24	*	*	80,443	Allow
TCP	*	80,443	223.20.13.0/24	*	Allow
*	*	*	*	*	Block

(a) What kind of security policy does the firewall try to implement?
(b) What security problem there is with the rules?
(c) Fix the firewall rules so that they implement the intended policy. (Explain also, what kind of features your solution requires from the firewall.)

Part 6: Denial of service

How you could you mount a resource-exhaustion DoS attack against a person or a small company using the following: email mailing lists, advertisements delivered by the postman, and people reading interesting web pages? Can these attacks be prevented with smart protocol design? Explain how or why.