T-110.5240 Network security
Lecturer: Tuomas Aura
Examination 2011-05-24

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

No instruments are allowed in this exam!

Part 1: Authentication protocols

Consider the following key-exchange protocol based on Diffie Hellman:

1.	$A \rightarrow B$:	g, p, g^x
2.	$B \rightarrow A$:	$g^y, E_{SK}(g^y, g, p, g^x, S_B(g^y, g, p, g^x), Cert_B)$
3.	$A \rightarrow B$:	$E_{SK}(g, p, g^x, g^y, S_A(g, p, g^x, g^y), Cert_A)$
The session key is $SK = h(g^{xy})$.		

What security properties are lost if the following changes are made to the protocol:

(a) The attacker learns the values g and p.
(b) The signature $S_B(\ldots)$ is not done.
(c) The server B saves computing resources by reusing the value of y for a day.

Part 2: Online service security

Noppa is a university web site where course material such as lecture notes and exercise questions as well as examination results are published.

(a) What security threats should be considered when designing this service? Prioritize the threats.
(b) Which of these security threats are mitigated by the use of TLS or SSL? Why?

Part 3: Wireless security

Aalto University students can use the eduroam wireless network (SSID="eduroam"), which is available on Aalto campus and at many other universities around the world. It uses WPA Enterprise or WPA2 Enterprise authentication and a global hierarchical system of RADIUS servers.

(a) Aalto users authenticate to eduroam with their Aalto NAI (e.g. *teemu.teekkari@aalto.fi*) and Aalto password. This works even at foreign universities. Does this expose the user password to the foreign university and its network administrators? Explain why.
(b) Aalto users should configure their computers to use PEAP password authentication for eduroam. Other universities may require their users to enroll TLS certificates for the client computers. Explain how it is technically possible for different universities to use different authentication mechanisms?
(c) Why might roaming between eduroam access points be slow even if the access points are close to each other in the same building? Explain briefly how enabling pre-authentication and PMK caching can mitigate this problem.

Please turn the paper for more problems.

Part 4: Kerberos

The Kerberos protocol:

1.	$A \rightarrow AS$:	Preauthentication, A, TGS, N_{A1}, $Addr_A$
2.	$AS \rightarrow A$:	A, TGT, $E_{KA}(K_{A\text{-}TGS}, N_{A1}, TGS, Addr_A)$
3.	$A \rightarrow TGS$:	TGT, $Authenticator_{A\text{-}TGS}$, B, N_{A2}, $Addr_A$
4.	$TGS \rightarrow A$:	A, Ticket, $E_{KA\text{-}TGS}(K_{AB}, N_{A2}, B, Addr_A)$
5.	$A \rightarrow B$:	Ticket, $Authenticator_{AB}$
6.	$B \rightarrow A$:	AP_REP

(a) Explain when and how a brute-force password cracking attack against Kerberos is possible. What protocol feature mitigates this threat and how?

(b) How is the security of Kerberos affected if the client reuses one of the tickets TGT or Ticket?

(c) Where can access control be implemented in Kerberos?

Part 5: IPsec

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

(b) What cryptographic keys are there in IPsec and where are they stored? (Hint: Consider the databases SPD, SAD and PAD and other potential storage locations.)

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

Part 6: Anonymity

Explain how the Tor onion router works and what are its security properties and limitations.