T-110.5240 Network security
Lecturer: Tuomas Aura
Examination 2011-01-14

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 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 client A does not send its certificate in message 3.
(b) The encryption $E_{SK}(\ldots)$ is not done.
(c) The server B saves computing resources by reusing the value of y for a day.

Part 2: Threat analysis

1. An Internet bookstore requires the user to log in with a password. It advertises that it has "VeriSign 128-bit security".

(a) What does the advertisement mean?
(b) What security threats are protected against?
(c) What security threats are not protected against?

Part 3: Wireless security

Alice has configured her wireless router (router with a built-in WLAN access point) and laptop computer to use WPA2-Personal. Explain the protocol that takes place when the laptop connects to the access point.

Part 4: DDoS

What different defense mechanisms are there against distributed denial-of-service (DDoS) attacks? Compare their potential effectiveness and the problems in deploying them.

Please turn the paper for more problems.

Part 5: Anonymity

Explain the difference between the security goals and threat models for

- an anonymizing email remailer
- the Tor low-latency anonymity system
- low-latency mix network for email

Part 6: TESLA

The picture below illustrates the TESLA protocol.

(a) Give examples of at least three potential applications for TESLA.

(b) What buffering requirements does TESLA put on the sender and receivers? Why?

(c) Can TESLA be used for group communication where everyone can send? Why?