T-110.5241 Network security
Examination 2014-02-21
Lecturer: Tuomas Aura
No electronic equipment or reference material is allowed in the examination.

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. Authentication protocols

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

1. $A \rightarrow B$: g^x
2. $B \rightarrow A$: g^y, $E_{SK}(g^y, g^x, Sign_B(g^y, g^x), Cert_B)$
3. $A \rightarrow B$: $E_{SK}(g^x, g^y, Sign_A(g^x, g^y), Cert_A)$

$SK = h(g^{xy})$

(a) What is the value SK, and for what two purposes is it typically used?
(b) Does this protocol implement perfect forward secrecy? Explain you reasoning.
(c) How do the security properties of the protocol change if we remove the encryption $E_{SK}(...)$ from messages 2 and 3 and, instead, send these messages as plaintext? Explain why.

2. IPsec

a) What are SPD, SAD and PAD in IPsec, and what is their purpose?
b) What headers are there typically on an IPsec data packet when it is used for VPN?

3. Wireless security

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

Are the following statements true or false (or both)? Explain the technical reasons for your answer.

1) Eduroam provides little security because anyone can spoof the SSID "eduroam".
2) Thanks to WPA2, accessing the Internet on any eduroam partner network is just as secure as if you were on the Aalto campus.
3) When connecting to the eduroam network at another university, you need to think carefully about whether it is safe to give your password to that university's RADIUS server.
4) When connecting to the eduroam network at another university, you need to configure your computer to use the *authentication method* (PEAP, EAP-TLS etc.) required by that university.

Please turn the paper for problems 4–6.

4. NFC and threat analysis

Some new bank cards (debit and credit cards) have an NFC payment feature. The card has a built-in NFC chip. Some shops have also started to install payment terminals that support NFC. To make a payment, the user simply taps the payment terminal with the bank card. The bank then transfers the money from the user's band account (or credit account) to the shop. The NFC payments are faster and easier to make than the currently dominant chip & PIN payments.

[Photo: www.nordea.fi]

How does the introduction of the NFC payment feature affect the security of the payment system?

(Hint: Consider both new or increased threats and reduced ones, if there are any. You can also explain some actual or potential security measures that mitigate the new threats, but that is not required.)

5. Denial of service

(a) Explain how cookies can be used to prevent denial-of-service attacks in the IKE key exchange.
(b) What attacks are prevented by the cookies, and what are not?

The IKE protocol *without* cookies is shown here:

1.	I → R:	HDR(A,0), SAi1, KEi, Ni
2.	R → I:	HDR(A,B), SAr1, KEr, Nr, [CERTREQ]
3.	I → R:	HDR(A,B), SK{ IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}
4.	R → I:	HDR(A,B), ESK(IDr, [CERT,] AUTH, SAr2, TSi, TSr)

6. Anonymity

What weaknesses are there in the Tor anonymity system?