T-110.5241 Network security
Examination 2012-01-13
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 → B: N_A, g^x
2. B → A: N_A, N_B, g^x, g^y, $Sign_B(N_A, N_B, g^x, g^y)$, $Cert_B$
3. A → B: $Sign_A(N_A, N_B, g^x, g^y)$, $Cert_A$

SK = $h(N_A, N_B, g^{xy})$

(a) What is N_A, and how does A obtain it?
(b) What is SK and how is it used?
(c) It is found that, because of a bug in the implementation, N_A and N_B are always set to zero. How and why does this bug affect the security of the protocol?

2. Web security

A home gateway router has a web interface for administration at the address `https://192.168.0.1/`. When you try to open this URL, the web browser says:
`There is a problem with this website's security certificate. The security certificate presented by this website was not issued by a trusted certificate authority.`
Users typically choose to continue, enter the admin password, and proceed to configure the router.

Analyse the security of the above scenario. Which protocols and authentication mechanisms are used? Which attacks are prevented and which are possible?

3. TLS

Explain the working principle and security properties of the RSA-based key exchange in TLS. (It is a good idea to sketch the protocol messages approximately.)

Please turn the paper for problems 4–6.

4. Wireless security

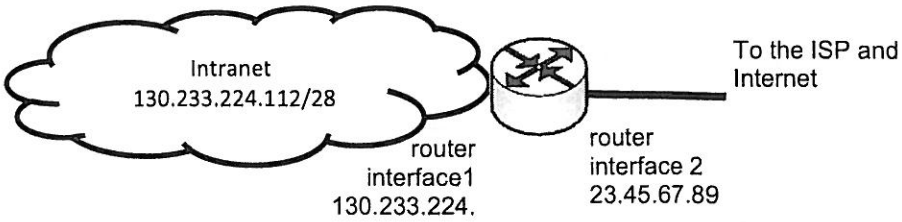
Aalto University students can use the eduroam wireless network (SSID="eduroam"), which is available on the Aalto campus and at many other universities around the world. It uses WPA2 Enterprise authentication and a global hierarchical system of RADIUS servers.

Which of the following statements are 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 Aalto services on any eduroam network is just as secure as if you were connected to a wire network on the Aalto campus.
3) When connecting to the eduroam network at another university, you need to think 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.

5. Firewalls

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



6. Anonymity

Explain the difference between the security goals and threat models for

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