T-110.6220 Special course in network security
Lecturer: Tuomas Aura
Examination 2009-01-07

**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:

1. $A \rightarrow B$: $N_A$, $g^x$, Certificate$_A$
2. $B \rightarrow A$: $N_B$, $g^y$, Certificate$_B$, Signature$_B(A,B,N_A,N_B,g^x,g^y,0)$
3. $A \rightarrow B$: Signature$_A(A,B,N_A,N_B,g^x,g^y,1)$

The session key is a one-way hash of the Diffie-Hellman secret: $K = \text{hash}(N_A,N_B,g^{xy})$.

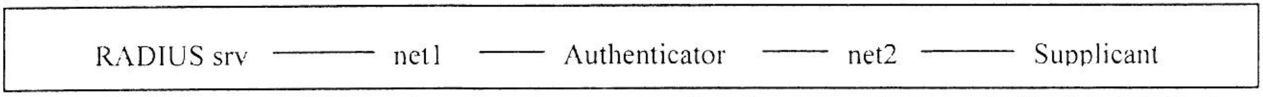
(a) Is he protocol vulnerable to a man-in-the-middle attack and why?
(b) Does the protocol guarantee the freshness of the session key to A and B key and why?
(c) Does the protocol provide forward secrecy?
(d) Does the protocol provide key confirmation?
(e) Describe a denial-of-service (DoS) attack against the protocol. Which resources does it consume?
(f) Modify the protocol to protect against DoS attacks from a spoofed source IP address.

**Part 2**: TLS/SSL

(a) Explain the meaning of this TLS cipher suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA.
(b) What security threats are there for a web site from which anyone can download free software?
(c) Which of them are solved by using TLS and how? Which are not and why?

**Part 3**: Wireless security

(a) Explain this picture in the context of WPA2:


RADIUS srv — net1 — Authenticator — net2 — Supplicant

(Hint: What is its purpose? Name the components, types of equipment, and protocols. Explain briefly the basic operation of the system.)
(b) Explain briefly the purpose and limitations of the following security measures on wireless LANs: MAC address ACL, disabling SSID broadcast

**Part 4**: Privacy and anonymity

(a) What kind of identity protection is provided by IPsec, SSL and WPA?

For problems (b)-(d), consider a mix network for email messages. Alice uses the mix network to send anonymous love letters to Bob. Bob's girlfriend Carol sees the messages arriving to Bob and wants to find out who is sending them. Carol sets up many mix routers until she controls about 10% of routers in the network. How and why would the following affect the anonymity of Alice?

(b) Alice decides to use a very long route, ten or more mixes.
(c) Alice's email application selects a new random route for each message.
(d) Each user's email application is told only a small subset of the mix routers, chosen based on the client IP address.

**Part 5**: Mobile security

Here is an authenticated key-exchange protocol:

| | | |
|---|---|---|
| 1. | X → Y: | RAND |
| 2. | Y → X: | A3 (Ki, RAND) |

Kc = A8 (Ki, RAND)
(a) Where is the protocol used, and what are X and Y?
(b) How do the properties of the protocol reflect the requirements of the application?
(c) Explain *in maximum two sentences* how the confidentiality and integrity of the session data are protected after the key-exchange.

**Part 6**: Multicast security

Hazardous-chemical storage facilities are monitored with CCTV cameras. A real-time video feed from any camera can be viewed at any of several remote monitoring locations and may be used as evidence for prosecuting intruders. The video streams are distributed using a proprietary multicast protocol. What security requirements are there for the video streams and how could they be protected?