LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / DSC
CH-1015 Lausanne
Phone : ++41 (0) 21 693 76 03
Fax : ++41 (0) 21 693 68 79
URL : http ://lasecwww.epfl.ch

Serge Vaudenay
Philippe Oechslin
07.07.2004

Security Protocols and Applications

Open book exam. Duration 1h45 hours.

Dynamic TESLA

We consider a communication graph in which nodes can communicate along the edges. The distance $d(a, b)$ between two nodes a and b is the minimal number of edges in a connected path from a to b. The diameter d of the graph is the maximal distance between two nodes in the graph. We assume that two adjacent nodes communicate with a protocol delay lower than τ_1. We further assume that each node a has its own clock t_a, and we define $B = \max_{a,b} |t_a - t_b|$.

A node s wishes to send a packet to a node r in an authenticated way by using the TESLA scheme.

1. Express the TESLA parameters τ and Δ in terms of d, τ_1 and B.
2. Recall what is the key management scheme (key generation, key usage, key disclosure) for s. Precisely describe the algorithms.
3. Recall what is the authentication validation scheme for r.
4. Explain what can happen if Δ is less than B.
5. Explain what can happen if τ is less than $d \times \tau_1$.
6. What shall we do if we wish to spread additional nodes and extend the graph ? In general, what shall we do if we wish to modify the graph topology ?

Ariadne Errors

The route from A to F goes through *B, C, D* and *E.* The route was established using the normal procedure with *route request* and *route reply* packets. Suddenly, D cannot reach E anymore and decides to generate a *route error* message.

1. Who will be the destination of this packet and what values will be in the fields *sending address, receiving address, time interval* , *error MAC* and *recent TESLA key.*

2. How many *route error* packets will have to be sent until B finally removes the route from its cache ?
3. In Ariadne, all pairs of nodes have a shared secret key. So, every node can authenticate itself to any other node. Explain why it is still necessary to have TESLA keys ?
4. What happens if an *active-0-x* attacker forges a *route error* message ?

Mobile Communications

Consider the following two ways of connecting your laptop to the Internet using a mobile phone.

– Use a normal GSM connection to call your ISP's phone number and connect using the 9'600 bps GSM modem of your mobile phone.
– Use GPRS to connect to your mobile operator's GPRS network

1. Which mode of connection do you consider more secure ?
2. Describe all differences in security that you can find between the connection modes.
3. What security advantages does UMTS have compared to GSM or GPRS ?

Security Choices for a New GSM Operator

Imagine you are a new GSM operator using the antenna infrastructure of others. Your business consists of setting up a "Home Location Register (HLR)" and an "Authentication Center (AuC)", getting customers and providing SIM cards. You have no proprietary communication network (no antenna...).

1. Which algorithms do you have to choose ?
2. What kind of attack will you face if you select COMP128 as A3/A8 ?
3. After all, why choosing an A8 algorithm ? You would like to take Ki as the encryption key as well. What can happen ?
4. Ok, so why not picking another key and use a fixed Kc ?
5. How about using a fixed challenge response value ?
6. Finally, as a wise engineer businessman, how will you select your algorithms ?