7261 Security Basics and Cryptosystems

Endre Bangerter

Exercises

1. Attack against Otway-Rees protocol

The Otway-Ress protocol has a vulnerability described in
`http://en.wikipedia.org/wiki/Otway-Rees`. Explain how that vulnerability is exploited.

2. Compromise of long term keys

Verify that for any of the symmetric key establishment protocols the following holds: If an attacker manages to compromise the long term keys at some point in time, then he can decrypt all past sessions, assuming that he has recorded the key establishment protocol messages.

3. Known session-key attacks

Recapitulate the notion of *known session-key attacks*. Argue why the Kerberos and the Otway-Ress protocol are secure against known session-key attacks.

4. Attacking synchronized clock protocols

Assume that an attacker can control the clocks of Alice, Bob, and the KDC, respectively. Can you come up with any attacks on the Kerberos protocol?

5. Man in the middle attacks

Describe a man in the middle attack on the Diffie-Hellman protocol. Why does the attack fail on the station to station protocol?