Homework 11 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

11.01.2011

Exercise 35. We investigate several attacks on identification schemes.

a) Describe a replay attack for a fixed password identification.
Propose a simple identification scheme prevent this attack.

b) The following challenge-response mutual authentication protocol is given

1) $A \rightarrow B : r_A$
2) $A \leftarrow B : E_K(r_A, r_B)$
3) $A \rightarrow B : r_B$

Explain how an eavesdropper E can authenticate to A without knowing the symmetric key K. This a reflection attack. Propose an improved protocol.

c) The following challenge-response protocol based on digital signatures is given

1) $A \rightarrow B : r_A$
2) $A \leftarrow B : r_B, S_B(r_B, r_A, A)$
3) $A \rightarrow B : r'_A, S_A(r'_A, r_B, B)$

Explain how an eavesdropper E can authenticate to B without signing any message with his own identity. This is an interleaving attack.

Exercise 36.

We consider a challenge-response mutual authentification based on digital signatures:

1) $A \leftarrow B : r_B$
2) $A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B)$
3) $A \leftarrow B : cert_B, A, S_B(r_B, r_A, A)$

The arguments of signature functions S_A and S_B are secured by a cryptographical hash function $h(m)$. The symbols r_A and r_B denote arbitrary large random numbers. The length of B and A is fixed.

a) Can A exploit this scheme to have B signed an arbitrary document?
Is this possible with certain limitations?

b) Calculate Bs ElGamal-signature for $r_A = 92, r_B = 27, B = 12$ and $A = 21$. We use private keys $x_A = 17$ and $x_B = 5$, a public prime $p = 107$, a primitive root $a = 2$ and session key $k = 71$. We employ $h(m) = m \pmod{99}$ as a simple hash function.