ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Ralf Sasse
January 2016

Verifying Security Protocols in Tamarin

Exercise Sheet 3

Assignment 3.1: Practical Tool Usage: Signed Diffie-Hellman

Define Signed Diffie-Hellman. Verify appropriate properties.

Assignment 3.2: Modeling Kerberos V and its properties

Consider the core of the Kerberos V protocol, where A is the initiator (or client), B the responder (or application server), and S the honest (authentication) server.

$$\begin{array}{lll} \text{M1.} & A \to S: & A, B \\ \text{M2.} & S \to A: & \{\!|B, K_{AB}, T_S|\!\}_{\mathsf{k}(A,S)}, \{\!|A, K_{AB}, T_S|\!\}_{\mathsf{k}(B,S)} \\ \text{M3.} & A \to B: & \{\!|A, K_{AB}, T_S|\!\}_{\mathsf{k}(B,S)}, \ \{\!|A, T_A|\!\}_{K_{AB}} \\ \text{M4.} & B \to A: & \{\!|T_A|\!\}_{K_{AB}} \end{array}$$

Here, K_{AB} is the session key generated by the server S, T_S is the associated timestamp, and T_A is a timestamp generated by A and included in the *authenticator* $\{\!|A, T_A|\!\}_{K_{AB}}$. We assume that initially each role shares a symmetric key with the server.

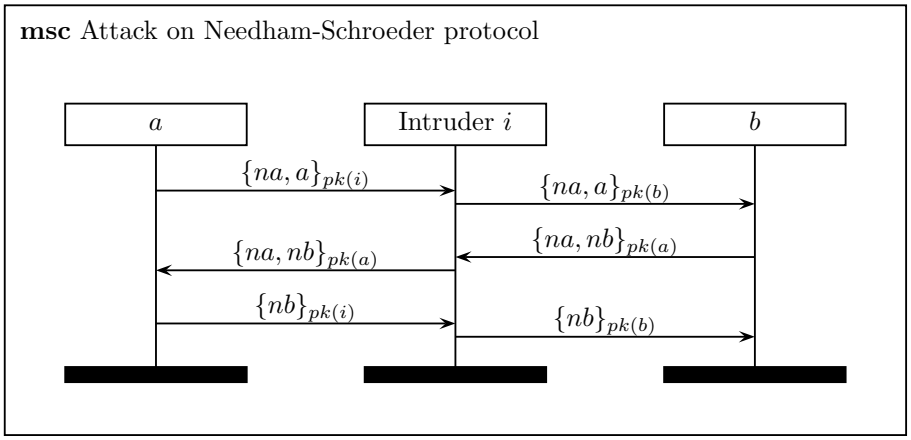
(a) Instrument the roles for four different agreements: each of A and B with S, and A and B with each other. For strongest possible properties, include as many fields as possible in the message M to be agreed upon. (Show this in form of an instrumented message sequence chart.)

(b) Let us first consider the timestamps as nonces as is the case in the protocol model from the lecture. Can the protocol in this view achieve an injective agreement in any of the four cases?

(c) Describe informally the additions that are needed to our protocol model for a more realistic model of timestamps that enables (i) recentness and (ii) injective agreements?

Assignment 3.3: Attack on NSPK

Consider Lowe's classical attack on the Needham-Schroeder Public-key protocol depicted below.



(a) Which of the following properties are violated by Lowe's attack? Consider the perspective of a and b separately.

(1) Secrecy of na,

(2) Secrecy of nb,

(3) Aliveness of other party,

(4) Weak agreement with other party,

(5) Non-injective agreement on na, nb

(b) Does NSPK satisfy aliveness of A for B? And vice versa?