Formal Methods for Information Security

Project report

Mathias Woringer
mworinger@student.ethz.ch

Gian-Luca Piras
gpiras@student.ethz.ch

April 15, 2021

1 PACE protocol

1.1 A simple challenge-response protocol

The following simple challenge-response protocol was formalized in Tamarin:

$$A \to B : x$$
$$B \to A : [x]_{k(a,b)}$$

The MAC function was realised by an user-defined function with two parameters in Tamarin. The details can be found in file **P1.spthy**.

1.2 Mutual authentication

The challenge-response protocol is extended in this subtask in that now it is not just Alice who sends a nonce x to Bob. Bob now also generates and sends a nonce y, which is sent to A. The goal of the protocol is to reach an agreement between the two roles A and B with both nonces. Formally, the protocol now looks like this:

$$A \to B : x$$
$$B \to : y$$
$$A \to B : [y]_{k(b,a)}$$
$$B \to A : [x]_{k(a,b}$$

Further details can be taken from the file **P2a.spthy**.

a) If we assume that there can be a network attacker who can eavesdrop on all the information exchanged. So we can assume that this protocol is vulnerable to *replay attacks*. Since neither Alice nor Bob include any information in their messages to authenticate the message, it can be intercepted by an eavesdropper and resent later. An attack scenario could look like following:

$$A \to A'_{eaves} : x$$
$$A'_{eaves} \to B : x'$$
$$B \to A : y$$
$$A \to B : [y]_{k(a,b)}$$

b) Fix the property

1.3 Introducing a session key

a) Solution a

b) Solution b

1.4 Replace the password by a nonce

1.5 Introducing Diffie-Hellman: The PACE protocol

a) Solution a

b) Solution b

c) Solution c

d) Solution d

2 The Off-the-Record Messaging Protocol

2.1 Modeling the original OTR Key Exchange

2.2 Authentication Failure

2.3 Improvement

2.4 SIGMA