Formal Methods for Information Security

Project report

Mathias Woringer and Gian-Luca Piras

April 12, 2021

1 PACE protocol

1.1 A simple challenge-response protocol

1.2 Mutual authentication

a) It's not secure against a replay attack. We have to add the identity of the corresponding role to ensure injective agreement.

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