Role based specification and security analysis of cryptographic protocols using asynchronous product automata *

Sigrid Gürgens Peter Ochsenschläger
Carsten Rudolph
{guergens,ochsenschlaeger,rudolphc}@sit.fraunhofer.de
Fraunhofer - Institute for Secure Telecooperation SIT
Rheinstrasse 75, D-64295 Darmstadt, Germany

Abstract

Cryptographic protocols are formally specified as a system of protocol agents using asynchronous product automata (APA). APA are a universal and very flexible operational description concept for communicating automata. Their specification, analysis and verification is supported by the SH-verification tool (SHVT). The local state of each agent is structured in several components describing its knowledge of keys, its "view" of the protocol and the goals to be reached within the protocol. Communication is modeled by adding messages to and removing them from a shared state component Network. Cryptography is modeled by symbolic functions with certain properties. In addition to the regular protocol agents an intruder is specified, which has no access to the agents' local states but to Network. The intruder may intercept messages and create new ones based on his initial knowledge and on what he can extract from intercepted messages. Violations of the security goals can be found by state space analysis performed by the SHVT. The method is demonstrated using the symmetric Needham-Schroeder protocol, and an attack is presented that does not involve compromised session keys. Our approach defers from others in that protocol specifications do not use implicit assumptions, thus protocol security does not depend on whether some implicit assumptions made are reasonable for a particular environment. Therefore, our protocol specifications explicitly provide relevant information for secure implementations.

*Full paper to appear in *DEXA 2002 International Workshop on Trust and Privacy in Digital Business*,