Formal analysis of key exchange protocols and physical protocols

Author(s):
Schmidt, Benedikt

Publication Date:
2012

Permanent Link:

https://doi.org/10.3929/ethz-a-009898924 →

DISS. ETH NO. 20856

FORMAL ANALYSIS OF KEY EXCHANGE PROTOCOLS AND PHYSICAL PROTOCOLS

A dissertation submitted to
ETH ZURICH
for the degree of
Doctor of Sciences

presented by
BENEDIKT SCHMIDT
Dipl.-Inf., Universität Karlsruhe (TH), Germany
born May 1st, 1980
Citizen of Germany

accepted on the recommendation of
Prof. Dr. David Basin, examiner
Prof. Dr. Srdjan Capkun, co-examiner
Prof. Dr. Ralf Küsters, co-examiner

2012

Abstract

A security protocol is a distributed program that might be executed on a network controlled by an adversary. Even in such a setting, the protocol should satisfy the desired security property. Since it is hard to consider all possible executions when designing a protocol, formal methods are often used to ensure the correctness of a protocol with respect to a model of the protocol and the adversary. Many such formal models use a symbolic abstraction of cryptographic operators by terms in a term algebra. The properties of these operators can then be modeled by equations. In this setting, we make the following contributions:

1. We present a general approach for the automated symbolic analysis of security protocols that use Diffie-Hellman exponentiation and bilinear pairings to achieve advanced security properties. We model protocols as multiset rewriting systems and security properties as first-order formulas. We analyze them using a novel constraint-solving algorithm that supports both falsification and verification, even in the presence of an unbounded number of protocol sessions. The algorithm exploits the finite variant property and builds on ideas from strand spaces and proof normal forms. We demonstrate the scope and the effectiveness of our algorithm on non-trivial case studies. For example, the algorithm successfully verifies the NAXOS protocol with respect to a symbolic version of the eCK security model.
2. We examine the general question of when two agents can create a shared secret. Namely, given an equational theory describing the cryptographic operators available, is there a protocol that allows the agents to establish a shared secret? We examine this question in several settings. First, we provide necessary and sufficient conditions for secret establishment using subterm-convergent theories. This yields a decision procedure for this problem. As a consequence, we obtain impossibility results for symmetric encryption. Second, we use algebraic methods to prove impossibility results for monoidal theories including XOR and abelian groups. Third, we develop a general combination result that enables modular impossibility proofs. For example, the results for symmetric encryption and XOR can be combined to obtain impossibility for the joint theory.
3. We develop a framework for the interactive analysis of protocols that establish and rely on properties of the physical world. Our model extends standard, inductive, trace-based, symbolic approaches with location, time, and communication. In particular, communication is subject to physical constraints, for example, message transmission takes time determined by the communication medium used and the distance between nodes. All agents, including intruders, are subject to these constraints and this results in a distributed intruder with restricted, but more realistic, communication capabilities than those of the standard Dolev-Yao intruder. Building on our message theory that includes XOR, we also account for the possibility of overshadowing of message parts. We have formalized our model in Isabelle/HOL and have used it to verify protocols for authenticated ranging, secure time synchronization, and distance bounding. The analysis of distance bounding attacks accounts for overshadowing and distance hijacking attacks.

Zusammenfassung

Sicherheitsprotokolle sind verteilte Algorithmen die in einem Netzwerk ausgeführt werden können, das von einem Angreifer kontrolliert wird. Dabei sollen die gewünschten Sicherheitseigenschaften des Protokolls in allen solchen Szenarien gewährleistet sein. Da es schwierig ist während des Protokoll-Entwurfs alle möglichen Ausführungen zu berücksichtigen werden oft formale Methoden eingesetzt, um die Korrektheit eines Protokolls sicherzustellen. Dabei wird ein formales Modell des Protokols und aller möglichen Angreifer genutzt, in dem die kryptographischen Operationen mit Hilfe von Term-Algebren symbolisch modelliert werden. In diesem Zusammenhang präsentieren wir drei Beiträge.

1. Wir präsentieren eine allgemeine Methode für die automatische symbolische Analyse von Sicherheitsprotokollen die Diffie-Hellman Exponentiation und bilineare Pairings benutzen um Sicherheitseigenschaften zu erreichen. Wir modellieren Protokolle als Multiset Rewriting Systeme und Sicherheitseigenschaften als First-Order Formeln. Unser Algorithmus zur automatischen Analyse solcher Protokolle basiert auf Constraint Solving und nutzt Ideen aus der Beweistheorie und von Strand Spaces. Wir demonstrieren die Anwendbarkeit unseres Algorithmus anhand von nicht-trivialen Fallstudien.
2. Wir betrachten die allgemeine Fragestellung ob zwei Agenten ein gemeinsames Geheimnis erzeugen können. Dabei gehen wir davon aus, dass die verfügbaren Operationen durch eine Term-Algebra und Gleichungen beschrieben werden. Wir beweisen mehrere Unmöglichkeitsresultate. Unter anderem beweisen wir Resultate für symmetrische Verschlüsselung, für XOR und ein Kombinationsresultat, mit dem Unmöglichkeitsresultate modular bewiesen werden können.
3. Wir entwickeln ein System zur interaktiven Analyse von Protokollen, die physikalische Eigenschaften der Umgebung in der sie ausgeführt werden nutzen und sicherstellen. Unser zugrundeliegendes Modell erweitert Standard-Modelle mit den Konzepten von Ort, Zeit, und Netzwerk-Kommunikation. Dabei ist die Netzwerk-Kommunikation eingeschänkt, so dass physikalische Gesetze nicht verletzt werden. Wir haben unser Modell in dem interaktiven Beweis-Assistenten Isabelle/HOL formalisiert und die Formalisierung benutzt um die Sicherheit von Authenticated Ranging, Secure Time-Synchronization, und Distance Bounding Protokollen zu analysieren.