Advancing automated security protocol verification

Author(s):
Meier, Simon

Publication Date:
2013

Permanent Link:

https://doi.org/10.3929/ethz-a-009790675 →

DISS. ETH NO. 20742

ADVANCING AUTOMATED SECURITY PROTOCOL VERIFICATION

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

presented by
SIMON MEIER,
Dipl. Ing. Inf., ETH Zürich
born on August 3rd, 1982
citizen of Luzern, Switzerland

accepted on the recommendation of
Prof. Dr. David Basin, examiner
Prof. Dr. Ueli Maurer, co-examiner
Dr. Steve Kremer, co-examiner
Dr. Cas Cremers, co-examiner

2013

Abstract

Security protocols are distributed algorithms for achieving security goals, like secrecy or authentication, even when communicating over an insecure network. They play a critical role in modern network and business infrastructures. This thesis focuses on the automated verification of security protocols in symbolic models of cryptography. The verification of security protocols is particularly important, as their design is error-prone, and errors may lead to the loss of money or even human lives.

The automated verification of security protocols has already been the subject of much research. Automatic verification of all protocols is however impossible to achieve, as protocol security is undecidable in general. The goal of existing research works and this thesis is therefore to extend the scope of automated verification to cover increasingly many practical verification problems. In this context, our development of the theory and implementation of the Tamarin prover represents a significant step forward. In particular, Tamarin is the first tool that supports, without requiring any bounds, the automatic falsification and verification of protocols making use of loops and non-monotonic state, and of protocols that use Diffie-Hellman exponentiation to achieve resilience against strong adversaries. The theory underlying the Tamarin prover is of particular interest because it is derived from a simple, but expressive security protocol model, and because it is constructed in a way that simplifies future extensions.

Apart from extending the scope of automated security protocol verification, this thesis also provides an answer to the question of how to improve the trustworthiness of a result obtained by an automatic security protocol verification tool. We explain a generic approach to construct proof-generating versions of security protocol verification algorithms. We validate this approach by implementing `scyther-proof`, a version of Scyther that generates *machine-checked* proofs. We demonstrate the practical applicability of `scyther-proof` and Scyther on the ISO/IEC 9798 standard for entity authentication, which is used as a core building block in numerous other standards. When analyzing the standard using the Scyther tool, we surprisingly find that the most recent version of this standard still exhibits both known and new weaknesses. We therefore propose fixes and use `scyther-proof` to generate machine-checked proofs of the correctness of our repaired protocols. The ISO/IEC working group responsible for the 9798 standard has released an updated version of the standard based on our proposed fixes.

Zusammenfassung

Sichertheitsprotokolle sind verteilte Algorithmen für den sicheren Datenaustausch über unsichere Netzwerke wie zum Beispiel das Internet. Sichertheitsprotokolle basieren oft auf kryptographischen Techniken und spielen eine kritische Rolle in modernen Netzwerken und Geschäftsprozessen. Diese Dissertation behandelt die automatische Verifikation von Sicherheitsprotokollen in symbolischen Modellen der Kryptographie. Die Verifikation von Sicherheitsprotokollen ist besonders wichtig, da ihr Design fehleranfällig ist, und weil Fehler in Sicherheitsprotokollen grosse Kosten verursachen können.

Die automatische Verifikation von Sicherheitsprotokollen war bereits Gegenstand von vielen Forschungsarbeiten. Es ist allerdings unmöglich eine Methode zu entwickeln, die alle Protokolle vollautomatisch verifizieren kann, da die Sicherheit von Protokollen unentscheidbar ist. Daher verfolgen sowohl die existierenden Arbeiten wie auch diese Dissertation das Ziel, die Anwendbarkeit von automatischen Methoden im Bezug auf praktisch relevante Protokolle zu erhöhen. In diesem Kontext ist unsere Entwicklung der Theorie und der Implementierung des Tamarin Beweisers ein signifikanter Fortschritt. Der Tamarin Beweiser ist das erste Werkzeug, das sowohl Protokolle mit Schleifen und nicht-monotonischem Zustand als auch Diffie-Hellman Protokolle im Bezug auf starke Angreifer vollautomatisch und ohne zusätzliche Beschränkungen verifizieren kann. Die Theorie, welche dem Tamarin Beweiser zugrunde liegt, ist aus zwei Gründen von besonderem Interesse. Erstens basiert sie auf einem einfachen aber sehr ausdrucksstarken Modell von Sicherheitsprotokollen. Und zweitens ist sie so strukturiert, dass zukünftige Erweiterungen einfach darauf aufgebaut werden können.

Abgesehen von der Entwicklung des Tamarin Beweisers, geben wir in dieser Dissertation auch eine Antwort auf die Frage, wie man die Vertrauenswürdigkeit der Resultate von vollautomatischen Verifikationswerkzeugen erhöhen kann. Wir formulieren einen generischen Ansatz, um einen Algorithmus zur Sicherheitsprotokollverifikation so zu modifizieren, dass er automatisch Sicherheitsbeweise generiert. Wir validieren diesen Ansatz indem wir `scyther-proof` implementieren. Dies ist eine Version des Scyther Tools, welche automatisch Sicherheitsbeweise generiert und in dem Isabelle/HOL Theorembeweiser überprüft. Wir demonstrieren die praktische Anwendbarkeit von `scyther-proof` und dem Scyther Tool an dem ISO/IEC 9798 Standard for Entitity Authentication, welcher eine Kernkomponente in weiteren Standards ist. Überraschenderweise stellten wir bei der Analyse der aktuellsten Version des Standards mit dem Scyther Tool fest, dass diese Version immer noch bereits bekannte und auch neue Mängel aufweist. Wir schlugen daher Reparaturen vor und bewiesen die Korrektheit unserer Reparaturen mit Hilfe von `scyther-proof`. Die für den 9798 Standard verantwortliche ISO/IEC Arbeitsgruppe hat daraufhin eine aktualisierte Version des Standards herausgegeben, welche auf unseren Reparaturen basiert.