Automated reasoning for security protocol analysis

Journal of Automated Reasoning (2006) 36: 1–3
DOI: 10.1007/s10817-005-9014-x

Automated Reasoning for Security Protocol Analysis

Experience over the past 20 years has shown that, even assuming perfect cryptography, the design of security protocols (or cryptographic protocols, as they are sometimes called) is highly error-prone and that conventional validation techniques based on informal arguments or testing are not up to the task. It is now widely recognized that only formal analysis can provide the level of assurance required by both the developers and the users of the protocols.

Work in this direction initially started in the security community, but recently there has been a tremendous progress thanks to contributions from different automated reasoning communities, such as automated deduction, model checking, and artificial intelligence. Moreover, there has been another wave of progress in foundations for analyzing protocols and their properties by applying nonclassical logics, such as epistemic and belief logics. A large number of formal methods and tools have thus been developed that have been quite successful in analyzing many protocols, that is, in proving the correctness of the protocols or in identifying attacks on them. Thus, this progress can be seen as one of the recent success stories of the automated reasoning community.

In July 2004, the first workshop on Automated Reasoning for Security Protocol Analysis (ARSPA '04) took place as a satellite event of the 2nd International Joint Conference on Automated Reasoning (IJCAR '04).

This special issue is based on 21 submissions, following an open call for papers motivated by the success of the workshop. After refereeing, we selected five papers for publication. These papers offer a good overview of the current research on automated reasoning techniques and tools for the formal specification, analysis, and verification of security protocols.

The paper *Verifying the SET Purchase Protocols*, by Bella, Massacci, and Paulson, details the first verification results for the complete purchase protocols of SET (Secure Electronic Transaction, a suite of protocols proposed by a consortium of credit card companies and software corporations to secure e-commerce transactions). Using Isabelle and the inductive method, they show that the protocols' primary goal is indeed met. However, a lack of explicitness in the dual signature makes some agreement properties fail: it is impossible to prove that the cardholder meant to send his credit card details to the very payment gateway that receives them. Although the protocols' complexity and size makes

verification difficult, compared with other protocols, the authors' effort has yielded significant insights.

In the paper *Formal Analysis of MultiParty Contract Signing* Chadha, Kremer, and Scedrov analyze the multiparty contract-signing protocols of Garay and MacKenzie (GM) and of Baum and Waidner (BW). They use a finite-state tool, MOCHA, that allows for the specification of protocol properties in a branching-time temporal logic with a game semantics. While their analysis does not reveal any errors in the BW protocol, in the GM protocol they discover serious problems with fairness for four signers and an oversight regarding abuse-freeness for three signers. They thus propose a complete revision of the GM subprotocols in order to restore fairness.

In the paper *Decision Procedures for the Security of Protocols with Probabilistic Encryption against Offline Dictionary Attacks*, Delaune and Jacquemard consider the problem of automatic protocol verification when some data, such as poorly chosen passwords, can be guessed by dictionary attacks. They propose an inference system that extends a set of Dolev–Yao intruder deduction rules with the introduction of a probabilistic encryption operator and guessing abilities for the intruder. They show that the intruder deduction problem in this extended model is decidable in PTIME. This result yields an NP decision procedure for the protocol insecurity problem in the presence of a passive intruder, while the same problem is proved to be NP-complete in the active case.

In the paper *Decidability Issues for Extended Ping-Pong Protocols*, Hüttel and Srba use techniques from process algebra to investigate the class of ping-pong protocols introduced by Dolev and Yao. They show that all nontrivial properties, including reachability and equivalence checking with respect to the entire van Glabbeek's spectrum, become undecidable for a very simple recursive extension of the protocol. The result holds even if a nondeterministic choice operator is not allowed, but reachability is shown to be decidable in polynomial time if only two parties are participating in the protocol. They also show that the calculus is capable of an implicit description of the active intruder, including full analysis and synthesis of messages in the sense of Amadio, Lugiez, and Vanackère. Further, they show that reachability analysis for a replicative protocol variant is decidable.

The starting point of the paper *Attacking Group Protocols by Refuting Incorrect Inductive Conjectures*, by Steel and Bundy, is the observation that automated tools for finding attacks on flawed security protocols often fail to deal adequately with group protocols. The reason is that the abstractions made to improve performance on fixed two- or three-party protocols either preclude the modeling of group protocols or permit modeling only in a fixed scenario, which can prevent attacks from being discovered. Their paper describes CORAL, a tool for finding counterexamples to incorrect inductive conjectures, which they have used to model protocols for both group key agreement and group key

management, without any restrictions on the scenario. They used CORAL to discover six previously unknown attacks on three group protocols.

This special issue could not have been possible without the excellent work of the additional reviewers, to whom we express special thanks: Pedro Adão (IST Lisbon, Portugal), Massimo Benerecetti (Università di Napoli 'Federico II', Italy), Carlos Caleiro (IST Lisbon, Portugal), Luca Compagna (Università di Genova, Italy), Giorgio Delzanno (Università di Genova, Italy), Pierre Ganty (Université Libre de Bruxelles, Belgium), Paul Hankes Drielsma (ETH Zurich, Switzerland), Pierre-Cyrille Héam (Université de Franche-Comté, France), Felix Klaedtke (ETH Zurich, Switzerland), Monika Maidl (Siemens AG München, Germany), Jacopo Mantovani (Università di Genova, Italy), Paulo Mateus (IST Lisbon, Portugal), Laurent Mazaré (VERIMAG, France), Adriano Peron (Università di Napoli 'Federico II', Italy), Graham Steel (University of Edinburgh, Scotland), Sorin Stratulat (Université de Metz, France), Tomasz Truderung (LORIA-INRIA-Lorraine, France), Mathieu Turuani (LORIA-INRIA-Lorraine, France), Laurent Vigneron (LORIA-INRIA-Lorraine, France), and David von Oheimb (Siemens AG München, Germany).

We further thank all the authors for their work in preparing and revising the papers, and the JAR editors who made all this possible.

The Editors of the Special Issue

Alessandro Armando
Università di Genova, Italy

David Basin
ETH Zurich, Switzerland

Jorge Cuellar
Siemens AG München, Germany

Michaël Rusinowitch
LORIA-INRIA-Lorraine, France

Luca Viganò
ETH Zurich, Switzerland