Electronic Notes in Theoretical Computer Science
Volume 174, Issue 4, 30 May 2007, Pages 117-130

A Method for Patching Interleaving-Replay Attacks in Faulty Security Protocols (Article) (Open Access)

Pimentel, J.C.L.[a] , Monroy, R.[a] , Hutter, D.[b]

[a]Computer Science Department, Tecnológico de Monterrey, Carretera al lago Guadalupe, Km 3.5, Atizapán, 52926, Mexico
[b]DFKI, Saarbrücken University, Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany

Abstract

View references (15)

The verification of security protocols has attracted a lot of interest in the formal methods community, yielding two main verification approaches: i) state exploration, e.g. FDR [Gavin Lowe. Breaking and fixing the needham-schroeder public-key protocol using FDR. In TACAs'96: Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems, pages 147-166, London, UK, 1996. Springer-Verlag] and OFMC [A.D. Basin, S. Mödersheim, and L. Viganò. An on-the-fly model-checker for security protocol analysis. In D. Gollmann and E. Snekkenes, editors, ESORICS'03: 8th European Symposium on Research in Computer Security, number 2808 in Lecture Notes in Computer Science, pages 253-270, Gjøvik, Norway, 2003. Springer-Verlag]; and ii) theorem proving, e.g. the Isabelle inductive method [Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. Journal in Computer Security, 6(1-2):85-128, 1998] and Coral [G. Steel, A. Bundy, and M. Maidl. Attacking the asokan-ginzboorg protocol for key distribution in an ad-hoc bluetooth network using coral. In H. König, M. Heiner, and A. Wolisz, editors, IFIP TC6 /WG 6.1: Proceedings of 23rd IFIP International Conference on Formal Techniques for Networked and Distributed Systems, volume 2767, pages 1-10, Berlin, Germany, 2003. FORTE 2003 (work in progress papers)]. Complementing formal methods, Abadi and Needham's principles aim to guide the design of security protocols in order to make them simple and, hopefully, correct [M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. IEEE Transactions on Software Engineering, 22(1):6-15, 1996]. We are interested in a problem related to verification but far less explored: the correction of faulty security protocols. Experience has shown that the analysis of counterexamples or failed proof attempts often holds the key to the completion of proofs and for the correction of a faulty model. In this paper, we introduce a method for patching faulty security protocols that are susceptible to an interleaving-replay attack. Our method makes use of Abadi and Needham's principles for the prudent engineering practice for cryptographic protocols in order to guide the location of the fault in a protocol as well as the proposition of candidate patches. We have run a test on our method with encouraging results. The test set includes 21 faulty security protocols borrowed from the Clark-Jacob library [J. Clark and J. Jacob. A survey of authentication protocol literature: Version 1.0. Technical report, Department of Computer Science, University of York, November 1997. A complete specification of the Clark-Jacob library in CAPSL is available at http://www.cs.sri.com/millen/capsl/]. © 2007.

SciVal Topic Prominence

Topic: Network protocols | Cryptography | cryptographic protocol

Prominence percentile: 87.880

Author keywords

Fault localization | patching | replay attacks | security protocols | verification

Indexed keywords

Engineering controlled terms: Authentication | Electric fault location | Mathematical models | Network protocols | Software engineering | Formal methods | Formal verification | Mobile security | Theorem proving | Verification

Engineering uncontrolled terms: Replay attacks | Security protocols

Engineering main heading: Network security | Network security

Engineering uncontrolled terms: Cryptographic protocols | Engineering practices | Fault localization | Inductive method | patching | Replay attack | Security protocols | State exploration

Funding details

Funding sponsor	Funding number	Acronym
Instituto Tecnológico y de Estudios Superiores de Monterrey	CCEM-0302-05	

Funding text

1 We are grateful to Alan Bundy, Graham Steel and the reviewers for their useful comments on an earlier draft of this paper. The research reported here was supported by ITESM CCEM-0302-05.

ISSN: 15710661
Source Type: Journal
Original language: English

DOI: 10.1016/j.entcs.2006.12.034
Document Type: Article