MAP-i Doctoral Program in Computer Science
Thesis Proposal

Topic

Automated verification of security protocols

Supervisors

- Rogério Reis (rvr@ncc.up.pt), Departamento de Ciência de Computadores,FCUP
- Nelma Moreira (nam@ncc.up.pt), Departamento de Ciência de Computadores,FCUP

Research Unit

LIACC - Laboratório de Inteligência Artificial e Ciência de Computadores (Web:www.liacc.pt)

Brief Description

Design and analysis of security protocols has been a challenging problem over 30 years. Computational approaches consider issues of complexity and probability. They capture a strong notion of security, guaranteed against all probabilistic polynomial-time attacks. Although realistic, they are too difficult to design automatic verification tools. Logic-based approaches rely on a symbolic model of protocol executions which enable significantly simpler and often automated proofs. However, their soundness with respect to security guarantees are many times unclear, or ,if strong enough, they became undecidable. Model checking, theorem proving, type systems, process calculi, automata-based methods and symbolic constraints programing have been considered to tackle with the several issues addressed: strong expressiveness, bounded/unbounded resources and sessions, etc.

The aim of this proposal is to contribute to the development of logical based methods for formally prove properties of security protocols (e.g. authentication, secrecy or confidentiality, freshness, ...). The formalisms to be developed should mainly address the following points:

- algebraic extensions of perfect secrecy of the Dolev and Yao model
- realistic abstractions of infinite-state systems
- identify classes of protocols with decidable security properties
- to be applicable to real-life protocols

References

[1] M. Abadi. Security protocols: Principles and calculi (tutorial notes). In Springer-Verlag, editor, *Foundations of Security Analysis and Design IV, FOSAD*, pages 1–23., 2007.

[2] M. Boreale and M.G. Buscemi. Method for symbolic analysis of security protocols. *Theoretical Computer Science*, 338(1):393–425, 2005.

[3] Edmund M. Clarke, Marius Minea, and Ferucio Laurentiu Tiplea, editors. *Verification of Infinite-State Systems with Applications to Security, Proceedings of the NATO Advanced Research Workshop "Verification of Infinite State Systems with Applications to Security VISSAS 2005", Timisoara, Romania, March 17-22, 2005*, volume 1 of *NATO Security through Science Series D: Information and Communication Security*. IOS Press, 2006.

[4] Cas J.F. Cremers. Unbounded verification, falsification, andcharacterization of security protocolsby pattern refinement. In ACM, editor, *CCS'08*, 2008.

[5] Danny Dolev and Andrew Chi-Chih Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[6] G.Bella. *Formal Correctness of Security Protocols*. Springer Information Security and Cryptography series. Springer-Verlag, 2007.

[7] Antti Huima. Efficient infinite-state analysis of security protocols. In *Proc. FLOC'99 Workshop on Formal Methods and Security Protocols*, 1999.

[8] Guoqiang Li. *On the fly Model Checking of Secutrity Protocols*. PhD thesis, Japan Advanced Institute of Science and Technology, 2008.

[9] Stéphanie Delaune et Pascal Lafourcade Véronique Cortier. A survey of algebraic properties used in cryptographic protocols. Technical report, Loria, Laboratoire Spécification Vérification, Laboratoire Verimag, Cril Technology and France Telecom, 2004.