Formal Analysis of Security Protocols

Ahmed BOUABDALLAH

IMT Atlantique
Campus of Rennes

The so-called security protocols are protocols using encryption primitives. This course begins with an overview of families of security protocols. In a second step, we will study in detail the family of fair exchange protocols, of which non-repudiation and electronic signature of contracts are special cases. The proposed analysis is conducted in a formal context. Supervised work and laboratory work dedicated to the study of a non-repudiation protocol illustrate the concepts introduced.

Syllabus

1. Introduction

2. Examples of security protocols
   a. Authentication
   b. Fair Exchange protocols
      i. Non repudiation
      ii. Contract signing

3. Formal Analysis of fair exchange protocols
   a. Formal methods and model checking
   b. Transition systems
      i. Representing a program with a transition system
      ii. Analysis of an elementary protocol
   c. Temporal logics
      i. Tree temporal logic CTL*, CTL
      ii. Linear temporal logic LTL
   d. A formal expression of the properties of the fair exchange
      i. Alternative temporal logic ATL
      ii. Fair exchange in ATL
      iii. Non repudiation in ATL

4. Supervised work
   a. From a textual description of a non repudiation protocol to a formal model

5. Labs work
   a. Formal analysis of the Zhou-Gollman non repudiation protocol using the MOCHA model-checker

References

Non-repudiation in electronic commerce
Jianying Zhou
Artech House, 2001

Asynchronous protocols for optimistic fair exchange
N.Asokan, V.Shoup and M.Waidner
Proc. 4th ACM Conf. Computer and Communications Security, pp.8-17, 1997.

An intensive survey of fair non-repudiation protocols
S.Kremer, O.Markowitch, J.Zhou
Computer Communications, Vol.25(17), 2002, pp.1606-1621

Abuse-free optimistic contract signing
J.A.Garay, M.Jakobson and P.D.MacKenzie
Advances in Cryptology – Crypto 1999, LNCS N° 1666, pp.449-466, 1999.

A game-based verification of non-repudiation and fair exchange protocols
S.Kremer, J-F.Raskin
Journal of Computer Security, Vol.11(3), 2003, pp.399 - 429

Alternating-time temporal logic
R.Alur, T.A.Henzinger, O.Kupferman
Journal of the ACM, Vol.49(5), 2002, pp.672 - 713

Reactive modules
R.Alur and T.H.Henzinger
Proc. 11th Symp. Logic in Computer Science, pp.207-218, 1996.

MOCHA tool
- Univ. Pennsylvanie ==> http://www.cis.upenn.edu/~mocha/
- EPFL ==>
http://mtc.epfl.ch/software-tools/mocha/download/c-mocha/distribution/