On-the-fly Model Checking of Security Protocols

Guoqiang LI
School of Information Science,
Japan Advanced Institute of Science and Technology

March 6, 2008

Abstract

Security protocols, although each of them only contains several flows, easily cause attacks even without breaking cryptography algorithms. Design and analysis of security protocols prove to be a challenging problem over 30 years. Many formalisms have been adopted to describe security protocols, and been analyzed by various automatic and semi-automatic techniques. Due to the complication of the network, methodologies for the analysis should be carefully designed to represent each infinity factor one assumed, such as, an unbounded number of sessions one principal participates, an unbounded number of principals one principal communicates with, and an unbounded number of messages intruders and dishonest principals produce.

A dilemma has occurred when one tries to propose a methodology for security protocol analysis, dealing with the infinity factors introduced above. On the one hand, a model for security protocols should be strong enough in expressiveness to describe any possible situation that a running protocol may reach, otherwise it may fail in detecting subtle attacks. On the other hand, analyzing a property on a model strong in expressiveness may be undecidable. Thus automatic techniques may not terminate when detecting flaws.

This thesis proposes a sound and complete model checking method to analyze various security properties under certain assumptions. That is, when flaws are not detected, the protocol is guaranteed to be secure under these assumptions. An environment-based process calculus is introduced to describe behaviors of security protocols. Deductive systems can be inserted freely in the model, to represent infinitely many messages intruders or dishonest principals generate, due to different security assumptions. A trace semantics is chosen for the calculus, so that each possible run of a security protocol can be represented explicitly by a concrete trace. The main contributions and achievements are:

- When various security properties of security protocols are analyzed under different assumptions, infinity factors are abstracted to be finite by several techniques, so that security properties can be checked automatically by a sound and complete on-the-fly model checking under these assumptions, including, (i) secrecy and authentication properties in bounded sessions, (ii) authentication property for recursive protocols, and (iii) non-repudiation and fairness properties in bounded sessions. Among them, (ii) and (iii) are first analyzed by model checking methods.
- Protocol-independent specifications for secrecy and authentication properties are proposed. In this approach, the specifications for secrecy and authentication properties can be generated automatically from a protocol description. In comparison, other approaches, especially process calculi based approaches, define a security specification dependent on a given security protocol manually .

The methodology is implemented by Maude. By the facility of the reachability analysis in Maude (implemented as `search`), each property can be checked at the same time when a model is generated.

Key Words: **Security Protocols, On-the-fly Model Checking, Secrecy, Authentication, Non-repudiation, Fairness, Recursive Protocols, Maude**