Luu, Anh Tuan; **Sun, Jun**; **Liu, Yang**; **Dong, Jin Song**

SeVe: automatic tool for verification of security protocols. (English) Zbl 1251.68142

Front. Comput. Sci. 6, No. 1, 57-75 (2012).

Summary: Security protocols play more and more important roles with wide use in many applications nowadays. Currently, there are many tools for specifying and verifying security protocols such as Casper/FDR, ProVerif, or AVISPA. In these tools, the intruder's ability, which either needs to be specified explicitly or set by default, is not flexible in some circumstances. Moreover, whereas most of the existing tools focus on secrecy and authentication properties, few supports privacy properties like anonymity, receipt freeness, and coercion resistance, which are crucial in many applications such as in electronic voting systems or anonymous online transactions. In this paper, we introduce a framework for specifying security protocols in the labeled transition system (LTS) semantics model, which embeds the knowledge of the participants and parameterizes the ability of an attacker. Using this model, we give the formal definitions for three types of privacy properties based on trace equivalence and knowledge reasoning. The formal definitions for some other security properties, such as secrecy and authentication, are introduced under this framework, and the verification algorithms are also given. The results of this paper are embodied in the implementation of a SeVe module in a process analysis toolkit (PAT) model checker, which supports specifying, simulating, and verifying security protocols. The experimental results show that a SeVe module is capable of verifying many types of security protocols and complements the state-of-the-art security verifiers in several aspects. Moreover, it also proves the ability in building an automatic verifier for security protocols related to privacy type, which are mostly verified by hand now.

MSC:

68Q60	Specification and verification (program logics, model checking, etc.)
94A62	Authentication, digital signatures and secret sharing
68M12	Network protocols

Cited in **1** Document

Keywords:

security protocols; model checking; process analysis toolkit (PAT); authentication; secrecy; privacy

Software:

AVISPA; Casper; PAT; ProVerif; SeVe

Full Text: DOI