Computationally Sound Mechanized Proofs for Basic and Public-key Kerberos

Bruno Blanchet[1] Aaron D. Jaggard[2] Andre Scedrov[3]
Joe-Kai Tsay[3]

[1]CNRS, École Normale Supérieure, INRIA
[2]DIMACS, Rutgers University
[3]Department of Mathematics, University of Pennsylvania

June 2008

Verifying Kerberos in the computational model

- Kerberos: a non-trivial, industrial security protocol.
  3 rounds, 4 participants, ...
- We study it using CryptoVerif, a mechanized prover for security protocols sound in the computational model.
  - CryptoVerif produces proofs by sequences of games as used by cryptographers.
  - It proves secrecy and correspondence properties.
  - It handles many cryptographic primitives.
  - It provides proofs valid for a polynomial number of sessions with an active adversary.
  - It provides a bound on the probability of an attack.
  - It works automatically or with little help from the user.

Properties proved

We consider both basic Kerberos and its public-key extension PKINIT.

We prove:

- Authentication properties
- Secrecy of keys (before they are used in the protocol)
- Key usability: when a key has been used for encryption, it is no longer secret (in the computational sense), but it may still be usable in future encryption.
  We extend a previous notion of key usability by Datta et al (CSFW'06), and prove our new notion using CryptoVerif.

Conclusion

- We provide the first mechanized proof of an industrial security protocol at the computational level.
- Our model of Kerberos is still fairly abstract; it would be interesting for future work to model some more details of the specification.
- CryptoVerif is a prototype, but it can already prove non-trivial protocols.
- This case study suggested a number of improvements to CryptoVerif.

Paper published at AsiaCCS'08, available with the CryptoVerif scripts at http://www.cryptoverif.ens.fr/kerberos/

Details on CryptoVerif at http://www.cryptoverif.ens.fr/