Mechanized Verification of Kerberos

Andre Scedrov - http://www.cis.upenn.edu/~scedrov/
Joint work with M. Backes, B. Blanchet, I. Cervesato, A.D. Jagiard, J.-K. Tsay and C. Walstad

Part of ongoing formal analysis of Kerberos 5 security protocol suite, partially supported by NSF and ONR

Kerberos

Widespread single sign-on authentication and key exchange protocol

- Repeatedly authenticates a client to multiple servers
- On IETF standards track (RFC 4120)
  - Public-key extension PKINIT (RFC 4556)
- Previously: computationally sound by-hand proofs of Kerberos 5 and public-key
  Kerberos using the BPW model of M. Backes, B. Pfitzmann and M. Waidner
  - Proofs in Dolev-Yao style model cryptographically sound, assuming provably secure primitives
  - Entity authentication holds in computational model but the exchanged keys not indistinguishable from random
  - Boldyreva and Kumar subsequently showed that primitives are available in basic Kerberos specs which meet our provable security assumptions

Cryptographically Sound Mechanized Security Proofs

Kerberos 5 and public-key Kerberos

- Using the mechanized prover Cryptoverif
- Verified entity authentication properties and key secrecy properties, assuming the same provably secure primitives as in previous work (e.g. IND-CCA2 and INT-CTX for symmetric encryption)

First cryptographically sound mechanized security proofs for industrial protocols

Cryptoverif

- Verifies security protocols directly in computational model
- Based on probabilistic polynomial-time calculus by P. Lincoln, J. Mitchell, M. Mitchell, A. Ramanathan, A. Scedrov and V. Teague
- Proofs as sequences of indistinguishable games
  - Initial game of the sequence represents protocol, in last game security properties should be obvious
  - Security of cryptographic primitives specified through indistinguishable oracles

Strong Key Usability

- Generalization of Key Usability
  - Stronger notion models more realistic scenario
- First mechanic verification of (Strong) Key Usability
- Keys exchanged during a Kerberos session are (strongly) usable for IND-CCA2 symmetric encryption, for the encryption scheme used during the Kerberos session

Work will be presented at ASIACCS’08