

Security Analysis of Public-Key Kerberos

Andre Scedrov – <http://www.cis.upenn.edu/~scedrov/>

Joint work with I. Cervesato, A.D. Jaggard, 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 protocol

- Repeatedly authenticates a client to multiple servers
- Available for all major operating systems
- On IETF standards track (RFC 4120)

PKINIT

Adds flexibility & security to Kerberos by relying on public-key infrastructure

- Replaces first exchange of Kerberos
- E.g., used for smart-card authentication
- IETF draft in May 2005

Attack

Man-in-the-middle attack on PKINIT draft

- Attacker can impersonate all servers to the client
Breach of authentication
- Attacker can monitor client's communications
Breach of confidentiality

Possible because PKINIT does not sign data identifying the client

Affected systems

- Recent versions of MS Windows
- Recent versions of Linux

Fix

Sign data identifying the client

- Sign entire first message: adopted by IETF (RFC 4556)

Authentication proof in the symbolic (Dolev-Yao) model

- Assuming pre-image resistance and secrecy of long-term keys

PKINIT fixed in Windows in Microsoft Security Bulletin MS05-042 (8/9/2005), which mentions our work

Our work was presented at IETF-63 and ASIAN'06

- IETF officials encouraged the use of formal methods in protocol development

Computationally Sound Security Proofs (with M. Backes)

Kerberos 5 and Public-key Kerberos (with fixed PKINIT)

- First computationally sound security analysis of an industrial protocol
- 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 key is not indistinguishable from random

- Future work: modularity

Our work was presented at ESORICS'06

