The Simple Public Key GSS API Mechanism (SPKM)

– UPDATE –

Carlisle M. Adams
Paul Van Oorschot
Bell-Northern Research

Dec. 5-9, 1994
31st Internet Engineering Task Force
San Jose, CA

Outline

- Background
  - Generic Security Service (GSS) [RFC 1508]
  - Kerberos 5 [draft-ietf-cat-kerb5gss-01.txt]
  - SPKM [draft-ietf-cat-spkmgss-00.txt]
- SPKM Feature Overview
- Changes from 00 to 01
- Implementation News
- Conclusions

Background

- Generic Security Service (GSS)
  - an interface specification
  - defines a set of calls for services which applications developers can use to incorporate security
  - actual mechanisms which implement these calls can be supplied independently and linked in with application code
  - many such mechanisms can be developed and should be interchangable with no application impact

Background (cont'd)

- Kerberos 5 (draft-ietf-cat-kerb5gss-01.txt)
  - a GSS-conformant Kerberos implementation
  - uses Kerberos-dependent authentication, integrity, and confidentiality
- SPKM (draft-ietf-cat-spkmgss-00.txt)
  - another GSS mechanism
  - based on public-key, rather than symmetric-key, infrastructure
  - introduced as draft id. in June 94 and reviewed at Toronto IETF (July 1994)

Outline

- Background
  - Generic Security Service (GSS) [RFC 1508]
  - Kerberos 5 [draft-ietf-cat-kerb5gss-01.txt]
  - SPKM [draft-ietf-cat-spkmgss-00.txt]
- ⇨ SPKM Feature Overview
- Changes from 00 to 01
- Implementation News
- Conclusions

SPKM Feature Overview

- Public Key Infrastructure
- Timestamp-based or random-number-based auth. (available to environments without secure time)
- Use of Alg. IDs wherever possible to allow maximum flexibility and growth
- Use of negotiation at context establishment to allow interoperability between environments
- QOP parameter (from application) selects data integrity mechanism: non-repudiation can be in effect over context if desired

Outline

- Background
  - Generic Security Service (GSS) [RFC 1508]
  - Kerberos 5 [draft-ietf-cat-kerb5gss-01.txt]
  - SPKM [draft-ietf-cat-spkmgss-00.txt]
- SPKM Feature Overview
- ➯ Changes from 00 to 01
- Implementation News
- Conclusions

Changes: Token-Affecting

- Syntax changes to better align with SESAME
- Clean-up of authentication terminology and SPKM-1 / SPKM-2 distinction:

random-number-based (SPKM-1)
- unilateral: 2-pass (Target authenticated to Initiator)
- mutual: 3-pass

timestamp-based (SPKM-2)
- unilateral: 1-pass (Initiator authenticated to Target)
- mutual: 2-pass

Changes: Token-Affecting (cont'd)

- "OBJECT ID" changed to "AlgorithmIdentifier"
  - facilitates interoperability since alg. parameters can be sent
- Context neg. now includes key estb. mech.
  - facilitates interoperability
- All tokens now specified in ASN.1 BER
  - removes ambiguity w.r.t. field lengths and encoding
- SPKM-REQ now specifies certif_data to be OPT
  - compensates by putting src_name in REQ_TOKEN

Changes: Token-Affecting (cont'd)

- SPKM-REQ now includes OPT Auth. Data field
  - for use as in Kerberos (RFC-1510)
- SPKM-REQ now includes OPT validity interval
  - validity interval for context key
  - may be used in computation of context lifetime
- Error token now includes enc. sequence num. of the token which caused this error ("guilty_seq")
  - allows receiver to re-send bad token or pass intelligent msg. back to its application

Changes: Descriptive

- 2 extra integrity algorithms given
  - no Alg. IDs specified yet
  - one allows single-pass integrity and encryption for data
  - other specifies encrypted MD5 hash of data
- Better distinction/use of context key, derived keys
- A few more error codes (minor status codes)
- Textual changes, more explanatory paragraphs

Outline

- Background
  - Generic Security Service (GSS) [RFC 1508]
  - Kerberos 5 [draft-ietf-cat-kerb5gss-01.txt]
  - SPKM [draft-ietf-cat-spkmgss-00.txt]
- SPKM Feature Overview
- Changes from 00 to 01
- ➯ Implementation News
- Conclusions

Two Independent Implementations

- BNR implementation is near to completion (due at end of '94)
- Our implementation is not public domain
  - some proprietary features / algorithms
  - high-performance versions of public algorithms
- Public domain version is being developed as a project at U. New Brunswick
- Interoperability testing over next 2-3 months; results to be discussed at April IETF...

Outline

- Background
  - Generic Security Service (GSS) [RFC 1508]
  - Kerberos 5 [draft-ietf-cat-kerb5gss-01.txt]
  - SPKM [draft-ietf-cat-spkmgss-00.txt]
- SPKM Feature Overview
- Changes from 00 to 01
- Implementation News
- ⇨ Conclusions

Conclusions

- SPKM is a useful GSS API implementation with some advantages over available alternatives:
  - flexibility
  - non-repudiation
  - negotiation of algorithms
  - no forced reliance on secure timestamps
  - no reliance on trusted on-line servers
- SPKM is being implemented by BNR and independently by Univ. of New Brunswick
- We propose progressing SPKM as a standards-track RFC