Kerberos Working Group

Interim Meeting Report

Interim Meeting Report

- February 12-13, 2002 at MIT
- 10 attendees
- 2 implementors

Interim Meeting Discussions

- Many desired changes
- Essential features for the next version
- Two documents
  - kerberos-clarifications
  - kerberos-extensions
- Items to be done in clarifications
- Items to be done in extensions
- Separate work

Essential items for the next document

- RFC1510 compatibility
- Clarifications to RFC1510
  - Name types
  - KDC replay cache behaviour
  - Implementation notes
- Modern crypto architecture
- How to find a KDC
- New network address types
- TCP

Clarifications vs Extensions

Problem: Conflicting requirements

- Clarifications to RFC1510 badly needed
- WG wanted extensibility
- IESG mandate for internationalization
- WG wanted various new features
- Features vs time-to-market

Clarifications vs Extensions

Solution: Two documents

- kerberos-clarifications
  - Clarifications and document cleanup
  - Critical new features
  - Minimal impact on implementors
- kerberos-extensions
  - Internationalization
  - Complete extensibility
  - Many new features

kerberos-clarifications

- Goals
  - Must be compatible with RFC1510
  - Must be compatible with existing implementations
  - Minimize implementation cost
  - Minimize testing cost
- Document Cleanup
  - Section with combined ASN.1
  - Drop description of KDB
  - Drop pseudo-code
- Clarifications
  - Name types are advisory
  - KDC replay cache behaviour
  - Implementation notes
  - Others

kerberos-clarifications

- New Items -- many from previous kerberos-revisions
  - Modern crypto
    - draft-ietf-krb-wg-crypto-00.txt
  - How to find a KDC
    - draft-ietf-krb-wg-krb-dns-locate-02.txt
  - TCP
  - Network address types (IPv6, others?)
  - Time skew
  - transited-checked
  - ok-as-delegate
- Update MUST-implement requirements

kerberos-extensions

- Goals
  - Must be compatible with RFC1510
  - Use message formats similar to RFC1510
- Internationalization
  - IESG mandate for internationalization
  - IESG mandate for UTF-8 encoding
  - Support UTF-8 in principals, realms, passwords
  - Migration for old just-send-8
- Future Enhancements
  - Ability for IETF to enhance/evolve protocol
  - Support for adding IETF and vendor extensions
  - Ticket extensions
  - Make PK* and other WG work items possible
  - Enable tying tickets to host/location/whatever

kerberos-extensions

- New Items
  - AES
  - New name types
    - XXX what are they?
  - Remove address dependencies
  - Cross-realm referrals
  - Client name canonicalization
  - Fix gnuftp.raeburn.org problem
    - XXX what is it
    - XXX separate document
  - Fix EDATA brokenness
  - Namespace restrictions
- Update MUST-implement requirements
- Authenticated cleartext ?

Additional Work

- Protect AS_REQ exchange from weak passwords
- PFS for KDC exchanges
- PFS for application exchanges
- Minor error codes
- Key exchange w/o authentication
- Timestamp-independence