Update on Kerberos Extensibility

`draft-ietf-krb-wg-rfc1510ter-03.txt`

Tom Yu

IETF 67

Overview

- Review 1510ter goals

- Open issues
  - Capability negotiation
  - Legacy strings
  - Number assignment policies
  - Authenticated plaintext

1510ter: Goals

- Compatible with existing where consistent (RFC1510)
- Minimize implementation, testing cost
- Where possible, support PK extensions
- Make sure other WG items can move forward
- Protocol guarantees shared KDB and keys
- Capability negotiation (allow pre-configured capability knowledge)
- Existing apps see no semantic or behavior change from RFC1510: If it worked in RFC1510, it should work now.

1510ter: New Additions

- Typed holes for vendor and IETF extensions
- ASN.1 extensibility markers for WG use
- Internationalization: Unicode names and pw; UTF-8
- Ticket extensions
- Client name canonicalization
- Authenticated plaintext
- Fix edata

1510ter: New Additions

- Additional flags: Consider anonymous
- Cross realm referrals (separate document?)
- Migration for old internationalization
- Update requirements again
- New and deprecated name types (SMTP)
- Name space constraints

1510ter: Things Enabled by Typed Holes

- Tie tickets to host / location / etc. (auth data)
- PFS for KDC and app. exchanges
- Encrypt KDC exchange (princ. privacy and reduce offline vulns)
- Prot AS-REQ weak password
- Minor error codes - implementation defined type hole

1510ter: If Done in Time

- Key exchange w/o authentication (KDC says don’t trust name - Nico)
- Timestamp independence
- Time stamp implementation reduction (?)

Capability Negotiation

- Client detects service capability via Ticket
- Service detects client capability via Ticket
- TicketExt only if all receiving instances support
- Mixes allowed (Ticket1510 containing EncTicketPartExt)
- U2U could be problematic (e.g., new service, old client)

Legacy Strings

- non-ASCII strings from old implementations
- mappings
- legacy characters not representable in Unicode?
- non-preauth case: try everything
- Extensions PDUs only have UTF8String? (except ticket weirdness)

Number Assignment Policies

Authenticated Plaintext