New Directions for the Updated Kerberos Protocol

Sam Hartman

Tom Yu

IETF 69

Terminology

- “New”: implementations supporting new messages & FAST
- “Old”: today’s existing implementations
- “Mixed”: “new” implementations supporting today’s (legacy non-ASCII) forms of internationalization

Motivation

- Provide internationalization support.
- Protect Kerberos exchanges (authenticated cleartext).
- Provide future extensibility for vendors and IETF.

Motivation: This Proposal

- Combine with FAST proposal for KDC protection and negotiation.
- Allow UTF8 strings.
- New enctype for ticket extensions.

Motivation: This Proposal (2)

- No one plans to implement extensions (rfc1510ter).
- Coupling proposals together increases desirability.
- Reduce implementation complexity of internationalization.

How Negotiation Works

- If FAST is offered by the KDC then these mechanisms MUST be supported.
- Encoding of ticket signals server support to the client.
- Clients use new messages as appropriate.

Mixed Mode Internationalization

- KDCs must know the old and new names of all principals.
- Clients must know the old and new name of their principal.
- Servers must be able to confirm that a given old name maps onto a new name.

Mixed Mode Internationalization (2)

- KDC can help the client talk to old servers by giving the client's old name.
- KDC can help new servers with old clients by giving the old and new name.
- Introduces complexity.

PDUs

- New protocol is diffs on top of RFC 4120.
- Keep changes to ASN.1 module of protocol minimal.
- No new APPLICATION tags, probably.
- Use correct tagging on UTF8String.
- Abandon SignedData; use FAST instead.

How Ticket Extensions Work

- Special enctype indicates that “ciphertext” of EncryptedData is a wrapper.
- Wrapper contains tagged extensions
- Wrapper also contains an EncryptedData containing actual EncTicketPart ciphertext.
- AEAD?

Forwarding Tickets

- You can tell from the service ticket whether the service is new or old. This assumes new services can always accept new forwarded tickets.

- Need a mechanism to request an old TGT to forward to an old server.

Sharing a Credentials Cache

- Multiple implementations sharing a cache is common on all hosted platforms.
- Need way for new clients to get old TGT for these cases.
- Retrieval and search interface must distinguish new and old tickets.
- Prevent old clients from using new tickets.

TransitedEncoding

- Intermediary new KDCs must know legacy encodings of old neighbors.
- Rewrite TransitedEncoding when crossing new/old boundary.
- What about multiple legacy encodings along path?

Open Questions

- Bootstrapping: null armor?
- Allow normal (unencapsulated) KDC PDUs after FAST negotiation? Probably not.
- How much progress do we make on unauthenticated cleartext?
- Do we care about AP-REQ?
- User-to-User