Questioning Kerberos Assumptions

Sam Hartman

IETF 63

Questioning Kerberos Assumptions

- Principal Names are not remapped in cross-realm
- The destination KDC is not involved in cross-realm
- Privacy of principal names

Why Remap Identifiers

- Liberty Alliance and other SAML consumers want to map identity.

- Mapping to reflect target account names may be useful.

Why Involve Destination KDC

- Symmetry of protocol
- Group membership and authorization data
- Single point of control for stoplists

Why Privacy

- Significant need in cellular and wireless communities for identifier privacy so that passive observers cannot know who is logging in.

- See the alien BOF.

Adding Identifier Mapping

- Need for client control
- Handling cases where different identities are needed
- Multi-hop Cross-realm

SAML: What is SAML

- SAML is an OASIS XML-based language for describing identity.
- SAML provides assertions about aspects of identity.
- These assertions can be included in other mechanisms.

SAML: SAML and Kerberos

- SAML Assertions in authorization data

- SAML Assertions replace principal name as important part of authentication as Microsoft PAC replaces the principal name

- SAML useful in preauthentication?

SAML: How SAML integration Might Work

- Client sends request including details of assertions service needs to KDC.
- KDC issues ticket with identity added/removed as appropriate.
- Client presents ticket to service.

SAML: Hard Problems

- How does a client know what assertions a server wants?
- How does a KDC decide what assertions are permitted?
- How do you manage all the possible tickets?

Mapping for Accounts

- Many platforms have a concept of mapping a foreign principal to an account within an infrastructure.
- Authorization data like the Microsoft PAC already supports this concept.
- Should core Kerberos?

Account Mapping: Questions

- Should the original authentication identity be preserved?
- To what extent is the client involved in remapping?
- How does this interact with GSS?

Involving the Destination KDC

Destination KDC: Symmetry

- Authorization data, ticket extensions and other protocol elements are added to TGTS.

- These elements are often realm specific.

- Handling on a per-service case for cross-realm problematic.

Privacy

Privacy: Types of Privacy

- Hiding identity from network eavesdroppers
- Hiding parts of identity from services and realms

Privacy: Possible Solutions

- Encrypt more of the KDC exchange
- Anonymous principals

Privacy: Questions

- Do we need privacy to the KDC?

- How do we handle legacy applications?

- How does this impact GSS?

Concluding Questions

- Are our current assumptions correct?
- If we change these assumptions can these changes be extensions or is the core protocol impacted?