Kitten BOF

New Challenges in GSSAPI Naming

Sam Hartman
MIT

August 2, 2004

Authentication and Authorization

- We need to draw a clear line between authentication and authorization.
- Authentication generates assertions as input to authorization.
- Authorization makes access decisions based on these assertions.

GSSAPI Authentication model

- GSSAPI asserts an authenticated name to both peers.
- All input forms of this name can be canonicalized to a single form.

Authorization with GSSAPI Names

- Canonical forms of names can be stored on ACLs.
- Without authentication a peer can generate canonical forms.
- More complicated structures are possible.

Difficulty of Canonical Forms

- Names change over time.
- Some mechanisms have no canonical representation.
- SubjectAltName creates problems for certificates.

Desire for New Authentication Assertions

- Membership in groups
- Initiatives such as Liberty and SAML require more complex assertions.
- Keeping names the same as people move in organizations

Possible Solutions

- Name attributes
- Extension to gss_canonicalize_name
- Credential extensions