Extended Names

for the Protection Service

Derrick Brashear

14 Sep 2010

PTS: Background

- PTS provides username and groupname mapping in AFS
- shadow -> 17985 (users are positive)
- shadow:shadow -> -3753 (groups are negative)

PTS: User use

- pts createuser, creategroup, delete
- pts adduser, removeuser, membership
- pts examine, listowned

PTS: Server use

- pr_GetCPS (gets a list of groups for an auth context)
- pr_GetHostCPS (above for a host context)
- pr_NameToId (converts a name to a number)
- pr_IdToName (converts a number to a name)

Limitations

- Authentication contexts tied to Kerberos identity.
- If you have multiple realms, they need to share a namespace.
  - What if you don't want to trust the other Kerberos admins that far? (foo/admin)

Limitations

- If you have multiple realms, they need to share a namespace.
  - What if you don't want to trust the other Kerberos admins that far?
    - Example: Trust them for users, but not admins

Limitations

- If you use a cell from more than one authentication context, different "you" don't share permissions.
  - shadow has one set of permissions
  - shadow@other.cell may not have the same ones.

PTS Extended Names

- Solution:
  - Allow multiple authentication names to be mapped to the same AFS ID.
  - Allow multiple authentication systems for mapping, so we are not tied to Kerberos 4, or even Kerberos 5.

New RPCs

- AuthNameToID
- AuthNameToIDFallback
- ListAuthNames
- WhoAmI
- AddAuthName
- RemoveAuthName

Name Types

- Kerberos 4
- GSSAPI (including Kerberos 5)
- More can be added

AuthNameToID

- Map name to ID
- GSSAPI:XXXXXXshadow@ANDREW.CMU.EDU -> 17985
- KERBEROS4:shadow@ANDREW.CMU.EDU -> 17985
- But this also allows you to name objects from other Kerberos realms.
- Fallback version includes implicit mappings

GSSAPI Name Type

- GSSAPI:XXXXXXshadow@ANDREW.CMU.EDU
  - XXXXX is really mechanism type OID and length data:
    - 2 byte TOK_ID (04 01)
    - 2 byte MECH_OID_LEN (00 0B = 11 bytes for krb5 OID)
    - (MECH_OID_LEN) byte MECH_OID (06 09 2A 86 48 86 F7 12 01 02 02)
    - 4 byte NAME_LEN (00 00 00 15 = 21 bytes for my name)
    - (NAME_LEN) byte NAME (shadow@ANDREW.CMU.EDU)

Usage case 1

- YOUR.REALM and WIN.YOUR.REALM
  - shadow in one is shadow in the other: both map to one AFS id
  - admin in one is not admin in the other: alternate mappings for AFS ids

Usage case 2

- YOUR.REALM and MY.REALM
  - Shared key between realms
  - shadow@YOUR.REALM can be made equivalent to shadow@MY.REALM such that only one user appears on the ACL, instead of a local user and a foreign user.
    - Allowed by the protocol, implementation would permit limiting of allowed realms.

WhoAmI

- Which credentials did you send the server?
  - Can be used to get a rendered form of your authentication name.
  - Note that GSSAPI includes exported names and display names, which may not match in rendering.

Add, List, Remove

- Analogous to current PTS operations
  - You obviously need to maintain this information.

When can you have it?

- RPCs need to be standardized.
  - http://tools.ietf.org/id/draft-brashear-afs3-pts-extended-names-06.txt
- Code in progress.

How can you help?

- Review the RPC draft!
  - Call for standards consensus soon.
- That's actually about it now.

Questions?