POSIX Authorization Data

Ben

Carrying POSIX Identity Information

- POSIX defines how the minimal set of Identity Information data should be provided to Operating Systems that adhere to the standard.
- Yet there is no real standard way to distribute this data across multiple networked systems in an efficient way at login time as POSIX deal only with local systems.
- Using LDAP is an option but has drawbacks

The PAD Authorization Data

- Carries all the necessary information to provide a full „POSIX profile“ for the user associated with the ticket client principal.
- Can be used by the OS if it trusts the information source
- Should be wrapped in the CAMMAC AD so that the KDC needs to request the information only once.
- usually generated at the time the TGT is created and returned to the client, but can be refresh or manipulated when copied into a TGS reply.

Use Cases

- Applications that know how to handle Kerberos Authorization Data but not know how or cannot access the POSIX Information source due to network segmentation or other limitations.
- Cross-Realm setups where one-way trusts are established such that the client can convey information to a service, but the service does not have an identity that allows it to query back the originating realm.

Required Data

- User Name (may differ from principal name)
- UidNumber and primary GidNumber, Home directory, Gecos, Shell
  - RFC2037/bis can be used as inspiration
- Group Memberships:
  - List of groups a user is member of, including group name and GidNumber
  - Origin Domain information for groups. (user of REALM A included in groups of REALM B)

Optional Data

- Alternative User Names or Identifiers
  - Alternative name spellings, email, etc.
- Additional User and Group UUIDs/GUIDs if available
- Non-POSIX group data if the original Identity Information storage provides such information, in this case a group type option would need to be included.

References

- Old PAD draft:
  - https://tools.ietf.org/html/draft-ietf-krb-wg-pad-01

- Benjamin Kaduk <kaduk@mit.edu>
- Simo Sorce <ssorce@redhat.com>