Kerberos referrals

IETF 70

Ken Raeburn

Changes coming in -10

- Info caching time per October email: optional expiration time field
- Removed MS appendix as planned
- Separate section introducing name type NT-ENTERPRISE

Issues

- Validation of client referral data
- Authorization data in cross-realm case
- NT-ENTERPRISE concept

Validation – one realm, shared pw

- Shared passwords allow MITM to cause client to use wrong principal
- Old defense was that client knew its principal name; no longer true when mapping enterprise principal names to other names
- PA-CLIENT-CANONICALIZED helps
  - Whichever account is used, it protects the returned copy of what the KDC saw requested

Validation – one realm, PKINIT

- No password!
- If one certificate can be used for more than one principal, same risk applies, and same solution.

Validation – multiple realms

- Attacker issues KRB-ERROR pointing client to wrong realm
- If new target realm has been compromised, attacker may be able to issue “authentic” alias info indicating the referral was valid
- Not a problem if KRB-ERROR is protected

Validation – multiple realms

- Limit accepted referral mappings by client-side policy to a cooperating set of realms that share alias info and are all trustworthy?
- To reduce risk, the realms must keep in sync

Alias “authorization” data

- AD-KDC-Issued description doesn't give any hints on how cross-realm cases should be addressed.
  - Trust path server can verify, or KDCs hop by hop?
  - General issue, not specific to referrals.
- For referrals, address local case only? Leave cross-realm case for further study.
  - Allow, but don't require, a KDC to re-sign the alias assertion itself if policy permits.

NT-ENTERPRISE

- How is it interpreted?
  - Does realm matter? Is realm ignored?
  - Must NT-ENTERPRISE names be processed specially wherever they may show up?
- Had two conversations this week, two very different answers

Other client c14n/referral

- Any reason to rule out client canonicalization or referrals with name types other than NT-ENTERPRISE?
- Not well described

More TODO

- Restore Windows appendix?
- List policies required, guidelines
- More examples!
  - Include u2u example
  - Cross realm?
  - Note when policy checks are required