Kerberos Version 5

John T. Kohl
Digital Equipment Corporation/Project Athena

Kerberos Status

- V4 Deployed in 85/86; now used world-wide
- V5 under construction
- V5 (with HP authorization extensions) to be included in OSF DCE
- V5 to be proposed as an Internet optional protocol

Goals for a Kerberos exchange:

- Authentication of Client to Server
- (optional) Authentication of Server to Client
- Secure Exchange of Encryption Key

Messages exchanged:

- C->KDC "gimme ticket"
- KDC->C ticket & key
- C->S ticket & authenticator
- (opt) S->C confirmation/mutual authentication

V4/V5 differences (protocol)

- principal names multi-component rather than foo.bar@baz
- new flags in ticket
- two-tgt user-to-user authentication
- encryption replacement
- address-type independence

Ticket flags:

- Forwarding (-able, -ed)
- Proxying (-able, -ied)
- Post-dating (may-, -ed, plus Invalid)
- Renewable
- Initial
- Duplicate-Session-Key

Two-tgt user-to-user authentication

- used when server can't hold secrets long (public workstation)

- server uses logged-in-user's TGT and session key as basis for trust

- client gets TGT, sends his & server's to KDC, then proceed as normal.

Encryption replacement

- V4 had only DES, in a funny mode

- V5 has essentially a “virtual function” for the encryption interface

- MIT code will provide DES with CRC-32 as a separate package.

Address-type independence

- Addresses encoded as {type, length, contents} tuple

- Addresses can be ignored by applications with little impact on security

- primarily useful to thwart theft of credentials

Implementation differences

- Separate "name space"; both V4 and V5 code can link into one server
- flexible credentials cache, server key, replay cache interfaces ("virtual functions")
- proper replay detection
- (eventually) "Generic" API

Compatibility issues

- v5 KDC will “do” v4 requests

- application servers can do both so you can phase in new clients

- “Generic” API will help

For more info: `info-kerberos@athena.mit.edu`

mailing list: `kerberos-request@athena.mit.edu`

v4 code, some v5 docs:

- FTP to `athena-dist.mit.edu`, /pub/kerberos/

- mail to `archive-server@athena-dist.mit.edu`, subject: index