AFTER THE KERBEROS 5 UPGRADE, WHAT NEXT?

Henry B. Hotz
hotz@jpl.nasa.gov
Jet Propulsion Laboratory, California Institute of Technology

with suggestions from
Jeffrey Altman
jaltman@secure-endpoints.com

June 23, 2005
Overview

• JPL’s new Kerberos 5 service
  • What we deployed
  • Surprises
• Future plans (and hopes)
Disclaimer and Corrections

• Following is general information and not guaranteed ;-)  
• In last year’s presentation the Heimdal / MIT comparison was based on old information about MIT.  
  • Both have new versions out since.  
  • Heimdal still doesn’t do password history or replay caching though.  
  • MIT still needs additional utilities for kaserver import and AFS KeyFile generation
What We’ve Done

• Replaced the kaserver with a Heimdal kdc
  • Heimdal provides Kerberos 4 and kaserver functions
  • No support for Kerberos 4 keys with the MIT string-to-key, only legacy interfaces supported

• Upgraded hprop to iprop

• Supports RC4 keys (Microsoft) and triple-DES
  • No AES, yet (now a required encryption type)
- Availability 0.99999999996 estimated lower bound.
- Performance measurement limited by test framework.
Surprises

• Kerberos Version 99
  • Transarc variant of Kerberos 4
    • adds pre-auth data and enables kaserver retry counting
  • Used by Windows AFS client
• Lifetime calculations for Kerberos 4 and KA
• DB access race condition for hpropd
• Inconsistent attribute setting
...and Statistics

- First two months of operation.
- Average auth/day
  - 336,000
- Maximum average auth/hour
  - 19,000
- 15,000+ principals
  - > 1/3 expired

June 23, 2005

Henry B. Hotz
Future Plans/Desires

• We do not promise to develop or release any of these things.

• We’d like to see them though.

• And I’ll probably do some of them.
Active Directory Name Change

- Have a Kerberos 5 realm and a Windows Domain
  - Both named JPL.NASA.GOV
  - Windows has custody of the SRV records
- Published Microsoft procedure for AD name change is being tested.
- Need to upgrade servers from 2K \(\rightarrow\) 2K3 first
- Windows users can’t use the main Kerberos realm until we do the change.
Non-Password Sign-In

- The human brain does not obey Moore’s Law.
  - All memorizable passwords eventually insecure

- SecureID
  - See Security considerations section in draft-ietf-krb-wg-kerberos-sam-02
  - Alternatively, could implement based on released code for older tokens.
    - Google: securid_expand_key_to_4_bit_per_byte

- PKINIT (standard not done)
  - Needs platform-dependent card drivers to be useable
Logging Improvements

- All request types
  - ka requests not (directly) logged in Heimdal
- Requested (or granted) ticket lifetime
- Hash of request
  - Post-facto replay detection possible
• Three flavors of token (so far)
  • Traditional Kerb 4
  • Version 213 “B2” — Kerb 5 single-DES-only
  • Version 256 — native Kerb 5

• Existing code for getting V256 tokens is in:
  • Windows aklog program.
  • Heimdal kafs library.
Token-Getting Library

- Need to minimize the effort of supporting different platforms’ login machinery.
- Need a general-purpose “get a token from a Kerb 5 tgt” library to support:
  - Pam module for Linux
  - Pam module for Sun (GSSAPI only)
  - MacOS X kinit plug-in
  - MacOS X Directory Services plug-in
  - Windows (without KfW, similar to Sun pam?)
    - Personally happy with KfW
• Apache module API supports separate authentication and authorization phases.
  • Authentication-only mod_auth_kerb
  • Authorization-only mod_auth_ldap
• RFC 2712 or successor.
  • Need some way to tie the Kerberos exchange to the transport-layer for Web.
BACKUP
Notice how information is encrypted (perhaps duplicated) with exactly the key needed for exactly who needs it.