CASE STUDY: KERBEROS INTEGRATION IN A LARGE ENTERPRISE

Wyllys Ingersoll
Sr. Staff Engineer
Sun Microsystems, Inc

Overview

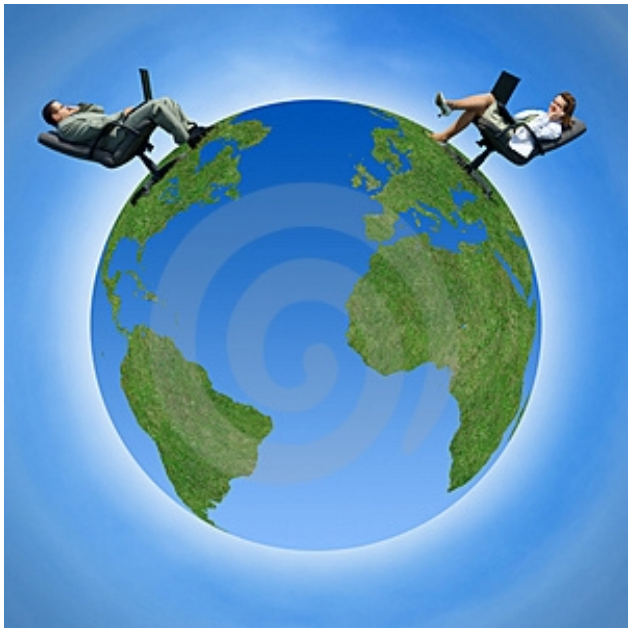
- Motivating factors
- Size and Scope
- Unique Problems + Solutions
- Progress
- Results
- Part 2: Contributing Back to MIT

Motivating Factors

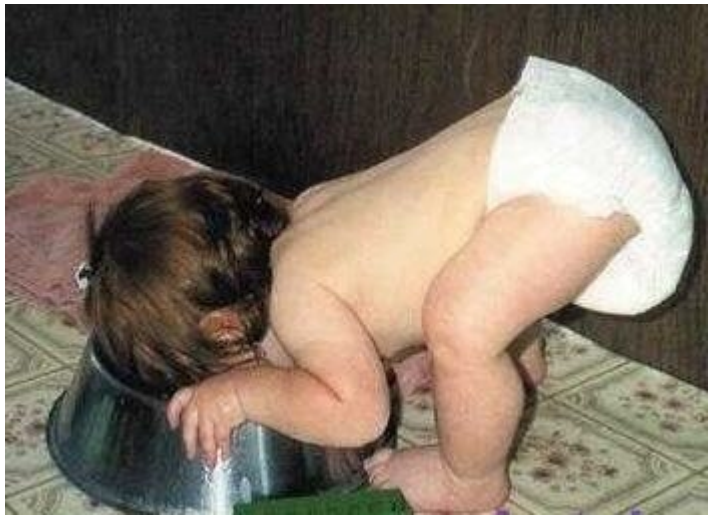
- Goal: Kerberize home directories (NFS)
- NFS is ubiquitous and insecure
  - Root user can impersonate anyone
- DH + DES are not secure enough
- New Government Regulations
  - Sarbanes-Oxley Act of 2002 requires publicly held companies to isolate and protect financial data internally and externally.

Size and Scope

- 30000+ Employees (roughly)
- Global network
- Multiple platforms with NFS access
  - Solaris, Linux, OS/X, Windows, …
- Application compatibility
  - SAMBA interop was critical
  - SSH, and other client apps also.
  - Web with Kerberos – *not so much*.
- 20 Distributed KDCs, 1 Master.
  - Incremental propogation (iprop)



Eating our own dogfood



- If we can't use it, how can we expect our customers to?
- Many bugs discovered and fixed (and given back to MIT)

- Leads to Useability Improvements
  - > Bootstrapping tools
  - > New config options
  - > Better understanding of scaling issues

Key Issues

- Bootstrapping Hosts
  - > Solution: zero-conf + scripts
- Password and Account migration
  - > Solution: pam_krb5_migrate
  - > + custom software and internal tools
- Propogating changes among KDCs
  - > Incremental propogation

Problems Encountered

- Crontab jobs
  - How to acquire credentials when a job runs
- With NFS/krb5, home dir access requires a ticket
  - Solution: Auto Renewal with a daemon (ktkt_warnd)
  - Eventually tickets cannot be renewed - lengthen allowable lifetime of a ticket
  - Other solutions: specialized crontab servers, unique principals dedicated to a specific user+service.

Problems Encountered

- Definition of a “Logging out”
  - User may logout of a host, but have shells that are still running that require access.
- Convenience vs Security
  - When to purge tickets
- Auto Renew feature only renews if logged in
  - check wtmp records
    - Imperfect, still edge cases.

Provisioning Problems

- Setting up clients without having elevated privileges.
  - Still need to be root to install keytabs.
- Kerberos is not the single account authority
  - Had to add custom backend utilities to existing enterprise applications to bind things together.
- No simple interface for provisioning users or new computers.
  - Patchwork solution of scripts and custom apps.
- Generating keytabs and new service keys
  - User must be registered as “owner” of a host first

Password Changing Issue

- Centralized Site for User Management
  - Website for user profile management, including passwords, phone numbers, etc.
  - Does not use PAM or kpasswd.
  - Custom Backend – added hooks to update KDC when users updated passwords
- Use of “passwd” not supported for Enterprise Wide updates.
- Security Policy dictates password changing periodically.

NFS Issues

- Goal – NFS w/krb5
  - auth only, no integrity or privacy modes by default
- Transition – NFS w/auth_sys + auth_krb5.
  - Not all NFS servers and clients can be updated simultaneously.
- Systematically eliminate auth_sys
  - Many SunRay servers (NFS Clients)
- GSSAPI Limitations
  - Single threaded
  - If GSSD is overwhelmed, NFS users lose access.
  - Fixes in progress.

Rollover issues

- The auto-renew daemon gave “Scary” messages
  - “Ticket expiration” warnings, etc.
  - Disable messages
- Non-Sunray Client Bootstrapping
  - SunRay easy – centralized, 1 client, 1 server.
  - Desktops hard – engineers control them with root priv.
- kclient script added to make it easier.
  - Minimal input needed from user.
  - Recently added AD support.

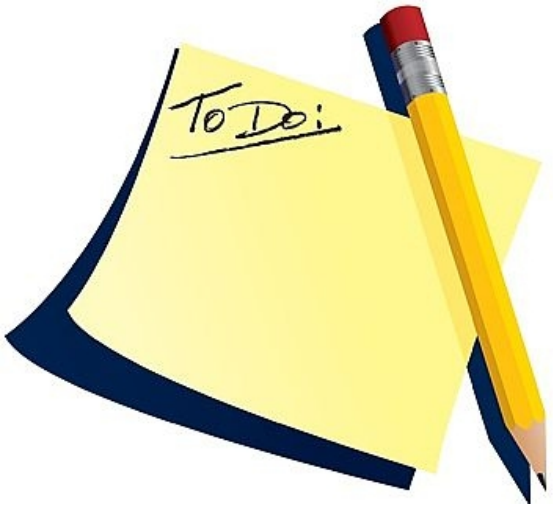
Other Kerberized Services

- Enterprise-wide Single Sign On is the goal
- SSH is primary terminal login app
  - Kerberized (GSSAPI)
- Thunderbird with GSSAPI
  - Only works on some engineering email servers (dovecot with GSSAPI support)
- Kerberized Web not catching on
  - Apache with mod_auth_gss possible.

What did NOT Happen

- Kerberized Web
  - Not catching on internally
- Internal Identity Management Service
  - Single Sign-On but not Kerberos
- Source Code Mgmt
  - Possibly just a configuration issue
  - SSH + Mercurial

TODO List



- Remote (VPN) Users and NFS
  - Hostnames may change
- Client side software needs to work without a host keytab.
  - Fixed in Solaris 10 – no need for root entry in keytab.
- Eliminate need for NFS + auth_sys everywhere
- Complete Solution for crontab issue
- Kerberize more services (mail, web)

Are we there yet??

- 98.5% of Users registered in KDC
  - 1.5% failures still being investigated
- 52% of homedirs
  - Larger rollout pending GSS fixes
- Bug fixing still in progress
  - GSSAPI scaling issues
  - Compatibility with earlier OS releases
    - Lack of strong crypto and newer features.

PART 2 – Contributing Back to MIT

- Project: Masterkey Stash File Format Change
- Change stash file format to keytab format
- Enabled masterkey migration (weak DES to stronger AES or better)
- Pros and Cons

Contributing Back – CONS

- Heavyweight process
  - > Full design, schedule and test plan required
- Project Wiki used for discussion and review comments was cumbersome
  - > Result: few people contributed comments
- Details on developing in MITKC Kerb build environment was poorly documented
- Test case development procedures not documented

Contributing Back – CONS

- Requirement for MIT.EDU credentials was hard to manage.
- Contributing from behind a firewall with port restrictions
  - Could not get TGT from MIT KDC
- Hard to manage tickets for multiple REALMS
  - Work principal in different realm. Kerberos code did not support > 1 primary principal in cred cache.

Contributing Back – PROS

- Build environment (once understood) does allow build and install in separate directories
  - Keeps source clean, allows for simple build, install, test process
- Tests (once understood) integrated in build tree- “make test”
- MITKC receptive to feedback and made changes based on suggestions along the way.
  - Process is now lighter weight
- MITKC developers were responsive to questions and comments.

References

- http://www.opensolaris.org/os/project/kerberos
  - OpenSolaris Kerberos Project page
  - Documents ongoing work and progress
- kerberos-discuss@opensolaris.org
  - Mailing list for all things Kerberos in Solaris

Kerberos Integration in a Large Enterprise

Wyllys Ingersoll
wyllys.ingersoll@sun.com