Who Let The Dog(s) In ?

An Update on the FERMI Strong Authentication Rollout

Contents

- ♦ Review of Goals and Deadlines
- ♦ The final stretch (Oct – Dec 2001)
- ♦ After the dust settled
- ♦ User community action/reaction
- ♦ Waivers
- ♦ Compliance scanning

Review of Goals

- Primary Goals
  - Eliminate reusable login passwords from network
  - "Positive Centralized control over access"
- Secondary Goals
  - Provide a single-signon environment
  - Simplify account management, especially termination
  - Integrate AFS accounts and systems
  - Enforce password policies

Review of Deadlines/Milestones

- Pilot Phase completed in summer ’00
- Fall ’00 - RunII experiments begin migration.
- Jan ’01 – Run II experiments central systems fully Kerberized. Deadline of 12/31/01 set for lab wide migration.
- March ’01 – clear full Windows migration would slip past 12/31. Estimate 4/02.

Review of Deadlines/Milestones

- April ’01 began to set migration deadlines
  - Each division/section was responsible for the migration of their users/systems
    - Coordination of obtaining kerberos principals
    - Establishing timelines for system migration
    - Training of users
    - Assistance could be obtained from Computer Security Team
  - Admins of systems were responsible for installing software within the above schedule
    - Sometimes this meant an OS upgrade first
    - Frequently required cross division coordination
    - Admins end up being the focal point for user complaints
  - Many groups used a staged migration
    - most resources were converted to kerberos but non-kerberized ssh was still open
    - This setup was originally frowned upon but found to be necessary.

The Final Stretch: Oct-Dec ’01

- Migrations set to occur earlier had (mostly)
  - Those systems managed by CD had primarily met their goals
- User questions were more and more frequent and getting more complicated
  - Questions handled through kerberos-users mail list, however experts still numbered only ~10.
  - Batch jobs or jobs run as a generic user
  - Connections from offsite not always simple

The Final Stretch: Oct-Dec ’01

- Many repeat questions
  - Misaligned clock was the number one source of problems.
    - Connecting from a home machine via ISP with NAT. (Windows users still require CryptoCard)
  - Default configuration was NOT to forward tickets. This was unpopular and required work to explain how to change it and to diagnose the root problem as trouble reports (“It doesn’t work”) were often sketchy. Eventually changed default to forward.
  - Web accessible and searchable archived mailing list helped to share the answers.

The Final Stretch: Oct-Dec ‘01

- Tutorials were offered in November
  - Intended for 2 user groups
    - Windows desktop users who access FNALU
    - UNIX desktop users who access FNALU
  - Attendance was moderate
  - Users could have benefited from Tutorials provided earlier in migration
- Official waiver rules established in December. Ended up with 300 machines on site with waivers. Most are either remote control PCs (PCAnywhere, Timbuktu, VNC, etc.) or legacy machines being shutoff soon.

The Final Stretch: Oct-Dec ‘01

- FNALU migration brought out more issues
  - AFS “group” accounts and batch/cron jobs
    - How to access these accounts and run unattended job as this “user” which does not have a kerberos principal
  - LSF and kerberos integration
    - Integration of kerberos V stub was not working
  - Forwarding credentials to get AFS tokens at login
    - FTP from WRQ with Windows did not do this
  - AFS token ‘stealing’ seen on several occasions
    - Kerberos V aklog not compiled to issue setpag before obtaining an AFS token
    - kcron “fixed” so it uses –setpag option
    - Recently found more instances of this and all connection binaries are being recompiled to issue pagsh

After the dust settled

- Despite much gnashing of teeth and wailing, the lab did NOT come to a screeching halt on Jan 1, 2002 (**except briefly as our GPS based master clock decided it was August 2020…**)
- Support load now reduced and comparable to usual "I forgot my password" level activity.
- Users
  - Requirement to use CryptoCard and not password from non-kerberized client the most frequent complaint.

User Community Action and Reaction

- For the majority of users, the addition of kerberos authentication had little or no impact (positive or negative)
  - Who is the majority? Users doing Unix -> Unix connections
  - This of course did not minimize complaints before its installation
  - Humans in general are not accepting of change
  - Just knowing that a change was going to have to occur caused trauma
  - A general statement from the lab directorate or an assigned representative about the need for this change would have helped
    - Many users had no idea of the number of security incidents the lab had been involved in or their impact
  - Outgoing desktop connections to other machines on site actually improve because no password is needed anymore

User Community Action and Reaction

- Non-majority user issues
  - Who is the non-majority?
    - Windows -> Unix connections (esp when AFS involved)
    - Transient or highly mobile users
    - Managers of a group analysis or code update procedure
  - These ended up being one-of situations
    - Required much more one on one problem solving
  - Users level of experience tended to affect the level of frustration
    - Shortage of experts added to higher frustration levels
    - Even more experienced users

User Community Action and Reaction

- ♦ Local admins are also considered users to some extent
  - – Significant work for this class of user
    - Software needed to be installed on each Unix machine
    - Determination of how kerberos would impact their particular compute environment
    - Had to learn how to use software as a user and admin
  - – Frequently filled role as user hand holder and complaint department

Deployment Status

- 3624 users
  - 2698 with CryptoCards
- 2583 service hosts
  - 99 off-site
- >300K tickets issued per day (Sun Netra KDC)
- Win2K Domain in production as separate (but synced) realm
  - ~400 users
  - Will not meet the 4/02 migration goal. Working on new estimate.

Waivers

- Some systems could not reasonably (yet) be fully Kerberized and so require exception handling.
- Currently some 100 exceptions granted (~300 systems). ~1/2 of these are Windows machines offering remote file access. 16 of these are legacy systems due to be shut off within 6 months. 10 are propriety software (backup is common) that requires unkerberized service (usually ftp or rsh). The remainder are various difficult cases typically running some unkerberized service restricted by tcpwrappers to a limited set of machines.

Compliance Scanning

- With the Fall wave of sshd probes, we have implemented a site wide scan every two hours for new machines on the network.
- Newly appearing machines (and some portion of previously seen machines) are scanned for services and compliance with FNAL policy
- Eventually this will include scanning of offsite machines running KRB5 clients configured to use the FNAL.GOV realm