Kerberos Deployment

• Two main realms:
  • UPENN.EDU: the main one
  • A central Windows based realm (1-way trust with UPENN.EDU)

• Various other departmental Windows server based realms that mostly also have 1-way cross realm relationship with the central Kerberos servers
Software & Hardware

- Central servers run MIT Kerberos 5 version 1.5.x
- Central servers run on Intel hardware and Red Hat Enterprise Linux 4.x (current generation > 4 years old)
- One active master (kadmin server); manual procedure in place to reconfigure alternate as master
Some statistics

About 1.5 to 1.7 million tickets issued per day (AS and TGS combined) and about 40,000 distinct users authenticated per day.

<table>
<thead>
<tr>
<th>Principal type</th>
<th>Count</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>196,928</td>
<td>98.94%</td>
</tr>
<tr>
<td>Service</td>
<td>1,887</td>
<td>0.95%</td>
</tr>
<tr>
<td>Kadmin (localism)</td>
<td>197</td>
<td>0.10%</td>
</tr>
<tr>
<td>Other</td>
<td>19</td>
<td>0.01%</td>
</tr>
<tr>
<td>Total</td>
<td>199,031</td>
<td></td>
</tr>
</tbody>
</table>
Native Kerberos vs. Password Verification

• We’ve spent a significant amount of time and energy trying to influence large scale use of native Kerberos authentication.

• Some successes but numerous failures. It’s difficult to do this in an environment of heterogenous, unmanaged computers.

• A number of application protocols (and their popular implementations) still don’t have good support for Kerberos.
Applications that support native Kerberos

- Windows domain login via cross-realm authentication
- Small amount of Web (HTTP/SPNEGO Negotiate)
- Jabber/XMPP
- E-mail: SMTP, POP, and IMAP
- Authenticated LDAP (Online directory etc)
- Local DNS content management system (custom protocol)
- Remote login (telnet/ssh) for sysadmin staff
Intermediate Systems

- Web Single Sign-On: CoSign (see weblogin.org)
- RADIUS
  - Primarily to support EAP-TTLS-PAP for wireless authentication
- Federation: Shibboleth (via CoSign)
- LDAP (authenticated access to online directory)
Kerberos for the Web

• Made several attempts in this area over the years, but solutions trialled have not yet gained much traction

• SPNEGO/HTTP Negotiate (+SSL for channel protection)

• KX.509 - Kerberos to obtain short term X.509 credentials

• Need: widespread support and adoption, and standardization (IETF)
Authorization Systems

• Kerberos: authentication only

• Applications need to consult separate authorization system (ours is based on Grouper)
  • http://www.internet2.edu/grouper/

• Many windows systems also use their usual methods (AuthZ data/PAC etc) for additional local policies
Near term enhancements

- Upgrade to current version of MIT code (1.9.x?)
- Adapt local changes to plug-in framework
- Investigate LDAP backend & multi-master KDC
- Migration to stronger encryption types
- IPv6 Support for KDC and Kadmind
Overview

• Basic Facts
• Web Authentication
• Other Authentication
• Database Propagation
• GULP
• AD Interop
• Two-Factor Authentication
• Upcoming Work
Basic facts

• 367K principals (was 341K last year)
  – 80K from current students, faculty & staff
  – Alumni
  – 600 host/service principals (central IT mostly)
  – Other
• 4 x 1-way trusts from various AD domains
• Many AD domains across campuses
  – No forest
• Running MIT krb5 1.9.1 on KDCs
  – 2 x RHEL5 64-bit 1U servers
Basic facts

- User principals provisioned based on data-feeds from HR, Registrar & departments
- All users have central “UNI” & possibly various AD passwords (might have different usernames)
- Most users use plaintext passwords, not GSSAPI
  - Easy to roll out
- GSSAPI used heavily for server-to-server authn/encryption
- 2.4M AS_REQ/day
- 1.8M TGS_REQ/day
Web Authentication

- Currently
  - Wind (CAS derivative)
    - Allows principal and demographic ACLs
  - Pamacea
    - Allows above + anything supported by .htaccess/.htpasswd
  - Shibboleth
- Next
  - Looking at CAS, Cosign, etc
  - Want to consolidate on single, unified authentication system
  - Must support guests
Other Authentication

• RADIUS
  – Wireless authentication
  – VPN concentrators
  – Router/switch logins by Network Engineers
  – Dial-up modems
Database Propagation Challenges – Solved!

• Used to have 550K principals that we kprop’d 1x/day
  – Deleted 210K principals so kprop was faster
• Switched to iprop last winter
  – Our monitoring system uncovered a bug when kvno hits 255
  – Otherwise, iprop rules!
GULP: Grand Unified Logging Program

• GULP helps Security Team automate lock-outs
• Detect suspicious logins
  – User logging in from 2 countries in too short a time
  – User logging in after multitude of failures
  – Too many users logging in from the same device
• Users are locked out and Security Team is notified
AD Interop

- AD supports 4K users of Exchange, filesharing, etc
- CTO declared that passwords must be sync’d between AD and MIT KDC
- Realm referral doesn’t play nice
  - Non-member workstations & Exchange 2010 were a show-stopper
- Looked at krb5-sync instead of having trusts
- Implemented krb5-adsync instead
  - [http://code.google.com/p/krb5-adsync/](http://code.google.com/p/krb5-adsync/)
  - Allows sync’ing only some users based on DN
Two-Factor Authentication

- Deployed RSA SecurID for IT sysadmins on Windows, Linux, and Solaris
  - Wrote our own PAM module
  - Removed it from Windows servers since it didn’t provide adequate protection
  - Cost prohibitive to roll it out for all 80K on-campus users, or all 367K principals
- Looking at OATH-based solutions
  - We would write a server & PAM module
  - Users could use free/low-cost OATH-compliant tokens
    - Yubikey
    - Google Authenticator
Upcoming

- Need to finish re-keying host/service principals
- Enable preauth for user principals
  - Need to test legacy applications (or just retire them already)
- Upgrade clients to krb5 1.9
- Use hardware tokens for preauth?
- Disable weak encryption types
  - Need to retire JDK 1.4/1.5 apps
Kerberos in Education Environments
MIT Kerberos Consortium
October 26, 2011
Andrea Beesing
Cornell University
Kerberos at Cornell

- Overview of Kerberos implementation
- Kerberos integration points
- Current and future challenges
Kerberos Implementation

- Two realms
  - NetIDs, ServiceIDs
  - ApplicantIDs, GuestIDs (legacy)
- Redundancy across two data centers
- Moving from physical boxes to VMs by mid-2012
- Software versions
  - Kerberos 5 release 1.7
  - RHEL 5
Integration Points: AuthN

- CUWebLogin for web SSO
- Radius for secure wireless, VPN
- kProxy – reverse proxy for webDav authN
- Shibboleth – federated authN
Integration Points: provisioning

- NetIDs
  - Administrative tool for creation/expiration/password resets
  - Automated mechanism for new student NetID creation based on PeopleSoft query
  - Self-service activation/password change & reset
  - KBA solution for alumni self-service: RSA VerID

- ServiceIDs
  - Self-service web app for service providers
Integration Points: Provisioning

- ApplicantIDs
  - Automated mechanism using PeopleSoft query

- GuestIDs (legacy)
  - Self-service app for creation and password management
  - Moved to Active Directory in 2010
Challenges

- MIT Kerberos/Active Directory roadmap
- Limitations of single factor, password-based authentication
- Certification requirements for federation
- Impact of cloud computing on how we do authentication and other IdM services
Kerberos in Education Environments
2011 Kerberos Conference

Phil Pishioneri
Information Technology Services
Penn State

pgp@psu.edu
Realms (plural)

- Access Accounts
- Friends of Penn State (FPS)
- Windows Active Directory
Access

- Students, Faculty, Staff
- 230K user principals, 10-15K rollover/year (students)
- Service principals/keytabs for daemon access
  - Web page for keytab generation
FPS

- Over 1.7 million principals
- Never deleted
Windows Active Directory Forest

- One-way trust to Access realm
- No direct login, passwords are:
  - Randomized
  - Not synchronized
- No NTLM
- Disjoint Namespace
Applications (1)

- Web Single Sign-On
  - CoSign (from Univ. of Michigan)
    - NSF Middleware Initiative
    - Chosen in part for Kerberos support
    - Password based, could use SPNEGO
    - Shibboleth IdP
Applications (2)

• “password authentication”
  • Email (IMAP, POP), also support tickets
    - WebMail (KPOP)
• Enterprise File System (IBM GPFS)
  • Samba (CIFS)
  • NFS v3/v4 (sec=krb5{i,p}, not IP based)
Background/History

- Access
- FPS
Access

- Started as AFS cell (K4)
- DCE/DFS cell
  - Performance issues (catalog size), led to separate realm for FPS
  - Lowercase realm name
- A Fall semester weekday
  - AS_REQ: 3,000,000
  - TGS_REQ: 800,000
FPS

- 2002
- Main consumers
  - Undergrad/Graduate Admissions
  - Bursar
  - Human Resources (non-PSU job application)
  - World Campus (Distance Learning) : non-degree
- Eventual merge with Access