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-stopped
- 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