PENNSTATE

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