Kerberos at Penn

Shumon Huque
University *of* Pennsylvania

Kerberos Conference, October 26th 2011
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

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

[Kerberos Conference, October 2011, MIT]

Penn
UNIVERSITY of PENNSYLVANIA

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

[Kerberos Conference, October 2011, MIT]

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.

Principal type	Count	% of total
User	196,928	98.94%
Service	1,887	0.95%
Kadmin (localism)	197	0.10%
Other	19	0.01%
Total	199,031	

[Kerberos Conference, October 2011, MIT]

Penn
University of Pennsylvania

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.

[Kerberos Conference, October 2011, MIT]

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

[Kerberos Conference, October 2011, MIT]

Penn
UNIVERSITY of PENNSYLVANIA

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 Conference, October 2011, MIT]

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)

[Kerberos Conference, October 2011, MIT]

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

[Kerberos Conference, October 2011, MIT]

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

[Kerberos Conference, October 2011, MIT]