Kerberos at Penn

Shumon Huque
University of Pennsylvania

Kerberos Conference, October 27th 2010
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

University *of* Pennsylvania

- Founded 1740, Philadelphia, PA
- 24,000 students, 4,000 faculty, 12,000 staff
- 50,000 IP addresses in use
- Some central and many decentralized IT units

Kerberos Deployment

- Initial deployment: 2000 through 2002
  - Replaced legacy homegrown system
- Campus-wide KDCs: MIT Kerberos 1.5.x
- Many departmental windows servers do (1-way) cross realm authentication
- Custom IDM/account management tools

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 **heteregenous**, **unmanaged** computers.
- A number of application protocols (and their popular implementations) still don't have good support for Kerberos.

Intermediate systems

- RADIUS
  - primarily to support 802.1x EAP-TTLS-PAP
- Web Single-SignOn: CoSign (UMich)
- Federation: Shibboleth (via CoSign)
- Authenticated LDAP
  - This is for authenticated access to our online directory. We strongly discourage using this for application authentication.

Kerberos for the Web

- Made several attempts in this area over the years, but has still not gained (much) traction
- SPNEGO/HTTP Negotiate (+ SSL for channel protection)
- KX.509 (from Univ of Michigan) - Kerberos to short term X.509 credentials
- Need: widespread support and adoption; official IETF standards

Multi-factor

- Investigated and piloted (no production):
  - CRYPTOcard
  - RSA SecurID
- Integration options:
  - Kerberos pre-authentication step
  - 2nd input to web SSO systems

Authorization systems

- Kerberos: authentication only
- Applications need to consult separate authz infrastructure (ours is based on the Internet2 Grouper system)
- Many windows systems also use their usual methods (Authz data/PAC etc) for additional local policies

Near term enhancements

- Upgrade to recent version of MIT code
- Adapt local changes to plug-in framework
- Test FAST (protect AS exch from offline dict attack)
- Incremental propagation
- LDAP back-end & multi-master (investigation)
- Migration -> stronger encryption types

Wants, hopes, desires?

- (Better) Native Kerberos for HTTP
- EAP method (wireless/802.1x authn)
- IPsec (does anyone use/implement KINK, GSS-IKE etc?)
- VoIP (SIP etc)
- Kerberos on mobile devices
- Multi-factor

Questions?

Shumon Huque
shuque@upenn.edu