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
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)

• Three servers, distributed on 3 distinct IP subnets, located in 3 distinct machine rooms around the campus

• One active master (kadmin server); manual procedure in place to reconfigure alternate as master

• Servers physically secured in machine rooms; run no extraneous network services, and provide limited access to the OS via an OOB console network protected by hardware token authentication
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><strong>Total</strong></td>
<td><strong>199,031</strong></td>
<td></td>
</tr>
</tbody>
</table>

~ 200,000 principals, mostly user principals. Accumulated over time, no automatic principal deletion after students/employees depart.
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.

• By contrast, easier in a managed Windows environment, where the details of Kerberos can be hidden from the user by integrating it into the workstation login process.
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
- NFS v4 (Engineering School)
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
  - we strongly discourage using LDAP as an application authN system

These are mostly using Kerberos as a password verification database.
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/](http://www.internet2.edu/grouper/)
- Many windows systems also use their usual methods (AuthZ data/PAC etc) for additional local policies
- We’re interested in looking at the PAC/PAD work in progress in the IETF
Multi-factor Authentication

- Investigated and piloted (but no production use yet):
  - CRYPTOCard (using SAM-2 Kerberos pre-authentication)
  - RSA SecurID (using 2nd input to CoSign web SSO)

- (We do use SecurID to authenticate access to out-of-band console sharing networks, but this doesn’t involve Kerberos)
Near term plans

• Upgrade to current version of MIT code (1.9.x?)
• Adapt local changes to plug-in framework
• Test FAST (protect AS exchange from offline dict attack)
• Investigate LDAP backend & multi-master KDC
• Migration to stronger encryption types
• IPv6 Support for KDC and Kadmind
Wants, desires..

- Standardized Kerberos support (and implementations) for as many protocols as possible
  - HTTP
  - EAP (Wireless/802.1x authentication)
  - IPsec (does anyone use KINK, GSS-IKE etc?)
  - SIP (Session Initiation Protocol) - for VoIP and other realtime apps
- Kerberos on mobile devices?
Questions?

Shumon Huque
shuque -@- upenn.edu