SAML-AAI/Kerberos integration

Rok Papež
ARNES
aaa-podpora@arnes.si

Loughborough university
Loughborough, 6.5.2009
Authentication protocol
  – (No) authorization

Single Sign On (SSO)

Cerberus
  – Greek and Roman mythology
  – 3 headed dog guarding the gates of Hades

MIT Project Athena
  – Versions 1-3 internal only
  – Version 4 – 1989 (public software release)
    • DES only, Protocol flaws, End of life
  – Version 5 – 1993 (RFC 1510)
  – GSS-API – Generic security services API
  – IETF Kerberos working group
Kerberos implementations

MIT Kerberos
- Krb5-1.6.3
- Krb5-1.7 beta (22.4.)
- Most popular
- Subject to USA cryptography export regulations

Heimdal
- Heimdals-1.2.1
- Developed in Sweden
- Better security track record
- More features

Microsoft Windows 2000 and later
- ActiveDirectory default authentication protocol
- AuthZ extension: PAC – Privilege Access Certificate
Inband for different protocols
- IMAP, POP, Telnet, SSH, Cisco routers ...

3rd party trust point - KDC
- KDC – Key Distribution Center
- Symmetric key cryptography

Client acquires TGT from KDC
- TGT - Ticket Granting Ticket
- Client-KDC trust via shared secret – password
- User prompted for password!

Client uses TGT to request Service ticket from KDC
- User isn't prompted for password
- KDC issues a time limited Service ticket for ServiceX
Kerberos diagram

1. Get TGT:
   (userX@org.eu)
2. Get service ticket:
   (userX@org.eu for imap@org.eu)
Simple Kerberos demo

Cheat sheet:

- kinit
- klist [-v]
- kgetcred <service>
- kdestroy [--credential=service]
Kerberos shortcomings

- Bad administrator documentation
- Horrible developer documentation
- Questionable security track record
- Not suitable to run as a „public“ internet service
  - From design-on treated as a LAN or campus service
  - Static 2-way or spoke and hub inter-realm trust
  - Always firewalled
- Bad authorization support
  - Kerberos doesn't provide enough data
  - Kerberos support in application: AuthN == AutZ
- SPNEGO for web applications
  - Simple and protected GSSAPI Negotiation mechanism
  - Limited to local network use
SAML – Security Assertion Markup Language
  – Data format / standard

Web applications
  – Separate login from application
  – Single Sign On (SSO)
  – User authenticates via „login application“
    • IdP – Identity Provider
  – Authorization data sent to „service application“
    • SP – Service Provider
    • Module in web server
    • Application library

SAML 1.0 – OASIS standard, 2002
SAML 2.0 – OASIS standard, 2005
SAML-AAI implementations

- Shibboleth IdP, SP
  - http://shibboleth.internet2.edu/
  - Older
  - Very configurable
  - Java

- SimpleSAMLphp IdP, SP
  - http://rnd.feide.no/simplesamlphp
  - Newer
  - Very easy to use
  - PHP
How SAML-AAI works

3rd party trust point
- Metadata distribution point (Web server URL)
- X.509 public key cryptography

Web browser redirects
- WAYF/DS – Where Are You From/Discovery Service

Auto-submit forms
- IdP sends authorization data from LDAP to SP

Cookies for SSO session at IdP
Video demo!

(screencast of user accessing Foodle and Adobe Connect applications
secured via web server integrated Shibboleth SP
login via SimpleSAMLphp IdP)
## Comparing SAML-AAI and Kerberos

<table>
<thead>
<tr>
<th>SAML-AAI</th>
<th>Kerberos</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Web applications</td>
<td>– (Mostly) Non-web applications</td>
</tr>
<tr>
<td>– Internet-wide</td>
<td>– Local/campus networks</td>
</tr>
<tr>
<td>– X.509 PKI</td>
<td>– (Mostly) symmetric keys</td>
</tr>
<tr>
<td>– SAML</td>
<td>– ASN.1</td>
</tr>
<tr>
<td>– Authorization data</td>
<td>– (Mostly) no authorization data</td>
</tr>
</tbody>
</table>

SAML-AAI and Kerberos are **not** competing protocols!
Hybrid web applications:
- Web interface
- Access to backend Kerberos protected services
- Login via SAML-AAI + get Kerberos ticket

Problems:
- Identity mapping
  - Which Kerberos principal name to use?
  - Kerberos principal name: userX@org.eu
  - org.eu is Kerberos LAN/Campus realm
  - SAML identity
    - EduPersonPrincipalName: userX@uni.eu
    - EduPersonTargetedId: kl83HlsnblqYskgh72Kfqkl
- User provisioning (new user?!)?
- Getting service tickets from KDC for userX@org.eu
Hybrid SAML-AAI with Kerberos diagram

0. Get TGT for a service: web@org.eu
   -- For every user --
2. Get service ticket for:
   user3.14@org.eu to web@org.eu
   (Kerberos mechanism S4U2Self)
3. Get service ticket for:
   user3.14@org.eu to imap@org.eu
   (Kerberos mechanism S4U2Proxy)

KDC - Key Distribution Center
Symmetric keys DB

Identity Mapper

Service
(imap, ssh ...)

SAML-AAI
Discovery Service

SAML-AAI "uni.eu"
Identity Provider

user3.14@org.eu
Web application
(with SAML-AAI SP)

userX@uni.eu

Access with service ticket

Kerberos
side

SAML-AAI
side
Questions?