Advanced Shibboleth topics

UF IT/CNS/Open Systems Group

University of Florida

March 3, 2011

Eli Ben-Shoshan (ebs@ufl.edu)
Martin Smith (smithmb@ufl.edu)
Laura Guazzelli (laura2@ufl.edu)

Important references

- UF IT - Shibboleth
  http://www.it.ufl.edu/identity/shibboleth
- CNS/Open Systems Group - Shibboleth
  http://open-systems.ufl.edu/shibboleth
- Internet2 - Shibboleth
  https://spaces.internet2.edu/display/SHIB2/Home

Goals

Discussion format; may include:

- Day-to-day SP management
- SP Securing & Monitoring
- Virtual hosting and multiple entity IDs
- Application-managed sessions
- Alternate SAML profiles and bindings
- Hard-to-shibbolize applications
- ARP Affiliations and ARP Group changes and their impact on applications.

Discussion topic: Daily tasks

- Keep current with latest releases
- Rotate log files for native.log, shibd.log, transaction.log
- Add new sites, remove old sites
- Don't need to update certs/keys for SAML

Discussion topic: Securing & Monitoring

- Process check for shibd, ensure webserver config is sound
- HTTP HEAD/GET on /Shibboleth.sso/Status
- Synthetic tests for as much as possible
- High-availability strategies
- Protecting other handler URLs under /Shibboleth.sso/
- Dealing with SE Linux, Logwatch
- Don't use Shibboleth as your only authn...

Discussion topic:Virtual hosting, multiple entity IDs

- Understand why metadata is FQDN specific
- Understand consistency with SSL
- What you can share (shibd, webserver module)
- What you may not be able to share (entity IDs, URLs, keys/certs)
- InCommon SPs and IdPs

Discussion topic: Application-managed sessions

- Know the various handler URLs
- Understand ShibUseHeaders
- Local Logout...
- Multiple principals & re-authn

Discussion topic:Alternate SAML profiles and bindings

- HTTP-POST, HTTP-Redirect
- AttributeService (ARS,ACS,etc) via SOAP
- SAML1...
- `https://login.ufl.edu/login.ufl.edu.xml`

Discussion topic:Hard to Shibbolize Apps

- Proxy it from Apache
- Java application server support (Oracle, BEA...)
- REMOTE_USER is a popular convention
- One-time tokens vended under Shibboleth
- Custom code... eek.

Discussion topic:Upcoming service changes

- IdP is now highly available
- (Mobile) login page changes on Sunday
- All separator characters are now dollar-sign $
- ARP-Affiliations: multivalued, de-duplicated
- ARP-Groups: Full distinguishedName, nested resolution
- Database performance will be improved

Questions?

Thank you.