# Origins: Requirements and Considerations

Mark Earnest
Lead Systems Programmer
The Pennsylvania State University

# PSU's Shib Experience

- Began testing in Spring 2002
- Soon running a limited production/test with Webassign
- By Spring 2003 Shib/Webassing was full blown production with ~1800 students
- Spring 2004 brought Napster into the fold with a trial of ~18000 students.
- Ongoing testing with various Digital Content vendors

# Infrastructure Requirements

- Some form of web authentication method
  - mod_auth_kerb, pubcookie, etc
- User attribute directory
  - LDAP, SQL, etc
  - eduPerson Schema

# Attribute Directory

- Shibboleth provides JDNI (LDAP) and JDBC (SQL) connectors to retrieve attributes
- eduPerson schema provides the attribute standards
- Recommended that sensitive data be protected and accessed via an authenticated bind
- Multiple directories can be used for separating data or fail-over.

# Directory Concerns

- Accuracy of data (ours not as good as we thought)
  - persistence of key data (eppn) must be addresed
- Security and privacy
- Time sensitivity
  - Batch vs real time

# Certificates

- In addition to standard SSL server cert for Apache, a signing cert is needed
  - keyUsage = DigitalSignature
  - Can be the same certificate
- Watch filesystem permissions.
  - The Tomcat server cannot read Apache's key if permissions are not changed.

# Tomcat Configuration

- In the ajp13 connector:
  - minProcessors=”10”maxProcessors=”260” acceptCount=”260”
  - MaxClients MUST be set lower than the maximum Tomcat connections.
- In catalina.sh:
  - JAVA_OPTS=”$JAVA_OPTS -Xms256M -Xmx512M”

# ARPs

- Setting good default ARPs is important
  - Our policy is to never reveal more than needed for an authorization decision.
- New as of 1.2 - regexps on multivalue attributes
  - <Value release="permit" matchFunction="urn:mace:shibboleth:arp:matchFunction:regexMatch">^URN\:PSU\.EDU\:COURSE\:UP\:PHYS(.*)</Value>

# TargetedID

- Requires “secret seed” value
- “ant genSalt”
  - creates value, stores it in persistent.jks
  - See Build.xml to change filename, password, etc.
- Consider pre-generating these values and storing them in a database to ensure they remain persistent.

# Logging/Auditing

- Our policy: always log at full volume
- Logs are rotated and archived
- If load balancing, it will be difficult to follow user sessions
- If the ability to track TargetedIDs is necessary, they should be pre-generated and stored.

# Capacity Planning

- Load testing
  - Software exists (webload), or roll your own
- Shibboleth is primarily CPU bound
  - Little or no RAM or IO bottlenecks
- Remember the authentication mechanism will add to your response time
  - WebISOs will REALLY add to it.

# Load Balancing

- Must use crypto handle method
  - requires handle.jks - build with “ant genSecret”
- Consider running multiple handle services, but perhaps only one attribute authority
- Keeping ARPs and configuration files synchronized a must
  - Consider using a network filesystem for this

# Monitoring

- Load testing scripts (limited to one connection attempt) make great monitoring tools
- Just because Apache responds does not mean Shibboleth is functioning (Tomcat may crash)
- Performance, tuning, monitoring, and debugging tools are needed. We are working on some.

# User Experience

- Shibboleth almost completely transparent.
- Create custom error pages
  - Users will not understand the default ones
  - Especially if your name is listed as the technical contact for the Origin
- As with any WebISO system, the security stakes are higher.

# Future Considerations

- User specific ARPs
  - Will users give up all personal data for benefits?
  - Will users unknowingly lock themselves out of Service Providers by restricting data?
- ARP Management in non web based applications
- Portals (three tier credential passing)

# Where to go for help

- Mailing lists:
  - shibboleth-users@internet2.edu
  - shibboleth-aca-sig@internet2.edu
- IRC Channel
  - #shibboleth on irc.freenode.net
- Walter's FAQ
  - https://umdrive.memphis.edu/wassa/public/shib.faq/shibboleth-faq.html