Shibboleth at NC State: Current and Future Plans

Charles Brabec, Technical Lead

History

Started with IdP 2.0.0, July 2008, as
joint project with UNC Identity Federation.

Joined InCommon Federation, Feb 2009.

Added our MyPack Portal, Summer 2011.

Server Configuration

shib.ncsu.edu = pool of 6 virtual machines.

LVS loadbalancer, uses VIP and IP tunneling.

Each server:

- Terracotta - java session sharing
- Tomcat - java engine
- Apache httpd - web handling

Server Configuration Management

Server configs kept in subversion master.

Changes are pushed to servers manually.

Usually adjustments to attribute filters, or custom settings for new SP sites.

Use a custom config file and perl script to simplify attribute-filter lists without XML.

Additional IdP Servers

“Other IdP” also runs on shib.ncsu.edu

  Used primarily for Parent access without Unity accounts.

Two additional pools of test IdPs,

  4 servers each, similar to production.

IdP Configuration

Main IdP is used for our Unity (SSO) accounts.

Login via AD.

Attributes from multiple LDAP calls and AD.

Affiliations are calculated on the fly.

UApprove for customer consent, uses mysql.

Other IdP uses different AD for login and all attributes.

Federations and Groups

- InCommon Federation, including
  - NC Trust
  - Research and Scholarship group
- UNC Identity Federation
  - Prod, Dev, Affiliates
- NCSU Federation

NCSU Federation

Managed in subversion master repository.

Sign up via form provides metadata for SP.

Script extracts data, and creates a generator to manage SP endpoints.

Another script assembles full metadata from pieces, validates, signs, and publishes.

Record keeping in a Google spreadsheet.

Security and Monitoring

Logs are kept from httpd, Tomcat, and IdP.

- Custom script on each server watches these for error patterns and sends alerts.

Nagios is used to monitor servers in general.

Suspicious User scripts monitor these and other logins for patterns of account abuse.

e.g. Library ezProxy abuse is common.

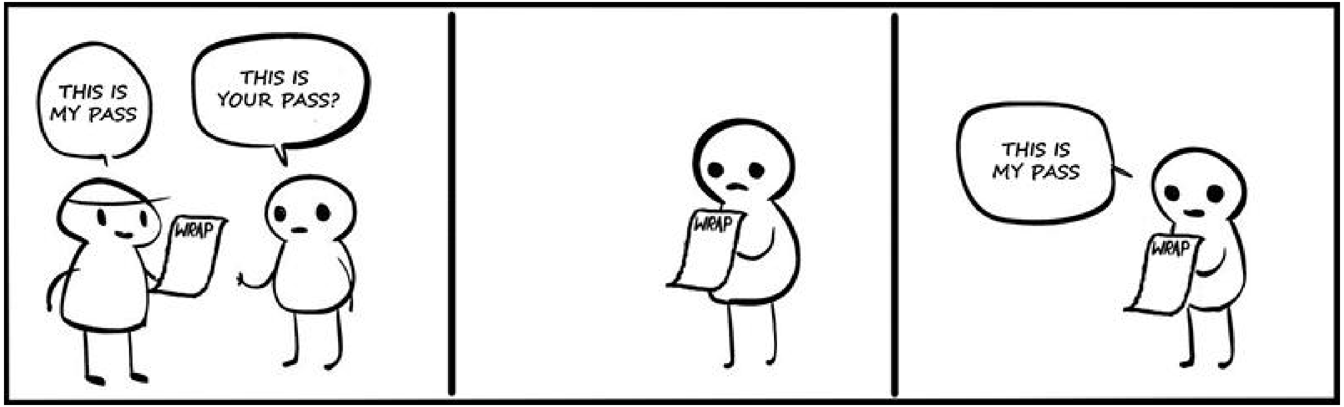
Future Plans

About WRAP

WRAP is our homegrown cookie-based auth.

It is used everywhere on campus websites.

It is no longer sufficiently secure.



WRAP Migration

Added lots of documentation.

- http://shib.ncsu.edu/

Help campus providers get onboard and debug their installations.

Working to move our own hosting pools to run the SP software.

- Adding SSL everywhere as part of this.

Fixing Old (Bad) Decisions

We allow logins with expired passwords.

Need more user groups or affiliations.

Need a separate scope for “Other IdP”.

Need to consolidate our attributes into a single source directory, and pre-calculate.

Upgrades

Our hardware is due to move to newer VMs.

IdP 2.4.1 security patch released Aug 13.

IdP 3.0 is coming, possibly Q4 2014.

Does this replace Terracotta? UApprove?

Need to stand up a dedicated dev IdP.

Future Enhancements

Two-factor authentication:

Buy Duo or use Google Authenticator?

Consider Social-to-SAML Gateway project.

Revisit use of SAML auth for Google Apps.

Any Questions?

Links:

https://shib.ncsu.edu/

https://www.duosecurity.com/docs/shibboleth

https://spaces.internet2.edu/display/socialid/Home

http://goo.gl/uEuvQ7 - these slides