ECP

Extended Client or Proxy (ECP)

DATE and TIME: Thursday, 26 May 2011, 9:00 - 10:00 am

CONVENER: Jim BASNEY

SCRIBE: Keith Hazelton

# of ATTENDEES: 41

MAIN ISSUES DISCUSSED

- SteveC: Project Moonshot: Building a mechanism to support the use of federated identity with non-browser applications (specifically, command line tools such as SSH, etc). The architectural approach they're taking is to create a new GSS-API mechanism that uses EAP to thread through RADIUS servers back to a user's home institution (essentially the eduRoam infrastructure). Many of the applications that they're concerned with use either GSS-API or SASL. Scott Cantor has authored an individual contribution out of the IETF Kitten working group. It is a proposal for a GSSAPI mechanism that would use SAML via ECP to deliver solutions to Moonshot use cases.

- GEANT is funding EAP approach dev for Moonshot
- Who would/will fund ECP approach to same problem space

- ScottK: OpenSSH devs are looking at patches to support Moonshot

- SteveC Yes, JoshH has gotten the owners of such code bases on board

- Scott Koranda Grid could never get that with GSI

Scott Koranda bash script ECP client demo
https://wiki.shibboleth.net/confluence/display/SHIB2/Contributions#Contributions-simplebash

- uses curl (curl can do POST)
- uses xsltproc command-line tool
- written for bash4 on Debian Squeeze

- ./ecp.sh Campus01 https:/campus01.edu/m/secret/page jsmith

- one parameter specifies which "tag" to use: e.g., define "LIGO" as a tag and associate a URL that is protected by basic auth. over SSL
- your client has to know which IdP to send users to
- configure SP properly
- it will deal with this stuff before session initiator is called
- sends a munged XML blob to IdP
- IdP authNs, sends new blob of XML back to SP
- SP reads from that who is being served & session cookie

- MRG: is there validation?
- ScottK: part of package that comes back from the SP is the assertion consumer URL. The IdP looks in the metadata, sends signed assertion to assertion consumer URL in the metadata for that SP
- Next version of ECP that Scott is writing will handle channel bindings for more verification

./ecp.sh *d(ebug) LIGO(a tag) https://parsely.phys.uwm.edu/secure/environment skoranda

- assertion consumer service .../sso/....
- posted to SP
- SP sends back the session
- GET the thing you wanted in the 1st place (in this test case the SP is a script that dumps the SHIB env. variables)

Script review...

- Hardest part was not the XSLT, but figuring out all the proper command line options for curl
- ScottK's IdP is on Tomcat/Apache
- Subversion client tools do not use libcurl, it will be HARD to ECP-enable it
- New Shib IdP 2.3.0 includes ECP by default, only have to protect the URL, no other configuration is strictly necessary.

ACTIVITIES GOING FORWARD / NEXT STEPS

https://wiki.shibboleth.net/confluence/display/SHIB2/ECP is the home for Shibboleth work around ECP support

[All] Add links on the SHIB2/ECP wiki page that *point to* other pages where this nascent ECP interest group's activities can be described. Use those linked pages as a home on the web for ongoing discussions

[Roland Hedberg, Scott Koranda] collaborate to deliver a Python ECP client module that returns a Python cookie-jar containing session cookies that allow your Python app to keep talking to the SP

[Arnie] Refactor his HPC access via SAML solution to use the ECP approach

[ACAMPScribe:ScottK] working with Condor group on ECP-enabled file mover.

[ScottK and all] Suggest to InCommon that they should consider recommending that sites protect their ECP endpoint on the IdP with X.509 certs. Otherwise there will be as many varieties of protection as there are ECP endpoints.

- Friday morning "ECP Continued" discussion: X.509 may be too limiting. Basic Auth use cases (Live@EDU) are common.
    - Multiple ECP endpoints? One for X.509 and one for Basic Auth?

REQUESTS:

- Todd Picket: Document other ECP clients & how you use them: PAM/Shib
- ECP reading list, tutorial??
- Followup ECP session on Fri. am.

REFERENCES:

- https://wiki.shibboleth.net/confluence/display/SHIB2/ECP

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to SteveO@internet2.edu

Thank you!