Return to Advance CAMP wiki

Advance CAMP Wednesday, Sept. 28, 2016

1:10pm-2:00pm

Tuttle Room

Federated SSH

CONVENER:
Kevin Hildebrand, University of Maryland
Andy Newman, Yale University

MAIN SCRIBE:
Matthew X. Economou, NIH/NIAID

ADDITIONAL CONTRIBUTORS:
Scott Cantor

# of ATTENDEES:
20-ish

DISCUSSION:

UMd has HPC clusters and wants to give access to them over SSH

- Project Moonshot
- ECP

Yale found that solutions were untenable:

- Hack involving shell scripts and manual key distribution and CILogon
- Many IdPs don't support ECP

Is this too narrow a characterization? What's the problem? What's the solution?

FeduShare:

- Use federated login to get X.509 cert (CILogon)
- Use federated login to register SSH public key (COmanage)
- Project Moonshot
- SAML ECP (GSS-ECP)

ECP is on by default in Shibboleth IdP V3 (but not advertised in metadata - which may or may not break federated SSH).

People who don't advertise ECP may not realize they can support it.

SSH public key vs. X.509 certificate?

- Is there a deprovisioning component?
- COmanage can provision the account and then set an expiration date on the COPerson record, but that doesn't take care of situations where someone's fired.
- Add refresh time requiring IdP re-confirmation?
- SWITCHaai attempts liveness checks using attribute resolution.

Hack it? Automate the trust handoff somehow? Provisioning is probably cleaner.

What's an acceptable user interface?

- User has no way to tell whether their credentials are going to the SSH server (bad) or the IdP (good).
- There's no way an ISSO will OK that.

Moonshot is different because it uses some kind of supplicant that maybe can go through another user interface?

- Moonshot uses 802.1x
- They intended to build a GUI to prompt for username/password.

Aside: What about Windows logons over RDP?

- If it uses SSPI, maybe it would work with GSS-ECP?

Tying ECP to Kerberos?

- Possible, but not done.
- ECP in practice is basic auth.

LIGO:

- Runs their own IdP
- Uses their own client that interfaces with CILogon
- Grid-enabled clients and servers
- Client is unmodified, just uses GSS library plugin
- Server must be patched

Moonshot may have demoed this with PuTTY on Windows.

Is anyone using some kind of web-based portal for the front-end?

- Science gateways targeting HPC resources
- Scientists hate this, but cloud vendors have forced these tools to become better.

OpenOnDemand uses VDI with X11.

XSEDE using federated logons to OpenStack to get access to virtual machines

- Keystone has built-in SAML support.
- Researchers are deploying images at scale to just run, a la Docker.
- Or a personal logon node or some kind?
- Temp VMs still have that deprovisioning problem.
- Set low VM lifetimes, force renewals, etc.

Once you authn with federation and get access to HPC cluster, how do you create accounts on the fly?

- What if the account isn't real?
- Can it be somewhat ephemeral?
- Where should long-lived data be kept?
- How would long-lived data get transferred? Globus?

Don't screen-scrape.

What about getting this into upstream?

- OpenSSH won't accept packages
- Distro package maintainers will generally accept packages
- Still difficult to keep vendor-specific repos up to date

Key differentiator: push for MFA on campus

Are we going to oblige some level of assurance for federated remote users?

- Duo iframe is not enough

ACTIVITIES GOING FORWARD / NEXT STEPS:

Flesh potential solutions out into an “options” document and refresh quarterly.