Moonshot SSH

Kalle Happonen, CSC

Moonshot Viikki workshop

29/05/13

Moonshooting SSH

- Moonshot client setup
- Moonshot server setup
- Testing
- Bringing SSH in

Disclaimer!

Some things to note

- Moonshot is heavily under development
- Not all packages are available at this time
- Limited operating system support for now

Moonshot client

Consists of

- Moonshot-ui – talks to the user
  - Manages user credentials
  - Verifying IdP?
- Moonshot libraries
  - Does the gss-eap integration
- Gss-client
  - Not needed, but great for testing

- Packaged for Windows, OSX, Debian and RHEL (almost)

Moonshot client

RHEL/CentOS example

- Instructions under
  - https://confluence.csc.fi/display/HAKA/Moonshot
  - Page will be opened

Moonshot client

Steps

- Install the yum repo
- Install the required packages
- Configure /etc/gss/mech
- Test!
- Yes, it is simple! (When we have packages)
- Later in production: Autoconfigure user identities?

Moonshot service provider

Consists of

- Moonshot libraries
  - Does the GSS integration
- The sibboleth2 libraries (and server, maybe)
  - The SAML attribute handling is done here
- Radius client
  - Connects to your local radius server
- Gss-server
  - Again, for testing

Moonshot service provider

RHEL/CentOS example

- Instructions under
  - https://confluence.csc.fi/display/HAKA/Moonshot
  - Page will be opened

Moonshot service provider

Steps

- Install the yum repo
- Install the required packages
- Configure /etc/gss/mech
- Configure /etc/radsec.conf
- Configure shibboleth
- Test!
- No it is not this simple! (Next slide)

Moonshot service provider user mapping

User mapping

- Default user mapping bad / wrong / just no
- We only get IdP side attributes form our radius message
  - E.g. Remote site user id, eppn, name?
- We need to use these to map them to local unix (nsswitch) accounts
  - eppn to username mapping our current idea
  - For new cases, eppn as the username works too
- Mapping can be done in shibboleth when handling the SAML
  - Site-local Attribute Authority for mappings?
  - Static AttributeResolver configs?

Moonshot service provider user mapping

User mapping

- Attirbute resolver example

```
<AttributeResolver type="Transform" source="eppn">
      <Regex match="^khappone@csc.fi$" dest="local-login-user">kalleh</Regex>
      <Regex match="^jsmith@csc.fi$" dest="local-login-user">johnsmith</Regex>
</AttributeResolver>
```

Moonshot testing

- Client side

```
gss-client -spnego servername gss@servername "Hello"
```

- Server Side

```
gss-server -verbose gss@servername
```

- Output too long for here
  - Great for debugging
  - SAML logs come here

Moonshot SSH

- Need moonshot SSH version (for now)
- Very minor configuration client + server
  - Enable GSS things in the configs

- That's it! The moonshot is the hard part

- Not sure if ssh has to be
  - ssh localusername@server or if it can be
  - ssh eppn@server or even
  - ssh -l “” server

Thank you!

Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv