Moonshot SSH

Kalle Happonen, CSC

Moonshot CSC workshop

5/02/14

Moonshooting SSH

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

Disclaimer!

Some things to note

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

- Main Janet resource https://community.ja.net/groups/moonshot
  - Will be moved to a confluence wiki

Moonshot client

Consists of

- Moonshot-ui – talks to the user
  - Manages user credentials
  - Authenticates to the radius server
  - Secure storage of credentials
- Moonshot libraries
  - Does the gss-eap integration
- Gss-client
  - Not needed, but great for testing

- Packaged for Windows, OSX, Debian and RHEL

Moonshot client

RHEL/CentOS example

- Instructions under
  - https://confluence.csc.fi/display/HAKA/Moonshot

Moonshot client

Steps

- Install the yum repo
- Install the required packages
- (Configure /etc/gss/mech)
- Autoconfigure user identities
- Test!

Moonshot client autoconfiguration

- Moonshot-webp tool for importing identity xml files
  - Defined in XML, looks like

```
<?xml version="1.0" encoding="UTF-8"?>
<identities>
  <identity>
    <display-name>khappone</display-name>
    <user>khappone</user>
    <password></password>
    <realm>csc.fi</realm>
    <selection-rules>
      <rule>
        <pattern>trustidentity</pattern>
        <always-confirm>false</always-confirm>
      </rule>
    </selection-rules>
    <trust-anchor>
      <server-cert>59b0c4e5d65f198095ece38bdac6394c7bf235bcee47b1c8276a0d3c2c80607e</server-cert>
    </trust-anchor>
  </identity>
</identities>
```

- Server certificate defined as the SHA256 hash
  - openssl x509 -in cert.pem -outform DER |sha256sum

Moonshot service provider

Consists of

- Moonshot libraries
  - Does the GSS integration
- The shibboleth2 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

Moonshot service provider

Steps

- (Preconfigure site radius)
- (preconfigure user mapping in site radius)
- 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

- 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 site-wide in local radius
- Mapping can be done in shibboleth when handling the SAML
  - Site-local Attribute Authority for mappings
- If only within a single organization
  - Static AttributeResolver configs

Moonshot service provider user mapping

User mapping

- Attirbute resolver example

```
<AttributeResolver type="Transform" source="eppn">
      <Regex match="^([^@]*)@csc.fi$" dest="local-login-user">$1</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 SSHD version (for now)
  - Need to rebuild SRPM for CentOS
- Very minor configuration client + server
  - Enable GSS things in the configs
- That's it! The moonshot is the hard part
- SSH as your username on the remote side
  - Nulluser patch for SSHD, but will probably not be mainstream

Thank you!

Connect | Communicate | Collaborate

www.geant.net

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