Contribution ID: **9** Type: **Oral Presentation**

Evolution of SSH with OpenId Connect

Friday, 29 March 2024 10:50 (20 minutes)

The Secure Shell Protocol (SSH) is the de-facto standard for accessing remote servers on the commandline. Use cases include
- remote system administration for unix administrators
- git via ssh for developers
- rsync via ssh for system backups
- HPC access for scientists.

Unfortunately, there is no globally accepted usage pattern for globally federated usage yet.

The large variety of users with different backgrounds and usage profiles motivated us to develop a set of different tools for facilitating the integration with federated user identities, which are being presented in this contribution. The main novelty is the integration of an ssh Certificate Authority (CA) into the existing motley-cue + oidc-agent mechanism. Oinit simplifies the usage of ssh-certificates by leveraging authorisation information via established federation mechanisms. The benefit is that - after an initial setup step - ssh may be used securely without interrupting existing flows. This allows for example the use of rsync.

To enable this, oinit consists of a collection of programs to enable OpenSSH login for federated identities based on certificates:

- The oinit-ca provides a REST interface to an ssh-ca at which authorised users obtain an ssh certificate for a specified host or host group. Authorisation decisions are made by motley-cue, the component that enables federated use of ssh on the ssh-server side. User provisioning may also be triggered at this point, via motley-cue & feudal.
- Users employ the oinit tool to add hosts to the oinit mechanism. Once established, ssh-certificates will automatically be retrieved, whenever this may be necessary and stored in the ssh-agent.
- Serverside tools and configuration for enabling ssh without knowledge of local usernames, which is particularly useful in federated scenarios.

We present the architecture, an initial security assessment, as well as a live demo of ssh with OpenId Connect, with oinit and selected components.

Primary authors: Dr GUDU, Diana (KIT); HARDT, Marcus (KIT); Mr ZACHMANN, Gabriel (KIT)

Presenter: HARDT, Marcus (KIT)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations