Contribution ID: **24** Type: **Short Talk**

Updates on SSH with OpenId Connect

Thursday, 3 October 2024 10:00 (20 minutes)

The Secure Shell (SSH) Protocol is widely recognized as the de-facto standard for accessing remote servers on the command line, across a number of user cases, such as: remote system administration, git operations, system backups via rsync, and high-performance computing (HPC) access.

However, as federated infrastructures become more prevalent, there is a growing demand for SSH to operate seamlessly and securely in such environments. Managing SSH keys in federated setups poses a number of challenges, since SSH keys are trusted permanently, can be shared across devices and teams, and do not have a mechanism to enforce the use of passphrases. Unfortunately, there is currently no universally accepted usage pattern for globally federated usage.

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. The main novelty that will be presented in this contribution is the integration of an SSH-certificate-based mechanism into the existing ecosystem for SSH with OpenId Connect, consisting of motley-cue and oidc-agent.

This new mechanism consists of a set of programs collectively referred to as "oinit". It aims to simplify the usage of SSH certificates by leveraging authorization information via established federation mechanisms. The main benefit is that, after an initial setup step, SSH may be used securely without interrupting existing flows, enabling the use of rsync, for example.

The core components of oinit include the following:

- oinit-ca: this component provides a REST interface to an SSH Certificate Authority (CA), allowing authorized users to obtain SSH certificates for specific hosts or host groups. Authorization decisions are handled 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 and feudal.
- oinit: client-side tool employed by users to add hosts to the oinit mechanism. Once configured, SSH certificates are automatically retrieved as needed and stored in the SSH agent.
- Server-side tools and configuration: these enable SSH usage without requiring knowledge of local usernames, a particularly useful feature in federated scenarios.

In addition to outlining the architecture and functionality of our solution, we provide an initial security assessment and offer a live demo of SSH with OpenID Connect, with oinit and selected components.

Topic

Trust and Security: Trusted computing:

Primary authors: GUDU, Diana (KIT); ZACHMANN, Gabriel (Karlsruhe Institute of Technology); BROCKE, Lukas (KIT); Dr HARDT, Marcus (KIT-G)

Presenter: GUDU, Diana (KIT)

Session Classification: Trust & Security