SCITOKENS SSH

Token-Based Authentication for Remote Login

You Alex Gao(Student author)
University of Illinois
yougao2@illinois.edu

Jim Basney
NCSA
jbasney@illinois.edu

Alex Withers
NCSA
alexw1@illinois.edu

SciTokens Project

- Introduces a ***capabilities-based* authorization infrastructure** for distributed scientific computing,
- Provides a **reference platform**, combining CILogon, HTCondor, CVMFS, and XRootD, and
- **Implements specific use cases** to help our science stakeholders (LIGO and LSST) better achieve their scientific aims.

Using Standards

- RFC 6749: OAuth 2.0 Authorization Framework
  - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
  - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
  - token signing keys, policies, endpoint URLs
- OAuth 2.0 Token Exchange (IETF OAuth WG I-D)
  - token delegation, drop privileges.

SciTokens SSH

- A token-based authentication method for remote login through SSH authentication via SciTokens
- Based on XSEDE OAuth SSH, SciTokens SSH routes SSH authentication requests to a PAM stack in which the module pam_oauth_ssh.so is used for sshd authentication.
- Can be configured to use Globus Auth and/or SciTokens for authentication.
- Verifies SciTokens using the SciTokens C++ Library, scitokens-cpp.

Authentication Flow

Example SciToken

```
{
  "scope": "ssh:vt20",
  "aud": "martok.ncsa.illinois.edu",
  "iss": "https://demo.scitokens.org",
  "exp": 1583855836,
  "iat": 1583855236,
  "nbf": 1583855236,
  "jti": "073ac358-4f07-4090-ae5f-b5c5be273269"
}
```

Example PAM modification (PAM Stack)

```
auth  required   pam_sepermit.so
auth  required   pam_env.so
auth  [success=done maxtries=die new_authtok_reqd=done default=ignore] pam_oauth_ssh.so
auth  requisite  pam_succeed_if.so uid >= 1000 quiet_success
auth  required   pam_deny.so
```

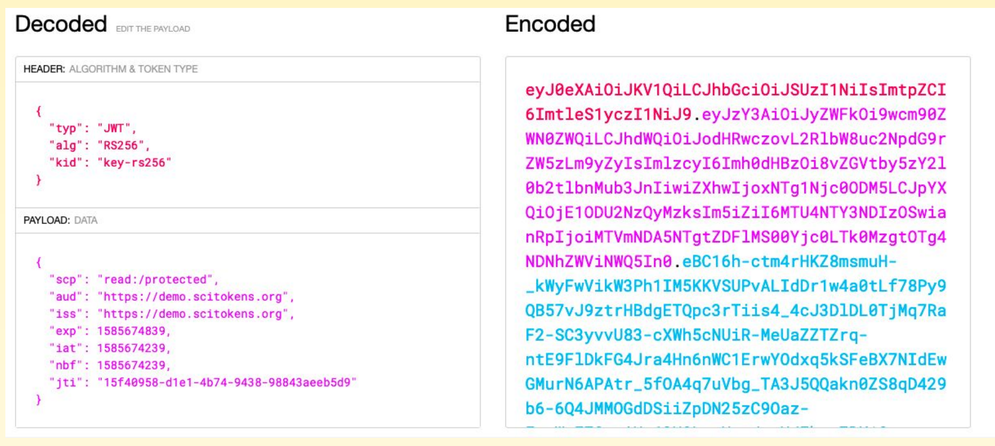
Using SciTokens SSH

```
[$ssh vt20@martok.ncsa.illinois.edu
[Enter your OAuth token:
 Last login: Wed Apr  8 15:57:57 2020 from vt20.security.ncsa.illinois.edu
 [vt20@martok ~]$
```

Authentication Succeeds

```
Enter your OAuth token:
Enter your OAuth token:
Enter your OAuth token:
vt20@martok.ncsa.illinois.edu's password:
Permission denied, please try again.
vt20@martok.ncsa.illinois.edu's password:
Received disconnect from 141.142.236.2 port 22:2: Too many authentication failures
Authentication failed.
```

Password prompt after token authentication fail



SciTokens Issuer

Related Work

- GSI-OpenSSH:
  Standard solution for remote login to scientific computing resource.
- Globus Auth SSH:
  Provides a pluggable authentication module (PAM) that accepts OAuth tokens for authentication.
- SciTokens:
  A JWT profile and associated open source implementation.

Evaluation and Security Analysis

- Eavesdropping access tokens:
  Attempt to obtain an access token when transported between the SSH client and server.
  - Countermeasure:
    Rely on the SSH protocol to encrypt the access token via an SSH public key encrypted channel.
- Leakage of tokens via log files:
  Access tokens may be logged.
  - Countermeasure:
    Log with just enough information to allow administrators and user to debug

Conclusions and Future Work

SciTokens SSH is a modification to Globus Auth SSH (a.k.a. XSEDE OAuth SSH) that adds support for SciTokens JWTs alongside the existing support for opaque Globus Auth tokens.

Future Work:

- Fine-grained access control:
  SciTokens can be issued with a restricted scope of claims. In the future, SciTokens SSH can integrate other SSH solutions that allow fine-grained access control.
- Automate authentication process:
  Currently, users will need to manually cut-n-paste the token to respond prompt.
- Account mapping and grouping:
  Globus Auth SSH allows mapping requested account to local account but currently, there is no need for SciTokens SSH to perform account mapping

https://scitokens.org/

This material is based upon work supported by the National Science Foundation under Grant No. 1738962. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.