Panel: XSEDE's Perspective on Token Assurance for Authentication and Authorization

Panelists:
Jim Basney (XSEDE, NCSA, CILogon, SciTokens), moderator
Lee Liming (XSEDE, University of Chicago, Globus)
Derek Simmel (XSEDE, PSC)
Brian Hom (XSEDE, SDSC)

WoTBAn&Az 2020 - December 1, 2020

XSEDE
Extreme Science and Engineering
Discovery Environment

NSF Supported by OAC 15-48562.

Introductory Remarks

Jim Basney

XSEDE Requirements Analysis & Capability Delivery (RACD) group activities:

- https://software.xsede.org/display/xci-205
  Identify user X.509 credential assurance use cases & how to maintain them w/ OpenID
- https://software.xsede.org/display/xci-694
  Add SciTokens support to SSH with OAuth
- https://software.xsede.org/display/xci-707
  Evaluate AARC-G048 (Guidelines for Secure Operation of Attribute Authorities and other issuers of access statements) for adoption
- https://software.xsede.org/display/xci-800
  Security Token Assurance for Authentication and Authorization interoperability

REFEDS Assurance, and Tokens

XSEDE IdP asserts REFEDS MFA and REFEDS Cappuccino

Enabled by mapping of REFEDS Cappuccino to https://igtf.net/ap/authn-assurance/birch

CILogon ID Tokens include "acr": "https://refeds.org/profile/mfa"
(but not eduperson_assurance)

AARC, AEGIS, and Token Issuers

XSEDE participates in the AARC Engagement Group for Infrastructures (AEGIS)
https://aarc-community.org/about/aegis/

AARC-G048: "Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements" - operational requirements for token issuers

- key management
- network configuration
- policy management
- metadata publication
- logging and auditability
- disaster recovery

Lee Liming

- XSEDE web applications use Globus Auth OIDC service (OIDC 1.0, OAuth 2.0)
- From the user's POV, allows identity linking
  - Users may link identities they have with several organizations (campus, XSEDE, ORCID)
  - Users may login to XSEDE applications using any of their linked identities
- From the developer's POV, allows apps to standardize on XSEDE identities
  - An application can request that it always sees the user's XSEDE identity, even if they login using a different (linked) organization
  - If no XSEDE identity is linked yet, Globus walks the user through linking their XSEDE identity and doesn't complete until an XSEDE identity is linked
- XSEDE web apps haven't needed to use Globus's session features (device & browser isolation, required identity authn, authn timeouts, etc.)
- Recent XSEDE REST APIs beginning to use Globus OAuth for user-specific API access
  - Apps can enable users to see their own job status & usage info, with proper OAuth consents

Globus Connect Server v5’s transition to OAuth

- XSEDE will benefit from GCS version 5’s transition to OAuth
  - Specific benefit is better support for Science Gateways
  - Science Gateway = independent web portal that uses XSEDE “behind the scenes”
  - IETF X.509 policy complicated Gateways because the main XSEDE IDP couldn’t issue X.509 certificates for “community accounts” (had to use an alternate CA)
- XSEDE had to wait for custom identity mapping feature (now available in 5.4)
  - XSEDE endpoints require an XSEDE identity, but then need to map to arbitrary local usernames (not the same as the XSEDE username)
  - XSEDE has a tool to generate the mapfile for a given resource, but needed GCS to support it
- XSEDE is currently working to roll out GCS v5.4 support for service providers who wish to use it with their XSEDE resources

OAuth-SSH

- X.509-based GSI-OpenSSH was too cumbersome to ask end users to install, so XSEDE's current SSH mechanism relies on a "jump host:" the XSEDE SSO Hub
  - Supports SSH connections using XSEDE username and password via PAM plugin
  - Delegates a short-lived X.509 cert for use with locally installed GSI-OpenSSH
  - Users can ssh to XSEDE resources from the SSO Hub without another authentication
- OAuth-SSH is slightly better, as the server-side PAM module expects the OAuth token in the password field, so it can be used with standard clients
  - The problem is getting the OAuth token in the first place, as that requires a web login flow
  - Ideally, the user experience would start in a web browser instead of the command-line
- XSEDE currently exploring OAuth-SSH in the context of Open OnDemand, an increasingly popular web interface for HPC systems
  - Open OnDemand already provides an "SSH in the browser" experience, so the web login flow would fit well within that experience

Derek Simmel

Senior Information Security Officer, Pittsburgh Supercomputing Center

Co-lead (along with Alex Withers, NCSA), XSEDE Security Operations

Team Member, XSEDE Cyberinfrastructure Integration (XCI)
Requirements Analysis and Capability Delivery (RACD)

Chair, The Americas Grid Policy Management Authority (TAGPMA)

XSEDE Security Policies

XSEDE Security Policies & Agreements

- XSEDE Security Working Group Charter
- XSEDE Acceptable Use Policy
- XSEDE Privacy Policy
- XSEDE Level1 Service Provider Security Agreement

XSEDE Security Standards

- XSEDE Enterprise Services Baseline Security Standard
- XSEDE Science Gateway Security Policy & Guideline

New: XSEDE Identity and Access Management (IAM) Policy

https://www.xsede.org/ecosystem/operations/security

TAGPMA and IGTF

TAGPMA is one of three regional PMAs, together with EUGridPMA and APGridPMA, that make up the Interoperable Global Trust Federation (IGTF, https://igtf.net).

Main focus to date has been in establishment of standard trust assurance profiles and policies, and accreditation of trusted authentication providers (X.509 certificate authorities) serving various relying party organizations in Research and Education (R&E) communities.

IGTF has spent over 17 years building a worldwide trust federation...

> What should IGTF's role(s) be in supporting essential trust relationships necessary for token-based authentication and authorization?

Brian Hom

Security Analyst, San Diego Supercomputer Center

Team Member, XSEDE Security Operations

- Tasked with creating a new XSEDE IAM Policy for groups within XSEDE and partners of XSEDE.

New XSEDE IAM Policy

Consists of three new IAM policy documents addressing different groups:

- XSEDE Staff
- Service Providers
- Identity Providers

Challenges and Scoping

- XSEDE consists of many different groups and users. Creating a policy that applies to all the major stakeholders is a large task.

XSEDE IAM Policy Future Goals

- Will need to decide what areas of token based authentication should be put into policy.
- Identify the stakeholders affected by this policy.
- Get the policy fully approved by XSEDE management.

Discussion

What are XSEDE's requirements on authentication strength (MFA, lifetime, key length, etc.) for tokens?

How will XSEDE users obtain/use tokens? Command-line? Web apps? SSH?

What authorization policies will XSEDE apply to tokens (e.g., data access, job submission)?

Who are XSEDE stakeholders for token security requirements (e.g., SPs, partner infrastructures)?

What is the role of IGTF?
What does XSEDE need from IGTF?

How should we integrate tokens into XSEDE's IAM policy (e.g., referencing AARC documents)?

Other Questions?

Thanks!

Links:

https://www.xsede.org/ecosystem/operations/security

https://software.xsede.org/

Contact:

bhom@sdsc.edu dsimmel@psc.edu jbasney@illinois.edu lliming@uchicago.edu