Integrating Science Gateways with XSEDE Security: A Survey of Credential Management Approaches

Jim Basney, Jeff Gaynor
University of Illinois
{jbasney,gaynor}@illinois.edu

Suresh Marru, Marlon Pierce, Thejaka Amila Kanewala
Indiana University
{smarru,marpierc,thejkane}@iu.edu

Rion Dooley, Joe Stubbs
University of Texas
{dooley,jstubbs}@tacc.utexas.edu

ABSTRACT
We present a survey of credential management approaches for science gateways to integrate with the X.509 security infrastructure used by XSEDE.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms
Security

Keywords
Science Gateways, X.509

1. INTRODUCTION
When accessing XSEDE resources, science gateways can use a variety of credential management approaches for authentication, accounting, authorization, and auditing [8]. In this short article, we discuss the pros and cons of different approaches and we highlight remaining challenges.

One of the key choices for the science gateway is whether to access XSEDE resources using individual user credentials, community credentials, or a combination of the two. Community credentials scale access to XSEDE resources by allowing the science gateway to locally manage users without requiring users to obtain XSEDE accounts. For users with XSEDE accounts, however, using their individual credentials via the science gateway can provide a greater level of access to XSEDE resources and avoid requiring a separate account at the science gateway.

Credential lifetime is another important issue for science gateways. Short-lived credentials limit exposure to compromise but introduce challenges of issuance, expiration, and renewal, while long-lived credentials can significantly simplify credential management. While the science gateway could manage its own long-lived community credential, security policy requires individual credentials to be only short-lived at the gateway.

In the next section, we discuss pros and cons of current approaches for managing credentials in XSEDE science gateways, including considerations of security risks, complexity, and usability. Then in the following section we conclude by discussing remaining challenges and open issues.

XSEDE '14, Jul 13-18 2014, Atlanta, GA, USA
ACM 978-1-4503-2893-7/14/07.
http://dx.doi.org/10.1145/2616498.2616559

2. APPROACHES
Community Credentials: In the community credential approach [12], the science gateway uses its own credential for authentication to XSEDE services. This credential may be a community user certificate or robot certificate or host/service certificate. **Pros**: 1) Widely supported by X.509 software, including Globus and UNICORE. 2) Certificates may be long-lived to avoid expiration/renewal concerns. **Cons**: 1) Long-lived credentials increase exposure to compromise. 2) Makes per-user accounting more difficult.

Per-User Attributes: A science gateway using a community credential may generate a proxy certificate containing per-user attributes for accounting purposes. This approach has seen limited adoption in XSEDE to-date [6]. **Pros**: 1) Enables per-user accounting by XSEDE resources. **Cons**: 1) Requires a complex software stack. 2) Not supported by UNICORE and other grid middleware.

MyProxy: In the traditional MyProxy approach [2], the user enters a username and password at the science gateway, which the science gateway uses to obtain a short-lived certificate for that user from a MyProxy server. **Pros**: 1) Multiple MyProxy client implementations are available. 2) Widely used and supported by projects and services. 3) The MyProxy server can be configured to support certificate renewal [1]. **Cons**: 1) Since it exposes the user's MyProxy password to the science gateway, XSEDE's MyProxy server no longer supports this approach. 2) The MyProxy protocol is not SOAP or REST, so it can be difficult to integrate with web services.

MyProxy Session Passwords: One method to address password exposure is to create per-session passwords by storing short-lived credentials in the MyProxy repository for each application [9]. A current application for this technique is activation of Globus Transfer endpoints, because the Globus Transfer API requires a MyProxy password. **Pros**: 1) Avoids exposure of long-lived passwords. 2) Works with applications that require MyProxy. **Cons**: 1) Requires a MyProxy repository server.

OAuth for MyProxy: In this approach, the science gateway redirects the user's browser to a MyProxy OAuth service where the user logs in and delegates a certificate back to the science gateway [3]. **Pros**: 1) Supported by XSEDE. 2) Protects the user's MyProxy password from exposure. **Cons**: 1) No credential renewal support. 2) No API support (i.e., browser-based). 3) Uses older OAuth 1.0 protocol.

MyProxy Gateway: When using the MyProxy Gateway (MPG) [7], the science gateway redirects the user's browser to the MPG service where the user logs in and grants permission for the science gateway to obtain a delegated credential. The gateway can then obtain a credential on behalf of the user as needed. **Pros**: 1) Full OAuth 2.0 support including credential refreshing and

multiple protocol flows (web, mobile, and device). 2) Supports per-user attribute injection via the MPG server, eliminating the need for complex attribute injection in the science gateway. 3) Protects the user's MyProxy password from exposure. **Cons**: 1) Not currently supported by XSEDE.

CILogon: CILogon [5] is an instance of OAuth for MyProxy that supports campus authentication via the InCommon federation. **Pros**: 1) Enables users to log in with their campus credentials. 2) Does not expose the user's password to the science gateway. **Cons**: 2) No credential renewal support. 2) No API support (i.e., browser-based).

Airavata Credential Store: The Apache Airavata Credential Store provides credential management that is closely integrated with the Airavata science gateway middleware [10]. **Pros**: 1) Supports credentials of different types (X.509 certificates, SSH keys). 2) Supports multi-tenant science gateway hosting via a shared middleware tier. 2) Provides credential expiry notifications and supports MyProxy certificate renewal. **Cons**: 1) Depends on the Airavata middleware.

3. CONCLUSIONS

A challenge that science gateways face is a continuously changing landscape: new software is released and support for old software is lost, new services are provided and old services are retired, security algorithms and policies change, etc. For example, currently multiple XSEDE science gateways must update their software to support the SHA-2 hash algorithm used in X.509 certificates, replacing the older SHA-1 hash algorithm which is now considered too weak. Supporting SHA-2 means replacing old software (such as JGlobus 1.0) that science gateways depend upon. Integrating with RESTful services, such as the MyProxy Gateway, can be an attractive alternative to introducing new software dependencies directly in the science gateway.

Credential management (the focus of this short article) is only one aspect of science gateway security. Science gateways must address a variety of operational security challenges including least privilege access, data integrity and isolation, software patching, intrusion detection, and incident response [4][11]. Leveraging existing security services, on campus and in the cloud, where possible, can significantly reduce risk and complexity for the science gateway developer and operator.

In conclusion, a variety of software and services are available to assist science gateways with managing credentials for accessing XSEDE resources. Multiple interfaces to MyProxy enable integration with campus credentials, multi-tenant gateway architectures, and RESTful APIs.

4. ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under grant number ACI-1127210.

5. REFERENCES

[1] Daniel Kouril and Jim Basney, "A Credential Renewal Service for Long-Running Jobs," 6th IEEE/ACM International Workshop on Grid Computing (Grid 2005), Seattle, WA, November 2005. http://dx.doi.org/10.1109/GRID.2005.1542725

[2] Jason Novotny, Steve Tuecke, and Von Welch, "An Online Credential Repository for the Grid: MyProxy," International Symposium on High Performance Distributed Computing (HPDC), August 2001, San Francisco, CA. http://dx.doi.org/10.1109/HPDC.2001.945181

[3] Jim Basney and Jeff Gaynor, "An OAuth Service for Issuing Certificates to Science Gateways for TeraGrid Users," TeraGrid Conference, July 2011, Salt Lake City, UT. http://dx.doi.org/10.1145/2016741.2016776

[4] Jim Basney and Von Welch, "Science Gateway Security Recommendations," Science Gateway Institute Workshop, September 2013, Indianapolis, IN. http://dx.doi.org/10.1109/CLUSTER.2013.6702697

[5] Jim Basney, Terry Fleury, and Jeff Gaynor, "CILogon: A Federated X.509 Certification Authority for CyberInfrastructure Logon," XSEDE Conference, July 2013, San Diego, CA. http://dx.doi.org/10.1145/2484762.2484791

[6] Jim Basney, Von Welch, and Nancy Wilkins-Diehr, "TeraGrid Science Gateway AAAA Model: Implementation and Lessons Learned," TeraGrid Conference, August 2010, Pittsburgh, PA. http://dx.doi.org/10.1145/1838574.1838576

[7] Rion Dooley, Joe Stubbs, Jim Basney, "The MyProxy Gateway," International Workshop on Science Gateways, June 2014, Dublin, Ireland. https://utexas.box.com/s/zdm72k0bnjj9jhqppls7

[8] Suresh Marru et al., "XSEDE Science Gateway Use Cases," Version 0.4, October 2012. http://hdl.handle.net/2142/43883

[9] Terry Fleury, Jim Basney, and Von Welch, "Single Sign-On for Java Web Start Applications Using MyProxy," ACM Workshop on Secure Web Services, November 2006, Alexandria, VA. http://dx.doi.org/10.1145/1180367.1180384

[10] Thejaka Amila Kanewala, Suresh Marru, Jim Basney, and Marlon Pierce, "A Credential Store for Multi-Tenant Science Gateways," International Symposium on Cluster, Cloud and Grid Computing (CCGrid), May 2014, Chicago, IL. http://hdl.handle.net/2022/17379

[11] Victor Hazlewood and Matthew Woitaszek, "Securing Science Gateways," TeraGrid Conference, July 2011, Salt Lake City, UT. http://doi.acm.org/10.1145/2016741.2016781

[12] XSEDE Security Working Group, "XSEDE Science Gateway Security Policy and Guideline," Version 0.3.3, January 2014. http://hdl.handle.net/2142/46966