CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

SciGaP-CTSC Engagement Summary

May 26, 2016

For Public Distribution

Randy Heiland, Scott Koranda, and Von Welch

About CTSC

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC, trustedci.org) is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to solve their specific problems, broad education, outreach and training to raise the practice-of-security across the community, and looking for opportunities for improvement to bring in research to raise the state-of-practice.

Acknowledgments

CTSC's engagements are inherently collaborative; the authors would like to thank the SciGaP team, especially Marlon Pierce and Suresh Marru, for the collaborative effort that made this document possible.

This document is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grant Numbers OCI-1234408 and ACI-1547272. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: http://trustedci.org/. 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.

Using & Citing this Work

Cite this work using the following information:
R. Heiland, S. Koranda, and V. Welch, "SciGaP-CTSC Engagement Summary," Center for Trustworthy Scientific Cyberinfrastructure, trustedci.org, May 2016. Available: http://hdl.handle.net/2022/20926

This work is available on the web at the following URL: http://trustedci.org/scigap

1 Introduction

The Science Gateway Platform as a service (SciGaP) project provides middleware services for science communities. SciGaP has several cybersecurity challenges as it integrates web, campus cyberinfrastructure, and cloud technologies. These challenges cover a broad range of topics: levels of trust between multiple entities, identity and access management, authentication and authorization, software assurance, and more. The engagement has helped clarify security challenges, generate actionable advice, and produce multiple reports that should be useful for general security issues for the broader NSF science community.

2 Engagement Summary

The following summarizes our engagement's goals and results:

- *Provide feedback on SciGaP's Credential Store.*

  CTSC reviewed a draft paper describing the SciGaP Credential Store[1]. A member/Co-PI of CTSC (Jim Basney) was a co-author on the paper and offered considerable experience in understanding and addressing the subject. The matter of using OAuth2 was addressed later in our engagement.

- *Provide a preliminary "best security practices" for SciGaP.*

  CTSC provided a document: *Suggested Security Practices for SciGaP: A Preliminary Report*[2]. This document summarized the different types of gateway models, listed several best practices relevant for SciGaP security, and demonstrated a static analysis tool (available from a free online service, SWAMP) applied to a snapshot of some core SciGaP code (Apache Airavata). More details can also be found in the final recommendations report.

[1] http://dx.doi.org/10.1109/CCGrid.2014.95

[2] http://hdl.handle.net/2022/20811

- *Provide an expanded description of trust models, especially as they relate to SciGaP.*

  CTSC provided a brief description of *brokered* and *transitive* trust models, in the context of science gateways. This can be found in Section 2 of the final recommendations report[3].

- *Analyze Apache Thrift and the Evernote service that uses it.*

  CTSC provided a report: *CTSC Recommended Security Practices for Thrift Clients: Case Study - Evernote*[4]*.*

- *Provide a summary of authentication and authorization options for SciGaP, with an emphasis on X.509 and OAuth2.*

  CTSC and SciGaP wrote a paper, *Authentication and Authorization Considerations for a Multi-tenant Service*[5], and presented it at the *The Science of Cyberinfrastructure: Research, Experience, Applications and Models* (SCREAM) workshop, June 2015. In addition, we had many conversations about Identity and Access Management (IAM), a topic in which CTSC has considerable expertise[6].

3 Conclusion

The SciGaP-CTSC engagement was quite unique. Its duration (about 18 months) was much longer than an average engagement; however, we met infrequently. This was primarily due to the fact that the SciGaP project had only recently begun and had many start-up tasks to address. This resulted in a longer-term, atypical consulting-style engagement. It is possible that CTSC will need to follow a similar approach for future projects that may just be getting started; therefore, it was a good learning experience. The range of security topics for SciGaP was very broad and some didn't become apparent until late in the engagement, e.g., OAuth. Portions, if not all, of the findings in the reports that resulted from this engagement should be applicable to future CTSC engagements with a software focus, especially if they involve software as a service. This was a highly productive engagement that led directly to SciGaP's current security infrastructure implementation.

[3] http://hdl.handle.net/2022/20927

[4] http://hdl.handle.net/2022/20620

[5] http://hdl.handle.net/2022/20619

[6] http://trustedci.org/iam/