Science Gateways and Cybersecurity: Learning from the Past and Preparing for the Future

Randy Heiland* and Von Welch,
Center for Applied Cybersecurity Research, Indiana University,
Bloomington, IN, 47408, USA; *email: heiland@iu.edu

Abstract: *Science gateways connect communities of scientists and engineers to distributed cyberinfrastructure (CI). Cybersecurity is therefore an important component to help protect the people, machines, and data from malicious activity and accidental mistakes. The Science Gateways Community Institute (SGCI) and Center for Trustworthy Scientific Cyberinfrastructure (CTSC) have partnered to address cybersecurity for gateway development and operation. This paper and presentation will provide an overview of and goals for this partnership.*

1. Introduction

Science gateways have an important goal: make science and engineering research and education more accessible. One way gateways achieve this is by providing value-added interfaces to distributed cyberinfrastructure (CI). Web-based portals, customized for particular communities, have been the most common interface in the past and will likely continue into the future. However, other interfaces will include mobile devices, e.g. phones and tablets, and perhaps even specialized visualization environments. Gateways lower the barrier to accessing CI resources, e.g. scientific/engineering instruments and data, high performance computing (HPC), high throughput computing (HTC), and cloud services. Given all this, developers and administrators of gateways need considerable cybersecurity expertise to help protect both the CI and the users. The recently announced NSF-funded Science Gateways Community Institute (SGCI) will undoubtedly increase the number of gateways, resulting in more diverse and growing user communities and CI. This also means there will be more gateway software development and operations that will require cybersecurity expertise.

2. SGCI and CTSC

SGCI has partnered with the NSF-funded Center for Trustworthy Scientific Cyberinfrastructure (CTSC) to provide this expertise. Founded in 2012 by a multi-institutional team of science-focused cybersecurity specialists, CTSC[1] has a mission to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. In 2016, CTSC was renewed as the NSF Cybersecurity Center of Excellence. A core activity of CTSC is to partner with other NSF projects through a formal *engagement* process[2]. Each engagement is unique and may involve one or more aspects of cybersecurity, e.g. policy, CI operation, identity and access management, software assurance, situational awareness, etc. The duration of an engagement will vary, but typically will be a few weeks to a few months (of part-time effort from staff in both projects). CTSC's goal is to disseminate and share lessons learned with the entire NSF community through final engagement reports. The reports maintain the privacy of any operational cybersecurity details, are sensitive to all projects, offer suggestions for improvement, and are constructive rather than unnecessarily critical.

The partnership between SGCI and CTSC is a much longer-term commitment than a typical engagement, running the length of the projects. Of the five *solution areas* defined by the SGCI, CTSC will work with the Incubator area. Incubator has responsibility for cybersecurity and software-engineering practices, among other foci.

In this presentation, we will discuss the process, experience, and results from a few past

[1] http://trustedci.org
[2] http://trustedci.org/application/

Presented at Gateways 2016, San Diego Supercomputer Center, La Jolla, CA, November 2-3, 2016.
https://gateways2016.figshare.com/

(and ongoing) CTSC engagements related to software and/or gateways, e.g. SciGaP [1], Globus [2], and HUBzero. We will also provide details of the training that CTSC plans to provide for the SGCI gateway developers and administrators.

3. Gateway Security

Gateways involve many aspects of cybersecurity that were mentioned above. Identity and access management has been and continues to be a significant challenge [3-6]. One primary contribution CTSC will provide the SGCI is training on secure software engineering practices [7]. Additional training could cover the overlapping areas of software assurance and situational awareness[3] (for software vulnerabilities). And further consultation may occur in identity and access management.

One topic related to software assurance is static code analysis. CTSC has considerable expertise in using, for example, the Software Assurance Marketplace (SWAMP[4]), a no-cost cloud service providing multiple static analysis tools. Analyzing gateway-related software with one of these tools can highlight lines of code and their weaknesses (CWE[5]), e.g.:

CWE-398: Indicator of Poor Code Quality
CWE-547: Use of Hard-coded, Security-relevant Constants
CWE-252: Unchecked Return Value
CWE-571: Expression is Always True
CWE-584: Return Inside Finally Block
CWE-563: Assignment to Variable without Use
CWE-478: Missing Default Case in Switch Statement
CWE-495: Private Array-Typed Field Returned From A Public Method

But static analysis is just one of many software engineering best practices that address security. Others practices include the use of:

- (secure) software repositories and hosting services,
- issue tracking tools,
- continuous integration processes and tools,
- multiple levels of software testing – and automation when possible,
- vulnerability scanners for Web apps.

We will discuss these and more in our presentation. In addition to these technology-focused practices, it is important to establish and follow security *policies*, e.g., related to physical security, personnel responsibility, training, etc. CTSC provides many online training materials.[6]

4. Conclusion

The development and operation of science gateways touch on many aspects of cybersecurity. Users, data, and CI need to be protected. All three key principals of security: confidentiality, integrity, and availability are relevant for gateways. The goals of this project are to make the gateway community aware of CTSC and SGCI services related to gateways and cybersecurity, and solicit feedback from that community on their requirements.

5. Acknowledgments

This work is supported in part by the National Science Foundation through the awards ACI-1547611 and ACI-1547272.

[3] http://trustedci.org/situational-awareness
[4] https://continuousassurance.org/
[5] https://cwe.mitre.org/
[6] http://trustedci.org/trainingmaterials/

References

[1] R. Heiland, S. Koranda, and V. Welch, "SciGaP-CTSC Engagement: Final Technical Recommendations", Apr. 2016. http://hdl.handle.net/2022/20927

[2] R. Heiland, S. Koranda, and V. Welch, "Globus Data Sharing: Security Assessment", Nov. 2014. http://hdl.handle.net/2022/19165

[3] V. Welch, J. Barlow, J. Basney, D. Marcusiu, and N. Wilkins-Diehr, "A AAAA Model to Support Science Gateways with Community Accounts." *Concurrency and Computation: Practice & Experience* 19 (6). John Wiley & Sons, Ltd.: 893–904. 2007.

[4] J. Basney, V. Welch, and N. Wilkins-Diehr, "TeraGrid Science Gateway AAAA Model: Implementation and Lessons Learned." In *Proceedings of the 2010 TeraGrid Conference*, 2:1–2:6. TG '10. New York, NY, USA: ACM, 2010.

[5] J. Basney, and J. Gaynor, "An OAuth Service for Issuing Certificates to Science Gateways for TeraGrid Users." In *Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery*, 32:1–32:6. TG '11. New York, NY, USA: ACM, 2011.

[6] R. Heiland, S. Koranda, S. Marru, M. Pierce, and V. Welch, "Authentication and Authorization Considerations for a Multi-Tenant Service." In *Proceedings of the 1st Workshop on The Science of Cyberinfrastructure: Research, Experience, Applications and Models*, 29–35. SCREAM '15. New York, NY, USA: ACM. June 2015. http://dx.doi.org/10.1145/2753524.2753534

[7] R. Heiland and S. Sons, "Secure Software Engineering Best Practices (v1.0)". Presentation at the NSF Cybersecurity Summit, August 2016. http://hdl.handle.net/2022/20970