2017 Cyber Security
R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.
The SWAMP Software Stack

James A. Kupsch | Software Assurance Marketplace (SWAMP) at University of Wisconsin - Madison

July 12, 2017
Team Profile

- Designing, building, and operating the SWAMP is a joint effort of four research institutions: Morgridge Institute for Research (lead), Indiana University, University of Illinois Urbana-Champaign, and University of Wisconsin-Madison.
From Continuous Integration to Continuous Assurance

- The software development community needs an open and powerful continuous software assurance capability, to lower the barriers to performing software assurance.
- Software developers need to effectively integrate continuous software assurance capabilities into development workflows without hindering time to market or project cost.
- Consumers of software need services to evaluate the quality of the components they deploy or integrate into their software stack.
The SWAMP-in-a-Box (SiB) Approach

- **SiB** is on-premise SWAMP software that compliments the SWAMP facility.
- **SiB** supports the customization of platforms and static analysis tools, and facilitates the unique needs of commercial tools (technical and legal).
- Private/local deployments of **SiB** offer privacy for sensitive software.
- **SiB** provides continuous assurance in a DevOps environment.

[https://continuousassurance.org/swamp-in-a-box/](https://continuousassurance.org/swamp-in-a-box/)
Integration of SWAMP into the SDLC

- Plug-ins for Eclipse, Jenkins, Git, and Subversion enable seamless integration with the SWAMP facility and local SWAMP-in-a-Box instances. 
  https://continuousassurance.org/plug-ins/
  - Investigating plug-ins for other software tools

Collaboration and Development Approach

- Collaboration with and upcoming deliverables from STAMP and ASTAM performers.
- Support SATE VI
- Planned key activities for SWAMP Project Year 6:
  - Partnering with the Underwriter’s Lab (UL), LLC.
  - Developing a tool to track vulnerabilities among different versions of the same open source package.
  - Visualization of metrics and weaknesses.
Benefits

- The broader adoption of continuous assurance technologies results in more secure software.
- Private/local SWAMP-in-a-Box installations enable building private/local “ready to go” customized, continuous software assurance facilities.
- SWAMP-in-a-Box is an open, community-owned, portable, continuous assurance capability supported by a centralized facility.
- Plug-ins for IDEs and Continuous Integration environments lowers the bar for continuous assurance.
Competition

- Commercial tool vendors (e.g. Coverity Scan, HP Fortify) offering software assessment services for open-source software.
- Providers of Continuous Integration services (e.g. Travis CI, SonarQube, Jenkins).
Current Status of the SWAMP Facility

- The SWAMP facility has been operational for three years.
  - 27 open source static analysis tools and three commercial static analysis tools are offered in the SWAMP.
- Five platforms, with 18 total versions, are provided in the SWAMP.
- 11 programming languages are currently supported.
- 500+ curated packages including NIST’s Juliet Test Suite for C/C++ and Java.
Current Status of SWAMP-in-a-Box

- SWAMP-in-a-Box (SiB) is available as an open beta.
  - Local instances of the SWAMP are being deployed at several organizations.
  - FAA, Raytheon, NASA IV&V
- Feedback from users and beta testers is being incorporated into future SiB software releases.
  - Reducing the footprint of a SiB deployment
  - Customizing a SiB instance
Status of Third-Party Integrations

- SWAMP-in-a-Box (SiB) has incorporated a BYOL (bring-your-own-license) model.
  - Users can incorporate already purchased or soon-to-be purchased commercial tools into their own SiB instances.
- Three plug-ins are available from the Eclipse Marketplace, Jenkins plugins index, and GitHub for integration into a SiB instance or the SWAMP facility.
- SiB can integrate with multiple identity providers
Transition/Completion Activities

- Identify and engage with contributors to the SWAMP open source software stack.
- Enhance and implement a distribution and support framework for a wide deployment of SWAMP-in-a-Box.
- Partner with the Underwriter’s Lab (UL), LLC.
- SWAMP-in-a-Box and the plug-ins are available for download from GitHub.
- The SWAMP software stack will remain open source and rely on support from the user community.
Lessons Learned (Part 1)

- Many obstacles to the adoption of software assurance (security) processes and technologies.
- Poor portability of compile/build environments.
- “My software will never leave my server!!!”
- Reducing the footprint of a SiB deployment.
- Limited (if any) interest in an open evaluation of software assurance technologies.
- Adding new tools to the SWAMP or a continuous assurance process requires can require significant time:
  - Tool can require additional capabilities to operate
  - Tools can have bugs
Lessons Learned (Continued, Part 2)

- SWAMP is ahead of its time.
  - Expertise to interpret and remediate reported weaknesses is rare (i.e., SWAMP is step 8 in a process and most are only at step 3 of the process).
  - Secure coding practices are neither common nor required in undergraduate curricula.
- Most development teams focus on functionality and release schedule; continuous software assurance is seen as diverting resources from these goals.
Contact Info

James A. Kupsch
University of Wisconsin-Madison
kupsch@cs.wisc.edu

SWAMP

General Information: swamp@continuousassurance.org
SWAMP Support: support@continuousassurance.org
+1-317-274-3942
@SWAMPTEAM

Join the SWAMP as a provider, consumer, or adopter at
2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.