Software Assurance Marketplace (SWAMP): Continuous Assurance

Miron Livny | John P. Morgridge Professor of Computer Science, Morgridge Institute for Research
March 18, 2019
Funded Contract Information
This material is based on research sponsored by the Department of Homeland Security, Science and Technology Directorate via contract number FA8750-12-2-0289.

No Endorsement Notification
Any reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Homeland Security or the United States Government.

Hyperlinked Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over materials on this website or the information on non-DHS Web sites.

Disclaimer Notification
The views, opinions, findings, conclusions, or recommendations expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or the United States Government. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in the materials assume all liability from such use.
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.

Miron Livny, Morgridge  
Jim Basney, UIUC  
Bart Miller, UW  
Von Welch, IU
Need for Continuous Assurance

- Software controls the locks and implements the safeguards to protect against cyber attacks.
- Software consumers and developers need:
  - An open, continuous software assurance framework to evaluate the quality of software they create, deploy, and integrate into their stack
  - Lower barriers to performing software assurance without hindering time to market or project cost
Need for Continuous Assurance

- Imagine the effects a “modified” cargo balancing algorithm or weights database may have on a ship or airplane.


Open Continuous Assurance

- Through the SWAMP’s open, continuous software assurance framework, there are two ways to bring continuous assurance capabilities to the developer community:
  - SWAMP is a ready-to-use open facility located at mir-swamp.org.
  - SWAMP-in-a-Box is an open distribution of SWAMP software available for download on GitHub or swampinabox.org.
SWAMP-in-a-Box (SiB)

- SiB is on-premises SWAMP software that complements the SWAMP facility.
- Local deployments offer privacy for sensitive software giving developers easy access to continuous assurance capabilities.
- Can be used without internet access.
- Supports the customization of platforms and static analysis tools, and facilitates the unique needs of commercial tools (technical and legal).
Integration into the Software Development Life Cycle (SDLC)

- SWAMP supports continuous assurance in a DevOps environment.
- A Java command line interface (CLI) and plug-ins for Eclipse, Jenkins, and Git/Subversion enable seamless integration with the SWAMP facility and local SWAMP-in-a-Box instances.
  - https://continuousassurance.org/plug-ins/
Benefits

- **Improve quality and security** of your own software
- **Educate students or employees** about secure coding practices and how to mitigate vulnerabilities
- **Reduce costs and Increase ROI**: find and fix weaknesses earlier in development (before releasing software) and use SWAMP at no-cost
Ease of Use – Package Upload

Upload a package: Tell us how to build your software; we automate the rest.
Ease of Use – Assessments

Select a platform and/or tools:
No added effort to run multiple tools. All tools and platforms are installed, configured, and maintained by SWAMP.
Ease of Use – Results

View results: Native viewer provides a static view of tool output. Code Dx viewer consolidates and normalizes tool output.
Collaborations and Interoperability

- SWAMP is vendor-neutral and open to partnerships or collaborations with third parties in effort to increase the broader adoption of continuous software assurance practices.
- SWAMP-in-a-Box (SiB) uses a BYOL (bring-your-own-license) model.
  - Users can incorporate already purchased or soon-to-be purchased commercial tool licenses into their SiB instances (e.g. CodeSonar, Parasoft’s C/C++test or Jtest).
Interoperability cont’d

- SiB can integrate with multiple identity providers (e.g. LDAP, AD).
- Three plug-ins are available from the Eclipse Marketplace, Jenkins plugins index, and GitHub for integration into a SiB instance or the SWAMP facility.
Current Status of the SWAMP Facility

- The SWAMP facility has been operational for nearly five years.
  - 31 open source and four commercial static analysis tools
  - Six platforms, with 19 total versions
  - 11 programming languages
  - 10,000+ curated packages are available, including NIST’s Juliet Test Suite for C/C++ & Java and the BugInjector suite.
  - A framework for integrating software assurance tools
Current Status of SWAMP-in-a-Box

- SWAMP-in-a-Box (SiB) is open source and available on GitHub.
  - Local instances of the SWAMP are being deployed at several organizations.
  - Hosted SiBs are being used by SWAMP collaborators.
  - Feedback from users is being incorporated into future SiB software releases.
    - Customizing a SiB instance
    - Support for containers
Collaboration and Development Status

- Deliverables from STAMP and ASTAM performers → 9,774 BugInjector packages/versions added to SWAMP (Sep. 2018) for user testing
- Assessing S&T-Funded GovReady software in a hosted SiB
- Contributing to the OASIS SARIF (Static Analysis Results Interchange Format) Technical Committee → a common output format to make it easier to understand and manage results across static analysis tools
- Planned key activities for SWAMP Project Year 7:
  - Support for .NET on Linux (Feb. 2019), containers, and Go language
  - Visualization of metrics and weaknesses
Transition/Completion Activities

- 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.
- 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.
Lessons Learned – Obstacles

- “My software will never leave my server!!!” → Developed SiB
- SiB optimization & ease-of-use: reducing the footprint, simplifying installs, clarifying requirements → Feedback-driven, ongoing enhancement of SiB
- Limitations of tools, vendor lock-in → Multiple tool approach, BYOL model; SWAMP is vendor-neutral, positioned as a partner
- SWAMP is ahead of its time. Expertise to interpret and remediate reported weaknesses is rare. Secure coding practices are neither common nor required in undergraduate curricula. → Support educators using SWAMP in the classroom
- Development teams focus on functionality and their release schedule. Adding new tools to continuous assurance processes takes time; continuous software assurance is seen as diverting resources from these goals. → Plug-ins fit SWAMP into DevOps/SDLC, add SWAMP to get many tools
Contact Info
Miron Livny
John P. Morgridge Professor of Computer Science
Morgridge Institute for Research
miron@cs.wisc.edu

SWAMP
General Information: swamp@continuousassurance.org
SWAMP Support: support@continuousassurance.org
@SWAMPTEAM
continuousassurance.org

Visit Booth 20 for a SWAMP demo during the Technology Showcase, today at 4pm-6pm.