2016 I Cyber Security Division
R&D SHOWCASE AND TECHNICAL WORKSHOP
February 17–19, 2016
Washington, DC
SWAMP: Improving Software Assurance Capabilities

Morgridge Institute for Research
Miron Livny

02/19/2016
The Software Assurance Marketplace (SWAMP) Team

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.
Consumer Needs

- Developers of software assurance tools need effective means to continuously evaluate their technologies.
- Software developers need to effectively integrate continuous software assurance capabilities into their development workflows without significantly impacting their time to market or project costs.
- Consumers of software components need services that enable them to evaluate the quality of the components they deploy or integrate into their software stack.
- Educators need to expose their students to a diverse collection of state-of-the-art software assurance technologies.
- The community as a whole needs an open and powerful **facility** that supports the managed sharing of tools and software packages and the viewing of combined results of multiple tools as well as a **portable** continuous assurance capability.

**Lower the barriers and increase the value!**
Approach

- Offer a unified and portable interface to a diverse set of software assurance tools
  - Develop software capabilities for invoking tools and collecting assessment results
  - Facilitate the unique needs (technical and legal) of commercial tools
  - Keep tools and configurations up-to-date to maximize effectiveness
- Provide a rich suite of software packages for tool evaluation
- Design, build, and operate an open facility and a portable capability that meets the diverse and changing needs of the community
  - Flexible data model that treats packages, tools, platforms, and assessment results as first-class objects
  - Secure operation that supports privacy and enables managed sharing in a project oriented framework
  - Powerful and extensible processing and storage capacity
  - Active interaction with the community to identify trends, promote adoption, and collect feedback
Approach (cont.)

- Allow the deployment of private/local SWAMP in the Box capabilities for sensitive software (build a network of SWAMPs)
  - All software is developed under Apache license
  - Managed as an open-source project
  - Support dynamic customization and evolution of tools, packages, and platforms
  - Support exchange of assessment results and federated identity management

- Allow for easy integration of SWAMP capabilities with existing software development workflows via application programming interfaces (APIs)
  - Minimize the barriers to registration, uploading software packages, running assessments, and viewing the results from multiple tools
  - Integration with commonly used IDEs
  - Integration with commonly used software repositories
Analytics!

CWEs in Curated Java packages with all the SWAMP tools

Total Lines vs Total CWEs for Curated Java packages

Curated Packages sorted by Total Lines of Code vs Total Number of CWEs
Same for Juliet Java

CWEs in Juliet Java packages with all the SWAMP tools

Total Lines vs Total CWEs for Juliet Java packages

- Total Number of Lines
- Total Number of CWEs

Juliet Packages
Broader adoption of higher quality software assurance technologies that results in more secure deployed software

- Easy access to an integrated view of assessment results from multiple tools
- “Do it early, and do it often.” (continuous) approach to software assurance
- Making life easier for tool builders through tool automation, integration with viewers, and integration with repositories and IDEs
- Managed sharing of tools, test suites, and results
- Classroom integration of powerful software assurance capabilities
- A testing and evaluation ground for new and mature software assurance tools and technologies
- Private/local SWAMP (in the Box) installations enable building private/local “ready to go” continuous software assurance facilities.
- Open and community owned portable continuous assurance capability
Competition

- Software assessment services for open-source software offered by commercial tool vendors (e.g. Coverity Scan)
- Providers of continuous integration services (e.g. Travis CI)
The **SWAMP** facility has been operational for two years.

20 software assurance tools are available for public usage.

- C/C++ (Clang Static Analyzer, CppCheck, GCC warnings, Parasoft C/C++test, Red Lizard Goanna)
- Java (FindBugs with Find Security Bugs, PMD, Checkstyle, error-prone, Parasoft Jtest)
- Python (Pylint, Flake8, Bandit)
- Ruby (Brakeman, Dawn, Reek, Rubocop, Rubylint)
- Android (Android Lint, RevealDroid; Gradle, Maven, Ant build systems)

Agreements with four commercial tool vendors to include their tools in the SWAMP (Parasoft, GrammaTech, Veracode, Red Lizard). Access to these tools has restrictions/limitations.

550+ software packages are available for public usage.

- Including the NIST Juliet and SATE test suites for C/C++ and Java

Fully integrated **viewing** of multiple assessment results with Code Dx and ThreadFix

Support for **GitHub** identities and uploading software packages from git repositories
Current Status (cont.)

- **Activity on the SWAMP facility**
  - 884 Unique user sign-ups
  - 137,356 Assessment Runs
  - 5,558 Viewer launches

- **Bowie State University (BSU)**
  - Spring Semester 2015 119 assessments run in the SWAMP
    - 2 classes, 3 sections, 46 students
      - COSC 113 Computer Science II/Programming II
      - COSC 214 Data Structures & Algorithms
  - Fall Semester 2015 71 assessments run in the SWAMP
    - 2 classes, 2 sections, 27 students
      - COSC 113 Computer Science II/Programming II
      - COSC 190 Intermediate Computer Programming
  - Teaching Assistants (TA's) have used the SWAMP in their own research as part of the Forensic Technology Information Cyber Squad
    - Took first place in a poster contest at BSU Research Day
    - Presented SWAMP findings to Department of Energy Director, Dot Harris ([http://www.cs.bowiestate.edu/FTI/index.html](http://www.cs.bowiestate.edu/FTI/index.html))
Coming Soon (2nd Quarter 2016)

- Support for scripting languages: JavaScript, HTML, CSS, XML, and PHP
- Additional tools: JSHint, ESLint, Flow, htmltidy, weblint, csslint, xmllint, PHP_CodeSniffer, and PHPMD
- Sonatype Application Health Check (AppCheck)
- Host CodeSonar (GrammaTech)
- Code Metric Tools for C/C++, Java, Python, and Ruby: cloc, lizard, flog, and radon
DHS Projects in the SWAMP

- DHS Science & Technology Directorate (DHS S&T) Transitions (Past, Present, and Future).
  - Already transitioned projects from DHS S&T in the SWAMP.
    - Code Dx
    - ThreadFix
    - RevealDroid
  - What is happening now in the SWAMP with DHS S&T Projects?
    - Sonatype’s AppCheck
    - GrammaTech’s CodeSonar
  - What does SWAMP plan on adding from DHS projects in the future?
    - RAM Lab’s RASAR
Transition

- Develop and implement a distribution and support framework for a wide deployment of SWAMP in the Box.
- Identify and engage contributors to the SWAMP open source software stack.
Lessons Learned

- Many obstacles to the adoption of software assurance (security) processes and technologies
- It's easy to underestimate the cost and complexity of installing, using and maintaining a tool, let alone a suite of tools. There's a real value in letting someone else take care of this for you.
- Poor portability of compile/build environments
- “My software will never leave my server!!!”
- Limited (if any) interest in an open evaluation of software assurance technologies
- Adding new tools to a continuous assurance process requires new capabilities
- Translating “interest” in the SWAMP into a classroom activity is a slow process
Join the SWAMP as a provider, a consumer, or an adaptor at https://continuousassurance.org

- PI and Director: Miron Livny, mlivny@morgridge.org
- Chief Scientist: Bart Miller, bart@cs.wisc.edu
- Asst. Project Manager: Irene Landrum, ilandrum@morgridge.org
- SWAMP Support: support@continuousassurance.org
2016 | Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP