CONTINUOUS ASSURANCE

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

Software Assurance Marketplace (SWAMP) – A Continuous Assurance Platform

Von Welch

Indiana University

A Multi-Institutional Team

- *Morgridge Institute for Research (Morgridge)*
- *University of Illinois Urbana-Champaign, National Center for Supercomputing Applications (UIUC)*
- *University of Wisconsin-Madison (UW)*
- *Indiana University, Center for Applied Cybersecurity Research (IU)*

Miron Livny
Morgridge

Jim Basney
UIUC

Bart Miller
UW

Von Welch
IU

Driven by the need for more secure software and committed to advancing the effective adoption of software assurance tools through technologies and education

Driving Principles

- Community (impact) focused
- Sound (principled) design and execution
- Open source software
- Commitment to training and education
- Serve as an honest facilitator
- Leverage our widely adopted automation and scale-out technologies

It is (almost) all software!

Why should you care about software assurance if you are running Critical National Infrastructure?

Almost everything that you do to **prevent kinetic effects** and protect against **cyber-attacks** is controlled by software. Software controls the locks and software implements the safe-guards. If a software weakness can be exploited, it can allow unauthorized access and/or weakening of a safeguard.

A Kinetic Effect

Imagine the effect a “modified” cargo balancing algorithm or weights database may have on a ship or a plane.

Many Excuses!

Limited adoption of software assurance tools is a result of many factors:

- Software functionality is the main force in software development
- Too labor intensive
- Limitations of software assurance tools
- Expertise required for effective usage of tools
- Vendor lock-in

Continuous Assurance

From Continuous Integration to Continuous Assurance (CoA)

- The software development community needs an open and powerful **continuous** software assurance capability to lower the barriers to executing 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.

Broader adoption of continuous assurance technologies results in more secure software.

"Do It Early! Do It Often!"

Keys to Continuous Assurance

Assess early and assess often

Use multiple tools

Manage assessment process

Access to Continuous Assurance

- **There are two ways to bring the continuous assurance capabilities to the developer:**
  - **SWAMP** is the ready-to-use, open facility located at https://www.mir-swamp.org/. It's a good way to get started and to try (test drive) continuous assurance.
  - **SWAMP-in-a-Box** (**SiB**) is an open-source distribution that is downloadable from GitHub. It is an on-premises version of the open facility.
- Both are available at no-cost (open source) and support an array of open-source and commercial software assessment tools as well as a comprehensive results viewer (CodeDx).

Opens the door to multi-tool assessments

Integrating into the SDLC

Support for Integrated Development Environments (IDEs) and continuous integration/ development (CI/CD) environments enables seamless integration with the SWAMP facility and local SWAMP-in-a-Box instances.

Plug-ins for **Eclipse**, **Jenkins**, and **Subversion/Git**: https://continuousassurance.org/plug-ins/

By the Numbers

- The **SWAMP** facility has been operational since 2014.
  - 27 open source static analysis tools and four commercial static analysis tools are offered in the **SWAMP**.
  - Five platforms, with 19 total versions, are provided in the **SWAMP**.
  - 11 programming languages are currently supported.
  - 10,000+ curated packages including NIST’s Juliet Test Suite for C/C++ and Java and the BugInjector test suite.

Local Continuous Assurance

- **SiB** is an on-premises continuous assurance (CoA) capability.
- **SiB** supports the customization of platforms and static analysis tools, and facilitates the unique needs of commercial/proprietary tools (technical and legal).
- Private/local deployment of **SiB** offers total control for sensitive software.
- **SiB** can be interfaced to local identity management and software repositories.
- https://continuousassurance.org/swamp-in-a-box/

Road Ahead

- Continue to develop the Continuous Assurance framework and to refine the implementation
- Evolve our training and education activities
- Enhance our support infrastructure for SiB installations
- More Functionality
  - Support for containers and Go
  - Support for more commercial tools
  - Support for more open source tools
  - API improvements
  - Reducing the footprint of a SiB deployment
  - SiB user interface customization

Contact Information

- **Website:** https://continuousassurance.org/
- General Contact
    - swamp@continuousassurance.org
- Support Contact
    - support@continuousassurance.org

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov