Bringing Continuous Assurance to Your Code with the SWAMP

Barton P. Miller

bart@cs.wisc.edu

Vilas Distinguished Achievement Professor
Chief Scientist, DHS Software Assurance Market Place
Computer Sciences Department
University of Wisconsin-Madison
Key Term: Software Assurance

The code that you write and the code that you deploy puts you at risk.

Security must be an integral part of your software development process and that of your suppliers.

There are tools to help you evaluate your code and these tools must be in easy reach of your programmers.
The Risks

The risks are clear and well published.

Successful attacks are expensive and affect assets:

- Money
- Reputation
- Data
- Services
- Infrastructure
- Intellectual property
- Digital identities
- Physical damage
Physical Risks are Real

Imagine the effect a **hacked** cargo balancing program or weights database can have on a ship or a plane.
Key Term: Continuous Integration

A discipline of regular software commits to a share repository

Supported by a regular build and test of each new code update (commit).

A view into the process to provide early monitoring of divergences

Often supported by tools such as Jenkins or TravisCE.
Key Term: Continuous Assurance

Bringing software assurance tools and techniques into the CI cycle.

Enormously reducing cost of security flaws if caught early.

Integrating software assurance tools into the programmer’s workflow . . .

. . . from the IDE, from the CI tool, from the repository.

Do it early and do it often.
Software Assurance Tools

The most basic and accessible class of tools do static analysis

A wide variety of both open source and commercial tools for almost every language.

Not the final answer, but essential to raising the base level of assurance on your code.

Using multiple tools improves the kind of problems that you can detect.
The SWAMP

The Software Assurance Market Place is:

- A facility that provides simple, safe and automated running of software assurance tools.
- The MIR-SWAMP: An open service where you can upload your code and have it assessed.
- SWAMP-in-a-Box: A locally-installed version of the SWAMP for organizations that cannot export their code.
SWAMP Driving Principles

Community (impact) focused: **Open access and open source.**

Secure: All assessment runs contained in VMs. **Safe supply-chain evaluation!**

Automated and integrated: **Low bar to entry and low overhead for the programmer.**

A neutral broker: We don’t have a vested interest in selling a tool.
Easy to Run Them Early and Often

The SWAMP offers:

• The automation to run tools easily: applying a tool to a new software package takes little effort.
• Integration: get feedback on each code update or commit.
• The resources to run many tools over each software package on each relevant platform.
• The smarts to combine results in unified reports.
• The ability to track progress and trends over time.
Help for Both the Novice and Expert

The newbie will be able to start using assurance tools with little effort or preparation.

*With management guidance that requires clean commits, the code stays in stable condition.*

The expert does familiar tasks, but with less effort and more precision.

*Running tools is easier, tracking results is easier, and understanding their performance over time is easier.*
Plug-ins to fit your programmer’s workflow:

From the IDE (Eclipse): Simply push the “SWAMP” button and get: submit, assess and view.

From the CI framework (Jenkins): Automated assessment with each CI cycle: submit, assess and view.

From your repository (git, svn): Automated assessment on each commit: submit and assess.
A Multi-Institutional Team

- Morgridge Institute for Research
- University of Illinois Urbana-Champaign, National Center for Supercomputing Applications
- University of Wisconsin-Madison
- Indiana University, Center for Applied Cybersecurity Research

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

Each and every assessment is performed in a “fresh” Virtual Machine (VM) that runs in isolation.

- Input Disk includes software package to be assessed, tool to perform assessment, and tool configuration
- Output Disk includes assessment results and logging information
- Monitoring Disk used to stream information about the assessment

Execution of the assessment is managed by the widely adopted HTCondor distributed job and resource management system.

All information about the assessment is recorded in a database management system.
Currently in the SWAMP

Languages: C/C++, Java source, Java bytecode, Python, Ruby, PHP, JavaScript, HTML, CSS, XML

Platforms: Multiple Linux, Android, .NET (Core)

Tools: https://www.mir-swamp.org/#tools/public

- Open source tools: Android lint, Bandit, Brakeman, checkstyle, Clang Static Analyzer, cppcheck, CSS Lint, Dawn, error-prone, ESLint, Findbugs, Flake8, Flow, GCC, HTML Tidy, JSHint, OWASP Dependency Check, PHP_CodeSniffer, PHPMD, PMD, Pylint, Reek, Retire.js, RevealDroid, RuboCop, ruby-lint, SpotBugs, XML Lint

- Commercial tools: Synopsys Static Analysis (Coverity), GrammaTech’s Code Sonar, Parasoft’s C/C++test and Jtest, Sonatype’s Application Health Check
How Can We Help?

Try out the SWAMP (it’s free).

Ask us questions.

Learn from us: We teach about
- Secure programming techniques
- Software assurance tools
- In-depth vulnerability assessment
Contact Information

Website: https://continuousassurance.org/

SWAMP-in-a-Box User Community Mailing List
swampinabox@lists.discovery.wisc.edu
Sign-up:
https://lists.cosalab.org/mailman/listinfo/swampinabox

SWAMP-in-a-Box Support
sib@continuousassurance.org

General Contact
swamp@continuousassurance.org
Bringing Continuous Assurance to Your Code with the SWAMP

Barton P. Miller
bart@cs.wisc.edu

Vilas Distinguished Achievement Professor
Chief Scientist, DHS Software Assurance Market Place
Computer Sciences Department
University of Wisconsin-Madison
Software Offerings

- Hosted CoA facility (open to the public)
  - [https://www.mir-swamp.org](https://www.mir-swamp.org)

- SWAMP-in-a-Box (open source)
  - Local instance of the SWAMP software, providing full local control and isolation for those with privacy concerns
  - [https://continuousassurance.org/swamp-in-a-box/](https://continuousassurance.org/swamp-in-a-box/)

- SWAMP plug-ins (open source)
  - Eclipse (Java and C/C++), Jenkins, Git and Subversion
  - [https://continuousassurance.org/plug-ins/](https://continuousassurance.org/plug-ins/)

- Additional open source software
  - SCARF, Java CLI, assessment frameworks, result parser
  - [https://continuousassurance.org/open-source-software/](https://continuousassurance.org/open-source-software/)
Many Excuses!

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

- 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
We first introduced the term “Continuous Software Assurance” in our response titled “Continuous Assurance Through a National Marketplace” to a DHS BAA in 2011.

Our proposal and ongoing work has been based on experience in developing, deploying, operating, and maintaining (distributed) software systems.

We have been funded by the DHS Science and Technology Division since 10/2012.