SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in
the software eco-system

Welcome!

The live event will begin at 2PM ET.

A Q&A session with the presenters will follow.

Please have your speakers turned on.

Do you hear the music?

Event powered by T.E.N.

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in the software eco-system

Shaping Your Approach – The Executive's Role in Software Assurance

Jan. 22, 2014

Event powered by T.E.N. TECH EXEC NETWORKS

Agenda

Agenda:

2:00pm EST - Welcome Remarks – Kevin E. Greene

2:10pm EST – SWAMP High Level Overview – Miron Livny

2:25pm EST – Executive Insight & Customer Testimonial – Jerry Davis

2:45pm EST - Q&A

3:00pm EST – Program conclusion

You may earn 1CPE for this event. If you would like us to submit on your behalf, please email your certification number to Deb Jones at djones@ten-inc.com.

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in
the software eco-system

The Software Assurance Marketplace – Channeling the Mission of DHS

Kevin E. Greene, Program Manager

Department of Homeland Security,
Science and Technology Directorate,
Cyber Security Division

Discussion Points

- Channeling the Mission of DHS
- Tackling the Problem
- Advancements and Breakthroughs
- The Challenge Remains

Channeling the Mission of DHS

Cyber Security Division – the *Software Assurance Marketplace*

•Develop ***tools and techniques*** to defend and secure current systems to better protect *critical infrastructures* against attacks from our adversaries

•Facilitate ***technology transition*** through a marketplace approach where a collection of innovative technologies can be harnessed by the community to improve *software assurance capabilities*

•Provide ***leadership*** in the research community by which DHS customers, agencies of the U.S. government, academia, private industry and international partners can exchange technical and research ideas to help advance software security and quality improvements.

DEVELOP → **TECH TRANSFER** → **LEADERSHIP**

Tackling The Problem

The CHALLENGE is growing

- Software is ***UBIQUITOUS***
- Arguably – Software is more ***COMPLEX***
- Tools not ***KEEPING PACE*** with software evolution
- Tools are not adopted ***EARLY*** in the Software Development process
- Software Failures are on the ***RISE***

Advancements and Breakthroughs

Driving Innovation

•The SWAMP shaping and forming new paradigms for software development activities – ***Continuous Assurance***

•Create ***SYNERGISTIC*** capabilities to support an array of software needs

•Leverage the SWAMP to improve ***TOOL COVERAGE***

•Learning environment for improving software coding practices

The Challenge Remains

We've Heard This Before

- Software Assurance adoption early in Software Development process
- Better collaboration and technical exchange for innovation
    - Government, Academia and Private Industry
- Putting the "**A**ssurance and the **T**rusted" back in Software
- Reinforcing good secure coding practices early in the learning process
- Creating better performing tools – that keep pace
    - ***Soundness, Precision, and Scalability***

Thanks and Enjoy the SWAMP

Kevin E. Greene

Email – kevin.greene@hq.dhs.gov

LinkedIn - www.linkedin.com/in/kevgreene

Twitter - @kevtorious

Contact me to learn more about the Software Assurance Marketplace

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in
the software eco-system

Bringing the Software Assurance Marketplace (SWAMP) into the Software Assurance Program of your Organization

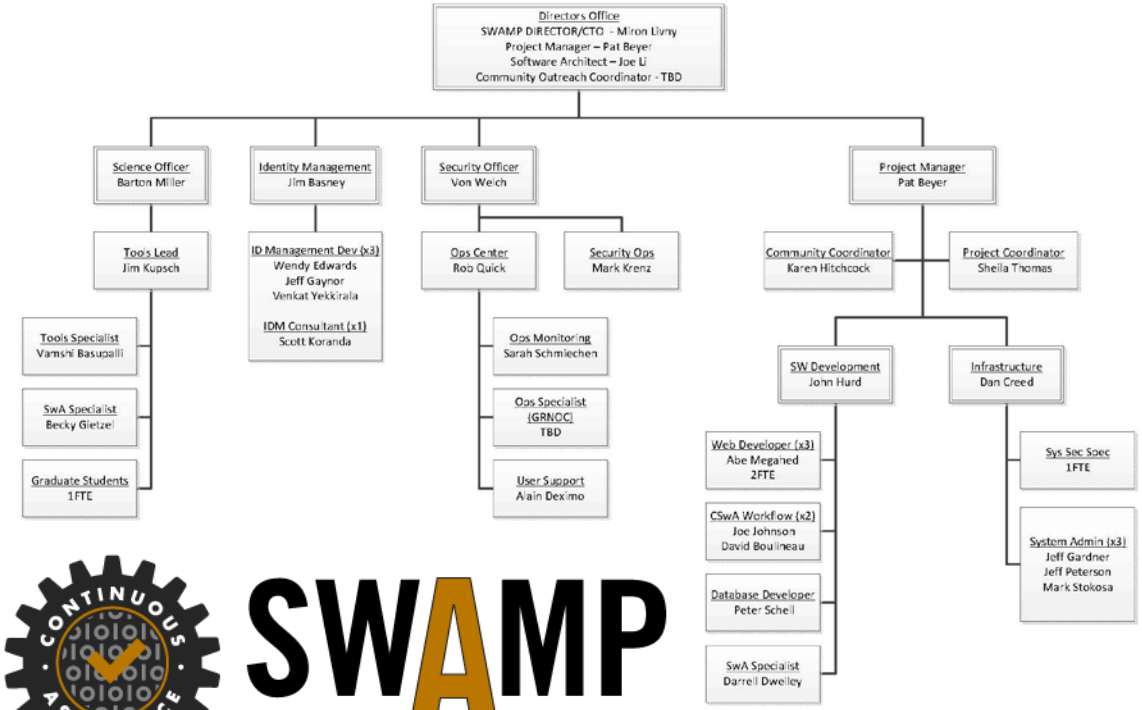
Miron Livny
Director and CTO of SWAMP
Morgridge Institute for Research
January 22, 2014

Discussion Points

- What is the SWAMP
- The driving vision
- The power of sharing
- Protecting your privacy and confidentiality
- How to get started?

A Multi-Institute Team Effort

Building and operating the **SWAMP** is a DHS S&T funded joint effort of four research institutions – Morgridge Institute for Research (lead), Indiana University, University of Illinois Urbana Champaign and University of Wisconsin – Madison

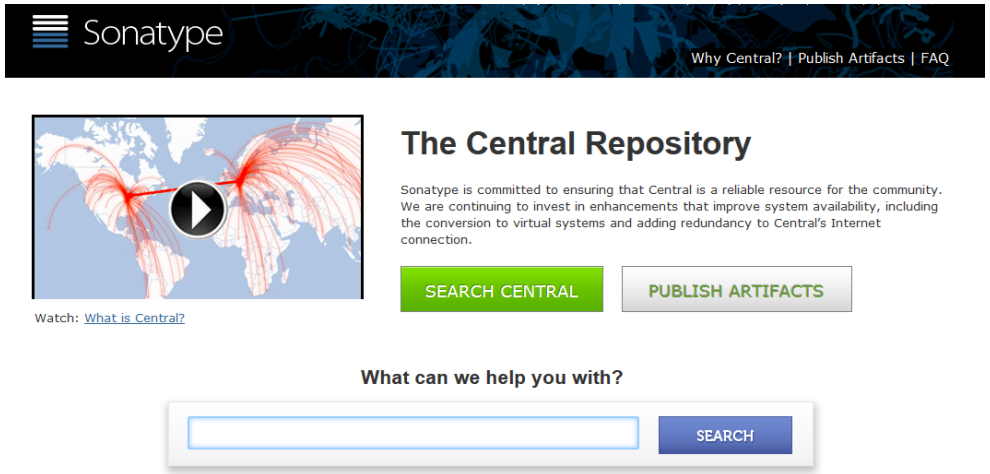


A Powerful and Flexible Facility

- A repository of software assurance (SwA) technologies
  - Assessment tools
  - Viewing tools
  - Integration and coupling tools
  - Risk assessment tools
- A repository of software packages
  - Common open source packages
  - Reference test suites
- A Continuous Assurance engine
  - A wide range of platforms
  - Automation of assessment workflows to support continuous invocation

Continuous Assurance at Work

We have been working with **Sonatype** to automatically (end-to-end) generate a FindBug assessment for each of the more than 60K Java packages (more than 500K versions) in their “central” (publically available) repository. In a trial run we processed 11K packages.



Driven by a Comprehensive Vision

Our target customers are all the members of the Software Assurance (SwA) eco-system – tool developers, software developers, facility managers, researchers and educators.

The community needs a continuous assurance facility that will enable significant improvement in the quality of SwA tools and will lead to a broader adoption of SwA tools and SwA methodologies.

While protecting your privacy and the confidentiality of your data, the SWAMP will :

- **Identify** new (possible) defects in **your** software every time **you** commit a change
- **Identify** new (possible) defects in a software/library/module **you** are using every time a new version is released
- **Profile** the ability of **your** SwA tool to identify (possible) software defects every time **you** commit a change
- **Expose your** tools and software to the SwA community

http://continuousassurance.org/wp-content/uploads/2013/10/SWAMP-VISION-10.28.13.pdf

Based on a Open and Evolving Framework

To meet the diverse and ever-changing needs and expectations of the different groups that compose the software assurance eco-system, a framework that offers the following key elements is required:

- *An environment where new tools can be added easily and efficiently*
- *An environment where new software packages can be added easily*
- *Support for tools that integrate and interpret the output of software assurance tools*
- *An open framework with access to software products and results at all levels*
- *A foundation for understanding the process of software assessment*

continuousassurance.org/wp-content/uploads/2013/11/White-Paper-Evolving-Framework.pdf

Managed Sharing for Stronger Assurance

Maximizing the impact of sharing requires tight protection of privacy.

Each user must maintain full control over the access to artifacts and information he/she owns.

Strong trust between the users and the SWAMP is key to the delivery of our vision.

Continuous Evolution of Capablities

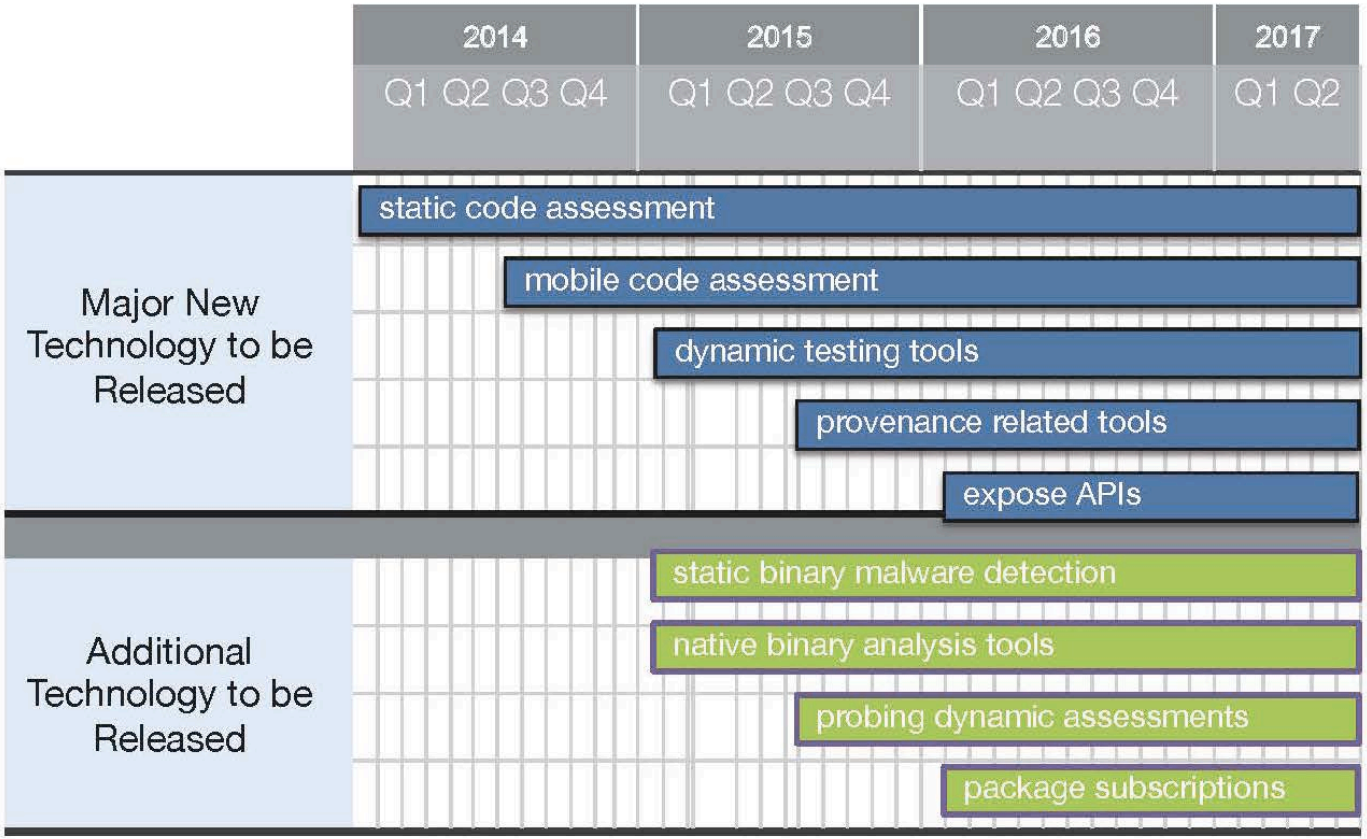


Figure 2: The SWAMP Roadmap post IOC

Get Involved!

- **Sign up** for a “test drive” of the SWAMP in the privacy of your personal project while leveraging publically available tools and software
- **Talk** to us about your software assessment needs, challenges and aspirations
- **Tell** us about your software assurance tools and methodologies
- **Join** us in our community building activities

Contact Information

Pat Beyer
Project Manager
pbeyer@ContinuousAssurance.org
(608) 316-4664

Miron Livny
Director and CTO
miron@ContinuousAssurance.org
(608) 316-4336

INDIANA UNIVERSITY
PERVASIVE TECHNOLOGY INSTITUTE

MORGRIDGE
INSTITUTE FOR RESEARCH

DEPARTMENT OF
Computer Sciences
UNIVERSITY OF WISCONSIN — MADISON

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in the software eco-system

Software Assurance: Because I'm Tired of Fixing Broken Toys

Jerry L. Davis

Chief Information Officer, NASA Ames Research Center

January 22, 2014

Discussion Points

- The Ubiquitous Presence of Software
- The Appetite for Assured Software
- Assured Software is Smartware
- By the Numbers
- Assured Software Benefits
- The Path Forward

The Ubiquitous Presence of Software

It's the driving force behind day-to-day life (literally)

•Right now, you are reading this rendering enabled by millions of lines of code…**software**

•Transportation: It runs your car's Controller Area Network (CAN) bus and manages control surfaces and a whole bunch of other stuff on aircraft…**software**

•Power: utilities, water, natural gas all delivered via...**software**

•Banking and finance: ATM, POS systems...yup **software**

•Manufacturing: Oh, that precision targeting maneuver performed by the gamma knife at the medical center…..uh-huh, **software** controlled

*We put a **lot** of faith in **unassured** and **incompetent** software. Would you let a 7 year old drive you around on the highway? Pilot an aircraft or balance your checkbook?*

The Appetite for Assured Software

The organizational appetite for assured software is driven by the net losses realized from compromised software

•The consumer has been living with nearly 60 years of poorly developed and incompetent software.

•Hundreds of millions of dollars are spent annually on post software compromise and incident recovery, lost opportunities and productivity (ask me).

•Insecure software represents a pervasive kinetic threat to critical infrastructure and our way of life…..make no mistake about it.

The prudent approach is to take a proactive one. That is, software assurance measures must be a top integration priority in the enterprise cyber security risk management schema.

Assured Software is Smartware

Smartware is software which contains superior qualitative and qualitative attributes. It is:

- **Secure** – Free of common vulnerabilities and exposures

- Safe – Any single function does not conflict or impede upon other software functions resulting in severe and deleterious outcomes

- Reliable – Code can perform repeatedly, as expected, over extended periods of time without degradation

- Functional – Code is efficient and is designed to only perform a discrete (purposeful) function and no more

- Extensible – Code is modular and has strong reuse characteristics (secure, safe, reliable and functional)

By the Numbers

Feel my pain. Lack of a good software assurance program is a painful experience

At one time – 127 applications were tested and;

•81 (64%) contained high vulnerabilities that facilitated exposure of sensitive data or system take over;

•45 applications (36%) exposed Personally Identifiable Information (PII)

At another time – 50 applications were tested and;

•41 applications (82%) hosted OWASP top 10 defects

•5 applications (10%) taken offline due to high risk

•19 (38%) contained high vulnerabilities that facilitated exposure of sensitive data or system take over

•12 applications (24%) exposed PII

Assured Software Benefits

Programs such as the SWAMP provide excellent bottom line and programmatic benefits.

- Over time, application development gets faster and software quality increases significantly because developers learn to code securely (Thank you John Keane)
- Program managers can clearly demonstrate cost avoidance through defect identification and remediation during the development and test stages
- Software built under assurance standards processes streamline security approvals. Subsequent applications that adhere to the same standards can readily inherit accreditation and authorization

The Path Forward

The SWAMP is ripe for providing assurances that software is secure. The time to implement software assurance in the development lifecycle is now.

•Patching is passé. Frankly, I'm tired of buying toys that are already broken when I take them out of the box

•Given the austere budget environment, showing value through ROI and cost avoidance goes a very, very long way

•The SWAMP provides mechanisms that can render the security posture of the enterprise "measurable better"

•Community. This must be a community effort. No single tool, process, person or organization can solve this issue. While this challenge appears intractable, it is not. The whole is in fact greater than the sum of its parts and to that end, we must continue to take on the challenge as a community.

Any questions?

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

A transformative force in the software eco-system

Thank you for attending!

An on-demand version of today's event with Q&A session will be offered soon for viewing by you and your colleagues. An announcement will be emailed when the on-demand event premiers.

Event powered by TEN