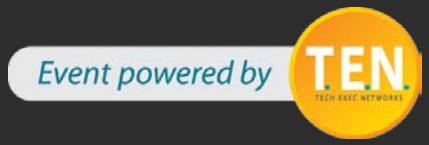
WELCOME!

- The live event will begin at 2PM ET.
- Q&A sessions with the presenters will follow.

- Please have your speakers turned on.
- Do you hear the music?

- Tweet with us live @SWAMPTEAM @TENandISE



SWAMP is funded by Department of Homeland Security, Science and Technology Directorate, Cyber Security Division (CSD)

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

YOUR GUIDE THROUGH THE SWAMP:

AVOIDING PREDATORS IN A MURKY WORLD

May 22, 2014

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

SWAMP is funded by Department of Homeland Security, Science and Technology Directorate, Cyber Security Division (CSD)

AGENDA

- **Agenda:**
- 2:00pm EST – Welcome Remarks – Marci McCarthy
- 2:05pm EST – An Ounce of Prevention is Worth a Pound of Blood – Arthur Hicken
- 2:20pm EST – How YOU can use SWAMP / Demonstration – Miron Livny & Irene Landrum
- 2:40pm 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

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

AN OUNCE OF PREVENTION IS WORTH A POUND OF BLOOD

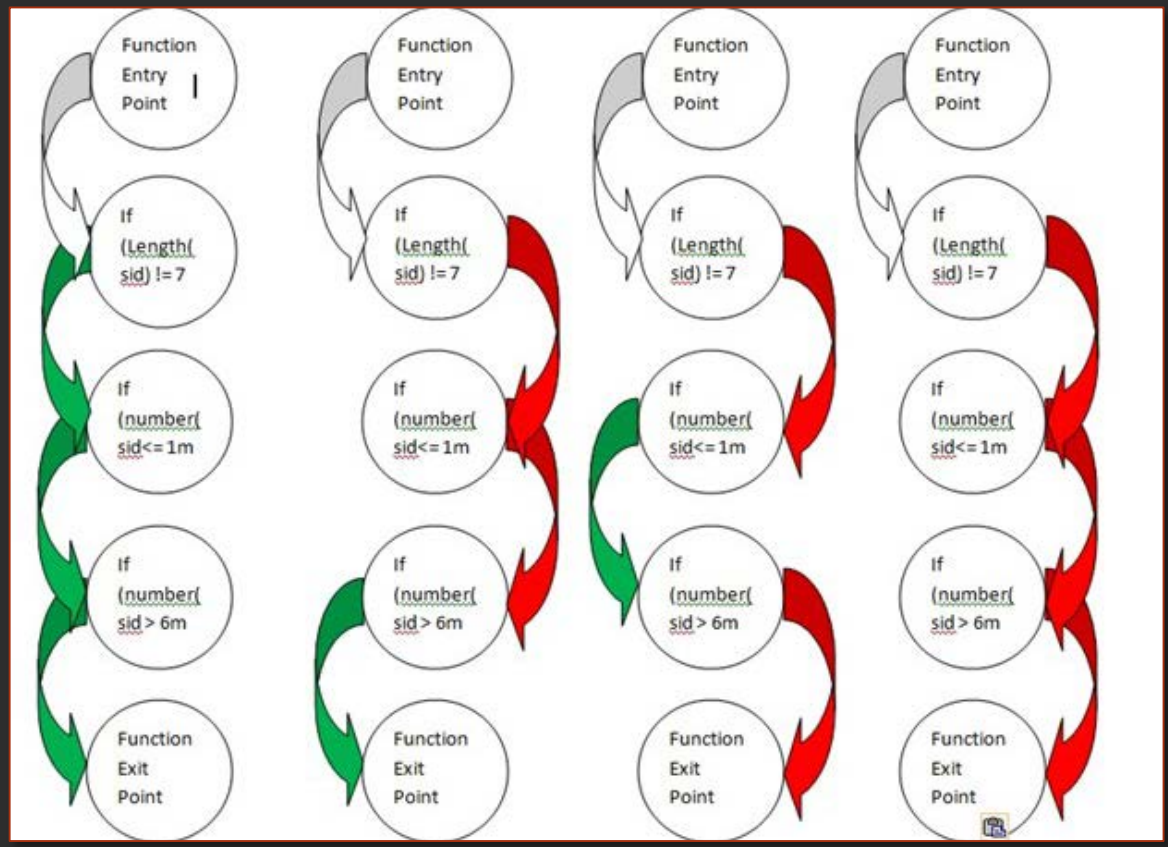
Arthur Hicken (aka the Code Curmudgeon)

Evangelist

Parasoft Corporation

FLOW ANALYSIS IS HARD

- Path limitations
- Flavor-of-the-month
- Incomplete coverage
- False negatives
- Tracking pointers



SWAMP
SOFTWARE ASSURANCE MARKETPLACE

AN OUNCE OF PREVENTION

Prevention

Your software is secure – Have a great day!

Early Detection

You have security problems. Fixing them will delay your release. You don't have time to address the root cause, so you'll have to triage which things you can fix and just patch some of them.

- **Which would you prefer?**

PREVENTATIVE STANDARDS EXAMPLES

Object-Oriented

- Avoid "public"/"protected"/package-private instance fields
- Do not override an instance "private" method
- Do not hide inherited fields

Best Practices

- Avoid returning "handles" to internal data from const member functions.
- Declare at least one constructor to prevent the compiler from doing so.
- Declare reference parameters as const references whenever possible

Unused Code

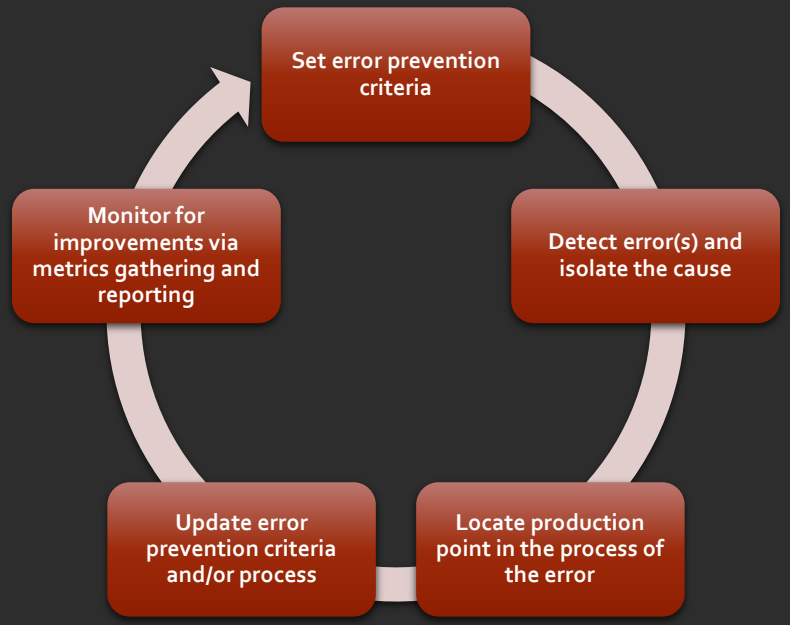
- Avoid unused local variables
- Avoid unused "private" fields

Class Metrics

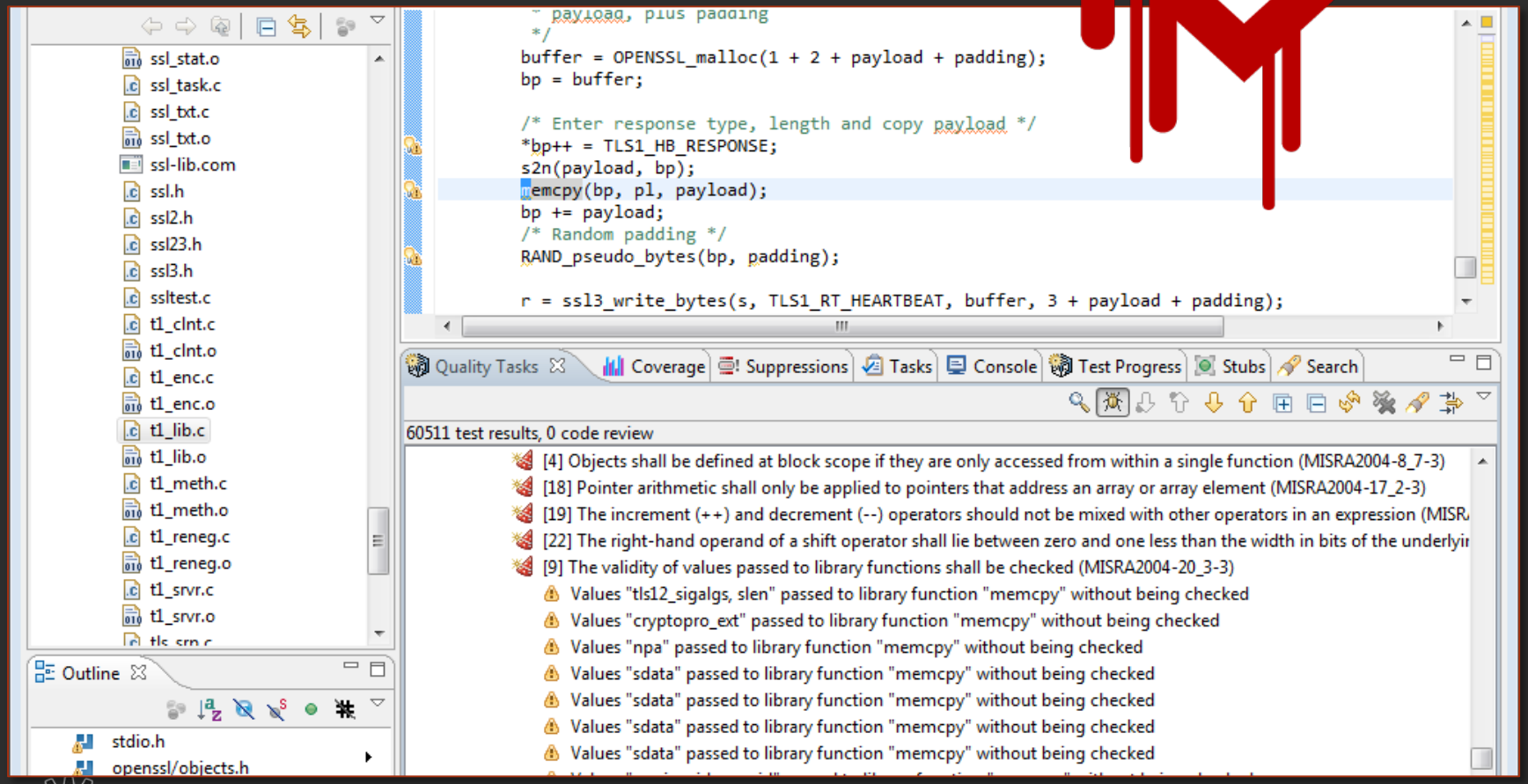
- Follow the limit for Cyclomatic Complexity (default<30)
- Follow the limit for number of "<type>" fields (private,etc.)
- Follow the limit on class hierarchy depth

CONTEXT IS EVERYTHING

- The important rules
- The right code
- Static analysis config
  - Code review
  - Regression
  - QA
  - Field bugs



HEARTBLEED FOUND



SWAMP
SOFTWARE ASSURANCE MARKETPLACE

HEARTBLEED AVOIDED

MISRA C 2004 20.3

- "The validity of values passed to library functions shall be checked"

CWE-20

- "Improper input validation"

CWE-114

- "Process control"

CWE-125

- "Out-of-bounds read"

CWE-130

- "Improper handling of length parameter inconsistency"

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

CLEAN YOUR CODE – IN THE SWAMP

- Easy to setup
- The price is right
- Run early, run often
- Each tool is different
- More is better

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

An Open Continuous Assurance Facility

Miron Livny

Director and CTO of the SWAMP

Morgridge Institute for Research

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 the confidentiality of your data and your privacy, the SWAMP can help you:

- **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

SWAMP Vision Document

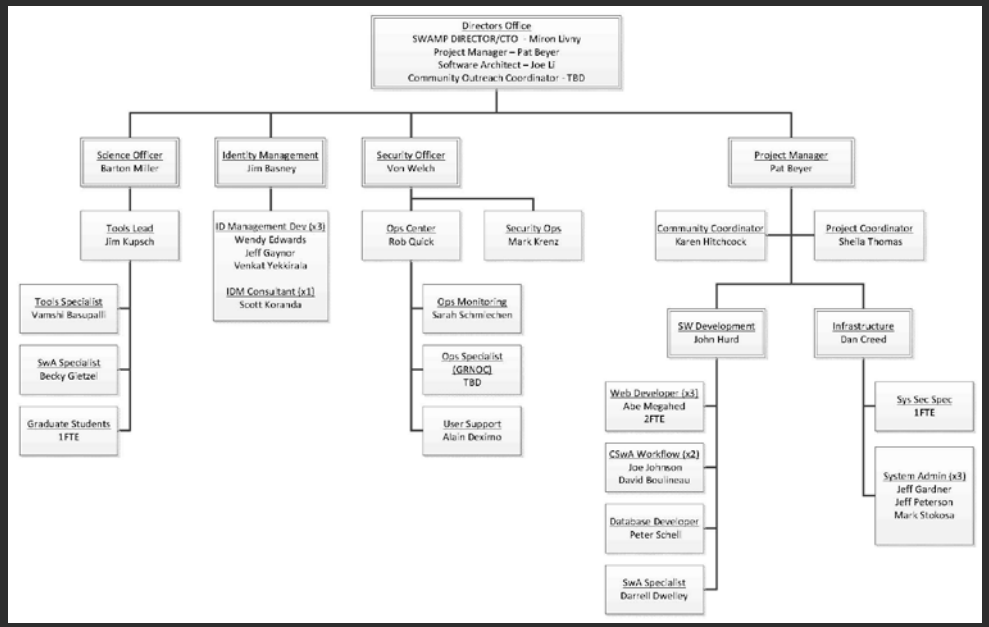
Open to a Diverse Community

On 02/02/14, the Software Assurance Marketplace went "live" through a public web interface.

- Five public static assessment tools (two public and one private tool added)
- State-of-the-art viewer of assessment results
- "Plumbing" that simplifies access to SwA tools
- A hundred software packages (more than 350 today, 286 of which are from the NIST Juliet Test Suite)
- Secure and dependable facility
- Access to powerful computing capabilities (700 cores, 5 TB of RAM, 104 TB of HDD space, off site backup, state of the art networking)
- Provides a framework for building and managing SwA projects
- Supports managed access (sharing) to tools, packages, and results

A Team Effort

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, MIR

Jim Basney, UIUC

Bart Miller, UW

Von Welch, IU

Open & 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 an environment with the following key elements is required:

- *New software packages can be added easily*
- *New tools can be added easily and efficiently*
- *Support for tools that integrate and interpret the output of software assurance tools*
- *Access to software products and assessment results at all levels*
- *Understanding the process of software assessment*

Evolving Framework White Paper

A Balancing Act

The SWAMP needs to strike a balance between competing forces:

- *Easy access vs. legitimate use*
- *A few big, long-lived projects vs. many small, short-lived projects*
- *Public domain vs. commercial tools*
- *Web access vs. API access*
- *Mobile applications vs. server applications*
- *Neutrality vs. offering guidance and ranking*

DO IT EARLY
AND
DO IT OFTEN!

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

ANY QUESTIONS?

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

THANK YOU FOR ATTENDING!

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