A Collaborative Marketplace for Continuous Software Assurance

NYC OWASP Chapter – Feb. 5, 2013
A Growing Need...

Pacemaker hacker says worm could possibly 'commit mass murder'

By Darlene Storm
October 17, 2012 5:43 PM EDT  10 Comments

It seems like something is very wrong with the picture when you read the news and it sounds more like a science fiction novel than a newflash. For example, Barnaby Jack showed how an attacker with a laptop, located up to 50 feet from a victim, could remotely hack a pacemaker and deliver an 830-volt shock.

Ruxcon BreakPoint security conference in Melbourne must have been the place to be, as RiskyBiz said it kicked off with a bang featuring "mass murder, Windows exploits, hacking Apple and owning spy agencies." Jack was just one presenter and he showed a video that he doesn't want released to the public since the manufacturer would be named. Maybe it's time to name and blame, cause this is some seriously scary stuff!
Software Assurance Marketplace

- Six proposals submitted
- Awarded to Morgridge Institute for Research with Indiana University, University of Illinois Urbana-Champaign, and UW–Madison as subcontractors
- Offers industry, academia and government agencies **no-cost access** to a secure research facility with analytical and reporting capabilities
- Will help the software assurance community improve the security of software used in the nation’s critical infrastructure
Use Cases

Software Developers
Upload software packages for analysis by a suite of software assurance tools and view results via dashboard.

Software Assurance Tool Developers
Upload SWA tools and evaluate against large corpus of SW packages and test suites with known weaknesses.

Cybersecurity Researchers
Review data on tool coverage and common weaknesses to improve standards, education and certification programs.
SOFTWARE ASSURANCE MARKETPLACE
A national cybersecurity resource offering continuous software assurance.

INPUTS
- Unvetted Software
- Software Assurance Research
- Software Assurance Tools
- Software Packages
- Identity Management
- User Training and Support

OUTPUTS
- State-of-the-Art Software Assurance
- Analysis and Baseline Repository
- Best Practices, False Positives
- Assessment Reference Data Sets
- Enhanced Cybersecurity
- Vetted Software

PEOPLE
- Software Assurance Researchers
- Software Assurance Tool Developers
- Software Developers
- U.S. Department of Homeland Security
- National Institute of Standards and Technology
- Partner Resources
- U.S. Air Force
- National Security Agency
- High Performance Computing Clusters

RESOURCES

User Communities
- SWA Tool Developers
- Software Developers
- SWA Researchers
- Educators & Students
- Infrastructure Operators

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE
Major Deliverables

SWAMP Operational (Version 1.0 of CoSALab and Metronome)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Year</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build</td>
<td>1</td>
<td>Oct. 1, 2012</td>
</tr>
<tr>
<td>Beta</td>
<td>2</td>
<td>Feb. 2, 2014</td>
</tr>
<tr>
<td>Enhance</td>
<td>3</td>
<td>Sep. 30, 2015</td>
</tr>
<tr>
<td>Operate</td>
<td>4-5</td>
<td>Sep. 30, 2017</td>
</tr>
</tbody>
</table>

- V1 Stable Release of Metronome
  - First SWAMP User’s Meeting
- V2 of CoSALab and Metronome
  - Second SWAMP User’s Meeting
- V3 of CoSALab and Metronome
  - Third SWAMP User’s Meeting
- Fourth SWAMP User’s Meeting
- Final Metronome Release
Initial Tool Selection for the SWAMP

At initial operating capability (IOC) a goal of 5 open source tools operating on 100 packages.

Guiding the selection of tools are weakness from published studies, communications with practitioners, and our experiences in performing in-depth software vulnerability assessments.

Weakness class examples include:

- Command injections
- SQL injections
- Use of inherently dangerous OS interfaces
- Buffer overruns
- Resource leaks (allocated but not freed resources)
- Pointer usage errors (e.g., NULL pointer usage, double freeing, use after free)

- Format string attacks
- Integer overflow/truncation errors
- Cross-site scripting/Cross-site request forgery
- URL redirection (Open Redirect)
# Initial Tool Selection for the SWAMP

<table>
<thead>
<tr>
<th>Tool Description</th>
<th>Languages</th>
<th>Targeted Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Findbugs</strong>: widely used for Java source code analysis; incorporated into many commercial tools.</td>
<td>Java</td>
<td>Injection attacks, number handling, web deceptions, and resource leaks.</td>
</tr>
<tr>
<td><strong>cppcheck</strong>: community-wide open source tool hosted at sourceforce.net.</td>
<td>C, C++</td>
<td>Targets common coding errors, addressing buffer handling and resource leaks.</td>
</tr>
<tr>
<td><strong>Clang and Clang Static Analyzer</strong>: contributions from a wide community, including active participation from Apple and Google.</td>
<td>C, C++, Objective C (for MacOS)</td>
<td>Targets common coding errors, addressing injections, buffer handling, resource leaks, and number handling.</td>
</tr>
<tr>
<td><strong>Oink</strong>: based on CQual++ for its basic analysis. Reputed to be quite solid and has whole program analysis abilities.</td>
<td>C, C++</td>
<td>Targets common coding errors, addressing injections.</td>
</tr>
<tr>
<td><strong>PMD</strong>: a community wide tool under active development, hosted on sourceforge.net.</td>
<td>Java, limited support for XML, Javascript, JSP</td>
<td>Targets number problems, resource leaks, and programming errors. A focus on correctness, now adding security checks.</td>
</tr>
</tbody>
</table>
Platform Selection for the SWAMP TBD

Guidelines:
• Minimally sufficient set. Initial DHS target is 8.
• Most relevant for SWA and OSS communities
• Updated current version and previous version

<table>
<thead>
<tr>
<th>Platform</th>
<th>Versions</th>
</tr>
</thead>
</table>
| Linux    | Debian and/or derivatives  
           RedHat and/or derivatives  
           Others? |
| Mac?     | OSX 10.8 (Lion), OSX 10.7 (Mtn Lion) ... |
| Windows  | Windows7, Windows8 ... |
You are the key!

- **We need your input** – how do you envision using such a resource? What tools, packages, policies, topics, platforms would help you?
- **We need your involvement** – help with tools, packages, standards, technical literature, seminars, training.
- **We need your feedback** – the good, the bad, and the ugly.
Backup Slides
U.S. Department of Homeland Security Science and Technology Directorate

- Software Assurance Marketplace project part of $70+ million multi-year Cyber Security Division effort to improve security of nation’s critical information infrastructure

- BAA 11-02 involves 34 awards to 29 academic, commercial and research organizations in 14 technical areas focused on detecting, preventing and responding to cyber attacks
Relationship to other DHS projects

Significant collaboration

TTA-1 Software Assurance Tools

TTA-14 Software Assurance Marketplace

Other Technical Topic Areas

Some collaboration
Software Assurance Marketplace Organization

~ 24 Team Members

Morgridge Institute for Research

Software Assurance Marketplace Director
Miron Livny

Chief Operations Officer
Brooklin Gore

Chief Security Officer
Von Welch

Chief Scientist
Barton Miller

Identity Mgmt. Lead
Jim Basney

Software Development

Production

User Support

Operations Center

Security Operations
Indiana Univ. Pervasive Technology Institute

Software Assurance Tools and Standards
U. of Wisconsin Middleware Security and Testing Group

External Resources
U. Of Illinois NCSA Cybersecurity Directorate