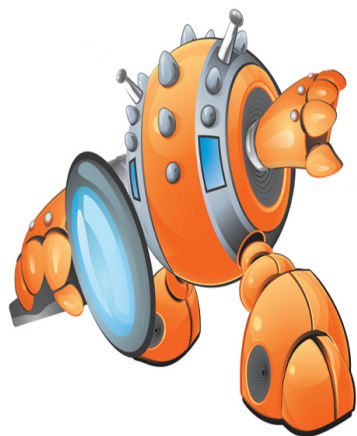


NIST workshop on Software Measures and Metrics to Reduce Security Vulnerabilities



SwMM-RSV

Tuesday, 12 July 2016
NIST
Gaithersburg, MD



<https://samate.nist.gov/SwMM-RSV2016.html>



Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the products are necessarily the best available for the purpose.

The Object of Interest is ...

- **Software (as a product)**
- **Measures and Metrics on Software ...**
- **that help dramatically reduce security vulnerabilities.**

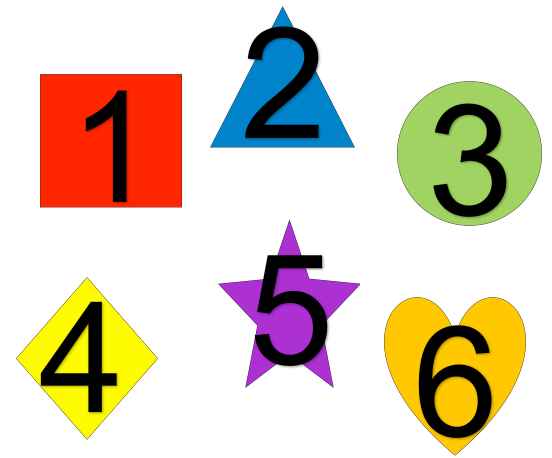
Some Statistics

- **20 Position statements submitted**
 - 10 accepted
- **Over 90 people attended**
 - primarily **Federal Government** or those supplying to the government.
 - many representing **tool makers or software developers.**
 - **hand full of academics**

Presentations from

- **White House Office of Science and Technology Policy**
- **BlackBerry**
- **University of Wisconsin-Madison**
- **Consortium for IT Software Quality (CISQ)**
- **NIST**
- **Vector Software**
- **US Naval Research Laboratory**
- **Software Engineering Institute**

Six Break-Out Sessions



- **How can the Federal Government best use taxpayer money to identify, improve, package, deliver, or boost the use of software measures and metrics to significantly reduce vulnerabilities?**

Some Ideas

- **Code should be amenable to automatic analysis.**
- **Standardize tool outputs.**
- **Boilerplate contract and procurement language:
“Code should be ...”**
- **Share findings: about tools, about libraries, etc.**
- **Business cases: secure code saves \$**
- **Liability**
- **Education: more programmers need to understand security.**

Next Steps

- **We will write a report for the workshop.**
 - Plan to have it done by September.
- **Incorporate ideas in the Federal Cybersecurity Research and Development Strategic Plan.**