The SAMATE Project and How it Helps Enhance Software Trustworthiness

Vadim Okun
National Institute of Standards and Technology
http://samate.nist.gov/
vadim.okun@nist.gov

SAMATE and SAM

- NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project
- Software Assurance Meta-model (SAM)
- SAMATE efforts can serve as a resource for SAM

Goals of the SAMATE Project

- Sponsored by DHS to
  - develop metrics for the effectiveness of SwA tools
  - assess current methods and tools in order to identify deficiencies which can allow software product failures and vulnerabilities

The SAMATE Project

- Surveys
  - Tools
  - Researchers and companies
- Workshops and conference sessions
  - Taxonomy of SwA functions and techniques
  - Order of importance (cost/benefit, criticalities, …)
  - Gaps and research agendas
- Enable tool evaluations
  - Write detailed specification
  - Develop test plans and reference material
  - Collect tool evaluations, case studies, and comparisons

SwA Tool Taxonomy

- A common reference/classification of tool functions
- It is a “first step” in defining a functional specification for a type of tools

Contribution to SAM: Help frame the argument that appropriate tools were used

SAMATE Reference Dataset

- Publicly available at http://samate.nist.gov/SRD
- A reference dataset for comparing SwA tools of the same class permits an “apples to apples”comparison between tools

Contribution to SAM: Help test and compare tools

Common Software Flaw Taxonomy

- There are multiple taxonomies (CVE Plover, CLASP, Fortify Software, Klocwork …)
- Integration effort is under way

Contribution to SAM: What flaws are and are not in the application?

Tool Metrics

- Define metrics for evaluation of SwA tools
  - Completeness (what percentage of total flaws a tool detects)
  - Number of false positives and false negatives
  - …

Contribution to SAM: How useful are tools?

Contact Information

- Vadim Okun
  vadim.okun@nist.gov
- Paul E. Black
  SAMATE Project Leader
  paul.black@nist.gov
- SAMATE Web Site
  http://samate.nist.gov/