VIBRANCE Java Security Tool

Kestrel Institute

Technical Summary

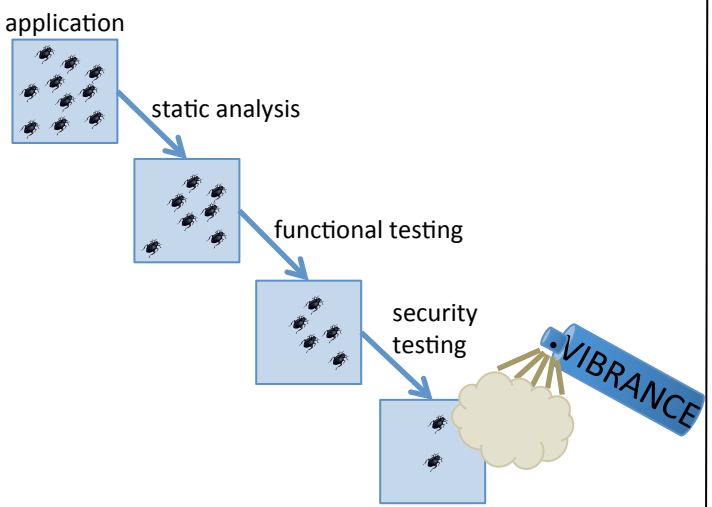
Kestrel Institute's VIBRANCE Java security tool is a software tool that automatically hardens compiled Java code so that attacks are automatically detected, blocked, and remediated at runtime.

VIBRANCE protects Java applications from the following **important weaknesses**, which lead to **data theft/loss** and **denial of service**:

- injection
  - SQL – #1 of CWE/SANS Top 25
  - OS command – #2 of CWE/SANS Top 25
  - LDAP, XPath, XQuery
- tainted data
  - unrestricted file upload – #9 of CWE/SANS Top 25
  - file path traversal – #13 of CWE/SANS Top 25
  - loop bound – e.g. Apache Tomcat CVE 2014-0050
  - server crash
- number handling (e.g. integer overflow)
- error handling (e.g. uncaught exception)
- resource handling
- concurrency handling
  - race conditions
  - deadlock breaking

The VIBRANCE Java security tool can block attacks missed by other technologies such as Web Application Firewalls, static analysis tools and dynamic testing.

VIBRANCE addresses the security bugs that "slip through" the development process.



Operational Capabilities

The VIBRANCE Java security tool is new technology that is complementary to existing tools and methods.

- Blocks attacks on vulnerabilities that have slipped through static analysis and dynamic testing
- Automatic remediation of many attacks allows an application to continue normal operation
- Can block zero-day attacks
- Automatic remediation of zero-day attacks enables normal operation until the newly discovered vulnerability is fixed in a normal upgrade cycle

Development Objectives

In order to commercialize the VIBRANCE tool, the following development objectives are planned.

- Develop a feature-complete version of VIBRANCE for release that can be used in a testing environment
- Test VIBRANCE to ensure its usability and performance in preparation for commercial release
- ANDROID applications could be protected by an extended VIBRANCE

Commercial Applications

The VIBRANCE Java security tool is suited for a variety of commercial settings including:

- Applications with access to sensitive data
- Applications that can take input from unvalidated users
- Applications susceptible to Denial of Service attacks
- Applications supplied by a vendor for which you do not have source code

Relevant Government Programs

The VIBRANCE Java security tool is relevant to a variety of federal software assurance initiatives and programs including:

- Department of Homeland Security (DHS) "Build Security In" strategic Initiative
- National Security Agency (NSA) Center for Assured Software
- Department of Defense (DoD) Program Protection Plan (PPP)
- NASA Office of Safety and Mission Assurance (OSMA) Software Assurance Research Program (SARP)
- National Institute for Standards and Technology (NIST) Software Assurance Metrics and Tool Evaluation (SAMATE)

See http://vibrance.kestrel.edu for additional information, including a demonstration video.

Point of Contact: Alessandro Coglio | 650-493-6871 | vibrance@kestrel.edu