Advances in Software Security Assessment and Verification Research

David P. Gilliam, John D. Powell
Jet Propulsion Laboratory,
California Institute of Technology
John.Powell@jpl.nasa.gov

Abstract

There are a multitude of applications that are network aware and which often provide services including login credentials. A key security issue is the inadvertent compromise of the resident system and/or its data due to common problems such as race conditions or buffer overflows, and other potential security problems. An otherwise secure system can be compromised easily if the system, or application software on it, or on a linked system, has vulnerabilities. Currently, there is a lack of security assessment tools for use in the software development and maintenance life cycle to mitigate these vulnerabilities.

NASA has funded a research proposal to develop a suite of software security assessment tools and utilities for use throughout the software life cycle. The suite contains:

- A Vulnerability Matrix (VMatrix)
- Security Assessment Tools (SATs)
- Property Based Tester (PBT)
- Model Based Verification (MBV) with the use of a Flexible Modeling Framework (FMF)
- Software Security Checklist (SSC)

The following are currently available to the internet community: 1) VMatrix, 2) SATs, 3) PBT, and 4) A Report on MBV methodology for security.

The vulnerability database is an outgrowth of a vulnerability matrix developed for NASA. Its purpose is to provide information about various vulnerabilities including the exploit used to gain access, how to protect against the exploit and the Common Vulnerabilities and Exposures (CVE) listing. The information is being transferred to the UC Davis Database Of Vulnerabilities, Exploits, and Signatures (DOVES) where it will be maintained and updated as new exploits are discovered. This information is used to extract properties and requirements that express potential network vulnerabilities for utilization by the PBT tool and FMF.

The SATs are a up-to-date collection, description and an assessment of publicly available software security code checking tools available on the Internet that can be used to test for potential weaknesses of software code.

The PBT tool performs formal verification of properties, including those obtained from the vulnerability matrix, at the code level through slicing techniques and search for specific vulnerability properties.

Like the PBT tool, the FMF aids in formal verification of properties based on an abstract model of the system prior to actual code development.

The SSC has two foci: 1) a checklist to verify that software released by NASA does not have unauthenticated access into NASA networks, or provide other information

about NASA's, processes, systems, networks, or other sensitive data (such as IP Address space, HR data, or processes that can be exploited); 2) a checklist for software developers to write secure code for applications. Identify tools to integrate security into the various stages of the software life cycle.

This collection of tools and utilities can be used individually or in concert to ensure the security of network aware software application and systems.

Acknowledgement

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The work was sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program lead by the NASA Software IV&V Facility. This activity is managed locally at JPL through the Assurance and Technology Program Office.

For further information about this ongoing research, refer to http://rssr.jpl.nasa.gov