DHS Science and Technology Directorate

Software Quality Assurance

Software controlling critical infrastructure is more essential, but more vulnerable

The essential software that controls our nation's critical infrastructure has grown more capable and more complex than ever. However, complex software is also more susceptible to bugs and weaknesses that prospective adversaries can exploit. Quantifying this risk in a 2012 research report, the Judge School of Business at the University of Cambridge estimated software errors cost the global economy almost $300 billion annually.

Software Quality Assurance aims to reduce software vulnerabilities

The Department of Homeland Security, Science and Technology (S&T) Directorate's Software Quality Assurance project (SwQA) is developing innovative approaches to reduce the risk and cost of software failures. SwQA aims to make improvements in the following ways:

- Advancing research and development in new tools and techniques to improve software developers' capabilities to analyze software for potential vulnerabilities.
- Applying new and improved capabilities in testing and evaluation activities to correct vulnerabilities and reduce the probability and frequency of exploitation by prospective adversaries.

Advancing the state of software quality assurance

S&T will leverage flexible contracting tools (such as the Small Business Innovation Research program [SBIR], broad agency announcements, long range broad agency announcements, and inter-agency agreements with other federally funded research programs) to drive innovation and improve the security and reliability in software systems and software development activities. For example, S&T has achieved these early successes in software quality assurance technologies through its Software Assurance program:

- Successful completion of Phase I SBIR, Hybrid Analysis Mapping (HAM). HAM is designed to bring together disparate static and dynamic application security testing tools to improve the identification of vulnerabilities and exposures in software.
- A software assurance and analytics tool that visualizes and correlates vulnerabilities detected by disparate static analysis tools.
- Improvement in a static analysis tool that finds platform specific bugs in software, improves build-and-test technology to harness cloud resources, and performs hybrid analysis for source and binary representation.

Reducing software vulnerabilities decreases costs

Reducing software vulnerabilities can save the U.S. economy more than $22.2 billion annually. Tools and technologies developed through SwQA will provide software assurance professionals with the capabilities to improve security assessments and software development activities. New and improved software quality assurance tools may be adopted by software developers earlier in the coding process. Numerous studies show that the later a bug is discovered in the software development life-cycle, the higher the costs to fix it. Early detection of bugs will be essential to reducing vulnerabilities and thereby decreasing the costs of a software development project.

New Research and Tools in Development

S&T recently awarded research and development contracts to private sector and academic institutions that aim to improve the techniques in software quality assurance tools to help fill gaps that exist in state-of-the-art technologies. The focus of SwQA is to create better performing software analysis tools that can keep pace with evolving software. These contracts address specific areas: dynamic tracing to improve static analysis capabilities, hybrid static verification and runtime monitoring systems to vet unknown software. The SwQA project also addresses static analysis capabilities to measure the effectiveness of unsound analyzers in finding software weaknesses in C source code and risk management and compliance validation.

SwQA Performers

Secure Decisions, Northport, N.Y.: *Code Pulse: Dynamic Augmented Static Analysis* and *Code Dx: Software Assurance Visual Analysis Tool*

HRL Laboratories, LLC, Malibu, Calif.: *Tunable Logic-Based Information Flow*

Kestrel Technology, LLC, Palo Alto, Calif.: *A Gold Standard for Benchmarking C Source Code Static Analysis Tools*

Grammatech, Inc., Ithaca, N.Y.: *CodeSonar improvements through program analysis*

University of Nebraska Omaha: *Security Requirements and Software Weakness.*

Homeland Security
Science and Technology

To learn more about Software Quality Assurance project, contact sandt-cyber-liaison@hq.dhs.gov.

2014-11-03