Homeland Security SWAMP Program Takes Aim at Software Bugs

Hilton Collins | August 13, 2014

Codenomicon's discovery of OpenSSL's "Heartbleed" flaw this past spring highlighted the increasing importance of source code assurance and quality control as software grows in prominence in daily life. The Heartbleed memory leak opened the door for infiltrators to obtain passwords and security keys to decode encrypted data — a vulnerability that allegedly still threatens enterprise systems months after its discovery, according to a recent report.

But Kevin Greene (pictured at left), a project manager in the cybersecurity division of the U. S. Department of Homeland Security's Science and Technology Directorate, claims that he has the answer to these kinds of problems. He manages a program called the Software Assurance Marketplace, aka SWAMP, an online platform that allows software developers to submit their code for vulnerability analysis free of charge.

According to Greene, SWAMP could have detected the Heartbleed flaw early in its development phase where other vulnerability tools apparently failed.

"None of the tools were able to detect the weakness that led to Heartbleed, so to me, using SWAMP, a software researcher can identify the type of anomalies that are in these tools and start working on the techniques that exist in the state of the art tools," Greene said.

He told *Government Technology* that one of SWAMP's advantages over other vulnerability-finding tools is that it combines multiple assessment methods in one place, hence the "marketplace" portion of the acronym. It's a place where users can pick, choose or use all options within the same tool.

"We're leveraging the different sweet spots of each tool in a way that kind of creates one big sweet spot that can give value to the software developer in terms of, 'How do

we improve the accuracy of results?"' Greene said. "One tool alone doesn't give you the full coverage you need to do an assessment. If we can leverage multiple tools, we improve our coverage in terms of how we can detect weaknesses in software."

SWAMP currently offers five static analysis tools: FindBugs, for discovering Java coding errors, injection and web attacks; PMD, which probes Java, XML and JSP for web programming errors; Cppcheck, for C and C++ coding errors; Clang and Clang Static Analyzer, additional C and C++ coding error scanners; and Oink, an analysis tool for C and C++ that uses CQual++ for basic analysis.

They're called static analysis tools because they test and evaluate applications by examining code without executing the application, whereas dynamic analysis tools test and evaluate applications during runtime. SWAMP launched in February 2014 with the static toolset above, but future iterations also will incorporate dynamic analysis. Additional supported programming languages will include Python, PHP and Javascript.

The DHS' main goal with SWAMP is to facilitate the creation of strong software with fewer vulnerabilities, preventing more Heartbleed-like scenarios from happening in the future. Users log into SWAMP to create a free account, upload their code, and run assessments. The results show developers what's wrong in their software, so they know how to write their code more efficiently the next time. The system currently supports Linux platforms but will be modified to support the Microsoft Windows, Mac OS X and Google Android platforms eventually.

"If we can have an environment where software developers can use a wide range of software analysis techniques and capabilities, it raises the quality of software," Greene said.

Greene joined the SWAMP project in 2012, the same year the DHS' Science and Technology group awarded $25 million for its development. Four research institutions created and maintain it and its housed software development, infrastructure management and facility operations. The University of Indiana handles security and user support, the University of Illinois leads identity management, and the University of Wisconsin handles the software assurance technologies and software package integration.

Greene claimed that SWAMP currently runs about 650 assessments a week, an impressive number for a platform that's only been live for about six months.

"It's to the point now where we see a lot of folks starting to sign up, use it, [and] recognize the importance of software security," he said. "Our goal is to test early and often."

http://www.govtech.com/security/Homeland-Security-SWAMP-Program-Takes-Aim-at-Software-Bugs.html