NIST improves tool for hardening software against cyber attack

November 23 2011

(PhysOrg.com) -- Computer scientists at the National Institute of Standards and Technology (NIST) have dramatically enlarged a database designed to improve applications that help programmers find weaknesses in software. This database, the SAMATE Reference Dataset (SRD), version 4.0, is a freely available online tool aimed at helping programmers fortify their creations against hackers.

A complex piece of software like an operating system or a Web browser usually requires the combined effort of multiple programmers to write up to millions of lines of computer code. Before their software hits the market, it first must be put through its paces to make sure it not only works as desired under a multitude of different circumstances, but also that it is not vulnerable to cyber attack. The act of checking out software in this fashion has become so complicated in and of itself that developers created another type of labor-saving program called a "static analyzer" to help with the checking. Static analyzers doggedly run through the code looking for obvious problems, but they can only find the weaknesses they have been programmed to find—which is where the SRD comes in.

"The SRD is for companies that build static analyzers, whose use is expanding within the software industry," says SRD project leader Michael Koo. "It will help their products catch the most common errors in the software they are supposed to check. It brings rigor into software assurance, so that the public can be more confident that there are fewer dangerous weaknesses in the software they use."

The weaknesses might be compared to grammatical errors in a page of writing—errors that inadvertently instruct a computer to do things that leave itself open to cyber attack. SAMATE, which stands for Software Assurance Metrics And Tool Evaluation, is a NIST project with the goal of minimizing these errors in commercial software. SRD version 4.0 contains 175 broad categories of weakness types that encompass more than 60,000 specific cases of code errors—an addition of 100 more categories and 30 times the number of cases in SRD version 3.0. Each specific case is about a page of computer code showing a problematic way of composing functions, loops, or logic operations written in languages such as Java, C and C++. The dataset is fully searchable by language, type of weakness and code construct, and search results are available in a downloadable Zip file.

The NIST team says the next step for improving the dataset is to include errors in more languages, as well as in far longer stretches of computer code. The 4.0 release includes mostly short examples, but Koo says there are plans to explore vulnerabilities in large open-source software packages of up to a million lines of code and expand the SRD to include these in the near future. "We welcome contributions from other computer security researchers," Koo says.

More information: The SAMATE Reference Dataset (SRD), version 4.0 is available online at samate.nist.gov/SRD

Provided by National Institute of Standards and Technology

Citation: NIST improves tool for hardening software against cyber attack (2011, November 23) retrieved 18 April 2024 from https://phys.org/news/2011-11-nist-tool-hardening-software-cyber.html