Toward Precise and Accurate Descriptions of Weaknesses

Submitted by Paul E. Black on Fri, 04/25/2014 - 10:20am. Contributor:
Paul Black

Abstract:
MITRE's Common Weakness Enumeration (CWE) http://cwe.mitre.org/ is a list of several hundred classes of weakness that may be found in software. While it is a huge amount of progress over what was available a decade ago, there is still a lot of work to do. We propose some directions to significantly improve CWEs. These directions come from semantic templates, software fault patterns, and other work. To motivate our proposal, we give examples of some ambiguities, gaps, and problems that we found while checking the SATE V Ockham Sound Analysis Criteria http://samate.nist.gov/SATE5OckhamCriteria.html Even "simple" CWEs, such as uninitialized variable, don't correspond well to the warning classes that static analysis tools produce. For instance does CWE-457: Use of Uninitialized Variable cover the case when just one field of a structure is not initialized before it is used? Or does that fall under a far-more-general CWEs, like CWE-824: Access of Uninitialized Pointer, CWE-665: Improper Initialization, CWE-824: Access of Uninitialized Pointer, or CWE-908: Use of Uninitialized Resource?

Presenter Bio:
Dr. Black has nearly 20 years of industrial experience in areas such as developing software for IC design and verification, assuring software quality, and managing business data processing. He is now a Computer Scientist for the National Institute of Standards and Technology (NIST) in the Systems and Software Division of the Information Technology Laboratory. He leads the SAMATE team there.
Dr. Black earned a B.S. in Physics and Mathematics in 1973 and a Ph.D. at Brigham Young University in 1998. Black has organized several workshops dealing with static analysis and has published in the areas of static analysis, software testing, software configuration control, networks and queuing analysis, formal methods, software verification, quantum computing, and computer forensics. He is a member of ACM, IEEE, and the IEEE Computer Society.

Other available formats:

Toward Precise and Accurate Descriptions of Weaknesses
Switch to normal viewerSwitch to experimental viewer

Common Weakness Enumeration CWE Ockham sound analysis National HCSS Conference 2014 NIST U.S. Government Poster HCSS'14 HCSS'14: Poster Session