Tutorial: The Bugs Framework (BF) "Hands-On"

Submitted by Paul E. Black on Tue, 03/07/2017 - 9:23pm. Contributors: Paul E. Black Irena Bojanova

ABSTRACT: Advancements of scientific foundation in cybersecurity rely on the availability of accurate, precise, and non-ambiguous definitions of software weaknesses (bugs) and descriptions of software vulnerabilities. The Bugs Framework (BF) organizes software weaknesses into distinct classes, such as buffer overflow (BOF), injection (INJ), faulty operation (FOP), and control of interaction frequency (CIF). Each BF class has an accurate and precise definition and comprises: * Attributes that identify the software fault; * Causes that bring about the fault; * Consequences the fault could lead to; * Sites in code where the fault might occur.

Through a "hands-on" approach the attendees will be able to analyze definitions and (static) attributes of bugs' classes, along with their related dynamic properties, such as proximate, secondary and tertiary causes, consequences and sites. The focus will be on at least three of the developed BF classes, as well as on examples of applying the BF taxonomy to describe vulnerabilities such as Heartbleed and Ghost. The audience will be involved in describing particular software vulnerabilities, and in discussions about the benefits of BF. The organizers are the BF Principal Investigators and are proposing this tutorial as a way to help researchers and practitioners more accurately and quickly diagnose, describe, and measure security vulnerabilities.

Irena Bojanova is a computer scientist at NIST. Previously she was a program chair at UMUC, an academic director at JHU-CTY, and a co-founder of OBS Ltd. (now CSC Bulgaria). She earned her Ph.D. in Mathematics/Computer Science from the Bulgarian Academy of Sciences in 1991. Irena serves as Member at Large on IEEE CS Publications Board, AEIC of IEEE IT Professional, co-chair of IEEE RS IoT TC and founding member of IEEE TSC on Big Data. Irena was the founding chair of IEEE CS Cloud Computing STC (now TC) and EIC of IEEE Transactions on Cloud Computing. She writes cloud and IoT blogs for IEEE CS Computing Now.

Paul E. 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 U.S. National Institute of Standards and Technology (NIST) near Washington, D.C. The web site he began and edits, the on-line Dictionary of Algorithms and Data Structures, (http://www.nist.gov/dads/) is accessed almost 20,000 times a day from all over the world. He is a member of the Software Quality Group in the Systems and Software Division of the Information Technology Laboratory at NIST.

Dr. Black earned a B.S. in Physics and Mathematics in 1973 and an M.S. in Computer Science in 1983. He began his Ph.D. at UC Berkeley, then transferred to Brigham Young University where he graduated in 1998. Dr. Black has been active in the formal methods research community, and has served as a reviewer for DAC (Design Automation Conference) for several years. He has taught classes at Brigham Young University and Johns Hopkins University. Dr. Black 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 and IEEE Computer Society and a senior member of IEEE.