



**The George Washington University  
Department of Computer Science  
Colloquium**

**March 11, 2008, 4:00pm  
Room 736 Academic Center**

**Zhenkai Liang, Ph.D.  
Carnegie Mellon University**

**Automated Software-Error Detection by Finding Deviations in Binaries**

**ABSTRACT**

In this talk, the author presents his work on automatically detecting errors in software binaries. He observed that software errors usually cause two implementations of a specification to contain deviations, i.e., differences in the way they process their inputs. Based on this observation, his approach finds deviations to detect software errors related to input processing. Given two binaries implementing the same specification and an input, his approach builds a symbolic formula for each binary to characterize how it interprets the input. From the formulas, his approach generates new inputs that can demonstrate deviations/errors in the two binaries. By directly working on a binary program, his approach is precisely faithful to the binary and is not limited by the availability of source code; by generating inputs from symbolic formulas characterizing program execution, his approach significantly reduces the number of inputs needed to find deviations and software errors. The author's approach is implemented by his BitBlaze binary analysis platform. In the talk, he will also discuss other related solutions he has developed using BitBlaze.

**BIOGRAPHY**

**Dr. Zhenkai Liang** is a postdoctoral researcher at Carnegie Mellon University. His main research interest is system and software security with focuses on signature generation for remote attacks, malicious program analysis and confinement, vulnerability diagnosis, and web security. He is also interested in operating systems and software engineering. He got his Ph.D. degree (2006) and M.S. degree (2004) in Computer Science from Stony Brook University, and his B.S. degree (1999) in Computer Science and B.S. degree (1999) in Economics from Peking University. He received the best paper award at USENIX Security Symposium in 2007, and the outstanding paper award at Annual Computer Security Applications Conference (ACSAC) in 2003.