

Thursday, January 14

Scaife Hall Auditorium

Room 125

4:30 p.m.

Refreshments at 4:00 p.m.



David Brumley

Assistant Professor
Carnegie Mellon University

David Brumley is an Assistant Professor in Electrical and Computer Engineering at Carnegie Mellon University. He earned his Ph.D. in Computer Science from Carnegie Mellon University, a Masters in Computer Science from Stanford University, and a Bachelors in Mathematics from the University of Northern Colorado. His current work focuses on software security. His research and interests include all areas of security, as well as programming languages, compilers, formal methods, and systems.

Analysis and Defense of Vulnerabilities in Binary Code

New vulnerabilities are constantly discovered and exploited by attackers. A major focus of my research is developing techniques for protecting vulnerable applications when the program is only readily available as binary (i.e., executable) code. Since most programs are available in binary form, and binary-only analysis does not require cooperation of the source code vendor, this line of research is likely to impact a wide audience.

In this talk, I show two new security applications of binary code analysis: automatic patch-based exploit generation, and automatic input filter generation. In this first part, I show how binary analysis can be used to automatically generate exploits based upon patches released from Windows Update. An immediate consequence of this line of research is that many current vendor patching practices are insecure because they allow attackers to create new exploits before all vulnerable hosts can receive a patch. All is not lost, however. In the second part of this talk, I show how to defend against exploits by automatically generating input filters. Input filters remove exploits from the input stream, thus allowing the vulnerable application to continue to operate normally even under attack. The generated input filters are guaranteed to only filter out exploits, thus safe to automatically deploy.

ECE Seminar Hosts

Jeyanandh Paramesh paramesh@ece.cmu.edu

Onur Mutlu onur@cmu.edu

Gabriela Hug ghug@ece.cmu.edu