Attackers only need to find a single exploitable bug in order to install worms, bots, and other malware on vulnerable computers. Unfortunately, developers rarely have the time or resources to fix all bugs. This raises a serious security question: Which bugs are exploitable, and thus should be fixed first?

My research team’s vision is to automatically check the world’s software for exploitable bugs. Our approach is based on program verification, but with a twist. Traditional verification takes a program and a specification of safety as inputs, and checks that all execution paths of the program meet the safety specification. The twist in AEG is we replace typical safety properties with an ‘un-exploitability’ property, and the ‘verification’ process becomes finding a program path in which the un-exploitability property does not hold. Our analysis generates working control flow hijack and command injection exploits for exploitable paths. I will discuss our results with a data set of over 33,000 programs. I will also discuss current challenges and future directions in symbolic execution.

David Brumley is an Assistant Professor at Carnegie Mellon University with a primary appointment in the Electrical and Computer Engineering Department, and a courtesy appointment in the Computer Science Department. He works in computer security, with an emphasis on software security. Prof. Brumley has a PhD in Computer Science from Carnegie Mellon University, an MS in Computer Science from Stanford University, and a BA in Mathematics from the University of Northern Colorado. He served as a Computer Security Officer for Stanford University from 1998-2002 where he handled thousands of computer security incidents. He is the faculty mentor for the CMU Hacking Team, which has been internationally ranked in the top 2 for 3 years. He has received the USENIX Security best paper awards in 2003 and 2007, selected for the 2010 DARPA CSSP program, a 2010 NSF CAREER award, the 2010 United States Presidential Early Career Award for Scientists and Engineers (PECASE) from President Obama, and the 2013 Sloan Foundation award.