Analysis of Program Binaries for Vulnerability Detection and Patching

Abhik Roychoudhury
Professor, National University of Singapore

ABSTRACT

Due to the absence of source code for parts of a software system - analysis methods which work on both source code and binaries are of value. We have studied security vulnerability detection techniques which work on both source code and binaries. Our detection techniques combine the essential ingredients of various aspects of fuzz testing - model-based black-box fuzzing, coverage based greybox fuzzing, and symbolic execution based whitebox fuzzing. Apart from detecting security vulnerabilities, these capabilities can also be used for reproducing crashes from crash reports or clustering "similar" crashes. Finally, we have also studied methods for automated program repair, where vulnerability patch suggestions can be generated automatically. All of our fuzz testing and patching techniques have been evaluated on large scale and well-known systems such as detecting vulnerabilities in the Adobe Acrobat reader or Windows Media Player, or patching the well-known Heartbleed vulnerability.

SPEAKER BIOGRAPHY

Abhik Roychoudhury is a Professor of Computer Science at School of Computing, National University of Singapore. Abhik received his Ph.D. in Computer Science from the State University of New York at Stony Brook in 2000. Since 2001, he has been employed at the National University of Singapore. His research has focused on software testing and analysis, software security, and trust-worthy software construction. He has been an ACM Distinguished Speaker (2013-19). He is currently leading the TSUNAMi center, a large five-year long targeted research effort funded by National Research Foundation in the domain of software security. He is also the Lead Principal Investigator of the Singapore Cyber-security Consortium. He has authored a book on "Embedded Systems and Software Validation" published by Elsevier (Morgan Kaufmann) Systems-on-Silicon series in 2009, which has also been officially translated to Chinese by Tsinghua University Press. He has served in various capacities in the program committees and organizing committees of various conferences on software engineering including ICSE, ISSTA, FSE and ASE, including being the program chair of ISSTA 2016 and general chair of FSE2022. He is currently serving as an Editorial Board member of IEEE Transactions on Software Engineering (TSE).