Good Code, Bad Code and Vulnerable Code

Munawar Hafiz

Assistant Professor, Department of Computer Science and Software Engineering
Auburn University, Auburn, AL

Abstract

Coding is like gardening; it requires a good plan, good supplies, but most importantly continuous nurture and maintenance. In this talk, I will concentrate on refactorings and program transformations that help nurture good code by removing code smells and vulnerabilities. I will describe OpenRefactory/C, an infrastructure for building program transformations for C programs. C, in spite of its popularity, has IDEs with a limited portfolio of program transformations, with limited scalability and limited applicability to real-world programs. OpenRefactory/C aims to have full support for the C preprocessor, support for static analyses, and an API and environment that make it easy for new developers to contribute new refactorings. Refactorings that we have implemented on OpenRefactory/C are bug-free, unlike the refactorings featured in commercial IDEs such as Eclipse CDT, Microsoft Visual Studio, etc. I will also describe three complex, security-oriented program transformations that fix C integers. These transformations fixed all variants of integer vulnerabilities featured in benchmark programs of NIST's SAMATE reference dataset and 5 open source software, making the changes automatically on over 15 million lines of code. Being integrated with source code and development process, refactorings and program transformations not only helps maintain good code, but also teach developers about how to write and appreciate good code.

Bio

Dr. Munawar Hafiz is an Assistant Professor at the Department of Computer Science and Software Engineering, Auburn University. His research focuses on applying program analysis and program transformation technologies and exploring empirical data to promote tools and methodologies that effectively improve programming experience. Dr. Hafiz leads the Software Analysis, Transformation, and Security (SATS) research group. The group currently consists of one postdoctoral research associate, five graduate, and two undergraduate students. His work is supported by a grant from NSF. Dr. Hafiz received his Ph.D. and MS in Computer Science from University of Illinois at Urbana-Champaign (UIUC) and his B.Sc. Engg. degree in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET). He was a postdoc at UIUC for one year before joining Auburn University in Fall 2011. For more information: http://www.munawarhafiz.com

MONDAY, SEPTEMBER 16, 2013, 4:00 P.M.

235 BROUN HALL

http://www.eng.auburn.edu/~pagrawal/seminar/2013/index.html