BUET ACM CHAPTER

presents

From Theory to Practice: Deployment-grade Tools and Methodologies for Software Security

Speaker: **Sazzadur Rahaman**

Assistant Professor, Department of Computer Science, University of Arizona

Sazzadur Rahaman (https://www.sazzadur.com/) is an assistant professor in the Department of Computer Science at the University of Arizona. He works towards making security research more democratized and affordable. He is broadly interested in computer security and privacy problems, specifically in building robust systems and methodologies by using program analysis, formal verification, applied cryptography, and machine learning-based techniques. His research stirred both industry and academic interests, over the years. Sazzadur completed his Ph.D. from Virginia Tech. In recognition of his work, he received several fellowships (Bitshare fellowship and Pratt fellowship) at Virginia Tech. Prior to joining Virginia Tech, he worked as a software engineer. He has 3.5+ years of industry experience in building health care, payment, and financial technology solutions. He received his B.Sc. in computer science from Bangladesh University of Engineering and Technology (BUET).

Abstract

Automated software checking for security is a challenging problem with a remarkable impact. Most of the solutions are hindered by the practical difficulty of reducing false positives without compromising analysis quality. In this talk, I will share my experiences with building high precision tools and methodologies for automated software security checking (i.e., detecting software non-compliance and vulnerabilities).

In the first part, I will present my work on building robust methodologies to evaluate the payment card industry (PCI) data security standard (DSS) certification process for e-commerce websites. Our study confirms that 86% of the websites have at least one PCI DSS violation that should have disqualified them as non-compliant. In the second part, I will talk about our solution for high precision (98.61%) detection of cryptographic API misuse vulnerabilities massive-sized (e.g., millions of LoC) programs. Oracle has implemented this in its internal code analysis platform, Parfait and found new issues that were previously unknown. I will also share my insights on secure coding in the light of our findings in several high-profile opensource projects.

When: Saturday, 26th September, 2020 (9:00 PM)

Where: Online. Zoom Meeting ID: 627 8663 7409, Password: 462174

Organized by BUET ACM Chapter, Dept. of CSE, BUET.