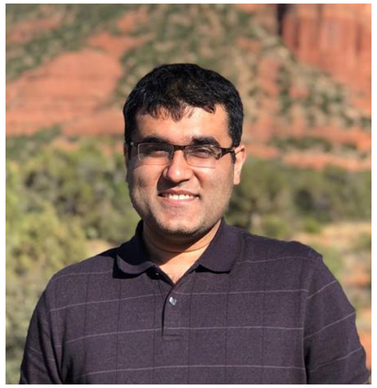
BUET ACM CHAPTER

presents

Automated Reasoning of Security and Privacy of Networks and Cyber-Physical Systems

Speaker: **Syed Rafiul Hussain**

Assistant Professor, Department of Computer Science and Engineering, Pennsylvania State University



Syed Rafiul Hussain is currently an Assistant Professor in the Department of Computer Science and Engineering at Pennsylvania State University. Before joining Penn State, he worked as a postdoctoral researcher at Purdue University from where he also received his Ph.D. in December 2018. His research interests broadly lie in network and systems security with a focus on the fundamental improvement of security and privacy analysis of emerging networks and cyber-physical systems, including cellular networks and Internet-of-Things. His papers have received awards and nominations, including ACSAC'19 distinguished paper award, NDSS'19 distinguished paper award honorable mention, and ACM SIGBED EWSN'17 best paper award nomination. He has been inducted twice in the Hall of Fame Mobile Security Research by GSMA for his contribution in identifying 20+ new protocol flaws in 4G and 5G cellular networks. His findings led to several changes in the 4G and 5G cellular protocol designs and in operational networks. His work has been featured by mass media outlets worldwide, including the New York Times, Washington Post, Forbes, MIT Technology Review, ACM TechNews, and The Register. More details can be found at `https://relentless-warrior.github.io/`.

Abstract

Security and user privacy for complex networks and cyber-physical systems are often considered as afterthoughts. This leads to inadequate security evaluation early on the development cycle that fails to identify missing security and privacy guarantees in protocol and system designs. To make matters worse, unsafe practices and operational oversights stemming from unvetted simplification of complex specifications further contribute to the deviation of deployments from designs. In this talk, I will highlight how my research addresses these problems by developing principled techniques for analyzing design specifications and deployments of complex networks and cyber-physical systems. I will first present a new adversarial reasoning technique combining the capabilities of a symbolic model checker and a cryptographic protocol verifier that enabled us to identify 20+ new vulnerabilities in 4G and 5G cellular network design specifications. I will then discuss three new side-channel attacks in 4G and 5G networks uncovered with our probabilistic reasoning technique. Next, I will talk about a fuzzing technique which is more effective than the state-of-the-art in reasoning about correctness of an implementation when direct feedback on code coverage information is missing. Finally, I will conclude with a discussion on opportunities for prospective PhD students and research collaboration with BUET.

When: Saturday, 10th October, 2020 (8:00 PM)

Where: Online. Zoom Meeting ID: 683 5965 9220, Password: 320990

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