FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

Adversarial-Resilience Assurance for Mobile Security Systems

Wei Yang, Ph.D. candidate

University of Illinois at Urbana-Champaign

Date: March 15, 2018, Thursday, 1:00-2:00pm **Room:** JMH 342

Abstract: For too long, researchers have often tackled security in an attack-driven, ad hoc, and reactionary manner with large manual efforts devoted by security analysts. In order to make substantial progress in security, I advocate to shift such manner to be systematic, intelligent, and adversarial resilient. Over the course of my Ph.D. research, I have developed software engineering techniques to automate decision makings in security systems, and built defenses and testing methodologies to guard against emerging attacks specifically adversarial to these newly-proposed techniques. In this talk, I will first highlight one of these systems for mobile security: AppContext, a malware detection system extracting execution contexts of an app's security-sensitive behaviors through program analysis. Then I will show how an adaptive adversary can attack these systems and how we can generate adversarial inputs ahead of time for testing and further strengthening these systems. I will conclude by discussing how future research efforts can leverage the interplay among software engineering, security, and AI techniques toward a defense-driven security ecosystem.

Bio: Wei Yang is a PhD candidate in Computer Science at the University of Illinois at Urbana-Champaign. He works with Profs Tao Xie and Carl Gunter on a variety of topics related to software engineering and security. He has designed and built intelligent security systems to defend against evolving attacks. Specifically, he has been working on using program analysis, natural language processing, cognitive analysis, and machine learning techniques to bridge the gap between user perceptions and security-sensitive behaviors in mobile security systems. Recently, he is focused on enhancing the robustness of newly-proposed intelligent security techniques in adversarial settings. Wei received his bachelor's degree from Shanghai Jiaotong University in 2011 and a master degree from North Carolina State University in 2013.