CASE SCHOOL OF ENGINEERING
CASE WESTERN RESERVE UNIVERSITY

Department of Civil Engineering

Bingham Bldg. Room 208
10900 Euclid Ave
Cleveland, OH 44106

Department of Civil Engineering Seminar

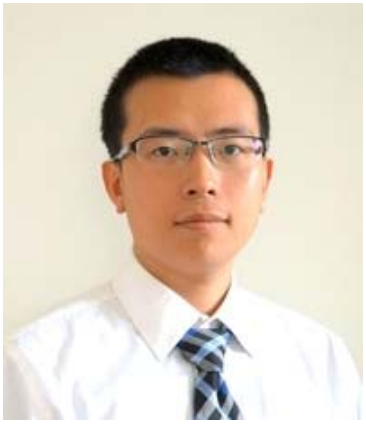
Improving Mobile App Security via Synergy of Program Analysis and Machine Learning

Xusheng Xiao, Ph.D., Assistant Professor
Department of Computer and Data Sciences, Case Western Reserve University

Friday October 11, 2019, 11:30-12:30PM @ Bingham 103
Lunch and discussion at 11:00PM at Bingham 102 (Vose Room)

Abstract

Smartphone applications (i.e., apps) are providing more and more services to our daily life. However, certain behavior of the apps is less than desirable and aggressive in using users' sensitive data, such as disclosing users' GPS data without notifying the users. To protect users' data, mainstreamed smartphone platforms employ the permission-based access control mechanism, which asks users to grant permissions for the first-time uses of sensitive data. However, it has shown little success since undesired behaviors appear to be indistinguishable from that of benign behaviors (e.g., apps sending GPS data to find nearby restaurants). In this talk, I will present my research in addressing the challenges of detecting undesired behaviors that exploit users' sensitive data. The key insight of my research is that the context that triggers the sensitive behavior is a strong indicator of whether the behavior is expected to use the sensitive data. Based on this insight, I have developed techniques that models the contexts of sensitive behaviors to detect undesired behaviors. In particular, my techniques focus on Android apps and explore the synergy of machine learning and program analysis to address the challenges in Android apps: (1) we develop program analysis to analyze the different types of contexts (system contexts and UI contexts), constructing a high-quality training dataset from popular apps, and (2) we develop machine learning techniques to learn context-behavior models from the training dataset constructed from real apps and detect undesired behaviors based on the learned model.



BIO: Xusheng Xiao is an assistant professor of Computer and Data Sciences at Case Western Reserve University. He received his Ph. D. degree in Computer Science at North Carolina State University in 2014. He was a visiting student in Computer Science department of the University of Illinois at Urbana-Champaign in 2013-2014. His research interests are in software engineering and computer security, with the focus on making software applications and computer systems more reliable and secure via program analysis, software testing, text analysis, and system monitoring. His research has been presented at top-tier venues such as ICSE, FSE, ISSTA, ASE, USENIX Security, CCS, and VLDB. His work in attack investigation for Advanced Persistent Threat (APT) attacks was selected as one of the top ten finalists for CSAW Best Applied Security Paper Award 2018. His work in mobile security was selected as one of the top ten finalists for CSAW Best Applied Security Paper Award 2015, and produced a static analysis tool that was deployed in TouchDevelop of Microsoft Research. His research is supported by NSF and Samsung. More details of his research can be found at his homepage, http://engineering.case.edu/groups/xusheng-xiao/.