**COLLOQUIUM**

Department of Computer Science and Engineering

University of South Carolina

**Improving Software and Systems Security via Software Analysis**

**Lannan (Lisa) Luo**

Date: **March 3, 2017**

Time: **10:30-11:45am**

Place: **300 Main B101**

# Abstract

As the digital brainpower of the IT revolution, software has become an important driving force of today’s economy as well as an indispensable element of personal life. Hence, the security of the software and systems becomes increasingly important. In this talk, I will present my work on analyzing and enhancing software and systems security, which applies rich and powerful software analysis methodologies. A particular emphasis is placed on two problems: automatically detecting software plagiarism and automatically discovering vulnerabilities in Android Framework. First, I will present CoP, a technique that can be applied to detect software plagiarism. Identifying similar code segments among programs is faced with a notorious challenge caused by code obfuscation and is even more difficult when the source code is unavailable. I will present how CoP addresses them. Then, I will present Centaur, a technique that applies symbolic execution to Android Framework aiming at discovering vulnerabilities and generating proof-of-concept exploits automatically. Android Framework is an integral and foundational part of the Android system, containing multiple million lines of code. Despite extensive work on Android, most of the existing tools are only capable of analyzing Android applications. There is a severe lack of techniques and tools for insecurity analysis of the underlying framework code in Android. Due to unique characteristics of Android Framework, many challenges are raised when conducting such program analysis as symbolic execution and taint analysis. I will show how we overcame these challenges and implemented the system for insecurity analysis of Android Framework. Finally, I will conclude the talk with a brief discussion on future research directions.

**Lannan (Lisa) Luo** is a Ph.D. candidate in the College of Information Sciences and Technology at The Pennsylvania State University, under the supervision of Prof. Peng Liu. She received her B.S. in Telecommunications Engineering from Xidian University, Xi’an, China in 2009, and M.S. in Communications and Information Systems from The University of Electronic Science and Technology of China in 2012. Her research interests are software and systems security. During her PhD study, she mainly works on the software piracy problem and mobile computing security. Her research work has been published in FSE (Best Paper Award nomination), ICSE, DSN, and TSE. She did an internship at Microsoft Research Asia in 2015. Find more about her here: <http://www.personal.psu.edu/lzl144/>.