COMPUTER SCIENCE RESEARCH SEMINAR

On the dissection and instrumentation of a commercial Android application

Aravind Prakash
Department of Computer Science, Binghamton University

Friday, April 7th at noon in room R15, Engineering Building

Abstract: With over 1.5 million activations per day, Android is now the most widely used mobile platform in the world. Understanding the inner workings of an application is beneficial to multiple stake holders (i.e., application store owner and end user). For example, an application store owner seeks to verify whether or not an application has malicious behavior. Similarly, an end user may want to retrofit an application with custom security and/or functional features. However, without access to source code, dissecting an app and recovering various program elements is hard.

This talk will delve into the internals of an Android application. Motivation and design goals behind Dalvik byte code will be presented. Challenges in automated Dalvik byte code analysis, instrumentation and recompilation will be discussed. Different granularity of instrumentation (instruction-, basic-block- and function level) will be considered. Our preliminary work indicates that functionality-preserving transformations can be performed on commercial Android applications. Some evaluation results will be presented. The talk will conclude with a discussion on opportunities and challenges in Android byte code and native code analysis.

Bio: Aravind Prakash obtained a PhD from Syracuse University in May 2015 and is currently an assistant professor in the Department of Computer Science at Binghamton University. His research focuses on static and dynamic program analysis and binary reverse engineering.

Co-sponsored with GSO and partially paid for by student activity fees.

Pizza will be provided!