William Paterson University
College of Science and Health
Department of Computer Science

*UPS Computer Information Technology Lecture Series**

Dr. Hossain Shahriar
Assistant Professor of Computer Science
Kennesaw State University

March 26, 2015 (Thursday), 12:30 PM – 1:45 PM
SCIE 5036

Secure and Reliable Android Applications: Challenges and Approaches

Abstract

Android has become the leading smartphone Operating System in the world and currently occupying more than 50% of the global market share of smartphone. An increasing number of Android mobile applications are being developed to meet various needs of end users including SMS messaging, social networking, and game playing. It has been estimated that the revenues from mobile applications are expected to rise globally from $68Bn in 2013 to $143Bn in 2016. Unfortunately, this emerging area is not free from security and reliability issues.

A recent study shows that more than 50% of mobile devices have unpatched vulnerabilities, opening to malicious applications (malware) and attacks. Malware on a smartphone can make a phone partially or fully unusable, cause unwanted billing, or steal contact information stored in a phonebook. Further, benign applications may contain vulnerabilities due to the lack of developer knowledge and malware applications can exploit the known vulnerabilities by providing

malicious inputs. Android applications may also suffer from resource leakage. Particularly, memory leak can occur when users navigate applications in devices though screen rotation and pressing of built-in buttons leading to the crash of applications.

This talk is intended to provide a basic overview of Android malware, content leakage vulnerability and memory leak issues. We provide an overview of built in security features of Android followed by a set of common malware types. We show application of reverse engineering tools that can be used to inject arbitrary code in benign Android applications. We then provide an overview of recent development in academia and industry to combat against malware. In the second part, we introduce the content leakage vulnerability in android applications. We show examples of best programming practices to reduce the exposure of content leakage issue. In the third part, we address the memory leak issue. We demonstrate a number of common memory leak patterns followed by some practices of preventing them. We also discuss future research directions. The discussion would argue that existing tools can address the challenge for building reliable and secure applications partially.

Biography

Dr. Hossain Shahriar is an Assistant Professor of Computer Science at Kennesaw State University since Fall 2012. He received his Ph.D. (Computing) and M.Sc. (Computing and Information Science), and B.Sc. (Computer Science & Engineering) in 2012, 2008, and 2003, respectively. Dr. Shahriar's current research interests include but not limited to security vulnerabilities and mitigation techniques of applications, metric-based attack detection, and security risk assessment technique. He has published over 50 peer-reviewed research articles in international journals, conferences, and books. His publications have received over 350 citations (based on google scholar) and awards including the Best Paper Award in IEEE DASC 2011, an Outstanding PhD Research Achievement Award 2011 from Queen's University, and IEEE Kingston Research Excellence Award 2008. He is a reviewer of international journals (Computers & Security, Journal of System and Software, ACM Computing Surveys) and PC member of many international conferences (ACM/SIGAPP SAC, ACM/SIGSAC SIN). He is also an Associate Editor of International Journal of Secure Software Engineering. Currently, Dr. Shahriar is a professional member of ACM, SIGAPP, IPSJ, and IEEE.

*** The UPS Computer Information Technology Lecture Series is made possible by a generous grant from the UPS Foundation of UPS.**

All are welcome. This lecture series is open to everyone in the William Paterson University community. For further information, please contact Dr. Cyril S. Ku (kuc@wpunj.edu) or Dr. Salimur Choudhury (choudhurys3@wpunj.edu), Department of Computer Science, William Paterson University, Wayne, New Jersey.
