Title: Automatic Discovery of Flaws in iOS Sandbox Profiles

Speaker: Assistant Professor Razvan Deaconescu
University Politehnica of Bucharest, Romania

Date/Time: 21 July 2017, Friday, 02:00 PM to 03:30 PM

Venue: SR5, COM1-02-01

Chaired by: Dr Chin Wei Ngan, Associate Professor, School of Computing (chinwn@comp.nus.edu.sg)

Abstract:

Recent literature on iOS security has focused on the malicious potential of third-party applications, demonstrating how developers can bypass application vetting and code-level protections. In addition to these protections, iOS uses a generic sandbox profile, called container, to confine malicious or exploited third-party applications. In this presentation, we present the first systematic analysis of the iOS container sandbox profile. We propose the SandScout framework to extract, decompile, formally model, and analyze iOS sandbox profiles as logic-based programs. We use our Prolog-based queries to evaluate file-based security properties of the container sandbox profile for iOS 9.0.2 and discover seven classes of exploitable vulnerabilities. These attacks affect non-jailbroken devices running later versions of iOS. We have been working with Apple to resolve these attacks, and we hope SandScout will play a significant role in the development of sandbox profiles for future versions of iOS.

Biodata:

Razvan Deaconescu is an Assistant Professor at University POLITEHNICA of Bucharest, Romania. He has always been fond of operating systems and low-level programming with current interest in runtime application security and reverse engineering. He enjoys working with binaries, executables and assembly language. He is currently doing research in operating system security, focusing on the lower-layers of the Apple iOS software stack. He has also been involved in local practical security related activities such as CTF contests and summer schools.