Attacks on Android Systems and a Systematic Security Analysis on Vendor Customization

This talk consists of two parts. For the first part, I will present some of the recent attacks/vulnerabilities that we have identified, including the code injection attacks on the HTML5-based apps, the hanging attribute reference vulnerability, and data residue vulnerabilities in Android OS. In the second part, I will present a systematic analysis on the security impact of the vendor customization. Android customization offers substantially different experiences and rich functionalities to users. Every party in the customization chain, such as vendors and carriers, modify the OS and the pre-installed apps to tailor their devices for a variety of models, regions, and custom services. However, these modifications do not come at no cost. We have systematically identified security features that, if altered during the customization, can introduce potential risks. We conducted a large scale analysis on 591 custom images to detect inconsistent security features.

Brief Bio: Wenliang (Kevin) Du received his Bachelor's degree from the University of Science and Technology of China in 1993 and Ph.D. degree from Purdue University in 2001, all in Computer Science. Kevin is currently a professor in the Department of Electrical Engineering and Computer Science at Syracuse University. His background is in computer and network security. His current research interest focuses mobile system security. He is also interested in developing instructional laboratories for security education, and the labs that he developed have been used by over five hundred universities, colleges, and high schools worldwide. His research has been sponsored by grants from National Science Foundation, Army Research Office, JP Morgan Chase, and Google. He is a recipient of the ACM CCS Test-of-Time Award in 2013.

Free Seminar - Open to the Public

Monday, April 3, 2017

4:00pm to 5:00pm

University at Buffalo - North Campus - Davis 113A