Seminar Talk

Rui Ning
PhD student
Department of Electrical & Computer Engineering
Old Dominion University

Friday, February 08, 2019
3:00 p.m. KH 224

Title: DeepMag: Sniffing Mobile Apps in Magnetic Field through Deep Convolutional Neural Networks

Abstract:

We report a newfound vulnerability on smartphones due to the malicious use of unsupervised sensor data. We demonstrate that an attacker can train deep Convolutional Neural Networks (CNN) by using magnetometer or orientation data to effectively infer the Apps and their usage information on a smartphone with an accuracy of over 80%. Furthermore, we show that such attacks can become even worse if sophisticated attackers exploit motion sensors to cluster the magnetometer or orientation data, improving the accuracy to as high as 98%. To mitigate such attacks, we propose a noise injection scheme that can effectively reduce the App sniffing accuracy to only 15% and at the same time has a negligible effect on benign Apps.

Bio:

Rui Ning is a current Ph.D. student in Old Dominion University’s Department of Electrical and Computer Engineering and conducts his research under the direction of Dr. Hongyi Wu. He received the master degree in Computer Science from the University of Louisiana at Lafayette, in 2016. His research interests include cybersecurity, secure AI, and ML-based side channel attacks. Rui Ning has received the Mark Weiser Best Paper Award at the IEEE International Conference on Pervasive Computing and Communication (PerCom).