Profiling User-Trigger Dependence for Android Security

Speaker: Karim Elish, *Virginia Tech*

Date and Time: February 12 (Thursday), 2015 - 2:00pm-3:00pm

Location: 1014 SERC (PLEASE NOTE THE SERC LOCATION, NOT SEC)

Abstract:

As mobile computing becomes an integral part of the modern user experience, malicious applications have infiltrated open marketplaces for mobile platforms. Malware apps stealthily launch operations to retrieve sensitive user or device data or abuse system resources. Existing malware detection solutions (signature-based scanning tools) are reactive and need to be constantly updated to detect evolving malware. In this talk, we present new anomaly-detection technique for ensuring the trustworthiness and integrity of Android apps. Our method statically extracts and enforces benign data-flow properties on how user inputs trigger sensitive API invocations, and detect anomalies in program code. Our experimental evaluation on thousands of free popular apps and known malicious apps gives high detection accuracy that is better than, or at least competitive against, the state-of-the-art. Our analysis also discovers new malicious apps in the Google Play market that cannot be detected by virus scanning tools. Our thesis in this mobile app classification work is to advocate the approach of benign property enforcement, i.e., extracting unique behavioral properties from benign programs and designing corresponding classification policies.

Biography:

Karim Elish is a PhD candidate in the Department of Computer Science at Virginia Tech. He is a member of the Human-Centric Security Laboratory at Virginia Tech, where he is working as a graduate research assistant. Karim obtained his MS degree in Computer Science from Virginia Tech in 2011. Before joining Virginia Tech, he was working as a lecturer in the Information and Computer Science Department at King Fahd University of Petroleum and Minerals where he obtained his first MS degree in Software Engineering in 2008. His current research interests focus on software security, Android malware analysis and detection, software refactoring, and software quality predictive models.