

Mitigating Android Application Risk Through Permission-Based Analysis and Risk Assessment Technique

The Oakland University and School of Engineering and Computer Science communities are invited to attend Ali Alshehri's defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.

Mitigating Android Application Risk Through Permission-Based Analysis and Risk Assessment Technique

Committee: Huirong Fu, Ph.D. (Chair), Anyi Liu, Ph.D.,
Debatosh Debnath, Ph.D., Albert J. Meehan, Ph.D.

Time: 10:00 a.m. – 12:00 p.m.
Date: Wednesday, July 10, 2019
Location: 347 EC

Android has become the most prevalent and fastest growing platform due to its availability, lower cost, and open source philosophy. However, Android has become an attractive target for adversaries; who construct different types of malicious applications and use different social engineering approaches to attract users to download and trust their applications. Android applications pose many security risks that affect the security and privacy of their users.

This dissertation introduces PUREDroid (**P**ermission Usage and **R**isk **E**stimation for **A**ndroid), a risk assessment model that informs the user about the risk level of an application and its requested permissions to help users make the right or better decision about whether to grant or deny a requested permission. PUREDroid measures the risk associated with the requested permissions within an application based on the application category. The security risk of the Android application is measured by extracting some information from the inspected applications by utilizing a static analysis technique and different supervised learning models to generate risk scores. PUREDroid is evaluated on more than 23000 applications, including 17316 benign applications and 5739 malware applications belonging to seven different categories.

This paper proposes **P**ermission Usage and **R**isk **E**stimation for **A**ndroid (PUREDroid) to measure the security risk of Android applications and their permissions and the magnitude of harm resulting from granting extraneous permissions requests.

