

Seminar

Department of Computer Science

Dr. Amiangshu Bosu

Assistant Professor, Department of Computer Science

DIALDroid: A Scalable System to Identify Inter-app Data-leak Vulnerabilities and Collusions among Android Apps

Date: Wednesday, October 19, 2016
Time: 2:00 – 3:00 p.m.
Location: EGRA309C, CS Conference Room

Abstract

Inter-Component Communication (ICC) provides a message passing mechanism for data exchange to facilitate the communication among Android applications. However, ICC model can be utilized by malicious application pairs to leak sensitive information. Many single-app program analysis techniques have been reported that screen an Android app individually for malicious data-flow patterns. However, very few analysis tools readily support pairwise app analysis, which is necessary for detecting inter-app data leak vulnerabilities and collusion attacks.

We utilize static analysis techniques to detect inter-app ICC anomalies. Our focus is on balancing the accuracy of data-flow analysis and the scalability of pairwise operations.

For accuracy, we present a new robust Android string analysis tool that discovers 28% more intents than IC3. For scalability, we design a database-based ICC linking and querying system. Our prototype DIALDroid substantially outperforms the two leading pairwise analysis tools, IccTA (coupled with ApkCombiner) and COVERT, in benchmark accuracy evaluation.

We also evaluate over 100K real-world apps from Google Play Market and report several types of inter-app ICC anomalies detected.