Deniz Aytemiz

CS 5590: Paper Summaries for April 4

1. Collusive Data Leak and More: Large-scale Threat Analysis of Inter-app Communications

   In this paper real world vulnerable ICC apps are examined and analyzed in large scale based on the interapp data flows. Inter Component Communication (ICC) is a data exchange mechanism for android applications and is vulnerable to malware aiming collusion attacks. The writers provide an android security tool for analyzing vulnerable data flow.

2. Detection of Repackaged Android Malware with Code-Heterogeneity Features

   The repackaging of Android apps makes them vulnerable due to the possibility of malicious modifications or insertions. There are mechanisms to detect this vulnerability however they are limited in terms of differentiating malicious and non-malicious code. In this paper, a new method for detection based on partitioning code into dependence based regions is proposed and tested on real world applications to test its performance.

3. Checking is Believing: Event-Aware Program Anomaly Detection in Cyber-Physical Systems

   Cyber physical systems suffer from data oriented and control oriented attacks. The detection mechanisms currently are insufficient due to lack of runtime execution semantics. In this paper a new methodology caled Orpheus is proposed for defending cyber physical systems against data oriented attacks. Writers present a new behaviour model eFSA that incorporates event checking for anomaly detection and is able to detect if a specific event is missing. The performance of the prototype is evaluated for data oriented attacks and showed that eFSA is successful in terms of performance.