COVERT: Compositional Analysis of Android Inter-App Permission Leakage

Abstract

Android is the most popular platform for mobile devices. It facilitates sharing of data and services among applications using a rich inter-app communication system. While access to resources can be controlled by the Android permission system, enforcing permissions is not sufficient to prevent security violations, as permissions may be mismanaged, intentionally or unintentionally. Android’s enforcement of the permissions is at the level of individual apps, allowing multiple malicious apps to collude and combine their permissions or to trick vulnerable apps to perform actions on their behalf that are beyond their individual privileges. In this paper, we present COVERT, a tool for compositional analysis of Android inter-app vulnerabilities. COVERT's analysis is modular to enable incremental analysis of applications as they are installed, updated, and removed. It statically analyzes the reverse engineered source code of each individual app, and extracts relevant security specifications in a format suitable for formal verification. Given a collection of specifications extracted in this way, a formal analysis engine (e.g., model checker) is then used to verify whether it is safe for a combination of applications—holding certain permissions and potentially interacting with each other—to be installed together. Our experience with using COVERT to examine over 500 real-world apps corroborates its ability to find inter-app vulnerabilities in bundles of some of the most popular apps on the market.
EXISTING SYSTEM

Enforcing permissions is not sufficient to prevent security violations, as permissions may be mismanaged, intentionally or unintentionally.

DRAWBACK OF EXISTING SYSTEM

- Fail to identify vulnerabilities.
- Cannot be detected by techniques that analyze a single app in isolation.

PROPOSED SYSTEM

Compositional analysis of Android inter-app vulnerabilities. COVERT’s analysis is modular to enable incremental analysis of applications as they are installed, updated, and removed. COVERT combines static analysis with formal methods.

ADVANTAGE OF PROPOSED SYSTEM

- Increase the security properties from individual apps.
- Increase the scope of application analysis.

SYSTEM SPECIFICATION

Hardware Requirements

- System: Pentium IV 2.4 GHz
- Hard Disk: 40 GB
- Floppy Drive: 1.44 Mb
Monitor : 15 VGA Colour
Mouse : Logitech
Ram : 512 Mb

Software Requirements

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Windows Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td>eclipse</td>
</tr>
<tr>
<td>Technology Used</td>
<td>Java</td>
</tr>
<tr>
<td>Backend Used</td>
<td>SQLITE</td>
</tr>
</tbody>
</table>