Collusion Attack Implementation by Retrofitting Android Apps
Lance Chao, Ke Tian, Danfeng (Daphne) Yao
Department of Computer Science, Virginia Tech
(kisseki, ketian, danfeng)@cs.vt.edu

Motivation:
• To develop a Trojan-type malware that is buried inside multiple android applications
• To develop malware that is undetectable by traditional anti-virus scanners

Background
ICC(inter-component) communication:
• An app is composed of several components: activity, service, broadcast.
• Components interact through ICC objects (intsents).
• Intents can bind with sensitive data. (geo, phone info)

Collusion Attack with ICC:

<table>
<thead>
<tr>
<th>Malicious App 1</th>
<th>Malicious App 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp A</td>
<td>ICC Communication (send data)</td>
</tr>
<tr>
<td>Comp B</td>
<td>ICC Communication (send data)</td>
</tr>
<tr>
<td>Comp X</td>
<td>ICC Communication (send data)</td>
</tr>
<tr>
<td>Comp Y</td>
<td>ICC Communication (send data)</td>
</tr>
<tr>
<td>Comp X</td>
<td>ICC Communication (send data)</td>
</tr>
<tr>
<td>Comp Y</td>
<td>ICC Communication (send data)</td>
</tr>
</tbody>
</table>

Attack Steps:
1. Comp A in app1 steals device ID info.
2. With ICC, Comp X in app 2 receives ID info.
3. App 2 will abuse the info for profit.

Fig.1 a sample of 2-app collusion attack

Challenges for Detection
1. Analyzing data flow & control flow between two-app is complex.
2. Minimizing permission usages for each app makes traditional anti-virus tools difficult to detect.

Techniques of Our Approach
Repackaging:
1. Decompiling an app into intermediate representation(IR).
2. Modifying IR to meet the requirements with code rewiring.
3. Recompiling IR into a new app.

App Retrofitting:

Experiment Results
Two originally independent, benign apps, modified to communicate with each other (See the left figure)

Acknowledgement
This work is supported by DARPA APAC award FA8750-15-2-0076.

Conclusions and Future Work
1. Pair-wise attacks is a growing problem in android security, and it cannot be reliably detected yet.
2. We wish to develop a tool to automatically achieve the collusion attack and an anti-virus tool to detect this kind of attack in the future.

References: