ICU: A tool for Intent Filtering on Android devices

Evita Bakopoulou
Athens University of Economics and Business
mpakopoulou@aueb.gr

Ioannis Boutsis
Athens University of Economics and Business
mpoutsis@aueb.gr

Panagiotis Thanopoulos
Athens University of Economics and Business
panagiotis.thanopoulos.89@gmail.com

Vana Kalogeraki
Athens University of Economics and Business
vana@aueb.gr

ABSTRACT
The usage of smartphone and mobile devices has increased tremendously in recent years and nowadays the most popular OS for smartphones is the Android OS. However, a significant percentage of the users does not realize that there are applications that can threaten their privacy. Any user can download freely applications from the Google Play Store, without being aware of the consequences to his/her privacy. The majority of such downloaded application work with “Intents”. Intents are signals that represent an action to be executed within the application or in order to propagate data to remote applications that act as recipients. The problem we study in this paper is how to protect user privacy by intercepting and controlling the Intents. The approach we propose in this paper is to enhance the user’s privacy through “Intent” filtering. Specifically, our application intercepts some designated Intents (implicit and broadcast “Intents”, featuring suspicious actions) and alerts users with a message containing information about the “Intent” and the action to be executed. Finally, the user can block or allow the “Intent” at will, after reviewing the content of the alerting message.

CCS Concepts
• Security and privacy → Mobile platform security;
• Privacy protections; Malware and its mitigation;

Keywords
Android OS, Apps, security, privacy, Intent, implicit, filter intents, broadcast, intercept, block

1. INTRODUCTION
The number of smartphone users has tremendously increased in recent years. Android OS is the most popular mobile OS and its Google Play Store is the largest App store having numerous applications available to users. A percentage of these applications may bear suspicious actions that can harm user’s privacy. A malicious application in the Android OS may obtain access to the user’s private data, such as his/her pictures, videos, text messages, emails, location or private health information, and forward this data to unwanted recipients without the user’s permission.

The downloaded applications in the Android OS can communicate with one another via Intents. Intents are signals that represent an action to be executed within the application or in order to propagate data to remote applications that act as recipients. There are three categories of Intents: Explicit, Implicit and Broadcast. Explicit Intents have a designated receiver and the Intent can be caught only by it. The implicit Intents can be intercepted by activities or applications that have a suitable filter in their manifest file. The broadcast Intents can be intercepted by activities or applications that use a broadcast receiver, having an acceptable filter. Broadly speaking, this kind of Intents correspond to the system’s actions. Moreover, an Intent contains an action, the necessary data for its execution, a category, a type, a destination component and an “Extras” field.

In this paper we present ICU (Intent Controlling Utility), an application for intercepting potentially harmful Intents (implicit and broadcast) on Android mobile devices. We focus only on these two Intent types, since it is true that there is no way to intercept explicit Intents. It is possible to track explicit Intents only via the task manager, which means that these Intents are already executed and cannot be stopped. The main challenge we overcame in ICU’s development was the diversity of the Intents in existing applications in Google Play. To intercept the majority of the Intents, we examined the Intent Filters of various applications, and added them to ICU’s filters. Our contribution is an application that aims to inform the user about the Intents that are exchanged within his/her device, providing the option of blocking the Intent in order to evade malicious actions from being executed.

2. ICU ARCHITECTURE
Our proposed ICU architecture consists of the modules shown in Fig. 1. Intent Catcher intercepts implicit Intents and the Broadcast Receiver [3] catches broadcast Intents. After the Intent is captured, we destroy it and create an identical one to give to the user the choice of allowing it or not. Next, depending of the user’s choice, the Intent is executed or not and his/her answer and the Intent’s details...
are saved into a local database for future reviewing.

The ICU’s Broadcast Receiver runs “over” a Service [5], which needs to be started before receiving such Intents. It has the maximum priority in order to intercept first the broadcast Intents. After intercepting broadcast Intents, we use the method abortBroadcast() to stop the broadcast, we inform the user and if he or she chooses to continue, ICU creates a replicated Intent and broadcasts it.

To intercept implicit Intents, we added an extended Intent filter [4] in the ICU’s manifest file. Each time an implicit Intent is intercepted, the user must choose an application to handle the intercepted Intent. Selecting the ICU will inform him/her about the Intent’s action, data and extras, and the user will have the option to allow the Intent’s action or not.

Moreover, we implemented the Modes module, which allows the user to stop ICU from intercepting certain Intents and thus, provides a friendlier user interface. ICU offers four different modes; GPS, Photos/Video, Music and Contacts Mode.

3. EXPERIMENTS/ USE CASES

We tested a sample of applications from Google Play to intercept various Intents, as shown in Table 1. In Fig. 2 we present the content of two captured Intents.

<table>
<thead>
<tr>
<th>Application</th>
<th>Version</th>
<th>Intent captured description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrica</td>
<td>2.4.2(30)</td>
<td>implicit intent to share photo</td>
</tr>
<tr>
<td>Brain Training</td>
<td>2.1</td>
<td>implicit intent to open an ad in browser</td>
</tr>
<tr>
<td>Piano Tiles 2</td>
<td>1.1.0.766</td>
<td>implicit intent to send email</td>
</tr>
<tr>
<td>exDialer</td>
<td>191</td>
<td>implicit intent to send sms</td>
</tr>
<tr>
<td>In Touch</td>
<td>2.0.6</td>
<td>implicit intent to share a contact</td>
</tr>
<tr>
<td>Location Tracker</td>
<td>3.2.3</td>
<td>implicit intent to share location</td>
</tr>
</tbody>
</table>

Table 1: Tested Applications

As shown in Fig. 2(b), with ICU it is possible to examine the URL of an advertisement before opening it in the browser. Also, if the user clicks by mistake on the advertisement, he/she can block the Intent and prevent it from being executed. Hence, malicious/spoofed URLs can be avoided by blocking the corresponding Intents.

4. RELATED WORK

A related application is a broadcast receiver in [2], however, it intercepts only broadcast Intents. Another similar application is Intent Intercept [1], which attempts to intercept system-wide Intents only, such as Intents that are related to Bluetooth actions. ICU is different to these works, since it is a tool for intercepting broadcast and implicit Intents, with a function to examine the content of these Intents and allow them or block them.

5. CONCLUSION AND FUTURE WORK

ICU offers security and privacy to the user, while providing the opportunity to get information about the action and the data of every Intent (implicit or broadcast) captured. By reviewing the Intent’s content, it is possible to examine spoofed Intents and block them. Thus, it is feasible to discover malicious applications and block their actions.

As for our future work, one direction that ICU could be extended would be to infer automatically user’s preferences from his/her previous answers so that certain intents will be assumed as “safe”. For example, if the user has permitted multiple times a certain intent, ICU will permit it without asking the user.

6. ACKNOWLEDGEMENTS

This research has been financed by the European Union through the FP7 ERC IDEAS 308019 NGHCS project and the Horizon2020 688380 VaVeL project.

7. REFERENCES