Chapter 6

ANALYZING MOBILE DEVICE ADS TO IDENTIFY USERS

Jayaprakash Govindaraj, Robin Verma and Gaurav Gupta

Abstract User browsing behavior is tracked by search providers in order to construct activity profiles that are used to fine-tune searches and present user-specific advertisements. When a search input matches a commercial product or service offering, ads based on the previously-saved interests, likes and dislikes are displayed. The number of web searches from mobile devices has exceeded those conducted from desktops. Mobile devices are being used for critical business tasks such as e-commerce, banking transactions, video conferences, email communications and confidential data storage. Companies are moving towards mobile-app-only strategies and advertisers are displaying ads on mobile apps as well. Mobile device ads can often reveal information such as location, gender, age and other valuable data about users. This chapter describes a methodology for extracting and analyzing ads on mobile devices to retrieve user-specific information, reconstruct a user profile and predict user identity. The results show that the methodology can identify a user even if he or she uses the same device, multiple devices, different networks or follows different usage patterns. The methodology can be used to support a digital forensic readiness framework for mobile devices. Additionally, it has applications in context-based security and proactive and reactive digital forensic investigations.

Keywords: Smartphones, advertisements, user behavior, user identification

1. Introduction

A 2014 mobile security survey by Checkpoint [5] reported that 64% of Android devices, 16% of Apple/iOS devices, about 16% of Windows phones and about 36% of BlackBerry devices are vulnerable to security threats. Insecure web browsing accounted for 61% of the total factors impacting the safety of mobile data. Meanwhile, 82% of security professionals expect mobile security incidents to increase, 98% have concerns
about the impact of mobile security incidents and 95% face challenges with bring your own device (BYOD) policies.

Mobile devices can be taken anywhere, increasing the possibility of the devices getting stolen or tampered with. Smartphones enable users to access the Internet from anywhere. Mobile devices are vulnerable to remote attacks through SMS/MMS or via the exploitation of insecure connections. Unlike hard disk drives, it is challenging to forensically-image phones without changing the states of the devices. Since phones use flash memory, every time an extraction is made, a different hash value is obtained.

All forensic images of phones are not equal. Logical extraction only provides a dump of the existing files such as call history, SMS and text messages; it does not acquire a dump of the unused space on the phone. Physical extraction can obtain a complete memory dump, but the process is difficult to perform without invasive techniques that could damage the phone. Most commercial forensic tools cannot bypass passcodes of smartphones [1]. Smartphones have to be jailbroken or rooted to access evidence required in digital forensic investigations.

Most mobile forensic solutions and products are designed for use in post-incident scenarios. At this time, there is no well-defined digital forensic readiness framework for mobile devices. Data collection is a key requirement in readiness scenarios [6, 10]. However, it is not clear what evidence to collect, how to handle situations where the collected evidence has been tampered with [11] and how to monitor and target particular evidence. Without question, there is a great need for new ways to identify users before security incidents occur as well as after the incidents.

Tracking a user’s search keywords is one way search providers are gathering user preferences and targeting the most appropriate ads to display to users [13]. It is often the case that potential criminals plan their crimes using Internet searches or make purchases of objects or services needed to perpetrate their crimes. Knowledge of an accused’s ad preferences could be useful in attempting to establish the sequence of events involved in the planning and execution of the crime. If the suspect had used mobile devices, the kind of ads that he clicked/viewed could reveal information about himself, including his motives and behavior. Although browser history may reveal more information, the specific ads that the suspect clicked and the websites he visited can reveal valuable information about his interests and behavior [4]. This is the principal motivation for analyzing the ads clicked by a user to identify the user.

This chapter describes a system that can track clicked ads in real time, extract the ads, analyze them to retrieve personal information and use