Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Evaluating the privacy of Android mobile applications under forensic analysis

*Christoforos Ntantogian**, *Dimitris Apostolopoulos*, *Giannis Marinakis*, *Christos Xenakis*

Department of Digital Systems, University of Piraeus, Piraeus, Greece

ARTICLE INFO

Article history:
Received 30 October 2013
Received in revised form
16 January 2014
Accepted 20 January 2014

Keywords:
Privacy of mobile applications
Mobile forensics
Android
Memory dump
Mobile applications
Volatile memory
Authentication credentials

ABSTRACT

In this paper, we investigate and evaluate through experimental analysis the possibility of recovering authentication credentials of mobile applications from the volatile memory of Android mobile devices. Throughout the carried experiments and analysis, we have, exclusively, used open-source and free forensic tools. Overall, the contribution of this paper is threefold. First, it thoroughly, examines thirteen (13) mobile applications, which represent four common application categories that elaborate sensitive users' data, whether it is possible to recover authentication credentials from the physical memory of mobile devices, following thirty (30) different scenarios. Second, it explores in the considered applications, if we can discover patterns and expressions that indicate the exact position of authentication credentials in a memory dump. Third, it reveals a set of critical observations regarding the privacy of Android mobile applications and devices.

1. Introduction

According to recent reports (http://blog.flurry.com/bid/88867/iOS-and-Android-Adoption-Explodes-Internationally), the global adoption of smart phones and tablets has been growing faster than any other consumer technology in history. These small factor devices introduce a new processing and communication paradigm, enabling end-users to access and manage a broad set of data and services, while on the move. To materialize this, a wide range of mobile applications have been developed, which are extending from entertainment and gaming to critical mobile banking and proprietary enterprise applications for accessing corporate resources.

Along with great opportunities, mobile devices reveal new attack vectors for the involved parties (i.e., users, service providers, data owners, etc.) (Mylonas et al., 2013). It is a fact that mobile devices can be easily stolen or misplaced, due to their compact size. The loss of a mobile device can lead to major privacy breach, since emails, social activities, pictures or any other stored data can be disclosed. A study in 2011, named as the lost smart phone problem (Ponemon Institute LLC, 2011), determined that in a 12-month period 142,708 out of 3,297,569 employee smart phones were lost or stolen, i.e., 4.3 percent per year. Moreover, in 2012, researchers from Symantec presented their results of the Smartphone Honey Stick Project (Wright, 2012). In this project, 50 smart phones were, intentionally, lost in cities around the U.S. and Canada.

* *Corresponding author*. Tel.: +30 2104142776.
E-mail addresses: dadoyan@unipi.gr (C. Ntantogian), apostolopoulos@unipi.gr (D. Apostolopoulos), marinakis@unipi.gr (G. Marinakis), xenakis@unipi.gr (C. Xenakis).
0167-4048/$ – see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2014.01.004

The phones were loaded with logging software, so that Symantec could keep track of all activities. The study came to the result that in the 96 percent of the cases, the finders had accessed the personal data (e.g., email, photos, etc.) that was stored in the lost devices. Moreover, on nearly half of them (43 percent), the finders had attempted to access the owners' online banking applications.

The proliferation of mobile devices has also led to the birth of mobile digital forensics, a branch of digital forensics that deals with the recovery of digital evidence or data from mobile devices, under forensically sound conditions. The latter denotes the acquisition of identical copies of the entire available evidences/data, without causing any alteration to the underlying device. Currently, most of the forensic research on mobile devices has been focused on: (i) the acquisition and analysis of the internal flash NAND memory and SD Cards; (ii) the understanding of the employed file systems; and (iii) the scrutinizing of the application files for identifying malware. However, little attention has been paid to the research on the acquisition and analysis of the volatile memory, also referred as random access memory (RAM), of mobile devices. This is the motivation of the present work, which focuses, explicitly, on the volatile memory of mobile devices. Moreover, this type of memory holds, temporary, the authentication credentials (i.e., *usernames* and *passwords*) submitted by the users to activate security critical applications (e.g., mobile banking, password managers, etc.).

Previous research has proved that forensic investigators can discover critical information in the volatile memory of desktop computers, like users' authentication credentials (Karayianni et al., 2012). Thus, it is motivating to examine if we can discover such information in the volatile memory of mobile devices. Considering that 61 percent of the Internet users reuse authentication credentials on multiple websites/services (Consumer Survey, 2012), we realize that sometimes the disclosure of a *username* and/or *password* is sufficient to compromise the privacy of all the user's applications (Mylonas et al., 2013). Especially, in case of applications that deal with sensitive data or functionality (e.g., banking, password managers, e-shopping, etc.), an exposure of authentication credentials can lead to major privacy breach.

In this paper, we investigate and evaluate through experimental analysis whether we can discover authentication credentials of mobile applications in the volatile memory of rooted mobile devices, following thirty (30) different scenarios (i.e., eleven (11) general scenarios with some time variations). We focus on mobile devices that operate with the Android operating system (OS), because it is the most widely used one (IDC Worldwide Quarterly, 2013). To perform the experiments, we follow a procedure for the acquisition of the volatile memory of rooted mobile devices, under forensically sound conditions. Throughout the carried experiments and analysis, we have, exclusively, used open-source, free forensic tools. In total, we have evaluated the privacy of thirteen (13) popular Android applications, which represent four common application categories (i.e., mobile banking, e-shopping/financial applications, password managers, and encryption/data hiding applications) that elaborate sensitive users' data. For every investigated application and each studied scenario, we have performed two set of experiments with different objective each one. In the first one, our goal was to check if we could recover our own submitted credentials from the memory dump of a mobile device. In the second experiment, the goal was to find out patterns that indicate where the credentials are located in a memory image. Overall, the contributions of this paper are as follows:

(i) Examine for each investigated application and studied scenario whether we can discover authentication credentials in the physical memory of mobile devices;
(ii) Explore in the considered applications, if we can discover patterns and expressions that indicate the position of authentication credentials in a memory dump;
(iii) Derive a set of critical observations that provide insights for the privacy of mobile applications under various mobile usage scenarios.

The rest of the paper is organized as follows. Section 2 gives background information for Android OS and the related work. Section 3 presents the procedure for the acquisition of the volatile memory of Android mobile devices. Section 4 analyzes the carried out experiments. Section 5 elaborates on the results, providing generic observations and remarks regarding the privacy of authentication credentials in Android devices. Finally, section 6 concludes the paper.

2. Background

2.1. *Android operating system*

Android is a Linux-based OS designed, primarily, for touch screen mobile devices such as smart phones and tablet computers. Since its appearance, Android followed an upward trajectory and wide acceptance, reaching triple-digit of growth for the last year (IDC Worldwide Quarterly, 2013). Today, it holds approximately 75 percent of the world market and there have been more than 48 billion of Android applications' installations so far, characterizing it as the fastest-growing mobile OS.

Android utilizes native open-source C libraries to perform OS tasks and Java as a language for developing applications. To execute them, it uses the Dalvik virtual machine (Bornstein, 2008), which creates Dalvik executable files *.dex* (i.e., byte codes from *.class* and *.jar* files), designed to be suitable for systems that are constrained in terms of memory and processor speed. Each Android application runs in a separate process within its own Dalvik instance, relinquishing all responsibility for memory and process management to the Android run time, which stops and kills processes as necessary to manage resources (http://mobworld.wordpress.com/2010/07/05/memory-management-in-Android/).

Android devices employ three different types of memory, each of which serves different purposes: (i) the volatile memory (i.e., RAM) that loses gradually its data when power is switched off; (ii) the internal, non-volatile memory that is based on NAND flash technology, which does not require power to retain data; and (iii) the external, expandable, non-volatile memory in the form of SD card. Both flash and SD card memory store the Android file system, named YAFFS2, as well as applications' and multimedia files.