Digital Investigation 14 (2015) S77–S84

Contents lists available at ScienceDirect

Digital Investigation

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

DFRWS 2015 USA

Network and device forensic analysis of Android social-messaging applications

Daniel Walnycky [a], Ibrahim Baggili [a, *], Andrew Marrington [b], Jason Moore [a], Frank Breitinger [a]

[a] University of New Haven Cyber Forensics Research and Education Group (UNHcFREG), ECECS Department, Tagliatela College of Engineering, USA
[b] Zayed University, Advanced Cyber Forensics Research Laboratory, College of Technological Innovation, United Arab Emirates

Keywords:
Network forensics
Android forensics
Instant messaging
Privacy of messaging applications
Application security testing
Datapp

A B S T R A C T

In this research we forensically acquire and analyze the device-stored data and network traffic of 20 popular instant messaging applications for Android. We were able to reconstruct some or the entire message content from 16 of the 20 applications tested, which reflects poorly on the security and privacy measures employed by these applications but may be construed positively for evidence collection purposes by digital forensic practitioners. This work shows which features of these instant messaging applications leave evidentiary traces allowing for suspect data to be reconstructed or partially reconstructed, and whether network forensics or device forensics permits the reconstruction of that activity. We show that in most cases we were able to reconstruct or intercept data such as: passwords, screenshots taken by applications, pictures, videos, audio sent, messages sent, sketches, profile pictures and more.

Introduction

Digital evidence from smartphone instant messaging applications is potentially useful in many types of criminal investigation and court proceedings. Text messages have been an important component of the evidence presented in numerous high profile cases in recent years, such as Ashby v. Commonwealth of Australia (Ashby v Commonwealth of Australia (No 4), 2012) and The State v. Oscar Pistorius (S v Oscar Pistorius (CC113/2013), 2014). In the latter, the messages concerned were not sent via Short Message Service (SMS) but by the instant messaging application WhatsApp. Applications like WhatsApp offer users a free or very low cost alternative to SMS for text messaging purposes, and frequently offer other additional features. It is therefore unsurprising that such instant messaging applications have become extremely popular, as a result of which, it is reasonable to expect that more and more cases will involve messages originally sent via such applications.

In this work we perform an experimental forensic study on twenty social-messaging applications for the Android mobile phone operating system. The sum total of the users of the tested applications exceeds 1 billion. Our study illustrates the potential for acquiring digital evidence from the mobile device, data in transit, and data stored on servers.

The remainder of this paper is organized as follows. In the "Related work" section, we discuss related work from the digital forensics and security literature. In the "Methodology" we discuss the research methodology and experimental setup. In the "Experimental results" section we provide an overview of our results, which we discuss in the "Discussion". We propose future work in "Future work" and conclude in "Conclusion".

* Corresponding author.
E-mail address: IBaggili@newhaven.edu (I. Baggili).

http://dx.doi.org/10.1016/j.diin.2015.05.009

Related work

Smartphones are typically kept in close physical proximity to their owners as compared to other potential sources of digital evidence, like computers. This enhances the potential value of digital evidence found on smartphones – suspects may interact with them continuously throughout the day and may take them to the crime scene. In addition to traces of the suspect's communications, a suspect's phone may contain evidence pertaining to their location, and with the advent of the smartphone, they may contain the same rich variety of digital evidence which might be found on computer systems (Lessard & Kessler, 2010). Mobile phones and their applications may be involved in a huge variety of criminal cases, including fraud, theft, money laundering, illicit distribution of copyrighted material or child pornographic images, or even distribution of malware in cybercrime cases (Taylor et al., 2012).

Even before modern smartphones, SMS text messages stored in the GSM SIM card were an important target for forensic examiners (Willassen, 2003). With modern smartphones, mobile applications providing messaging capability may supplement or even supplant SMS, meaning that there may be multiple message repositories on the phone for examiners to retrieve (Husain & Sridhar, 2010).

The majority of new smartphones are shipped with the Android operating system. There have been many different approaches to forensic acquisition of secondary storage of Android devices in the literature since 2009, encompassing both logical and physical acquisition, with some techniques requiring more potential modification to the Android device under examination than others (Barmpatsalou et al., 2013).

Generally speaking, logical acquisition can be performed on an Android device through various backup utilities, and requires no modification of the device or its system software. Physical acquisition techniques described in the literature, on the other hand, often require the installation of a rootkit (modifying the device's system partition) in order to facilitate full access to the device's secondary storage for acquisition through a tool like *dd*, as in Lessard and Kessler (Lessard & Kessler, 2010).

Since these rootkits are often of unknown provenance (in fact, they are most easily sourced from the hacking community), and since any modification to a device under examination ought to be minimized if not outright avoided, Vidas et al. proposed that the Android recovery partition might be more safely overwritten with a known safe forensic boot environment to facilitate physical acquisition of the remaining partitions (Vidas et al., Aug. 2011). By doing so, the system partition is not modified by the rootkit, but full access to the device's secondary storage is obtained by rebooting the device into a modified recovery mode incorporating the necessary software to perform a physical acquisition. This is similar to how a boot CD might be used to facilitate forensic acquisition on a computer system.

From a completeness perspective, physical acquisition is generally preferable to logical acquisition, as a physical image will include any data which exists in unallocated space, such as files that have been deleted but not yet overwritten. Despite this, logical acquisition can still yield significant quantities of digital evidence (Lessard & Kessler, 2010) and is still employed in many studies in the literature (Barmpatsalou et al., 2013; Al Mutawa et al., Aug. 2012; Grover, 2013).

Mobile applications for popular instant messaging or social networking platforms have been the subject of numerous studies in digital forensics literature. Early work on instant messaging applications on smartphones, such as Husain and Sridhar's study on the iPhone (Husain & Sridhar, 2010), examined platforms which were originally released for the Personal Computer (PC) either as a standalone application or via the web. Computer forensic techniques are described in the literature for the examination of artifacts from AOL Instant Messenger (AIM) (Reust, 2006; Dickson, 2006a), Yahoo! Messenger (Dickson, 2006b), other installed instant messaging applications (Dickson, 2006c; Dickson, 2007), web clients for popular instant messaging applications (Kiley et al., 2008), and instant messaging features of social networking websites such as Facebook (Al Mutawa et al., 2011).

As these instant messaging platforms from the PC world migrated to the smartphone with their own mobile applications, so did the digital forensics community move on to investigate activity traces left by these applications on mobile devices (Husain & Sridhar, 2010; Al Mutawa et al., Aug. 2012). In addition to these imports from the PC, instant messaging and social networking applications were developed primarily for the smartphone.

An example of a mobile messaging application is WhatsApp. Anglano analyzed WhatsApp on software-emulated Android devices in recent work providing forensic examiners with information about what data is stored on the Android device by the WhatsApp application, facilitating the reconstruction of contact lists and text conversations (Anglano, 2014). Most of the applications examined in this work fall into the same category as WhatsApp in that they are first and foremost smartphone applications, not PC portovers to Android.

Given the popularity of smartphones, it is not surprising that they have become targets for cyber attacks. Smartphone malware is a growing concern, and the sheer volume of mobile applications brings with it a plethora of potential attack vectors. For example, Damopoulos et al. developed malware which performed DNS poisoning on the iPhone's tethering (also known as personal hotspot) feature, and exposed important user data (such as location and account credentials) when the user employed the Siri service (Damopoulos et al., 2013). In their work on Android inter-application communication and its attendant attack vulnerabilities, Chin et al. found 1414 vulnerabilities in the top 50 paid and top 50 free applications then available for Android on what was then called the Android Market (Chin et al., 2011).

Instant messaging smartphone applications are no exception, as shown by Schrittwieser et al. who examined a set of nine popular instant messaging applications for Android and iPhone, and found vulnerabilities to account hijacking, spoofing, unrequested SMS, enumeration or other attacks on all of them (Schrittwieser et al., 2012). Especially given that smartphones contain so much personal information, it is clear that such threats to their security pose serious risks to user privacy.