Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Digital evidence from mobile telephone applications

Mark Taylor [a], *Glyn Hughes* [a], *John Haggerty* [b], *David Gresty* [c], *Peter Almond* [a]

[a] *School of Computing and Mathematical Sciences, Liverpool John Moores University, UK*
[b] *School of Computing, Science and Engineering, University of Salford, UK*
[c] *Independent Computer Forensic Analyst, London, UK*

Keywords:
Forensic investigation
Digital evidence
Mobile phones
Hacking
Malware
Money laundering

ABSTRACT

In this paper we examine the legal aspects of the forensic investigation of mobile telephone applications. Mobile telephone applications might be involved with a variety of types of computer misuse including fraud, theft, money laundering, dissemination of copyrighted materials or indecent images, or instances where mobile telephone applications have been involved in the transmission of malware for malicious or criminal purposes. In this paper we examine the process of the forensic investigation of mobile telephone applications, and the issues relating to obtaining digital evidence from mobile telephone applications.

1. Introduction

As more online retailers introduce mobile e-commerce applications, and more individuals use banking services via their mobile telephone, criminal hackers are increasingly targeting mobile telephone operating systems (Leavitt, 2005). Although there is continuing effort made to secure mobile payments, coordination between mobile payment developers, device manufacturers, and mobile operating system platform developers can be difficult, and hackers may take advantage of such. In addition, organisations are beginning to provide mobile telephone applications for use by some of their employees, which may be misused (Lawton, 2008). As well as commonly used applications such as email, organisations may also provide more specific applications such as stock control or fault reporting via mobile telephones for their employees. A recent crystal ball mobile telephone application allows managers to monitor employees' locations, incoming and outgoing telephone calls and messages, and internet traffic via the employee's company mobile telephone (Crystal ball, 2011).

Mobile telephones may incorporate a microprocessor, flash memory (which may be internal or attached to the device), read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, a liquid crystal display (LCD), and a SIM (Subscriber Identity Module) card (which has information pertaining to geographic location and account information). The operating system (OS) of the device is held in ROM, which with the proper tools typically can be erased and reprogrammed electronically. Random access memory which may be used to store user data by certain models of mobile telephones is kept active by batteries, whose failure or exhaustion would cause that information to be lost. Types of mobile telephones currently in use by organisations and individuals include basic telephones that are primarily simple voice and messaging communication devices; advanced telephones that offer additional capabilities and services for multimedia; and smart telephones or high-end telephones that merge the capabilities of an advanced telephone with those of a personal digital assistant.

The basic and advanced mobile telephones typically use a company proprietary operating system. Typically mobile smart phones use one of the following operating systems: Android, Symbian, Apple, RIM, Microsoft, or Bada (Edwards, 2008). Unlike the more limited, real-time kernels used in basic and advanced mobile telephones, these operating systems are multi-tasking and designed specifically to match the capabilities of high-end mobile devices.

With regard to attempting to prevent misuse of mobile telephone applications, Enck et al. (2009) discussed the security

0267-3649/$ – see front matter © 2012 Mark Taylor. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.03.006

enforcement approaches that can be used to protect mobile telephone applications and data for Android mobile telephones. In the general case, each Android mobile telephone application runs as a unique user identity, which can assist in limiting the potential damage of programming flaws. Application designers can assign the application a given collection of permissions to restrict access to software components.

Mobile telephone applications might be involved with a variety of types of computer misuse including fraud, theft, money laundering, dissemination of copyrighted materials or indecent images, or instances where mobile telephone applications have been involved in the transmission of malware for malicious or criminal purposes. In this paper we examine the process of the forensic investigation of mobile telephone applications, and the issues relating to obtaining digital evidence from mobile telephone applications.

2. Investigations of misuse involving mobile telephone applications

2.1. *Obtaining and disseminating confidential information*

Individuals and criminal gangs may use mobile telephone applications in order to obtain and misuse confidential information. Often mobile telephone users will store information on their telephone that could be used for identity theft (Higgins et al., 2008; Curran et al., 2010). In the UK, mobile telephone identity fraud increased by over 70 per cent in 2009 (Directgov, 2010). Types of personal confidential data stored on mobile telephones might include bank account details, PIN numbers and passwords (Furnell et al., 2008). Employees may download confidential corporate information such as company documents and spreadsheets or customer information on their company mobile telephones or their own personal mobile telephones. Downloading could be wired using the USB adapters, wirelessly using local wi-fi access, Bluetooth or even across a Virtual Private Network from anywhere in the world using GSM. Physical methods for stealing confidential data from an organisation using a mobile telephone could be a simple as a user typing sensitive data into a 'notes' facility on the mobile telephone, a dictaphone capability or even the commonly equipped camera facility.

2.2. *Fraud, theft and money laundering*

Given the increasing use of mobile telephone applications for banking services and for e-commerce transactions, these types of mobile telephone applications are increasingly being targeted by criminal gangs for fraud and theft. If an investigation of mobile telephone application misuse involved suspected or detected money laundering (MLR, 2007), then the matter would have to be reported to the police.

2.3. *Dissemination of malware*

There is increasing concern regarding the threat from malware for mobile telephones for both organisations and individuals (Lawton, 2008; Shih et al., 2008). While still small compared to the volume of personal computer malware, some companies have already launched antivirus products which scan and remove malicious applications from mobile telephones. Mobile telephone spyware has been a concern for some time. Legitimate software companies already provide mobile telephone applications that allow the user to monitor a spouse, children, or employees (Crystal ball, 2011).

Cyber criminals are increasingly exploiting vulnerabilities in smartphone operating systems to infect or takeover mobile telephones. Trojan horse programs are a common form of smartphone attack. These are smartphone applications that seem like legitimate downloads from online application stores, but which actually contain malicious code able to harm or takeover a mobile phone. Sections 125 and 126 of the UK Communications Act 2003 (COMA, 2003) might apply if a person was using a mobile telephone to dishonestly obtain an electronic communications service.

In some instances organisations might investigate the use of mobile telephone applications by employees when malware such as computer viruses, worms, Trojan software, and spyware infects the organisation's computer network after being downloaded across the Internet. Dissemination of malware via mobile telephone applications is covered by the UK Computer Misuse Act 1990 (CMA, 1990) sections concerning modification of computer materials, or unauthorized access with the intent to commit or facilitate the commission of further criminal offences such as theft or fraud. The dissemination of malware via mobile telephone applications might also be covered by the UK Police and Justice Act 2006 (PJA, 2006) in terms of the making, supplying or obtaining articles for use in computer misuse offences.

2.4. *Capture, storage and dissemination of indecent images*

Mobile telephones have increasingly been used with regard to indecent images (Beech et al., 2008; Childnet, 2004). Investigations of misuse of mobile telephones may concern the capture, storage and dissemination of indecent images (Gerald Bourne, 2011). If an organisation investigating the misuse of mobile telephone applications by employees suspected or detected the downloading or dissemination of indecent images by employees, then the matter would have to be reported to the police.

2.5. *Copyright infringement*

Organisations such as the Federation Against Copyright Theft (FACT, 2011) may contact individuals or organisations that have been involved in downloading or disseminating copyrighted material without the consent of the copyright holder via mobile telephones (Goode, 2010). The UK government through the UK Digital Economy Act 2010 (DEA, 2010) has developed legislation that will impose obligations on Internet Services Providers (ISPs) to send notifications to subscribers alleged by rights holders to be infringing copyright, and to monitor the number of notifications with which each subscriber is associated. The UK Digital Economy Act 2010 legislation will also oblige ISPs to make such notifications data