Multimedia Systems
DOI 10.1007/s00530-010-0216-7

REGULAR PAPER

Potential cyberterrorism via a multimedia smart phone based on a web 2.0 application via ubiquitous *Wi-Fi* access points and the corresponding digital forensics

Hai-Cheng Chu · Der-Jiunn Deng · Han-Chieh Chao

Abstract Cyberterrorism has become a hotly debated research issue in the past decades because of the convergence of mobile computing powers and the fledging multimedia communication computing capabilities. Cyberterrorism is the exploitation of computer network tools to incur malfunction or shut down critical infrastructures with several keyboard punches, which is dramatically different from traditional terrorism. Due to the ubiquitous multimedia communication tools, they have radically transformed the ways concerning data transmission. Unfortunately, it also incurs unprecedented opportunities for committing cyber crimes that we were not able to foresee two decades ago. Undoubtedly, the mushrooming proliferation of mobile phones spectacularly triggers the information security leakage while most people heavily rely on mobile phones for daily communication. As cybercrime or cyberterrorism surges, digital forensics (DF) of mobile communication devices still enormously lags behind than computer forensics. Hence, in this research paper, we provide a hypothetical case review concerning the DF of a potential cyberterrorist attack that was triggered by a mobile multimedia smart phone utilizing a popular web 2.0 application program via ubiquitous *Wi-Fi* access points. The corresponding DF of the mobile device was conducted in a step-by-step manner as well as the crime scene reconstruction based on the digital evidence collected, analyzed, and preserved.

Keywords Cyberterrorism · Mobile multimedia computing and embedded systems · Digital forensics · Web 2.0

1 Introduction

Due to unparalleled rapid growth of ubiquitous communication technologies and the shrinking physical size of portable communication devices, voluminous individuals are carrying more than one mobile phone from leisure motivation to business purpose globally. Undoubtedly, the mushrooming proliferation of mobile phones in our societies spectacularly changed the ways of communication. Evidently, these mobile communication devices become portable data carries. Under such circumstances, the data stored in those devices could be more confidential than those deposited in desktop computers. Currently, mobile phones outsell personal computers several times in the global market. Nevertheless, the digital forensics (DF) of mobile communication devices still enormously lags behind that of computer forensics [1].

Unfortunately, these cutting-edge mobile communication gadgets became the utilities for committing heinous criminal incidents in the modern society by sophisticated

H.-C. Chu
Department of International Business,
National Taichung University of Education,
Taichung, Taiwan, R.O.C
e-mail: hcchu@mail.ntcu.edu.tw

D.-J. Deng
Department of Computer Science and Information Engineering,
National Changhua University of Education,
Changhua, Taiwan, R.O.C
e-mail: djdeng@cc.ncue.edu.tw

H.-C. Chao (✉)
Institute of Computer Science and Information Engineering,
National Ilan University, Ilan, Taiwan, R.O.C
e-mail: hcc@niu.edu.tw

H.-C. Chao
Department of Electrical Engineering,
National Dong Hwa University, Hualien, Taiwan, R.O.C

Published online: 14 November 2010

technology-savvy perpetrators. Hence, cellular phone data is significantly approved as the probative evidence in US courts. Compellingly, this handheld multimedia communicating device is one of the most multitalented masterpieces of equipments ever invented for human beings. The vast range of the above illegal behaviors could range from negligible online pranks to devastating cyberterrorist attacks. Nowadays, some mobile multimedia communication devices are indisputably acting as mini portable computers.

Indeed, mobile multimedia communication devices are being applied in a mixture of distinct arenas. Unsurprisingly, more and more people utilize mobile phones to directly transfer money between accounts by the virtue of the current banking systems due to the portability, scalability, usability, and the interoperability of modern mobile phones. Generally speaking, a smart phone is a mobile phone with more features encompassing the functionalities of sending short message service (SMS) or e-mails, playing audio/video clips, taking snapshots or recording videos, conducting instant message (IM), and surfing on the Internet. In addition, the add-on content management software packages can deal with personal calendars and address books. Manifestly, countless users store a wealth of critical information within these mobile multimedia communication devices than desktop computers especially in some criminal cases. Therefore, the DF of the above devices plays a crucial role in a cybercrime investigation. Simultaneously, huge amount of smart phone application programs (APs) are being developed in a rapid pace encompassing word processors, spreadsheets, and database utilities.

Apparently, the diversity of the embedded OS in mobile multimedia communication devices makes the DF of mobile phone more difficult then desktop computers. Therefore, investigating smart phones is one of the most challenging tasks in DF realm with respect to those cutting-edge devices. Due to the variety of smart phone manufactures and the corresponding embedded OS being deployed, it is hard to have a single standard for how and where smart phones store messages although many smart phones exploit similar storage schemes. Unlike most people who start scrolling through contact lists, most recent incoming/outgoing calls, or missed calls, this paper suggested the general criteria for the anti-cyberterrorist squad team or the DF practitioners to ponder when they deal with the unprecedented cyberterrorist attacks via the smart phones. Investigating cell phones or mobile devices is one of the most challenging tasks in DF. Proper search and seizure procedures for cell phones and mobile devices are as important as those for computers. Cyberterrorist attacks by means of smart phones is an imminent and urgent issue.

Cyberterrorism has become a hotly debated research issue in the past decades because of the convergence of mobile computing powers and the fledging multimedia communication computing capabilities. Without loss of generality, cyberterrorism is the exploitation of computer network tools to incur malfunction, cripple, or shut down critical infrastructures such as energy, transportation, and government operations [2–5]. Traditional terrorist or extremist attacks launched devastating attacks in metropolitan areas with deadly explosive materials. Nowadays, modern terrorists are capable of executing traditional terrorist behaviors via state-of-the-art ubiquitous multimedia communication tools, which radically transform the way we live and provide unprecedented opportunities for committing cyber crimes that we were not able to foresee two decades ago [6, 7].

Corollary, the modern terrorist attacks could impose catastrophic slaughter or injury upon civilians, corporations, and the governments by just several keyboard punches in a public café and the unscrupulous syndicate are physically thousands of miles away from those critical infrastructure systems, which range from water-treatment stations to chemical disposal plants. The critical infrastructure systems provide the fundamental functionalities for governments and industry operators in most cases. Crucially, protecting national critical infrastructure assets from cyber attacks is an extraordinarily challenging task for the governments worldwide.

For every mobile phone, the user can often find a unique ID embedded on the printed circuited board beneath the battery pack. The ID is known as international mobile equipment identity (IMEI). This exclusive identifier is assigned to every GSM, WCDMA, and iDEN mobile phone, as well as some satellite phones. The IMEI number is capable of exclusively identifying a specific mobile phone being used in a cellular network. Demonstrably, the law enforcement agencies can use this number to query the mobile carriers for detailed reports of the wireless communication concerning a distinct subscriber during a certain time period as probative evidences in a court of law.

The essence of the paper was to provide the law enforcement agencies as well as the DF practitioners with appropriate knowledge and procedures respecting the criminal incident using smart phones via the case review we constructed in this research. The paper suggested solid guidelines for them to collect, analyze, submit, and preserve those probative digital evidences concerning the cybercrimes exploiting smart phones.

We organized the paper as follows. In Sect. 2, we briefly reviewed the related research of portable electronic communication devices, especially the smart phones. In Sect. 3, we conducted a potential cyberterrorist attack review with step-by-step approach. In Sect. 4, we reconstructed the

hypothetical cyberterrorist conspiracy and performed a comprehensive analysis and discussion of the scenarios. Finally in Sect. 5, we stated the conclusion of our paper.

2 Related researches of portable electronic communication devices forensics

2.1 Computer forensics and the DF of smart phones

In the recent decade, computer forensics has become much more emphasized by law enforcement agencies to deal with thriving cyber crimes. If we state computer forensics in a generic manner, it encompasses the procedure of identification, collection, extraction, preservation and interpretation of the digital data that was present concerning a computer incident or confidentiality breached. The above serial procedures are considered to the standard operating procedures (SOP) with respect to the mushrooming cyber crimes. Similar domain knowledge and concepts can be adopted into mobile DF arena. Digital evidences are easily compromised or contaminated during related procedures. Hence, making image files of the RAM or internal/portable storages will be the decent strategy to fulfill the goal of DF.

The pervasive usage of mobile telecommunication devices has been exponentially expanded. Obviously, ubiquitous mobile networks have dramatically shifted the ways of communication in contemporary era. Mobile phones are utilized throughout the world in record numbers and their versatile functionalities rival those of desktop computers in many aspects. This prevalence will unquestionably link them to a greater number of crimes where they definitely play a critical role [8]. Mobile phones contain an overabundance of information in the handsets and the subscriber identity module (SIM) cards implanted within the handsets. SIM cards are commonly found in GSM devices and consist of a microprocessor and electronically erasable programmable read-only memory (EEPROM) with capacity ranging from 16 kB to 4 MB.

Generally speaking, the utilization of the SIM card encompasses from identifying the subscriber of the telecommunication network, storing personal information or service-related information, and address books as well as messages. Regrettably, the ever growing technology brings negative impacts in furtherance of criminal conspiracies. Mobile phones often play an essential role regarding certain criminal cases. There are a number of DF toolsets for downloading the SIM data in a forensically sound manner. These toolsets include forensics examination, SIM readers, and the manufacturer's tools. Currently, *PhoneBase*, *SIMIS*, *Paraben's Device Seizure*, and *Oxygen Forensic Manager* are the popular DF toolkits commercially available [9]. The above toolsets may utilize special cables, *Wi-Fi*, *Bluetooth*, or *Infrared* to extract stored data from modern handsets. The collective digital trails are probative evidences in a court of law concerning criminal cases in the United States. There is no doubt that those DF toolsets must provide flexible functionalities and sustain reliability during the associate DF investigations.

Without loss of generality, a mobile phone is also referred to as a cellular phone. As communication technology keeps progressing, small scale digital device forensics (SSDDF) is an extremely new research arena for scientists and the associate researchers, who are in dire need of directions. The small and versatile nature of the appliances makes these multimedia handheld communication devices difficult to be identified and investigated [10]. In the mobile phone realm, the personal digital assistant (PDA) is another technical breakthrough for mobile communication devices. As the functionalities of a modern PDA increase, this also stimulated the migration to the emergence of a smart phone. Hence, a smart phone could be considered as a PDA with the cellular communication capability embedded. The hardware of a smart phone consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone, a speaker, a keypad, a camera, GPS function, and the touch screen. Most smart phones have removable memory cards, where precious intangible digital data will be stored.

Contemporary smart phones usually have two or more of the following communication interfaces: GSM, GPRS, and UTMS embedded functionalities for long-distance communications. In the meanwhile, they use *Bluetooth*, *IrDA* (*Infrared Device Application*), and *Wi-Fi* (*Wireless Fidelity*) for short distance data transmission. Basically, they utilize three memory locations to store the data to be acquired: the SIM card, the memory card (MMC or SD), and the internal memory, which is composed of a unique block memory chip [11–14]. Typically, cellular phones store system data in EEPROM, which enables mobile carriers to reprogram phones without having to physically access memory chips. The OS is permanently burned in the ROM, which is the nonvolatile memory.

Fundamentally, smart phones are mobile phones with additional sophisticated functionaries equipped that are similar to those of desktop computers. As technology keeps progressing, the miniaturized multimedia handheld communication devices are capable of storing massive amounts of information with less consumption of battery power. Therefore, the overall performance of a smart phone represents miniature desktop computers with respect to the embedded or add-on APs. At the moment, a smart phone is the representative of modern handheld mobile multimedia communication devices with heterogeneous hardware design and the corresponding operating system (OS) being installed. The OS of a smart phone also spectacularly