MOBILE DEVICE FORENSICS AND CRYPTOGRAPHY

Students: Allyn Stott, Brett Kaplan, Sean Flannery, Dina Zotkina
allynstott@gmail.com, kaplanb1@gmail.com,
stk35876@go.stockton.edu, dinylya13@yahoo.com
Co-Advisors: A. Taneja, C. Tyska, S. Herath
Principal Advisor: Ajantha Herath
The Richard Stockton College of NJ, Pomona, NJ 08240

ABSTRACT

Organized cyber-criminals are launching a growing number of attacks on enterprise IT infrastructures with sophisticated threats. Using emails, instant messaging, and social networking sites, users are targeted with attractive but harmful content-based attacks that can bypass traditional network defenses to put critical resources at risk. Cryptography becomes more important as our need to ensure information and security increases. Similar to the increasing need for cryptography is our growing need to address criminal evidence acquired from these high tech devices. In this paper, we will examine how cryptography relates to the digital forensic analysis of mobile devices like mobile phones, smart phones, personal digital assistants (PDAs). Our approach will examine how cryptography is implemented in mobile technologies, how mobile device forensic investigators examine these devices, and how cell phone bugging and examination has been implemented in the past.

INTRODUCTION

Everyone has a cell phone. With handheld digital devices being so prevalent in our society, there is a growing need to address crimes relating to these mobile devices. Since many crimes involve some sort of communication, the assessment of these devices is rising in importance. The mobile devices often store highly sensitive information. A business executive may have company secrets or personal information stored on his mobile device. In order to address this issue of security, encryption is becoming more common on mobile devices.

Encrypting these mobile devices not only protects the innocent, but also the guilty. In this paper, we discuss the forensic procedures that forensic investigators must go through to obtain access to an encrypted Subscriber Identity Module (SIM) card. Also, we will discuss how investigators use cell phone bugging to obtain live information in the case of the Athens Affair.

ENCRYPTION OF MOBILE DEVICES

Portable media devices are now main stream. These devices have large storage capacities and are inexpensive. They can hold a large music collection or someone's entire college writing portfolio easily, with room to spare. The data stored on portable media devices is valuable and often confidential. Protecting this data is extremely important in both the personal and business sector. One of the ways to protect this data is to use encryption.

Cell phones fall under the category of portable media devices. There are millions of them in use all over the world today. They contain information like contact

information, call logs, and short message service (SMS) messaging logs [2]. Personal information and files can now be sent and received as more people are accessing email and utilizing smart phones as laptop replacements. Most cell phones are unencrypted. For instance, SIM cards on cell phones can easily be read and copied to obtain personal information and communication logs using free software called SIMbrush [3].

Like cell phones, the majority of portable devices do not have any native encryption methods [6]. Some flash-based disk drives and external hard drives have encryption software but it is normally proprietary, poorly implemented, and non-scalable. There are also some commercial software solutions available. These products will encrypt portable devices but often the solutions require costly infrastructure only feasible for businesses and are therefore too expensive for most personal devices [6].

Another issue with portable device encryption is user awareness. Even if native support were included and functioned well, the majority of users probably would not know how or when to use it. Furthermore, many users simply would not know what encryption was anyway. For this reason, the adoption of encryption for portable devices is gradual.

Businesses should be concerned about the growing number of portable devices and the lack of encryption. The amount of money lost due to compromised portable media devices is staggering. On average, companies have lost $226,000 to $22 million dollars because of lost sensitive data [6]. In the business world, the biggest threat to sensitive data is the employee. People who have access to the information are the ones who are most likely to lose it. A lack of encryption on systems will lead to an increasing threat of information lost or stolen by way of portable devices.

Portable media devices can be easily used for criminal acts. These devices are small and inconspicuous. They are easily hidden and transfer data very quickly making large acquisitions simple and fast. The storage capacity of many of these devices is over 100GB and their cost is relatively low making them dangerous tools in a sensitive environment.

Steps in the right direction are happening in new operating system software like Window Vista and Windows 7. Currently Microsoft Corporation offers a version of their Vista operating system with Bitlocker encryption built-in. However, it is not enabled by default and it is sold as the higher-priced “Business Edition” which may not appeal to the majority of home users. Pretty Good Privacy (PGP) encryption software is available free but setup is often too difficult for casual users to handle.

The biggest hurdle to overcome for adopting encryption techniques is education. The next hurdle is getting companies to invest in implementations for their respective devices and creating standards for portable devices themselves. Rules and policies concerning portable and mobile devices should be determined beforehand to ensure company privacy and overall protection of information.

MOBILE DEVICE FORENSIC TOOLS

In mobile devices, one of the most common digital networks, and the current standard in Europe and Asia, is the Global System for Mobile (GSM) Communications These networks are used by companies like Cingular AT&T and T-Mobile. GSM devices most commonly use SIM cards [11]. These SIM cards are extremely resilient to various conditions since they are usually well protected by the device. SIM cards area also able to

withstand temperatures up to ~450℃, the approximate maximum temperature of a house fire at desk height [8].

A SIM card is vital in the storing of information. It stores information about the subscriber like language preference which can help in determining the subscriber's nationality. It holds the list of the calls originating from the user. It holds the speed dial lists which are usually the most called numbers. This allows an investigator to see who the user is in contact with the majority of the time. The SIM card makes it possible to read every SMS message sent. More importantly, the investigator is able to determine time frame as messages contained received time as well as the status of messages sent [2]. So, not only can the investigator see what text messages were sent, but also if they were received. Besides other personal information, the SIM card also holds information about where the subscriber last registered the system, charge information, and the services enabled on the device. Table 1 gives a comparison of standard features on three levels of mobile phone devices: basic, advanced, and smart. The type of mobile phone will affect what type of evidence will need to be retrieved and analyzed.

Table 1: Software Characterization [7]

	Basic	**Advanced**	**Smart**
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS, Symbian
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook and Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds (Enhanced Text)	Text, Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP Server
Web	None	Via WAP Gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi

All of this information about the SIM card does not actually define a SIM card. A SIM card is a contact based smart card [2]. The importance of this definition is the security related to smart cards can now be related to SIM cards. These definitions are broken into four main meanings: confidentiality, authentication, integrity, and non-repudiation [3]. Confidentiality implies that the user's privacy is (almost) guaranteed by the encryption of voice and data information, implemented by cryptographic algorithms, traveling over airwaves and network lines. Authentication implies that no unauthorized user can gain access to the system. Integrity is definitely implemented because without it

a user would be able to change charge values which would cause major problems for the service provider. Non repudiation verifies that the since the recipient has received a particular message, that message holds binding force [2]. With all this available evidence it is clear that these SIM cards hold a great deal of valuable information for a forensics investigator.

Many digital forensics tools are not easily available and are either very expensive or only available to law enforcement agencies [2]. Open source tools that are forensically sound are a benefit not only for cost purposes, but because when source code is available it makes it easier for an expert witness to determine whether the tool uses a procedure and technique that is generally accepted in the forensic processing of data [1]. Some mobile forensic tools make data extraction possible without the use of a computer. Cellebrite's Universal Forensic Extraction Device (UFED) is a standalone device that can be carried in a carrying case so field extraction is possible [4]. The UFED support 95% of mobile phones and connects to all known connection interfaces including serial, USB, infrared, and Bluetooth [4]. Cellebrite works specifically with mobile phone providers to ensure continued support of all models. Tools such as the UFED are especially useful considering how many mobile phone models are produced each year.

MOBILE PHONE CRIME

Mobile devices not only hold a lot of information that is beneficial to forensic investigators, but they also wield a lot of power that criminals can abuse if encryption is not properly implemented. As with the case of the "Greek Watergate" where the Prime Minister of Greece and 100 other foreign defense and public order ministers had their mobile phones tapped during the time of the 2004 Athens Olympics [9]. Using illegally implemented software, the perpetrators were able to "bug" these mobile phones for months at a time [13]. The software code on the phones allowed for the use of wiretapping even though it was not implemented. The management system was not properly encrypted allowing the criminals to exploit the code leading to one of the first major infiltrations involving cell phones [13]. Poor software management could also lead to illegally obtaining personal details and abuse of disabled services [15].

Mobile phones also play a large role in communications related to illegal activity. Mobile phones are the most common form of communication used when people purchase illegal substances such as heroin, methamphetamines, and cocaine [10]. In South Korea, late 2004, subscriber information was stolen from a mobile phone carrier allowing the thief to create duplicate phones [10]. With these phones, purchases were made from the Internet using the stolen accounts.

MOBILE DEVICE FORENSIC EXAMINATION

The goal of a digital forensics investigation is to obtain and analyze digital information using a forensically sound method to be used as evidence in civil, criminal, or administrative cases [11]. It is important to emphasize that the purpose of digital forensics is not simply to obtain data, but to do so in a forensically sound method. Many of the tools available to digital forensic investigators are not appropriate for use in an investigation because they are not forensically sound.

Mobile devices vary widely in their capabilities. When a mobile device is recovered for forensic analysis, a forensic examiner can extract various types of data that

will benefit an investigation. Mobile devices such as cell phones are often found on the scene of an incident or crime because of their extensive use. Proper procedures should be followed when gathering evidence. For example, devices found turned on should not be turned off to avoid losing information stored in the mobile device's RAM [5].

In order to gain a better understanding of digital forensics, we took a tour of the New Jersey Regional Computer Forensics Laboratory (NJRCFL) on December 9, 2008, where we were given a detailed presentation on digital forensic investigation procedures and a tour of their facility. The NJRCFL opened in November 2004 and has handled more than 7,000 items of evidence and processed over 131 terabytes of data [12]. It is the first digital forensic laboratory in the northeast to have earned accreditation from the American Society of Crime Laboratory Directors-Laboratory Accreditation Board (ASCLD-LAB) in the Digital and Multimedia Discipline in both the computer and video sub-disciplines [12].

At the NJRCFL, a Faraday cage (an enclosed area covered with conducting material in order to block out external static electrical fields [14]) had been built. This cage blocked all network signals while the mobile devices were left on and charging. We were informed by our tour guide that people would try to overwrite the previous calls stored on the device by calling the phone repeatedly until all the convicting evidence was erased. It is imperative that mobile devices found as evidence be immediately blocked from their network signals. We analyzed various materials that can be taken easily and inexpensively into the field. Our results showed that a simple tin can, like one used for canned soup or paint, works as a very convenient and effective portable Faraday cage.

CONCLUDING REMARKS AND FUTURE RESEARCH

More and more portable devices are being produced all the time and they are reaching the hands of both educated and uneducated users. While these devices are convenient and useful tools, they are also very dangerous. It only takes one lost laptop with credit card information to adversely affect thousands of people. It is absolutely essential for encryption to become a standard on portable devices to protect data. Also, as these devices become more useful to criminal investigators, more tools that follow acceptable forensic procedures will need to be made available.

Digital crime will continue to rise as the use of networked electronic devices increases. The field of digital forensics must continue to expand in order to meet the growing digital crime rate. Future research will need to clearly define how data extraction tools should be implemented in order for them to produce forensically sound evidence. Without this research, digital forensics will not be able to hold up in court and the legal process of digital evidence will be brought into question.

ACKNOWLEGEMENTS

This project was funded by the Richard Stockton College Board of Trustees Fellowships for Distinguished Students. We have to thank the New Jersey Regional Computer Forensic Lab and detective David Costantino for their continued support beginning from 2004. We also wish to acknowledge the helpful guidance of the faculty advisors as they were an enormous asset to us. This project would not be successful without the strong encouragement, motivation, and guidance of Dr. Ajantha Herath.

REFERENCES

1. Carrier, Brian, Open source digital forensics tools: the legal argument, @*stake*, Research Report, Oct. 2002.
2. Casadei, F., Savoldi, A., Gubian, P., Forensics and sim cards: an overview, *International Journal of Digital Evidence*, 5, 20-21, 2006.
3. Casadei, F., Savoldi, A., Gubian, P., SIMbrush: an open source tool for gsm and umts forensics analysis, *Proceedings of Systematic Approaches to Digital Forensic Engineering, First International Work-shop, Proc. IEEE*, 105-119, 2005.
4. Cellebrite Mobile Data Synchronization, http://www.cellebrite.com/UFED-Standard-Kit.html, retrieved November 1, 2008.
5. Gratzer, V., Naccache, D., Znaty, D., Law enforcement, forensics and mobile communications, *Proceedings of the Third IEEE International Workshop on Pervasive Computing and Communication Security*, IEEE Press, 256-260, 2006.
6. Heikkila, F., Encryption: security considerations for portable media devices, *IEEE Security and Privacy*, 2007.
7. Jansen, W., Ayers, R., Guidelines on cell phone forensics, *NIST Special Publication 800-101*, www.csrc.nist.gov, May 2007.
8. Jones, B.J., Kenyon, A.J., Retention of data in heat-damaged sim cards and potential recovery methods, *Forensic Science International*, 2007.
9. Kyriakidou, Dina, "Greek Watergate" scandal sends political shockwaves, www.tiscali.co.uk/news/, March 2, 2006.
10. McCarthy, P., Forensic analysis of mobile phones, http://esm.cis.unisa.edu.au/ new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf, 2006.
11. Nelson, B., Phillips, A., Enfinger, F., Steuart, C., *Guide to computer forensics and investigations*, 3rd ed., Boston: Course Technology, 2008.
12. New Jersey RCFL: Regional Computer Forensics Laboratory, www.njrcfl.org, retrieved November 1, 2008.
13. Prevelakis, V., Spinellis, D., The Athens affair, *IEEE Spectrum*, www.spectrum.ieee.org, July 2007.
14. Wikipedia, Faraday cage, Nov 2008, http://en.wikipedia.org/wiki/Faraday_cage, November 29, 2008.
15. Wong, Ken, Mobile phone fraud -- are gsm networks secure?, *Computer Fraud & Security*, 11-18, February 1996.