Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2007

Profiling Through a Digital Mobile Device

Lee Fueng Yap
British Telecommunications

Andy Jones
British Telecommunications

Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/5

Profiling Through a Digital Mobile Device

Lee Fueng, Yap[1] Andy, Jones[2]

[1]British Telecommunications plc.
Asian Research Centre, Kuala Lumpur, Malaysia
[2]British Telecommunications plc.
Security Research Centre, Ipswich, United Kingdom;
Adjunct, Edith Cowan University, Perth, Australia

[1]leefueng.yap@bt.com, [2]andrew28@bt.com

Abstract

Mobile digital devices have evolved from telecommunications device to a lifestyle product over the years. These devices are used in all aspects of our daily life. As a result, more information is stored within the devices. Unprotected mobile digital device is susceptible to privacy invasion attack when the device falls into the wrong hand of any unscrupulous third party. The main objective of this paper is to provide an implication analysis on the possible risks of information leakage through digital mobile devices, in the case when users forget to, or choose never to apply any security protection to their devices

Keywords

Profiling, mobile devices, security protections

INTRODUCTION

In this modern era, digital mobile devices such as cellular phones and personal digital assistances (PDA) play a crucial role in all aspects, personal and business, of our daily life. The widespread usage of these devices in today's society is mainly due to the advancement of a range of technologies that enable the creation of an enhanced user experience. This includes faster and cheaper communication access technologies and cheaper and more powerful digital mobile devices in terms of processing speeds and storage capacities. Over the years, mobile digital devices have transformed from the most fundamental voice-base communication gadget into a multi functional device that incorporates a camera, multimedia player, personal organiser, file storage system, text editor and web browser functionalities. With these capabilities, increasing volumes of data are being stored and exchanged between the mobile digital devices. Hence, mobile devices have become a gold-mine for the forensic investigator in serious crimes investigations (Williams 2007) because of the possibility that useful evidence can be obtained or recovered from these devices.

Form Factor	2004	2005	2006	2007	2008	2009	2010
Clamshell	109,539.6	205,741.3	301,108.8	357,477.9	390,069.9	429,105.9	470,929.5
Candy bar	563,720.0	597,148.6	652,560.9	686,317.7	713,339.2	770,832.4	826,272.2
Slider	857.3	12,524.9	29,994.7	50,164.5	69,681.5	90,310.6	110,251.8
Other	-	1,116.5	4,544.8	8,638.6	13,365.6	19,254.6	23,328.9
Total	**674,116.9**	**816,531.3**	**988,209.2**	**1,102,598.7**	**1,186,456.2**	**1,309,503.5**	**1,430,782.4**

Source: Gartner Dataquest (March 2007)

Figure 1: Forecast of Sales of Mobile Devices to End Users, by Form Factor, Worldwide, 2004-2010 (Units of 1000)

According to the recent mobile device sales forecast by Gartner (2007), it is estimated that by year 2010, the total number of mobile device sold worldwide will reach 1.4 billion. As more people will be using the digital mobile device for multimedia communications, and e-commerce application, more critical information will be stored in the digital mobile device. Consequently more information can be obtained and recovered from the devices if sufficient security features have not been installed or implemented in these mobile devices.

This paper provide an implication analysis on how the information recovered from a totally unprotected second hand mobile device could be use to profile the owner of the mobile device and his other close contacts. Section 1 of this paper briefly discusses the digital mobile devices usage models evolution and the projected future of digital mobile devices adoption. Section 2 discusses the general public awareness towards the importance of protecting the information stored in their digital mobile devices and briefly goes through the existing technologies which can be used for information protection. Section 3 introduces the potential security implications towards the corporate and individual when no security protection discussed in section 2 is being implemented in the digital mobile devices. One real example is used to illustrate the type of information that could be collected, analysed and inferred from an unprotected digital mobile device. Finally, section 4 concludes the paper with a discussion on the creation of security awareness among digital mobile devices users in order to assist them in the protection of both their personal information and their corporate business secrets.

SECURITY AND MOBILE DIGITAL DEVICE

By default, information stored in most of the digital mobile devices is not protected against any privacy infringement action. This indicates that anybody who is able to get hold of the unprotected mobile device will be able to retrieve virtually every bit of information that resides within the digital mobile device. The information captured includes, but is not limited to, Short Message Service (SMS) and email history, business and private contacts information, calendar information, call histories and stored data such as images and files. The information may also include the owner's private data, social behaviour and social contacts. (Yap, Jones 2006) If used appropriately, the information could be enough to profile and finally track down the owner.

The most fundamental way to protect Global System for Mobile communications (GSM) based digital mobile device from information leakage in the event of the loss of one's mobile phone is through the setting of both the Subscriber Identity Module Personal Identification Number (SIM Pin) and device based power-on password or most frequently known as the security code (GSM Security 2006). These two security passwords aim to provide different level of protection to the mobile device users. The main motivation of setting the SIM Pin is to protect the SIM card from illegal access while the security code plays an important role in refraining unauthorized third party to use the mobile device even when a new SIM card is inserted into the mobile device's SIM slot. SIM pin and security code are commonly made up of four digits that are configurable by the owner of the mobile device.

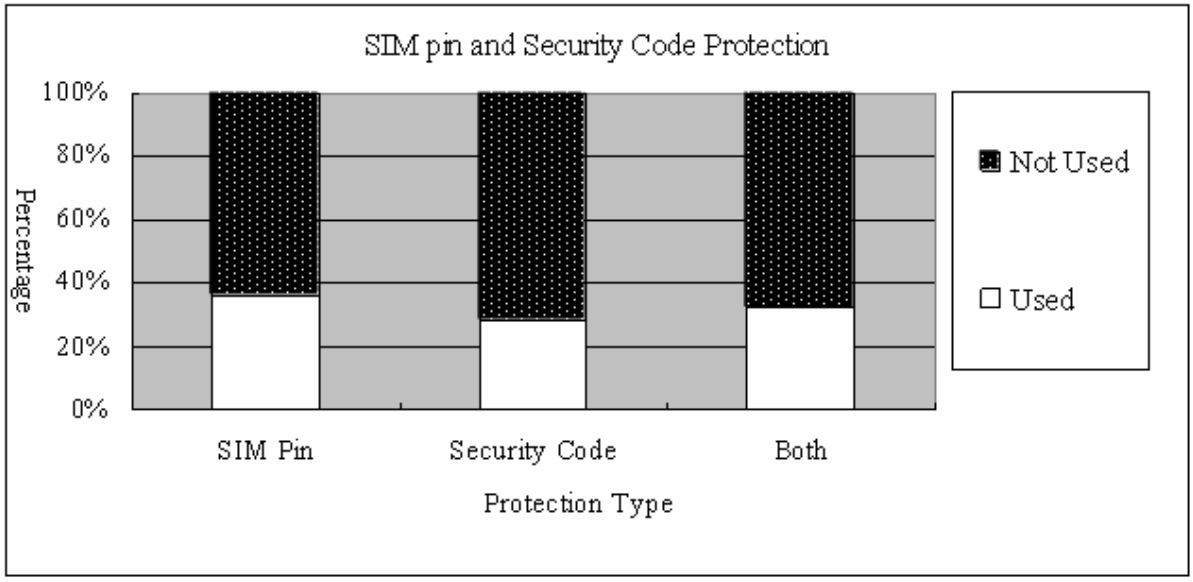

Figure 2: SIM Pin and Security Code Protection Survey

A survey on the habit of setting SIM Pin and security code on the mobile phones has been recently conducted on a sample of 25 Malaysians to gauge their attitudes towards applying non-physical security protection to their mobile phones (BT Research On-Going). The sample consists of both female and male working adults in the age range of 25 to 40. Figure 2 shows the results of the survey. Less than 35% of the people being surveyed apply both the SIM Pin and security code protection. From the responses obtained, the main reasons for not applying any security protection to their phones were a lack of awareness on how critical and useful the information stored within their mobile phones could be if their phones fall into the hands of any unscrupulous third party. The second reason is mainly due to ease of used consideration that deterred most of them from applying these security protections. A third reason being that there are too many passwords to remember nowadays such as

personal emails passwords, bank card's pin numbers and company's login credentials. They did not want to further increase the existing passwords list they managed. 20%of the respondents were totally not aware of the existence of the security code protection features within their mobile phone. All of the respondents had heard of SIM Pin protection features but only thirty six percent of them were using the protection. One of the most significant implications of not applying any security protection to the mobile devices was the compromise of privacy. A possible secondary implication would be potential of financial loss if the SIM in the mobile devices was used for other online transaction authentications such as online banking and e-commerce applications.

Other more complicated security protection mechanisms do exist for individuals or corporate users who are opting for implementing additional security protection to the information stored within their mobile devices. These mechanisms can be broadly classified into two categories namely the preventive and the restorative security mechanism. The preventive mechanism involving the protection of data stored within the mobile device from any aspect of third party illegal invasions while the restorative mechanism focusing on the destruction of data stored within the mobile devices when these devices are reported lost or stolen.

Example of preventive mechanism including data encryption support and authentication services which can be implemented using both software and hardware. Data encryption provides users with the ability to safeguard sensitive personal and corporate data stored in the mobile devices or memory cards. For mobile devices that support Microsoft Windows Mobile 5.0, Symbian, and the Palm Platform, encryption features are being bundled with the operating system. Third party encryption software solutions are also available for users that require slightly better encryption features than those offered by the mobile handheld operating software. The most popular encryption algorithm supported by these third party encryption solutions is the 128-bit/256-bit Advanced Encryption Standard (AES) algorithm (Pointsec 2006) (TrustDigital 2007) (Bluefire Security Technologies 2007). For the most comprehensive encryption protection, users should opt for the encryption capability offered by the Mobile Trusted Module which is a secured hardware base encryption solution. (Trusted Computing Group 2007) On the other hand, restorative mechanism usually relies on software based solution where a copy of automated remote wipe-off software is installed in the mobile device. The software can be triggered automatically through communication networks such as GSM or Wireless Fidelity (Wi-Fi) once the devices are reported lost. This software can not be formatted or removed by any third party and thus guarantee its protection viability.

Preventive mechanisms have several advantages over the restorative mechanisms described above. First, in preventive mechanisms, data has been encrypted and hence user needs to be authenticated to access the data stored in the mobile devices making any attempt to steal information by an unauthorized user deem technical challenging. On the other hand, restorative mechanisms do not mandate the implementation of encryption and authentication to the data stored in the mobile devices. Remote wiping can only be conducted when users report that their mobile device is lost and at the same time the mobile device is connected to the network. The software is then being triggered to erase all the data in that mobile device. Hence, in order to provide a more holistic protection against privacy infringements both preventive and restorative mechanism should be deployed.

Most of the additional security protection measures such as remote wipe-off usually do not come bundled together with standard mobile devices packages. A nominal service charge is usually required for individual that chooses these additional security protections. Nevertheless, the benefits of protecting your data can worth much more than the monthly or annual subscription fees required by the additional data privacy protection. An individual who does not plan to subscribe to any paid security protection service should at least use the data encryption features bundled with mobile operating system besides activating the SIM pin and security code protection that comes free with any GSM based mobile device.

RISKS AND IMPLICATION OF LACK OF SECURITY PROTECTION

The risks and implications of not applying any security protection mechanism described in section 2 are tremendous. For the purpose of security risk investigation and analysis, a second-hand and totally unprotected RIM Blackberry device, obtained from the United Kingdom was used. Essentially the information obtained from the Blackberry device includes both business and private information. With help from the Internet, such as the owner's employer web page, web based interactive maps and public directory servers, the identities of the owner and his contacts were tracked down.

The collected and analysed information was grouped into two categories for ease of explanation, namely business related information and personal information. However, some of the information collected from the Blackberry does not fit distinctly into either of these categories as it appears that it could belong to either category. This type of information is discussed at a separate sub section.

Business Information

Figure 3 summarised the categories and the information occurrence frequency of all business related information obtained from the Blackberry. Corporate email addresses were mainly captured from the inbox folder of the Blackberry while some were found in the address book. A total of distinct 90 corporate email addresses were recovered from the Blackberry excluding the count of customer and private email addresses. Nevertheless, only approximately 30 emails addresses had frequent interaction with the owner. There are a total of 249 address book entries found on the Blackberry, but less than 2% of the total numbers of corporate phone numbers captured were obtained from the address book. The address book of the Blackberry contained additional corporate customer contact information and some private contact information.

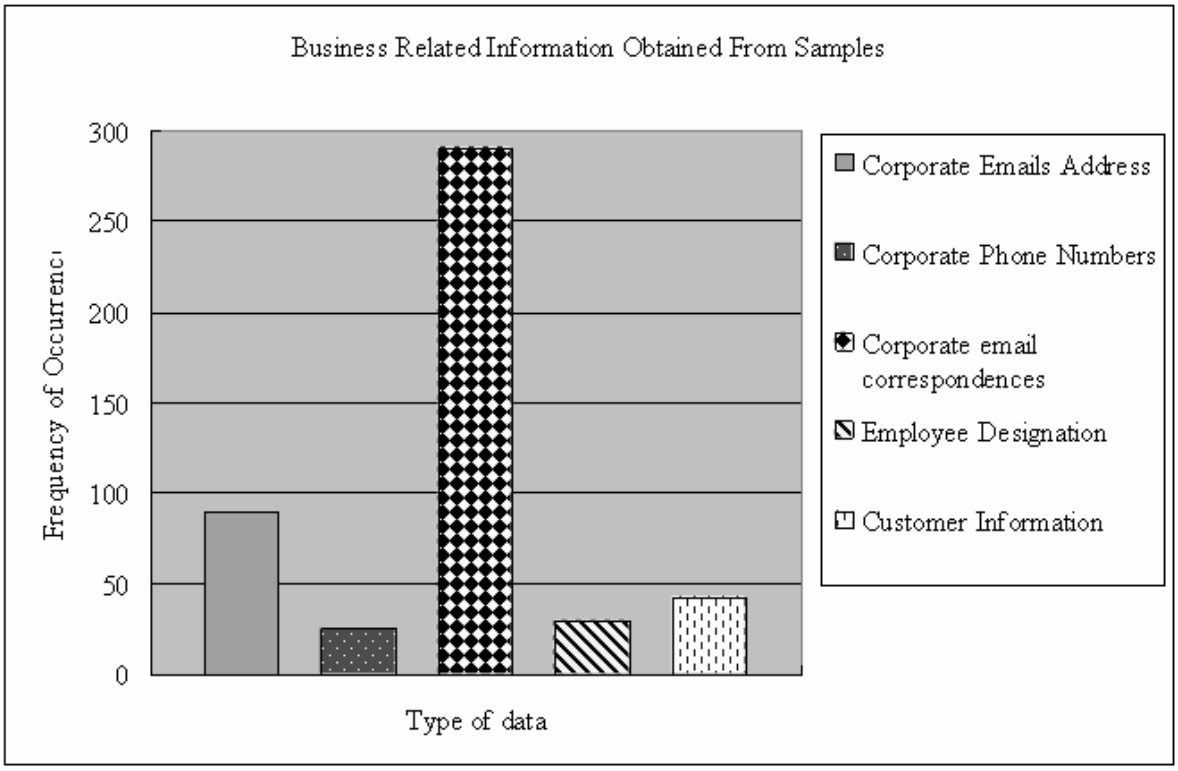

Figure 3: Business related information obtain from Blackberry

A total of 301 undeleted emails were found in the Blackberry. Out of these, 291 emails contained business related information. The email correspondences were identified as one of the best sources that could be used for effective profiling on the owner and his daily activities. From this information, it was found that not only superficial information such as the corporation to which the owner belonged, his roles and responsibilities in the corporation, the locations of the corporation offices, the core business of the corporation and its structure, it was also possible to recover business sensitive information. This information included corporate meeting minutes, sales forecast reports, product pricing strategies, correspondence with customers, competitor's information, products roadmaps and office politics information. From the corporate perspective, this information could be as valuable as the products and branding reputation of the corporation. This information, if used by an unscrupulous individual, could cause huge damage to the corporation in terms of financial loss and reputation damage.

From the email correspondence, a total of 29 employee designations have been identified. This information is useful for any outsider who intended to map out the organization chart of the corporate. Figure 4 illustrated the interpolated organisation chart for that corporation based on the information obtained from the Blackberry. The red box indicates the position of the owner of the Blackberry in the organisation. He is the continental managing director of a multinational organization. Directly under him, there are five main departments lead by individual department directors. The owner of the Blackberry is also in charge of the Group Strategy & Business Development team and the regional office managers. Under the main departments, various personnel have also been identified. The corporation name and individual names in the interpolated organization chart has been purposely omitted to protect the privacy of the individuals involved.

As shown in Figure 3, customers' information is one of the significant elements of information gathered from the Blackberry. A total of 42 customer entries have been identified from the address book, email

correspondences history, memo and task folders. Of these 42 customers, less than 15 are identified to have regular correspondences with the owner and his team members. The customers contact details include information such as their core business, phone numbers, email addressees and the relevant contact person with the Blackberry owner's sales team. This type of information would be valuable to competitors who are fighting for the same pool of customers.

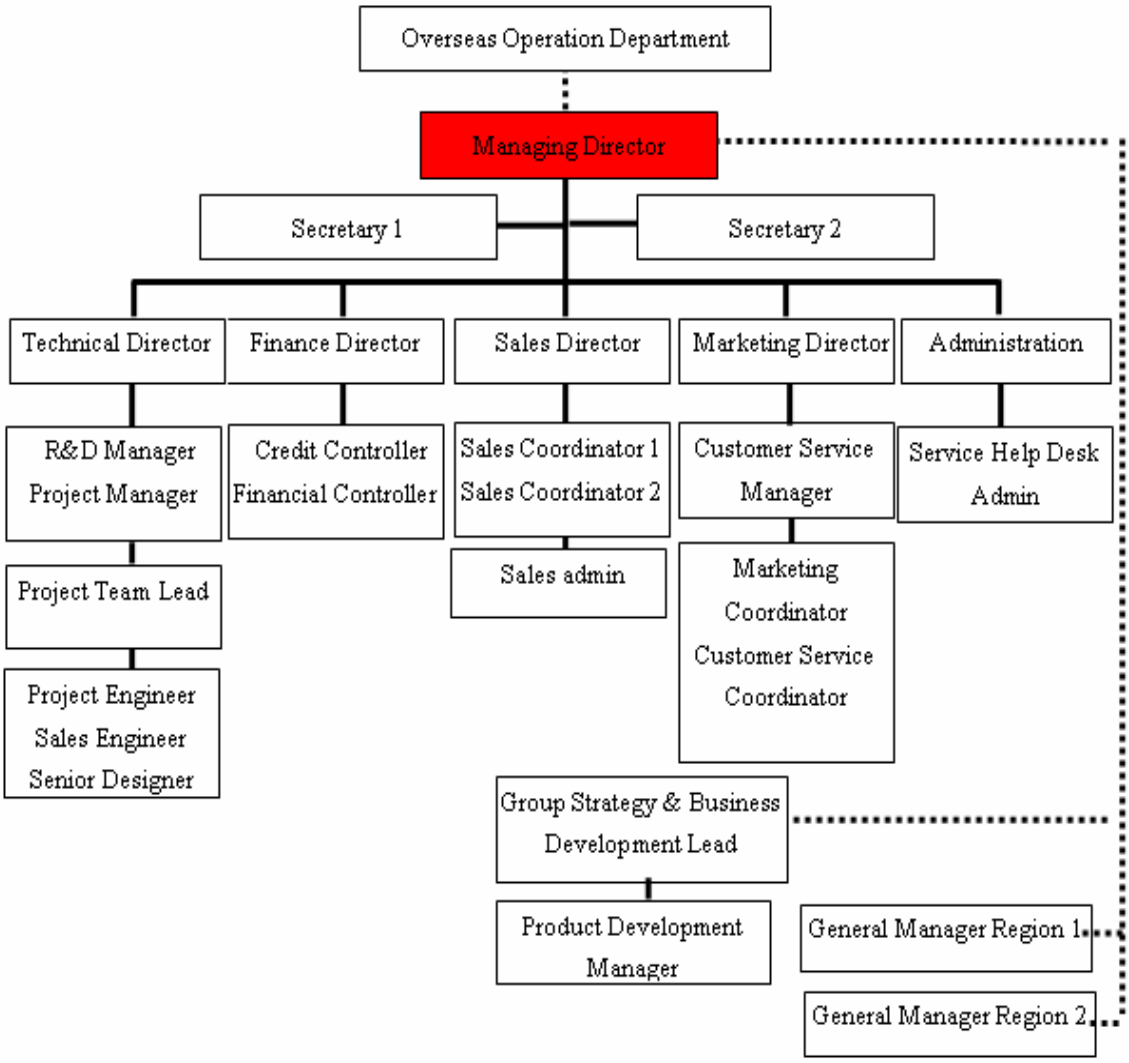

Figure 4: Interpolated Organisation Chart

Personal Information

Figure 5 illustrates the private information of the owner captured from his Blackberry. His home address information is stored insecurely in the Blackberry. By referring to the Internet based interactive map, the distances of his home and various frequently visited places such as office, laundry, florists, country club, and friends' houses are easily identified. By using the Google Map, it was also possible to interpolate the routes that the owner took to reach these places.

The owner also stored his car dealer and car registration information on his Blackberry. By referring to the car dealer information, we can possibly gauge the brand of car that he is driving and hence deducing his social class. The bank sort code obtained from the Blackberry was used to discover the bank where the owner does his financial transaction. Nevertheless, neither credit card information nor online bank login information was recovered from the Blackberry.

The owner's family information such as the family tree structure, the family members names, occupations, home addresses were all found in the Blackberry. From the email correspondences and the recovered deleted emails, it was found that the owner has two sons. One is working in the car industry and the other is still attending high school in a town near to where the owner stays. His oldest son shares his interest in football and it is common

for them to spend time watching football matches together. The younger boy's mother lives in a town that is about 30 miles away from the owner's home. No further information was found with regards to the relationship between the owner and the mother(s) of his sons.

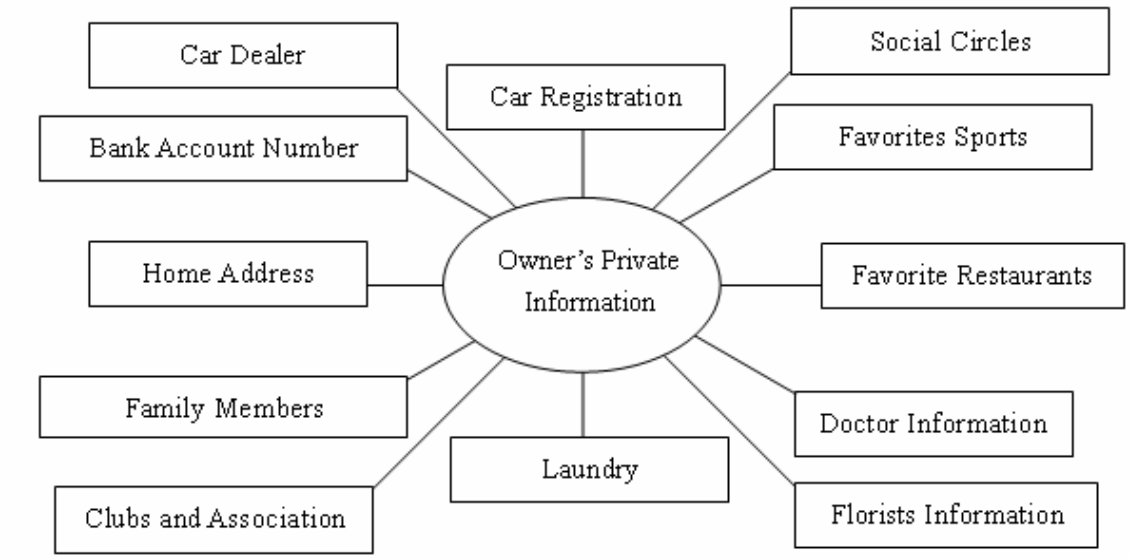

Figure 5: Owner's private information

Besides footballs, the owner is also an avid fan in golf; he owns a golf club membership and kept golf equipment shops contacts information in his Blackberry. However, no information was found on his golf playing skills or his handicap. It is probable that his role within the organisation as the managing director requires him to play this sport in order to socialize with business partners and customers. From the address book of the Blackberry, it was also possible to identify the doctor and local surgery which is approximately 3 miles from the owner's house. From the list of restaurants stored on the Blackberry, an indication of the tastes and dietary preference of the owner can be inferred. Almost 70% of the restaurants found on his Blackberry are Chinese or Italian restaurants. In general, these restaurants are dispersed into three main areas which are roughly 6 miles, 12 miles and 25 miles respectively from his home.

The social circle pattern of the owner can also be inferred from the email correspondences history and address book information. These people home addresses, phone numbers and interaction with the owner are all stored in the Blackberry. It was observed from the deleted email correspondence that was recovered that the owner has a very close relationship with one of his colleagues; they used to message each other when the owner was travelling aboard for business. There is no intend implication that any romantic relationship existed between these two people except for a close bond of friendship.

Interrelated Information

There was some information that was recovered from the Blackberry that could not easily be defined as either totally business related or personal. The information that fell into this grey area was that of the hotel and airlines choices of the owner. From the Blackberry, it was possible to recover a list of hotels and airlines contacts for which there are three possible explanations. First, these options are his corporate preferred hotels and airlines selection. Second, these options are his personal preferences. Finally, these options are a combination of his personal preferences and the option given by his organisation. Nevertheless, we can safely infer that there are high probabilities that the owner flies with one of the identified airlines or stays in one of the hotels when he was aboard either on business or holiday.

CONCLUSION:

With the introduction of mobile devices into the corporate network, the structure of traditional perimeter protection defensive measures implemented in the corporate networks has changed. Mobile devices including laptops, PDAs, Blackberries, smart mobile phones and I-pods which, if they are not securely protected, can be a good target for any individual who are keen in gathering information from a particular corporation or individual. At the time of the writing, security products and services available for PDAs, Blackberries, smart mobile phones and I-pods are limited when compared with the services offers for laptop computers. Furthermore, the awareness

of the need for protection of the information contained in small scale mobile devices is also poor. Awareness should be created in the corporate environment in order to protect both the business and individual privacy.

REFERENCE:

Bluefire Security Technologies, (2007) Bluefire Mobile Security® Enterprise Edition, URL http://www.bluefiresecurity.com/_assets/pdf/Bluefire_Products_Mobile-Security_Ent-Ed.pdf Accessed 15 September 2007

BT Research (On Going) BT Research into Residual Data On Mobile Devices, To be published on Jan 2008

Chris Williams., (2007) Mobile Forensics Turns Up Heat On Suspects, URL http://www.theregister.co.uk/2007/02/11/mobile_forensics_guidance/ Accessed 25 August 2007

GSM Security, (2006) GSM Security FAQ, URL http://www.gsm-security.net/gsm-security-faq.shtml Accessed 8 September 2007

Lee Fueng, Yap Andy, Jones, (2007) Deleted Mobile Device's Evidences Recovery: A Review, International Conference Media & Information Warfare

Pointsec, (2006) Pointsec® for Smartphone, Pointec URL, http://www.filtermax.hu/data/files/pointsec/Pointsec4Smartphone_Eng.pdf Accessed on 25 September 2007

TCG, (2007) TCG Mobile Trusted Module Specification, Specification version 1.0 Revision 1, Trusted Computing Group

TrustDigital (2007) Making Smartphone Security & Management Easy Smartphone Security Version 7, URL, http://www.trustdigital.com/downloads/SmartphoneSecurityv7_20507.pdf Accessed on 25 September 2007

Tuong Huy Nguyen, Annette Zimmermann, (2007) Forecast: Mobile Devices by Form Factor Worldwide 2004-2010, Gartner

COPYRIGHT

[Lee Fueng Yap, Andy Jones] ©2007. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.