2008

# A Study into the Forensic Recoverability of Data from 2nd Hand Blackberry Devices: World-Class Security, Foiled by Humans

Craig Valli
*Edith Cowan University*

Andrew Jones
*Edith Cowan University*

# A Study into the Forensic Recoverability of Data from 2nd Hand Blackberry Devices: World-Class Security, Foiled by Humans

**C. Valli and A. Jones**
School of Computer and Information Science
Edith Cowan University
Mount Lawley WA, Australia

**Abstract –** *Blackberry RIM devices are arguably one of the more secure platforms for email, calendaring and voice. It is one of the few devices in this arena that has approval for carrying restricted security classifications. Blackberry devices do suffer from the same basic fundamental flaw in that they have a human operator. This research was about the blind purchase of Blackberry devices from auctions. Of the 15 Blackberry examined in this study 3 were able to be fully recovered. They all revealed personal and corporate details about the users of the devices.*

**Keywords:** Blackberry, forensic, remnant, privacy, recovery, exposure

## 1 Introduction

The Blackberry as a device in its various guises is seen as the modern executive's talisman of technology. The Blackberry device family was one of the initial innovators removing it from a simple digital diary into a fully mobile fully functional electronic office suite. The modern Blackberry device captures SMS, e-mail, appointments all with full multimedia enhancement and attachment a complete corporate compendium.

One of the main selling points for the Blackberry is its stringent security features. It is one of the few Mobile devices that has approval for a lot a restricted security classifications from around the world including Canada, Australia, UK to name a few [1]. There is evidence to suggest that a Blackberry is a very secure device however, Blackberry has the same basic fundamental flaw it has a human operator. All of the best security measures in the world can still not account or mitigate against a human's innate ability to do seemingly sensible tasks so very wrong.

This paper gives results of a study of 14 Blackberry devices purchased at various auction sites for sale. All of the Blackberry were subjected to forensic examination to extract information from them. Of the 14 examined Blackberry devices three of them were able to be fully recovered.

## 2 Why Blackberry and not 3G?

The security of a Blackberry as mentioned before is one of the main selling points for these devices. The Blackberry is used as a telephony device, email, contact management and calendaring device by persons or institutions that want a "secure" means of interacting with stakeholders. The Blackberry as a device has a similar data footprint and capability as a modern 3G or WiFi phone. There is however, one important exception: Blackberry are typically used by corporate and government enterprises due to their security features and excellent corporate software. Of the 12 million subscribers to RIM services worldwide, over 8 million are corporate users [2]. This fact makes these types of devices a guaranteed 66% chance of potentially sourcing data from a corporate user that would presumably posess information that would have some value or purpose. This profile makes the Blackberry a target device for industrial spying, espionage or good old fashioned blackmail.

There is little argument that the Blackberry is a secure device but as mentioned previously people do silly things, such as leaving them unprotected or simply just misplace or lose the phone. Worldwide, the loss of phones either by theft or simple loss runs into the millions per annum, of which a percentage of these must be Blackberry. If this was not a problem then device location and protection tools such as Roblock, Findit, PhoneBAK [3] and Berry Locator [4] would not be produced or have a market. These software tools are produced to enable the ability to locate the phone via GPS, extract various types of data or disable and produce an audible alarm on the phone. That people or organisations are purchasing and sustaining development of these products at least confirms that someone is ascribing a value to the information stored on the device. Blackberry are desirable and expensive making them a viable theft for profit vector, it is argued that the erasure function may actually enable this. This could be partially due to the nexus created by the Blackberry erasure mode which ensures that the device is wiped after 10

unsuccessful login attempts i.e. there is no possible trace back to the original owner.

# 3 Forensic Analysis and Results

There is not currently a wide range of tools or literature commonly available to assist in the acquisition and forensic analysis of Blackberry Rim devices [5-7]. This is due in part to the corporate manageability of the Blackberry through the software tools available for managing Blackberry. This is in direct contrast to mobile phone forensics that has a growing selection of tools and an expanding literature. Therefore, the one tool that was used for this examination was Paraben Device Seizure 2.0.

The 15 Blackberry devices were purchased at auction in random manner as possible. The Blackberry were then charged and then simply turned on attached to a IBM laptop computer running Windows XP and Paraben Device Seizure 2.0 and attempts were made to acquire data from them. The Blackberry devices that asked for a password to be entered had default known passwords and if these were not successful they have been powered off. The author intends to try physical attacks against the devices to recover the data. None of the Blackberry devices in this study contained SIM cards.

The successfully acquired devices were then analysed using the capabilities of Paraben Device Seizure. Based profile evidence is able to be retrieved as a result of the analysis. This includes the telecommunications provider, the phone call logs, address books, calendars, any SMS and any emails, sent these all help build a profile of the user.

There are also specific settings that relate to the Blackberry device level of use and activation itself. These include the services used and also any applications installed that drive these. In addition there may be records of any extra installed or downloaded Blackberry applications. So in the case of a user there is an ability to rapidly profile an individual.

The following are vignettes of the cases that were able to be recovered from the three Blackberry.

### 3.1 Case 1 – Superannuation and Insurance

Apart from the name of the owner, his addresses and contact details. This case was a regional manager in New South Wales and Australian Capital Territory for a large superannuation entity. He was a Gold Flyer in an airline loyalty program the membership ID was recovered. From his address book apart from his business interests he had significant connection with the fishing industry which was further confirmed by a Google search. The device contained emails details of board meetings, meeting accommodation details, applications for the post of office manager, and comments on the suitability of the named and identified applicants.

### 3.2 Case 2 – Superannuation and Insurance

It was possible to extract the name of the owner, his addresses and various contact details. This case was a regional manager in Victoria and South Australia for the same large superannuation entity as Case 1. It should be noted that during the purchasing of these devices there were no multiple purchases of the Blackberry devices. Upon checking back on receipts the authors did purchase from one vendor twice but 23 days apart. There were no asset ids or markings to suggest that they were from the same entity.

Apart from his extensive calendaring of events, this user was also tracing his family tree. In addition either he or some he knew was interested in guitar as he had recently downloaded chords. The device contained emails related to the farming community, a medical appointment, meetings, a bereavement, performance reviews and also contained 19 names and addresses and call history.

### 3.3 Case 3 – Business

This user was a person involved in several business enterprises who was domiciled in an expensive part of Sydney. Apart from a full disclosure of name, address and contact details there were numerous emails relating to the various businesses this person was interacting with. The information found on the device potentially had some value as it specified limits and also conditions of various bids and contracts that were being negotiated. There were also comments and correspondence about various employees and associated problems some of which would not have been construed as complimentary if revealed. Likewise there were flight details and airline loyalty details that were able to be extracted from the emails.

There was a potential also for blackmail with some of the lurid and extensive exchanges between the user and his mistress. There was also an extensive list of contacts 200 plus and phone logs for the device in question that would allow mapping of interactions. The calendar was also likewise well documented with complete scheduling of all aspects of the persons life. This would have allowed a complete reconstruction of activities undertaken over the period.

# 4 Implications of Investigation

The three cases have uncovered significant personal details about each of the persons who were users of the devices. While two of the devices did not contain a significant volume of information, they both originated in the financial sector and both contained details of a personal nature of the owner and other individuals that would have caused embarrassment or distress if it had become publicly known. The implications of the information on these devices becoming available to individuals who might make use of it for a range of illicit activities could potentially, have devastating consequences for an organisation or an individual. The potential cost of these data losses, both in financial terms and to the reputation of the organisation or the individual, could be high and it is clear that additional effort needs to be expended to ensure that this information is protected.

The following are an outline of some methods of criminal or malicious activity that could be perpetrated on the individuals in these cases.

### 4.1 Identity Theft

All of the devices would enable identity theft of the previous user of the device. There is sufficient information in all cases to have the basis for solid engineering of identity theft. US research estimates of the number of people that have suffered some form of identity theft as high as 10 Million people and the cost to business and consumers at approximately $53 billion in the USA alone in 2002. In Australia recently there are moves to create laws that specifically prosecute identity theft [8]. Much of this is still largely not costed and speculative; evidence for this is that the figure of approximately $1 billion has been bandied about in Australia over a number of years in various guises [8-10].

Identity theft does not always have to have an immediate financial profit motive; there are other manifestations of malfeasance as a result of identity theft. In Case 1 and 3 there was significant personal data left on the device that could allow a malicious individual to manipulate and change schedules or flights for instance. The person was a member of the particular airline loyalty program which allows members to change seat allocations for flights on-line. So an interceding party could wait for Case 1 and 3 to select seats before check-in and then change the seat allocation immediately after this. The service also allows you to request special meals from diabetic to vegan, and make other special requests through the web. These annoyances while not in of themselves catastrophic acts could cause the user considerable angst, stress and delay in ones busy life.

### 4.2 Industrial Espionage

All cases revealed contact details for each individual in Case 3 this was extensive contacts in excess of 200. Two of the cases had information that could be embarrassing at best and litigious at worst should the information have become known. Also in Case 3 in a particular timely interception of some information in the emails could have had significant financial consequences.

In combination with call records and other communications it would be a possibility to create a social and business network for each user. Having mapped their interactions then one could then start a perception management campaign subtly casting doubt on the user of the device in a variety of vectors gleaned from their call records and emails.

### 4.3 Blackmail

Yes good old fashioned blackmail Case 3 was a man of means by his address in one of the more expensive neighbourhoods of Sydney, his business class flights and his outside of business hours associations. Case 3 however, was not a matter of all work and no play he kept a mistress.

Which from the content of two emails indicating a timetabling clash with subsequent email to readjust schedules did indicate the wife did not know of the others existence. This case in particular was potentially a very fertile ground for blackmail and extortion.

### 4.4 Stalking and Harassment

In all of the cases the devices yielded sufficient information to allow an individual to stalk or harass the user both in physical and cyber realms. All three people held positions of power and authority over personnel and customers, anyone of these people could have had a want to stalk or harass the users of these devices. This type of activity would have an increased probability should the mistress in Case 3 need to seek revenge or retribution should she become obsolete.

# 5 Conclusion

Companies and individuals use these Blackberry devices as they are demonstrably very secure when used properly. The loss of hand held devices that still contain significant amounts of information is not a new problem. Every year in Australia over 200,000 mobile phones are lost or stolen [11]. In the year 2005-06 it was reported that around 800.000 mobile phones were stolen in the UK [12]. These are not insignificant numbers and percentage of these would be Blackberry devices that would contain information.

Case 1 and 2 would indicate that the Blackberry in question had been supplied to a disposal company or may have been simply traded in. There needs to be some onus placed on the "disposal" companies to ensure that devices are adequately erased before resale this is best acquitted by enforcement of a contract. Current law in Australia sees no real applicable laws, however if these devices were UK based under the data protection laws in that country the owners could have been prosecuted.

It is also noteworthy that despite the availability of encryption as a set up option on the Blackberry device, three devices surveyed had not had this security feature enabled nor were they password protected. The work undertaken here also further confirms the need to make sure that sound end-user education is in place. An even basic security concept such as the need for passwords has been lost in these 3 cases. The use of passwords while sometimes inconvenient is still a valid security measure. The enablement of available encryption would have made the devices very secure.

Assuming that these devices were not stolen this initial research has uncovered what appears to be a significant and culpable failure to take adequate steps to protect the data on these devices that are capable of very strong security. As a result these devices could have resulted in a number secrets and sensitive information being revealed. The end result of which could have been significant criminal activity being perpetrated against the owners of the devices.

# 6 References

[1] na.Blackberry.com, "Blackberry - Blackberry | Wireless Handheld Devices, Software & Services from Research In Motion (RIM)," 2008.

[2] W. Dabrowski, "Business Spectator - US economy key to Blackberry sales," 2008.

[3] www.bak2u.com, "PhoneBAK BB: Anti-theft software for Blackberry," 2008.

[4] Mobireport, "Berry Locator : Retrieve your lost Blackberry by just sending an email," 2008.

[5] M. W. Burnette, "Forensic Examination of a RIM (Blackberry) Wireless Device," vol. 2008: Rogers & Hardin LLP, 2002.

[6] J. O'Connor, "Blackberry Security:Ripe for the picking?." Dublin: Symantec Security Response, 2006.

[7] Paraben, "Device Seizure," Paraben Corporation, 2007.

[8] M. Browne, "Australia needs ID-theft laws: Minister: News - Security - ZDNet Australia," www.zdnet.com.au,, 2008.

[9] S. Cant, "Identity Crisis," in *The Age*. Melbourne, 2004.

[10] I. Ferguson, "Identity theft battle high on federal agenda: News - Security - ZDNet Australia," www.zdnet.com.au,, 2006.

[11] www.amta.org.au, "Mobile Security Statistics and Quick Facts," 2008.

[12] J. Flatley, "HM Stationary office: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06)," HM Stationary Office, 2007.