



Certacs House
10-12 Westgate
Skelmersdale
Lancashire
L39 6SG

Phone Number: 01695 711246

Website: www.blackbeltdefence.com

Email: sales@blackbeltdefence.com

Erasing Data on Mobile Handsets

By Peter Harrison, CTO

Contents

Introduction	2
Previous Options	3
Platform Considerations	4
BlackBelt DataWipe	4
Implementation	4
Summary	5

Introduction

When considering the security of data and measures to prevent leakage, businesses and consumers rarely think about the risks they are exposed to through mobile phones. Most still think of mobile phones in the same way as they think of fixed line handsets which generally contain little data other than a list of phone numbers.

However, the typical mobile phone sold today is capable of storing up to 1 GB of data. Many can store up to 32 GB of data using a memory card.

And it isn't just phone numbers. A mobile phone may store:

- Mobile banking information
- Confidential documents
- Emails
- SMS messages
- Photos
- Media files
- Browsing history
- Social & business networking info
- And much more

If this information falls into the wrong hands it may be used for identity theft, fraud or similar. Corporate information may be used for industrial espionage. Indeed, leakage of company data through a mobile phone may raise compliance and legal risks, expose the business to bad publicity and lead to loss of customers.

When a handset is handed over to a recycler one may expect the recycler to ensure the security of their data by erasing it prior to reselling the device. As most users do not have the tools needed to erase data securely themselves, they have little option but to potentially expose their data through the selling process. There could therefore be clear business advantages for Mobile Phone Recyclers who can reassure

customers that all data will be securely deleted or, alternatively, provide the customer with the tools to erase the data themselves.

Previous Options

Some enterprises and an increasing number of consumers are aware of the issues surrounding data erasure from mobile devices. However, the approaches currently taken have associated disadvantages which are often not fully appreciated.

Physical Destruction

This approach usually involves crushing or shredding the handset. Provided the destruction is carried out properly, destroying the silicon chips contained within the handset, the data contained within the handset will also be destroyed. Even if the silicon chips are not destroyed, this approach will make the handset inoperable, putting the data beyond economic recovery.

Advantages

If destruction of handsets is carried out correctly this is an effective approach to preventing any subsequent data recovery. Large numbers of handsets can be destroyed at once. Any SIM cards or memory cards left in the handsets will automatically be destroyed along with the handset.

Disadvantages

Physical destruction of the handset also destroys the residual value of the device. The handset will not be available for re-use or re-sale, although it may still be possible to recover precious metals and other materials for recycling. A further issue is that physical destruction creates toxic debris and may pose an environmental risk, particularly if large numbers of handsets are being destroyed. There may be regulatory requirements to

be met relating to disposal of the waste. Finally, if the handsets are not destroyed correctly it may still be possible to recover data from the device's memory.

Resetting to Factory Condition

Many organisations and individuals still believe that this offers a complete solution for erasing the data from a handset. In fact there are significant security risks.

Advantages

This approach has no advantages. All of the data is still on the handset and can be recovered relatively easily with appropriate software.

Disadvantages

Resetting a handset to factory condition does not erase any of the data on the handset. It simply clears the file system index, removing filenames and references to the data. An attacker with access to the handset and appropriate software can still recover the information. Utilities designed to achieve this are readily available at little or no cost. A further major weakness in this approach is that data on the SIM card or memory card will be unaffected by resetting the handset to factory condition.

Reflashing the Handset

Another common method used to delete all handset data is to reflash the memory.

Advantages

Unlike resetting to factory condition, reflashing the memory overwrites the data in the phone's internal memory. The firmware and operating system are usually upgraded to the latest versions available for the handset at the same time.

Disadvantages

Reflashing the handset will only overwrite the data once. Whilst this is an improvement on resetting to factory condition, an attacker with appropriate

tools will still be able to recover the data. This process will be helped by the “wear levelling” technology built into the Flash memory chips used in mobile handsets. Wear levelling is designed to prolong the life of the memory chip. The way this is achieved means that overwriting data simply marks it as invalid with the new data going to a different location within the memory, allowing the original data to be recovered with appropriate tools. Finally, reflashing the handset will not affect the SIM card or memory card. Any data in those will remain intact.

Platform Considerations

The range of operating systems used by mobile devices is growing steadily.

Platforms currently available include:

- Android
- Symbian
- Windows Phone
- iOS (iPhone)
- BlackBerry OS
- webOS
- Maemo
- bada
- J2ME

Apple has added full erasure capabilities to iOS, allowing iPhones to be erased easily. Other platforms do not include such capabilities and the relevant vendors have not announced any plans in this direction. Any solution needs to cater for all platforms.

BlackBelt DataWipe

BlackBelt are specialists in security products for mobile devices, ensuring that the user is protected from threats to their mobile’s security and their privacy. Founded in 2004, BlackBelt has an unrivalled understanding of the issues surrounding mobile phone security. BlackBelt DataWipe has been developed

in response to the need for secure deletion of handset data.

BlackBelt DataWipe reliably erases all of the data in the handset’s memory. It is also able to erase data in the SIM card and any memory cards.

At the heart of the solution is a suite of platform-specific apps. The process of securely erasing data from a handset involves loading the appropriate app onto the device and running the BlackBelt DataWipe executable file. The app will overwrite the device’s memory multiple times, optionally including the SIM card and any memory cards in the handset. BlackBelt DataWipe guarantees that the handset data is beyond economic recovery.

Benefit 1

BlackBelt DataWipe ensures that all data in the handset’s memory is reliably erased.

Benefit 2

Any memory card in the handset can be reliably erased.

Benefit 3

All user information is reliably erased from the SIM card.

Benefit 4

In conjunction with the PC-based management console, BlackBelt DataWipe provides a full audit trail demonstrating that the handset has been erased.

Benefit 5

Using BlackBelt DataWipe to erase the data on a handset prior to disposal ensures regulatory compliance.

Implementation

There are several possible delivery solutions for BlackBelt DataWipe depending on need:

- BlackBelt DataWipe may be installed on memory cards so that the appropriate app will run when the memory card is inserted in a handset.
- The apps can be delivered direct to the handset via the internet.
- A PC-based management console enables the operator to plug handsets into the PC and initiate the BlackBelt DataWipe process. Once the erasure process has begun the handset can be unplugged. On completion of the erasure process the handset is again plugged into the PC, thereby allowing the PC to confirm that the data has been erased and gather appropriate statistics, providing a full audit trail.

Summary

Secure disposal of mobile handsets is an important issue, affecting both consumers and organisations alike. In a world where identity theft, corporate information theft and fraud are growing rapidly it is essential that data is securely deleted from mobile handsets.

BlackBelt DataWipe provides a secure approach to ensuring that all data on a mobile handset is permanently deleted and cannot be recovered by a malicious attacker. Use of the BlackBelt solution provides both enterprises and consumers with reassurance that their data is safe and cannot be misused.

A **BlackBelt** White Paper

For further information please contact:

BlackBelt SmartPhone Defence,
Certacs House
10-12 Westgate
Skelmersdale
Lancashire
L39 6SG
Phone Number: 01695 711246
Website: www.blackbeltdefence.com
Email: sales@blackbeltdefence.com