WE DO ITAD RIGHT

Lifespan

Thank you for your interest in this

WHITE PAPER

Wiping Data on Mobile Handsets

Introduction

When considering the security of data and measures to prevent leakage, many businesses and the vast majority of 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 and in excess of 1 gigabyte of data. Many can store up to 32 gigabytes of data using a memory card.

Furthermore we're not just storing phone numbers and a few text messages on mobile phones today. Handsets are commonly used to store:

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

As and when such information falls into the wrong hands it may be used to commit identity theft, fraud and other illegal activities. Corporate information may be used for industrial espionage. Indeed, leakage of company data through lost, stolen or recycled mobile phones may raise compliance and legal risks, expose the businesses to negative publicity and ultimately lead a to loss of customers.

When obsolete handsets are transferred into the recycling supply chain one might expect a responsible recycler to ensure the security of previous user data by wiping handsets prior to remarketing such devices. As most users do not have the tools needed to securely wipe data themselves, they have little option but to potentially expose their data through the remarketing process. There could therefore be clear business advantages for Mobile Phone Recyclers who can reassure customers that all data will be securely wiped or, alternatively, provide the customer with the tools to wipe the data themselves.

Previous Options

Some enterprises and an increasing number of consumers are aware of the issues surrounding wiping data 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 handsets, and at significant cost to the owner! Provided the destruction is carried out properly, destroying the silicon chips contained within the handset, the data contained within the device 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

The double whammy – physical destruction of handsets also destroys the not insignificant residual value of obsolete devices – not to mention having to pay for the physical destruction service! Handsets will not be available for reuse or remarketing, 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

environmental risks, particularly when large numbers of handsets are disposed of. There may also be regulatory requirements to be adhered to relating to disposal of such 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 organizations and individuals still believe that this offers a complete solution for wiping the data from a handset. In fact there are significant security risks posed to previous user data in the event of relying solely upon factory reset facilities.

Advantages

This approach has no advantages from the perspective of a consumer or enterprise customer. All of the data is still on the handset and can be recovered relatively easily with the appropriate software.

Disadvantages

Resetting handsets to factory condition does not wipe any of the data on the devices. It simply clears the file system index, removing filenames and references to the data. An attacker with access to second-hand handsets and appropriate software can still recover previous user data. Utilities designed to achieve this are readily available and in use at little or no cost. A further major weakness in this approach is that data on the memory card is unaffected by resetting handsets to factory condition.

Reflashing the Handset

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

Advantages

Unlike resetting to factory condition, reflashing memory overwrites the data in a 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 will only overwrite Previous user data once. Whilst this is an improvement on resetting to factory condition, attackers 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 in which this is achieved means that overwriting data simply marks it as invalid with the new data going to a different location within the memory, again allowing the original data to be recovered with appropriate tools. Finally, reflashing handsets does not affect memory cards. Any data they hold 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 wipe capabilities to iOS, allowing iPhones to be wiped 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.

Tabernus DataWipe

Tabernus Data Erasure are experts in developing software and hardware products for proper and certified data sanitization. Founded in 2004, Tabernus has ensured that users are protected from threats to their storage security as well as their privacy.

An unrivalled understanding of the issues surrounding storage security, Tabernus DataWipe has been developed in direct response to the need for secure deletion of handset data. Tabernus DataWipe reliably wipes all data stored in handset memory.

At the heart of the solution is a suite of platform-specific apps. The process of securely wiping data from handsets involves loading the appropriate app onto each device and running the Tabernus DataWipe solution. The app overwrites device memory multiple times. Tabernus DataWipe guarantees that the handset data is securely cleared down beyond commercial recovery.

Benefit 1

Tabernus DataWipe ensures that all data in a handset's memory is reliably wiped.

Benefit 2

In conjunction with the PC-based management console, Tabernus DataWipe provides a full audit trail confirming that handsets have been securely wiped prior to remarketing.

Benefit 3

Tabernus DataWipe produces a comprehensive report documenting the mobile phone by serial number that the erasure of information is complete and successful.

Benefit 4

Using Tabernus DataWipe to remove previous user data from obsolete handsets prior to disposal ensures regulatory compliance.

Implementation

There are a number of delivery mechanisms for Tabernus DataWipe depending on need:

- Tabernus DataWipe can be installed on memory cards, thus executing the app when the memory card is inserted into a handset.
- Tabernus DataWipe apps can be delivered direct to handsets via the internet.
- Most commonly, a Windows PC-based management console enables operators to connect volumes of handsets to a PC and initiate the Tabernus DataWipe process. Whereby the PC provides process updates in an easy-to-use GUI to confirm that the data has been wiped and gather appropriate statistics, providing a full audit trail.

Note that secure deletion can only be guaranteed when the PC-based management console is used.

Certifications

There are currently no standards or certifications for wiping data from mobile handsets. While some vendors claim to conform with standards such as HMG InfoSec Standard 5 or US Department of Defense Directive 5220.22-M, these standards are designed for use with magnetic media such as hard drives. Mobile handsets use solid-state memory to provide permanent storage. This is a completely different technology which requires an alternative approach. "Wiping" handsets in accordance with standards designed for magnetic media may leave some data remanence on the handset.

Tabernus is working with standards bodies to develop appropriate standards for wiping mobile handsets.

Summary

Secure disposal of mobile handsets is an important issue, affecting both consumers and organizations alike. In a world where identity theft, corporate information theft and fraud are more lucrative than drug trafficking it is essential that data can be securely removed from mobile handsets as and when required.

Tabernus DataWipe provides a secure approach to ensuring that all previous user data is permanently deleted and cannot be recovered from obsolete handsets by a malicious attacker. Use of the Tabernus solution provides both enterprises and consumers with the peace of mind that their data is safely disposed of and cannot be misused.