CMSGu2011-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Mobile Devices Security Guideline

CERT-MU

National Computer Board
Mauritius

Version 1.11

June 2011

Issue No. 1

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this document, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

Table of Contents

1.0 Introduction

1.1 Purpose and Scope

This guideline offers an insight into the risks associated with mobile devices in use today and gives details on the countermeasures available to minimise them. Organisations can make use of this document to enforce security and avoid incidents involving devices such as laptops, PDAs and smartphones. Users can use it to mitigate the underlying security risks and protect themselves from mobile attacks.

1.2 Audience

This document, while technical in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document includes mobile phones, PDAs, laptops and tablet PC users, security professionals, IT managers, system and network administrators involved in the support of mobile devices.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides a brief overview of the document's content.

Section 2 gives a background on mobile devices.

Section 3 presents the security concerns associated with mobile devices.

Section 4 elaborates on the countermeasures available to mitigate the risks, threats and vulnerabilities discussed in the previous section.

Section 5 concludes the document.

Section 6 contains a list of references used in drafting this document.

Appendix A provides a list of acronyms that have been used in the document.

2.0 Background

Mobile devices are a prerequisite nowadays. They are generally small and inexpensive, but have a variety of attractive functionalities, including sending and receiving e-mails, storing documents, delivering presentations, and remotely accessing data. These devices are useful to practically everyone; however, they also pose security risks to organisations as well as everyday users.

2.1 Types of Mobile Devices

Mobile devices have become very common in our society, be it amongst the younger generation or in organisations. To have a mobile phone these days is something absolutely normal, with practically no age restriction at all. Organisations take full advantage of smartphones, laptops and PDAs to ease the tasks of employees, for example, in checking their e-mails, organising their documents or delivering presentations.

2.1.1 Mobile Phones

Mobile phones can be classified into these categories

- **Basic Phones:** Limited to voice and messaging functions
- **Advanced Phones:** Offering enhanced capabilities and services
- **Smartphones/High-end Phones:** Merging the capabilities of an advanced phone with those of a PDA.

Similar to PDAs, advanced mobile phones support basic Personal Information Management (PIM) application for contacts, calendar and notes. They also support the synchronisation of PIM data with a desktop computer. Mobile phones can also synchronize data over-the-air with a server controlled by the cellular carrier, by making use of cellular network interface. More sophisticated devices enable Internet connectivity, access to web sites, e-mail exchange, multimedia and instant messaging. Some devices also enable PIM applications to work with specialised built-in hardware, such as a camera.

Smartphones allow users to review electronic documents (for example reports, briefing slides, and spreadsheets) and run a lot more special-purpose applications. In general, these devices are larger than the average mobile phone, provides a better display with higher

resolution (for example ¼ VGA and higher), and sometimes have an integrated *QWERTY*[1] keyboard or even touch sensitive screen. Other enhanced capabilities like built-in wireless communications such as Bluetooth and Wi-Fi, and synchronisation protocols to exchange data (for example graphics, audio and archive file formats) are also supported.

2.1.2 Personal Digital Assistants (PDAs)

PDAs originated in simple digital organisers for telephone number. The first proper PDA, the Newton from Apple was out in 1993. It provided functionalities such as fax, e-mail, PIM applications, character recognition of pen-based (stylus[2]) input entered on a touch screen and data synchronisation with a desktop computer. PDAs very much resemble handheld Personal Computers (PCs), but they do have distinct features. For instance, PDAs are specifically designed for mobility; therefore they are compact in size and are powered by battery. They usually store data in a solid-state memory rather than on a hard disk. They also hibernate to save battery power and time, meaning they do not require a reboot. PDAs are also tailored to synchronise data with a desktop computer. This is a useful feature because data retained in volatile memory can be lost and even data in non-volatile memory can be accidentally deleted.

2.1.3 Laptops

A laptop (notebook) is a personal computer meant for mobile use. It comprises most of the basic components of a desktop computer, including a screen, a keyboard, a pointing device (a touchpad, also known as a trackpad, and/or a pointing stick) and speakers, altogether and runs all sorts of applications that a computer does

Laptops can be categories into the following:

- **Full-size Laptop:** A full-size laptop is larger in size and can have room for a "full-size" QWERTY keyboard.

- **Netbook:** A smaller, lighter, more portable laptop, usually cheaper than a full-size laptop. It has fewer features and less computing power. Smaller keyboards can be more difficult to work with. There is no real difference between netbooks and inexpensive small laptops; some 11.6" models are marketed as netbooks. Since

[1] QWERTY: is the most common modern-day keyboard layout. The name comes from the first six letters (keys) appearing in the top letter row of the keyboard, read left to right: Q-W-E-R-T-Y.
[2] Stylus: is a writing utensil, or a small tool for some other form of marking or shaping used for a PDA.

netbooks, compared to laptops, are quite small in size, CDs cannot be used in these computers.

2.1.4 Tablet Personal Computers (PCs)

A tablet PC is a tablet computer which has the main characteristics of a personal computer in the tradition of the *Microsoft* Tablet PC, as a machine operated by an end user with no intervening computer operator. A portable tablet PC is equipped with a touchscreen as a primary input device. The term was made popular as a concept presented by Microsoft in 2001, but tablet PCs now refer to any tablet-sized personal computer, even if it is not using Windows but another operating system. Tablets may use virtual keyboards and handwriting recognition for text input through the touchscreen. Tablet PCs have a wireless adapter for Internet and local network connection. There are also various software applications for tablet PCs, namely office suites, web browsers, games, to mention only a few. However, portable computer hardware components typically have lower performance; hence heavy applications may not achieve a high-quality performance.

According to a study released by the law firm "*Olswang"* in 2011, the tablet market is in a premature stage with 3% of Americans owning an iPad and 2% owning some other kind of tablet, with Apple users being more common.

2.2 Mobile Operating Systems

Basic and advanced mobiles normally use a company-proprietary OS. Several real-time OS solutions are available for mobile phone manufacturers from companies specialising in embedded system software. Smartphones usually use these OSs: Palm WebOS, Windows Mobile, BlackBerry OS, Symbian OS, iPhone OS and Android. The OSs in basic and advanced phones are more limited and real-time kernels whereas those in smart phones are multi-tasking, full featured and designed in such a way to match the capabilities of high-end mobile devices.

2.2.1 Android

The Android mobile operating system is based on the Linux kernel. Google and other members of the *Open Handset Alliance* collaborated on Android's development and release.

The *Android Open Source Project* (AOSP[3]) is responsible for the maintenance and further development of Android. The Android operating system is the world's best-selling Smartphone platform. It has a large community of developers writing applications ("*apps*") that extend the functionality of the devices. There are currently over 200,000 apps available for Android. Android Market is the online app store run by *Google*; however apps can also be downloaded from third-party sites. The apps are primarily written in the Java programming language, controlling the device via Google-developed Java libraries.

2.2.2 BlackBerry OS

BlackBerry OS is a proprietary mobile operating system, developed by *Research In Motion (RIM)* for its BlackBerry smartphones. The operating system provides multitasking and supports specialized input devices that have been adopted by *RIM* for use in its handhelds, particularly the trackwheel, trackball, and most recently, the trackpad and touchscreen. Updates to the operating system may be automatically available from wireless carriers that support the BlackBerry *"over-the-air software loading"* (OTASL) service. Third-party developers can write software using the available BlackBerry API classes, although applications that make use of certain functionality must be digitally signed. On April 2010 *RIM* announced the new BlackBerry OS 6.0 version, which was released in the 3rd quarter 2010. *RIM* announced BlackBerry OS 7 on 2nd May 2011. It would be released in Summer 2011. RIM announced that current devices would not be updated to BlackBerry OS 7 (No Legacy Device Support). *RIM* also announced the BlackBerry Bold Touch (Blackberry Bold 9930 & 9900) which runs Blackberry OS 7.

2.2.3 Symbian

Symbian is both an operating system and a software platform designed for smartphones and currently under the responsibility of Nokia. The Symbian platform is the successor to Symbian OS and Nokia Series 60; contrary to Symbian OS, which needed an additional user interface system. Symbian includes a user interface component based on S60 fifth Edition. The latest version, Symbian 3, was officially released in Quarter 4, 2010, first used in the Nokia N8. According to some statistics, the average number of mobile devices shipped with the Symbian OS up to the end of Quarter 2, 2010, is 385 million. Nokia recently (April 5,

[3] AOSP: Android Open Source Project that provides information and source code required to build an Android-compatible device

2011) released Symbian under a new licence and made it a proprietary shared-source, but far from an open source project.

2.2.4 Windows Mobile

Windows Mobile is a mobile operating system developed by *Microsoft* used in smartphones and mobile devices. It is however becoming an end of life OS in specialised markets. Windows Phone 7 is taking over it and the latest version is Windows Mobile 6.5. It is based on the Windows CE 5.2 kernel, and comprises a suite of basic applications developed with the Microsoft Windows Application Programming Interface (API). Most Windows Mobile devices come with a stylus pen, which is used to enter commands by tapping it on the screen. Microsoft announced a completely new phone platform, Windows Phone 7, at the Mobile World Congress in Barcelona on February 15, 2010. Phones running Windows Mobile 6.x will not be upgradeable to version 7, officially. Some developers however, have installed Windows Phone 7 on devices originally running Windows Mobile, for example the HTC HD2. Windows Mobile's share of the smartphone market kept on falling annually, decreasing 20% in Quarter 3, 2009. It is the fifth most popular smartphone operating system, with a 5% share of the worldwide smartphone market (after Symbian, BlackBerry OS, Android and iOS).

2.2.5 Windows CE (WinCE)

Windows CE (now officially known as Windows Embedded Compact) is an operating system developed by *Microsoft* for embedded systems. WinCE is a distinct operating system and kernel, and not a trimmed-down version of desktop Windows. It is totally different from the NT-based Windows XP Embedded. Microsoft provides WinCE licences only to Original Equipment Manufacturers (OEMs) and device makers. The OEMs and device makers can then customise their own user interfaces and experiences. WinCE works well on devices that have minimal storage. A WinCE kernel may run in under a megabyte of memory. Devices are often configured without disk storage, and may be configured as a "closed" system that does not allow for end-user extension (for instance, it can be burned into Read Only Memory). WinCE is a real-time operating system, with deterministic interrupt latency. From version 3 and above, the system supports 256 priority levels and uses priority inheritance for dealing with priority inversion. The fundamental unit of execution is the thread. This helps to make the interface simpler and enhance execution time.

2.2.6 Apple iOS

iOS (known as iPhone OS prior to June 2010) is *Apple*'s mobile operating system. The user interface of iOS is based on the concept of direct manipulation, using multi-touch gestures. Interface control elements consist of sliders, switches, and buttons. The response to user input is immediate and provides a fluid interface.It was originally developed for the iPhone, but now has been extended to support other *Apple* devices such as the iPod touch, iPad and *Apple* TV. Apple does not license iOS for installation on third-party hardware. In late 2010, it had a 16% share of the smartphone operating system market in terms of units sold, third behind *Google*'s Android and *Nokia*'s Symbian. In May 2010, it accounted for 59% of mobile web consumption (excluding the iPad) in North America.

2.2.7 Palm webOS

webOS is a proprietary mobile operating system running on the Linux kernel, initially developed by Palm, which was later acquired by *HP*. Palm, *HP* and other sources use the term "webOS" as shown in the adjacent logo and in *HP* resources. In February 2011, *HP* announced that the *HP* Pre 3 and *HP* Veer smartphones will run webOS 2.2, and that the *HP* TouchPad, a tablet computer, will run the webOS 3.0. webOS version 1.4.5 runs on the Palm Pre, released June 6, 2009, on the *Sprint* network, the Palm Pixi, released on November 15, 2009, on Sprint, as well as "Plus" versions later issued on *Verizon* Wireless and *AT&T*, and some international carriers. webOS version 2 runs on Pre 2 phones released since October 2010 in France by *SFR*, 2010 December by *Rogers* in Canada, and 2011 February on *Verizon* in the U.S. Unlocked Pre 2 phones using webOS version 2 are available directly from *HP*. Plans for other webOS versions and devices were proclaimed by *HP* in February 2011, including the Touchpad, the Pre 3 and the Veer. In March 2011, *HP* declared that all PCs shipped by *HP* in 2012 will be able to run webOS in addition to Microsoft Windows. The *HP* Veer was launched on *AT&T* on May 15 2011, and is available in black and white.

2.3 Mobile OS Comparison

Individual employees carry along mobile devices into the enterprise, contrary to desktop computers. No wonder they have become the crucial consumer device compelling IT managers to support them. While Blackberry and Windows Mobile top the list of supported devices (see Figure 1). *Apple* iPhones and *Google* Android phones are not far behind (see Figure 2) It appears that the next challenge will be full support for iPads and other tablet PCs.

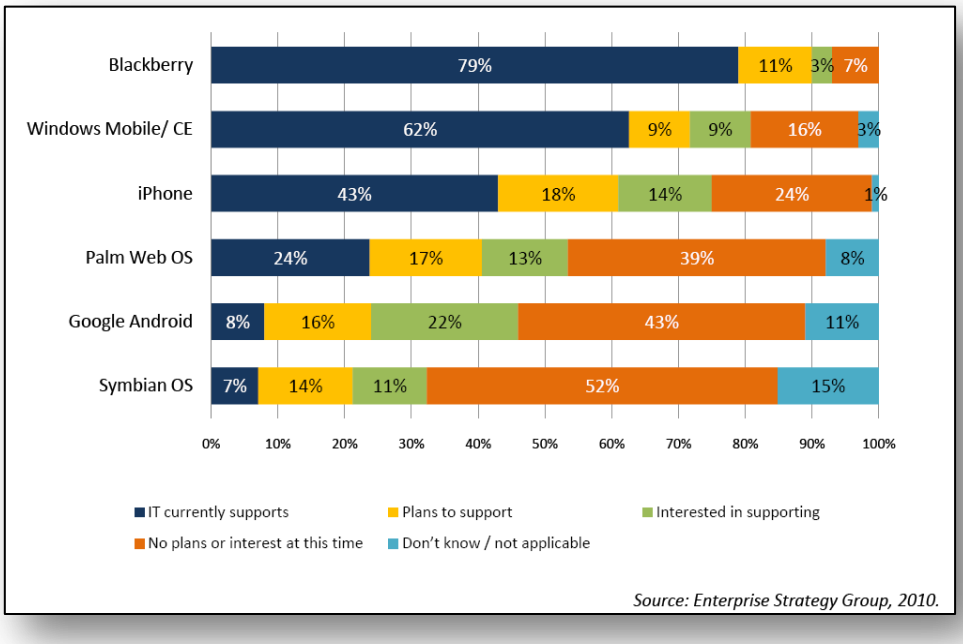

Figure 1. Mobile Device Platform Support

The pie chart below illustrates the OS market shares with *Google*'s Android and Apple having the greatest market shares. The survey was carried out by *Gartner* in 2010 Q4.

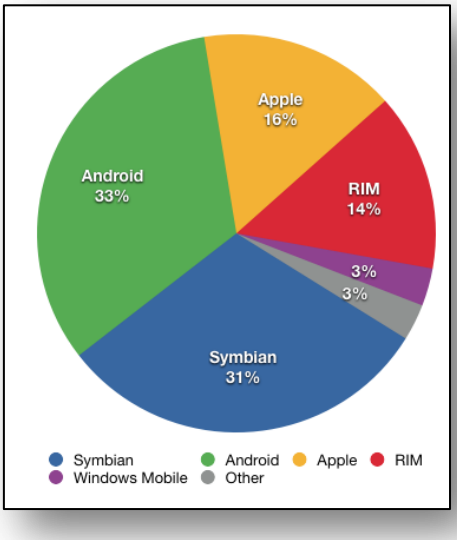

Figure 2. Share of smartphones sales to end users by operating system

2.4 Mobile Device Use

Amongst mobile devices uses, e-mail remains the most popular application, but 63% of large organisations provide mobile device access to internal networks and portals and 30% of enterprises also offer Customer Relationship Management (CRM), core business applications, location-based applications, industry applications, and custom applications (see Figure 3).

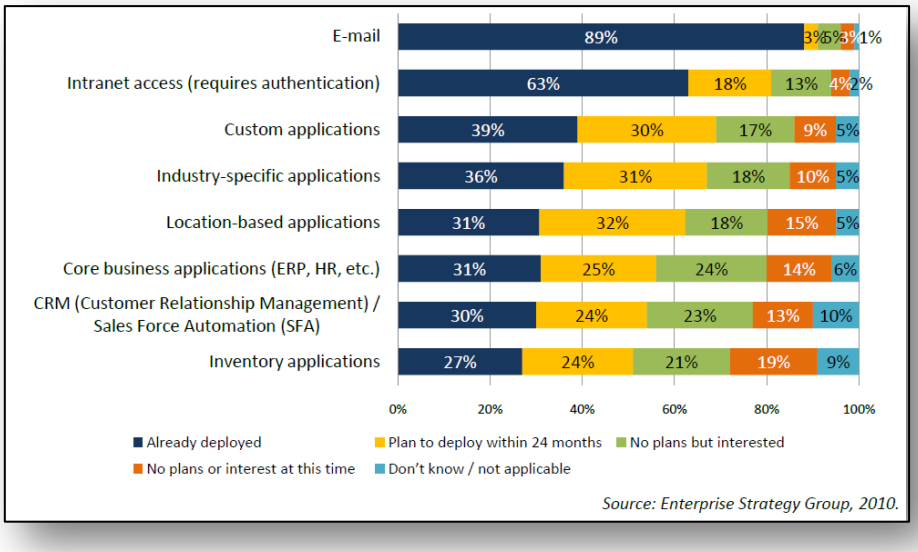

Figure 3. Mobile Device Application Support

Employees can also access a variety of data from their mobile devices and some of this data is classified as restricted or confidential. According to a survey carried out by the *Enterprise Strategy Group* in 2010, it has been observed that more employees use mobile devices to access and process company confidential data, followed by customer data; regulated data and intellectual property (see Figure 4). Consequently, it makes sense to say that mobile devices are critical for day-to-day business processes and productivity.

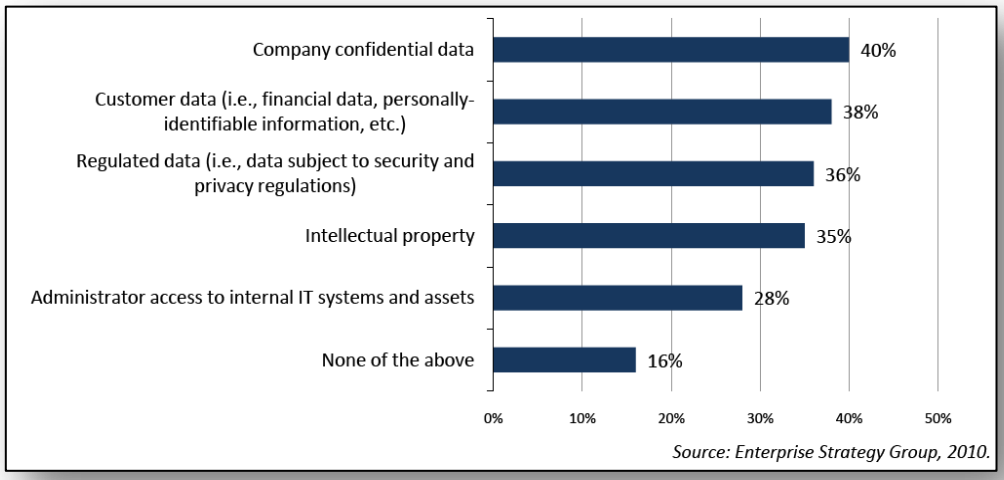

Figure 4. Confidential Data Entitlement Using Mobile Devices

3.0 Existing Risks, Threats and Vulnerabilities

Smartphones, PDAs, laptops, tablet PCs and other types of handheld devices are ubiquitous; they improve productivity and flexibility for individuals and employees. Almost everyone who has a smartphone or PDA uses it for both personal and business purposes. Personal use includes storage of confidential personal data (identity information, contact lists, bank account details, user names, PINs, credit card details, etc). Business information, as we have seen in the previous chapter, includes confidential data about your employer, co-workers, clients, suppliers, and about problems and issues which sometimes may be subject to privacy or data protection legislation.

According to ***"Symantec's Internet Security Threat Report 2010"***,

> *"In 2010, there were a significant number of vulnerabilities reported that affect mobile devices. Symantec documented **163** vulnerabilities in mobile device operating systems in 2010, compared to **115** in 2009. Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile "app" marketplaces in the hopes that users will download and install them. In March 2011, Google reported that it had removed several malicious Android applications from the Android Market and even deleted them from users' phones remotely. Attackers have also taken a popular legitimate application and added additional code to it in order to infect users' mobile devices, as happened in the case of the Pjapps Trojan for Android devices."*

The next sub-sections gives details on the various risks mobile devices are exposed to.

3.1 Viruses and other Malware

Mobile devices can be just as vulnerable to viruses as desktop computers. This is the new ground for hackers but, industry analysts expect viruses, Trojans, worms and all types of malware to grow as the mobile device market grows. A couple of examples encountered to date include the "*911 virus"* which caused **13 million** "*i-mode*[4]*"* users to automatically place a call to Japan's emergency phone number and the *"PalmOS/LibertyCrack"*, a known Trojan horse that can delete all applications on a Palm PDA.

There is no risk to a PDA or smartphone from malware if the device is not connected to any networks. However, as wireless connectivity brings a lot of benefits to users, it is not safe

[4] I-mode: is a mobile internet (as opposed to wireless internet) service popular in Japan.

from malware. The risk applies both to the PDA or smartphone and to any computer or corporate network to which it connects, in that the malware could be installed through the Sync/ActiveSync[5] function or through its direct connection to the network. One realistic solution would be to install and keep up-to-date anti-malware software.

3.2 Spam

Unsolicited Short Message Service (SMS) text messages, e-mail and voice messages from advertisers have begun to make their appearance on mobile phones. On top of the inconvenience of getting rid of them, charges may apply in some countries, for example, for an SMS message received or if we have exceeded the storage limit of a service plan. We can say that we are fortunate enough as in Mauritius there is no charge for any such inbound activities. Downloads as well are chargeable and the cost is even higher for the download of image attachments. Mobile spam sometimes also fraudulently convince users to call or send text messages to premium service numbers using social engineering techniques. Spam can also be in the form of phishing attacks, called "*Vishing*[6]*"*, in the mobile context. These attacks usually lure users divulging their credentials, bank account details, or other data via text messages. Phishing in the normal form is performed via Web pages and e-mail, causing the user to access a fake Web page or download malware attached to the message.

Spamming can also be in the form of instant messaging and multimedia messaging that spread malware. Malicious users can also make use of spam techniques to launch Denial of Service[7] (DoS) attacks. A good example would be repeated attempts to establish Bluetooth pairing with a phone that would block the user and prevent him/her from initiating a call until he/she acknowledges the prompt. Another example could be to send a specially-formulated vCard to a certain model of Nokia handset that would cause a temporary denial of service to the phone until it is rebooted.

3.3 Theft/loss of a Mobile Device

Theft or loss of a mobile device could be a very big problem for users as the theft of confidential information on computers is on the increase and wireless mobile devices appear to be the next targets to such attacks. Specific security risks exist, much greater than those

[5] Sync/ActiveSync: is a mobile data synchronization technology and protocol developed by Microsoft.
[6] Vishing (Voice Phishing): is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.
[7] Denial of Service (DoS): is an attempt to make a computer resource unavailable to its intended users.

related to basic cell phones. Users need to be really cautious as thieves and criminals very well know how much confidential information is stored on smartphones and PDAs, and how poor is the security on them. A simple and handy step would be to protect all information by using encryption on their device to make it inaccessible to unauthorised users. In many cases, contrary to the above, the thief only sees a valuable electronic device without having any idea what data is stored in it.

In addition to the above, most enterprise users do not enable the password/passcode function on their mobile devices. It is of utmost importance that users turn on device authentication so that in case their device is lost or stolen, no one will be able to use it fraudulently or access or personal details.

3.4 Bluetooth and other wireless interfaces

Bluetooth technology allows users to connect device, send messages or move files between them. Bluetooth device communications can be placed in these different modes:

- **Discoverable:** allowing the device to be seen by other Bluetooth-enabled devices
- **Connectable:** allowing the device to respond to messages from connected devices
- **Completely off**: undiscoverable by any other Bluetooth objects and preventing any information exchange.

Malware can be delivered to a mobile device using Bluetooth, Infrared or other wireless interfaces or available connectivity services supported by mobile devices if these are enabled.

3.5 Web Browser Security Loopholes

Several security measures are already in place by most Web browsers to warn users about unencrypted Web pages. However, various security loopholes still exist in these browsers:

- **Pop-up warnings:** Web browsers often use a pop-up dialog box to indicate that information being sent is not encrypted. However, these boxes offer the option to "turn off" the dialogue box so it never appears again. Even when enabled, many users are likely to ignore such warnings.
- **The "lock" icon:** Most Web browsers display a small padlock icon to indicate an encrypted Web page. They often are not. Additionally, hackers often register commonly misspelled domain names or ones that closely resemble legitimate sites. When a user is redirected to that page it will display the lock icon, and the

user may not notice the change in domain name. Thinking that the connection to the site may be encrypted, the user will access the site they think they are.

- **HTTPS and unfamiliar links:** Many financial services advertise the unencrypted version of their Web pages (https indicates a secure version; http, however, is easier to remember). When a user logs on to that page and clicks to enter the encrypted version, he/ she can be redirected to a page with a domain name that is different from the company's normal homepage. In a case where the user does not recall the name, it is hard for him/her to know if he/she has been redirected to the genuine company's homepage or to a hacker's webpage.

3.6 Wi-Fi Threats and "Evil Twin" Attacks

- **Wi-Fi (Wireless Fidelity):** Wi-Fi equipments are usually sold with their manufacturers' default settings. These settings often have a very low level of security or no security at all. If there is no security, anybody can connect to a wireless laptop or wireless network and use it for their own purposes – to access shared resources or individual data on a network. A malicious user could send spam or malware for cybercrime or cyber terrorism purposes by making use of an unsecured wireless laptop or network. "*Evil twin"* attacks are gradually increasing due to the rise in wireless device users doing business over the Internet. Below is an illustration of an "evil twin" attack on a notebook:

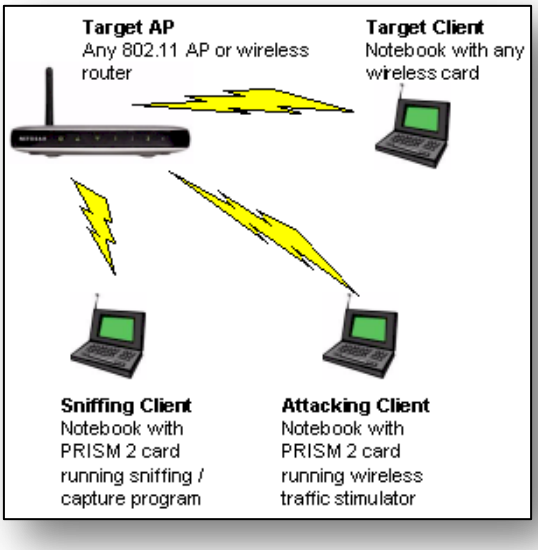

Figure 5. Example of an "evil twin" attack. *Source: prohackingtricks*

- **Unsecured hotspots:** Users often connect their laptops, PDAs and smartphones to an unsecured wireless network or hotspot. In the event where a legitimate user is trying to access a website and a hacker is in the same area as the user, the hacker can send out his/her own Wi-Fi signal that is identical to the log-in page of the legitimate website. This is what we call the "*evil twin*" attack. An intruder can launch this type of attack to degrade network performance or deny service completely. An evil twin will offer fake login prompts in order to steal user names and passwords, which can later be used by the attacker for fraudulent purposes. The attacker will wait for unsuspecting users to logon to the fake page and type in sensitive information such as credit card numbers, passwords and private company information.

- **New wireless technologies:** New trends in wireless technologies encourage hackers to spend a lot of their time in exploiting new vulnerabilities associated with mobile devices. Sometimes they make use of existing vulnerabilities in wired systems to discover security flaws. It is much more complex to locate the source of the attack in wireless systems as compared to wired environments, where there the attacker and the victim are physically connected. This intricacy in wireless systems is very appealing to attackers, thus making them happier to launch their attacks in the wireless world.

4.0 Countermeasures

4.1 Authentication

The first line of defence against authorised use of a mobile device is to verify an individual's claimed identity through authentication. The three common types of authentication are:

- Proof by knowledge (for example password)
- Proof by possession (for example smart card)
- Proof by property (for example fingerprint)

Two factor or three factor authentication can be done and generally provides additional security. The authentication techniques mentioned above are detailed below:

- **Password**

  Password is the first and most popular form of authentication that exists and is used on mobile devices. The security of your system is only as strong as the password you select to protect it. It is sometimes difficult to type complex passwords on some devices due to their small keypads, but it is important that you choose a strong, effective password that is not easily guessed.

  The two main categories of passwords that have evolved are firstly, those that require the user to remember and select a sequence of displayed images and, secondly, those that require the user to draw a series of lines over a grid or image templates. The first category of password has been implemented in various commercial security products for handheld devices.

- **Smart card**

  A smart card is a credit-card-size security token with an embedded computer chip containing an operating system, programs, and data. Extending it to handheld devices potentially offers benefits. For example, a smart card could convey user security credentials and policy rules to a device to govern user permissions and allowed behaviour. However, it is rather large in size and need to be incorporated or connected with a card reader with a similar size if the mobile device cannot accommodate it. Some full-size smart cards support wireless communication and even include a radio frequency. Others also have a USB connector at one end. However, very few handheld devices support host USB ports, which are required

to connect to these peripherals. With advances in technology, high-end mobile devices could potentially communicate with them.

Universal Subscriber Identity Module ((U)SIMs[8]) are reduced size smart cards that are used in certain types of mobile phones. As (U)SIMs are under the control of the network carrier and not normally readily accessible (i.e., removable of the battery from the handset is typically required), they are not recommended authenticating with a device.

- **Fingerprints**

  Fingerprints are the oldest technique that involves biometrics. A biometric[9] system operates by comparing newly captured data of some biometric characteristic, that is,physiological and behavioural) against a stored template derived from registered measures taken previously. Fingerprint authentication technology is incorporated in only a few handheld devices. A more common biometric targeted towards mobile devices that have touch-sensitive screen is signature dynamics, that involves measurements of speed, acceleration, direction, pressure, stroke length and pattern, and time and distance the writing stylus is lifted. Quite a few commercial security products for handheld devices have signature verification technology.

4.2 Reducing Data Exposure

- **Do not keep sensitive information on mobile devices:** Users should not keep sensitive information, such as PINs, passwords, user IDs and financial account information, on mobile devices although it might ease users' tasks in authenticating to online accounts. Accounts, passwords and any other sensitive information should never be transmitted unencrypted over a wireless network. Wireless network traffic can easily be sniffed. With advanced hacking techniques, some authentication mechanisms can be bypassed or broken and even deleted information can be restored. An alternative to keeping data on a mobile device would be to store sensitive data on removable memory cards, separate from the mobile device until it is needed.

[8] Universal Subcriber Identity Module ((U)SIM): a software application for UMTS mobile telephony which is inserted in a 3G mobile phone

[9] Biometric: consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. In computer science, in particular, biometrics is used as a form of identity access management and access control.

- **Encrypt data on mobile devices:** If users need to keep their confidential information on their handheld devices, the data should be encrypted and decrypted when required. There are some devices with built-in encryption capabilities. Users could opt for these. Examples of such devices are Symbian devices which provide a "*wallet*" mainly for storing personal information, such as credit card numbers, contacts, user names and passwords, all in an encrypted format. The "*wallet"* can be accessed only when the correct password is entered and closed automatically if the user becomes idle. There are other commercially available tools, specially customised for smart phones and PDAs. Some not only encrypt device contents but also memory card contents. To protect confidential information on a mobile device that has encryption capabilities is an effective control, especially for organisations. The "*Advanced Encryption Standard"* (AES) was developed for Federal developed for Federal departments and agencies to encrypt and decrypt such information.

- **Password Locking Mechanism:** Latest memory cards following the multimedia card security standards include a password locking mechanism that some handheld devices use. For example, a number of Symbian OS devices benefit from this feature. A case-sensitive password of up to 8 characters long can be used on a memory card. Once enabled, the password is required again whenever the memory card is removed and reinserted into the device. If the memory card is inserted into another card locking-compatible device, the user will be prompted to enter the password. Devices that do not have this feature, including desktop computers with card readers, cannot read the card. This feature can be a useful means of securing sensitive data kept separately from the device, particularly when encryption is also used. One possible shortcoming could be that the device fails and the user forgets the password needed to unlock the card.

- **Permanently erase data when it is not needed:** In an organisation, if an employee reaches the end of his service or if the employee's device is to be given to another employee, the device's memory containing sensitive data should be wiped out to prevent the contents from being recovered and manipulated. Memory erasers exist for some mobile devices and manually performing a hard reset clears memory for others. If no policy for data destruction is in place, the memory

should be physically destroyed (for example passing the whole device through a recognised shredder for destruction).

4.3 Wireless Interfaces

- **Turn off Wireless Interfaces when not required:** Bluetooth, Wi-Fi, Infrared, and other wireless interfaces should be turned off and used only when they are required. This is particularly important for Bluetooth devices due to the increased risk of encountering mobile malware in crowded environments, such as an airport, sports event, or concert, which offer a potential for an attack. Appearing invisible stops the device from being scanned and located and prevents its wireless interface to be used as an opportunity for attackers. The battery life of the device can also last longer if a wireless interface is disabled.

- **Disable automatic connections if not in use:** Automatic connections to services, such as GPRS[10] or EDGE[11], should be disabled if they are not in use. Staying offline prevents malware infections and may also prevent an infected device from sending data to other devices. If a phone automatically connects to data services, it could be that the phone is infected with malware attempting to spread itself. The Bluetooth wireless interface should be turned to discoverable mode only temporarily until pairing with another legitimate device is completed. This helps to avoid discovery attempts by malware trying to propagate itself, even though brute force attacks can prove successful in some implementations. Where possible, Bluetooth settings should be configured to notify the user of any incoming connection requests and to receive confirmation before proceeding. Some mobile phones enable the control of the Bluetooth functionality by enabling only the supported profiles required to interact with another device.

- **Do not perform device pairing in public areas:** Device pairing should be performed outside of public places, preferably in areas that are radio isolated, to prevent monitoring and recording exchanges "*over-the-air"* and prohibit attackers from using them to regenerate security keys required to eavesdrop. Using a long

[10] General packet radio service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication systems global system for mobile communications (GSM).

[11]Enhanced Data rates for GSM Evolution (EDGE) is a digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM.

random PIN is also advised to complicate the calculations required in certain attacks.

- **Password protect Bluetooth keys:** Bluetooth keys are generally stored on paired devices, so these devices should be password protected. It is also good to have a list of known trustworthy devices with which the device can connect via Bluetooth. If this feature is available, Bluetooth should be configured in such a way so as to use the lowest power setting needed for the connection. Power adjustment to a lower setting helps reduce the likelihood of an attack from long range.

- **Minimise functionality:** In addition to disabling wireless interfaces when not needed, disabling unneeded features through configuration setting is also a plus in preventing attacks. In some situations, it may be possible instead to remove a feature from a device completely to avoid it being reactivated. Similar consideration should be given to reducing the use of add-on applications and plug-ins. Once installed, these applications are able to access user content and device programming interfaces, and they may also contain vulnerabilities. Their benefits should be carefully evaluated against risks before installation, since such add-on functionality may be useful to attackers.

- **Disable cellular service agreements and service settings:** Cellular service agreements and service settings are another way to minimise functionality. For instance, disabling data service and subscribing to only voice service prevents full access to the Internet, which may not be required. It may also be possible to have the carrier restrict access to international destinations that are not used or bar other services. For example, many cellular carriers allow the subscriber to block text messages that comes from the Internet, which is the foundation of wireless spam.

4.4 Reporting of lost/stolen devices

- **Phone Lock:** In the event where a device is lost or stolen, deactivating it, locking it or permanently deleting its contents are useful actions that can be performed from a remote location. It is advised to contact the cellular carrier to report a lost

or stolen cell phone and terminate service. In various countries, including Mauritius, GSM carriers can also register the phone's identifier, i.e. the International Mobile Equipment Identity (IMEA) in a global database to prevent it from being used elsewhere.

- **Keep Track of Serial Number:** It is a good idea to take note of your device's serial number or engraving your device in case of theft/loss. It is also essential to be aware of the reporting procedure in advance of an incident and what information to provide, as stolen/lost phones can cost the subscriber a lot of money up to when the device was reported stolen/lost. In some companies, a copy of a police report may be required in order to waive the charges. Organisations should establish and inform users of procedures for reporting lost/stolen mobile devices to speed up the process and lessen the consequences.

- **Remote Protection Mechanism:** Certain devices, such as Blackberry devices and some mobile phones, offer the functionality of locking a device or erasing its contents remotely through a built-in mechanism. Memory cards may also be accessed using the same technique. Mobile devices and memory cards that have been locked can be unlocked by the user, if they are recovered. Some products are also available for devices to add in this feature. When evaluating such products, care should be taken to guarantee that the locking feature cannot be easily bypassed and that the removal process completely overwrites or purges data from memory.

- **Pre-registered Activation Code:** We can trigger the remote protection mechanism through the receipt of a message containing a pre-registered activation code. Thus, to turn on the mechanism, the device must be able to receive communications via the cellular network (e.g., not radio isolated). To activate the mechanism, the user enters the activation code and selects an option. A series of options from a device lock to a full content deletion may be available, or only a single choice, depending on the implementation. Notification of the user's identity module being replaced with another identity module (for example that of a thief) is occasionally a supported option. A device that is compromised through a remote attack, but still in the user's possession, can be deactivated through the means mentioned above. However, there are simpler actions that can be taken

more quickly to tackle problem until it is fully resolved. A compromised device may keep on operating and cause damage when service with a cellular carrier is discontinued or even when the device has been switched off.

- **Backup Battery:** Some mobile devices have a built-in backup battery to maintain power on a temporary basis. Nevertheless, removing the battery ultimately reduces the ability of the device. In the case where the battery cannot be removed, placing the device in a radio isolation bag blocks radio frequencies and communication, eventually causing the battery to be completely drained. The device's capability to authenticate and communicate with the cellular network when it is operating on the backup battery can also be disabled by removing any identity module present, but removal does not affect other wireless interfaces.

4.5 Avoidance of Questionable Actions

- **Communication Channels:** Malicious programs are mostly spread to mobile phones through communications channels such as multimedia messages. Messages or contacts received on a mobile phone from an unknown number or device should be treated with suspicion. Messages should be deleted without opening and the connections should be denied. We even have to be cautious about content received from a friend or colleague, since malware can make use of address book entries and message exchange capabilities to proliferate themselves, very often as an attractive attachment or link. For example, an MMS message or e-mail message from a familiar number or address, containing an executable file as an attachment, could be produced by a malicious program under the control of an attacker.

- **User Interation:** Most malware requires user interaction to be effective, making the option of taking no action when solicited a realistic prevention strategy. Up till now, malware-infecting mobile devices rely on the user accepting the installation of infected files or connections from other devices. For example, malware attempting to propagate via a Bluetooth connection cannot install itself without user approval. Any request from a mobile phone to accept the installation of an unfamiliar program whose installation was not initiated by the user be cancelled. Likewise, incoming connections of any type should not be accepted unless we are

expecting them. A program that constantly tries to download malware via a Bluetooth connection may in fact prevent the user from using the phone or disabling Bluetooth. In such scenarios, moving out of range of the other device can overturn its reattempts to connect. It is also important to keep the device configured to deliver notifications for user approval when there is an attempt to connect or download files.

- **Storage Media:** Media may seem risk-free, but it should be treated vigilantly, because it can be used by attackers to launch malware attacks. For instance, Windows Mobile devices can identify when a storage card is inserted and automatically load and execute an application from it, just like the way in which the "*autorun*" feature in Windows desktop systems works with removable media, such as CD and USB drives. Social engineering is a way of fooling users and inducing them into taking such actions. Several forensic tools have been implemented to exploit the "*autorun*" feature to recover data from handheld devices. The download of software from unknown or suspicious websites should be avoided at any cost

- **Application Security Features:** Some devices have application security features that prevent the installation of third-party applications unless they are digitally signed. Alternatively, many trustworthy and reliable sources for software, media, and other types of download exist and should be used to download content. Ideally, only programs that are from reputable manufacturers and have verified digital signatures are recommended.

4.6 Installing Prevention and Detection Software

The operating system and built-in applications on a mobile device are harder to update than those on a desktop computer. Thus, additional security controls that prevent and detect attacks against the device are a must. Prevention and detection software is an essential addition to defend against malware and other forms of attack. Various products for handheld devices, especially smartphones and PDAs have been developed and can be used to harden the security mechanisms already in place in a device. However, we have to bear in mind that add-on security software may contain or introduce weaknesses and should be properly evaluated prior to use. Security products, in general, include user authentication techniques,

including biometric and token-based mechanisms, device content and memory card encryption, firewall, antivirus, intrusion detection, antispam device content and memory card deletion and Virtual Private Networking[12] (VPN).

"Airscanner", "F-Secure", and *"Trend Mobile"* are goodexamples of antivirus and anti-spam solutions.

A number of products provide centralised security management of mobile phones and PDAs through the network infrastructure. Solutions typically involve augmenting the infrastructure with expansion of enterprise servers and the use of Lightweight Directory Access Protocol[13] (LDAP), Active Directory, or other similar directory services. Periodic communications with managed devices take place to ensure security and other configuration settings are accurate and in compliance with policy, as well as to perform updates to security credentials, downloads of log files, configuration updates, and other related functions. The capabilities vary from product to product.

The following items are some common examples:

- Device registration
- Installation of client software, policy rules, and control settings
- Controls over password length and composition, number of entry attempts, etc.
- Remote password reset
- Remote erasure or locking of the device
- Controls to restrict application downloads, access, and use
- Controls over infrared, Bluetooth, Wi-Fi, and other means of communication
- Controls to restrict camera, microphone, and removable media use
- Controls over device content and removable media encryption
- Controls over VPN, firewall, antivirus, intrusion detection, and antispam components
- Remote update of client software, policy rules, and control settings
- Remote diagnostics and auditing
- Reporting of device compliance status
- Denial of services to non-compliant or unregistered devices

[12] Virtual Private Network (VPN): is a secure way of connecting to a private Local Area Network at a remote location, using the Internet or any insecure public network to transport the network data packets privately, using encryption

[13] Lightweight Directory Access Protocol (LDAP): is an application protocol for reading and editing directories over an IP network.

4.7 Devising Deployment, Operational Plans and Policies

- **Centralised Security Management:** With organisation-issued devices, it is often important to consider centralised security management, since it simplifies the configuration control and management processes required to ensure compliance with the organisation's mobile device security policy. Addressing security issues of mobile phones and PDAs once deployment and implementation are ongoing is a difficult task. Security should rather be considered initially. Required device characteristics are often associated with available safeguards and can affect procurement decisions. Organisations are more likely to make decisions about configuring mobile handheld devices securely and consistently when they develop and follow a good plan.

- **Deployment and Operational Plans:** Plans should include ways of protecting data, authenticating users, accessing organisational networks and resources, and handling lost or stolen devices. The handling of compromised devices to limit exposure and resolve the problem is also a concern. Device issuance, backup and recovery, and content deletion before disposal or reissuing are other aspects to be addressed when preparing the plans. Planning should include any required business applications to be used with the devices and any required controls over the installation of third-party applications by employees, and address any anticipated security issues that relate to those applications from an organisation-wide angle. Developing such plans helps to spot critical issues and guides administrators in making trade-off decisions between usability, performance, and risk. The plans can also be useful in dealing with existing system contingency, continuity of operations, and disaster recovery.

- **Security Policy:** Organisations should have a security policy in place for mobile handheld devices. A security policy defines the rules, principles, and practices that establish how an organisation handles these mobile devices, whether they are issued by the organisation or personally owned. Individuals could also benefit from taking similar considerations with their own devices. The security policy should reflect an organisation's view on required safeguards, based on a consideration of the assets involved, the impact of loss or compromise, and the threat environment. The policy should cover the full life cycle of a device from its

issuance to the user to its retrieval after dismissal, transfer, or similar event, and comply with relevant regulations and legislation.

- **Policy on personal use:** Restrictions on personal use should be clearly stated, as well as the consequences if a device containing personal information is lost, stolen, damaged, or remotely wiped out. Information security in any organisation is largely dependent on the quality of the security policy and its implementation and enforcement. Technology alone cannot overcome a poorly planned or nonexistent security policy.

- **Policy on software download:** Organisations should also have policy in place about software downloads and could even work out an internal procedure for centrally managing software distribution and installation.

4.8 Raising Security Awareness through Training

User awareness of the organisational security policy and procedures for mobile devices is a requirement to their successful implementation. If the personnel are not familiar with the policy and procedures and the implications for violating them, they will not be compliant with the organisation's standards. Even organisation-controlled devices can create security issues if not used in the correct way. In addition to making employees aware of the policy and the consequences for noncompliance, actively monitoring and dealing with compliance issues helps to do away with risky activities.

4.9 Performing Risk Management and Configuration Control

- **Risk Management:** Security involves continually analysing and managing risks. Mobile devices have their share of risks and must also contend with a dynamically changing environment. A risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks. Risk management involves taking steps to reduce assessed risk to an acceptable level and maintain that level of risk. Ongoing risk analysis and management is an important organisational activity that is increasingly being mandated by law and regulation.

- **Configuration Control:** Further to risk management, configuration control should be considered as it ensures that the system is protected against the introduction of improper modifications before, during, and after system deployment. Configuration control leads to compliance with the organisation's mobile devices security policy. Changes to a configuration should be vetted and tested before deploying to the production environment.

  Here are some considerations to take when preparing standardised software configurations:

  1. Available patches and upgrades to the operating system security-wise
  2. Unnecessary services and applications that can be disabled
  3. Necessary applications that require installation and proper configuration
  4. User authentication and access controls enabled on the device
  5. Other security-related control settings available on the device (e.g., notifications and alarms, inactivity timer lock, logging options, memory allocation)
  6. Certify and accredit handheld devices.

- **Security Certification:** The security certification of an information technology system requires that the system is analysed to determine how well it meets all of the technical and non-technical security requirements of the organisation. A system can only be accredited when the organisation's management accepts that the system meets the organisation's security requirements. Both are a must to deploying handheld devices, especially if other constituents of the network infrastructure are also engaged. Such network infrastructure components typically involve enterprise servers used to connect to devices to provide services.

4.10 Data Backup

To use a mobile device as the only means for important information calls can be risky. The device can not only be lost or stolen, but it can also be accidentally damaged. To safeguard valuable data on a mobile device, a backup of the contents should be done regularly so that the data can be restored in case of a disaster. Data may be synchronised with a desktop computer as a primary means of backup and also for possible dual use. Data includes personal information management data, electronic documents, photos, music, software applications, and network settings, amongst others.

Backing up data on the memory card is a substitute for backup, but is helpful only if the card is kept separately away from the mobile device. If not, the device and card could be lost or stolen together, reducing the security benefits essentially to situations where the device fails. Contact data such as phone numbers and addresses can also be printed out and kept in a diary as a form of physical backup. We also have to consider using multiple backup mechanisms and if we travel, we can have a portable backup device that we can carry along with us.

4.11 Maintaining Physical Control

Physical security is a key concern for mobile devices. Keeping an eye on a mobile handheld device is important. Its use should be treated similarly to a credit card, maintaining control at all times and storing it securely if left unattended. Besides the cost of the device itself, the loss or theft of a handheld device places the confidentiality of the device's contents at risk, as well as the computational resources contents accessible by it.

Lending our personal mobile phone to somebody can be an opportunity for misuse to the person, and in the worst case, can lead to the installation of malware or activation of unwanted services, such as device tracking. Unexpected costs due to toll calls placed or services used could be incurred and sensitive data on the phone could be tampered with. An intimidating call or message placed from a phone would likely be associated to the owner by authorities. The security settings of the device could also be altered, making the phone susceptible to other hazards that could be ignored due to the changes.

4.12 General Security Principles for PDAs and Smartphones

- Password protect your PDAs and smartphones, preferably with a strong password (eight digits or longer and alpha-numeric)
- Do not leave your mobile devices unattended if not secured in a locked device/room.
- Disable the wireless port on your PDAs and smartphones when not in use (to prevent transmission of confidential data to unauthorised individuals)
- Install appropriate anti-malware software on your mobile devices and keep it up-to-date.
- Install the latest patches on your mobile operating system (to keep yourself abreast with your supplier's Web site(s), as automatic updating is not yet supported by PDAs and smartphones).

- Encrypt any confidential (including corporate) information stored on your mobile device.
- Back up your mobile device regularly by synchronising the device with a linked computer.

5.0 Conclusion

Mobile devices are becoming more and more common in our society due to their small size, ease of use and sophistication. Unfortunately, they are also introducing a lot of information security risks. People do not really care about the security aspects of mobile devices as long as these tools meet their expectation in terms of functionalities and look. Many organisations do not provide enough control to deal with mobile security issues. It is vital to have good control over mobile devices that are connected to the Internet if one wants to minimise security risks.

6.0 References

- National Institute of Standards and Technology (NIST): http://www.nist.org
- Information Technology, Planning, Implementation and IT Solutions for Business – News & Reviews: http://www.baselinemag.com
- Techtarget, Where Serious Technology Buyers Decide: http://www.techtarget.com
- TechRepublic – A Resource for IT Profressionals: http://www.techrepublic.com
- Wikipedia: http://en.wikipedia.org
- GetNetWise | You're one click away: http://www.getnetwise.org
- Symantec: https://www.emea.symantec.com
- Prohackingtricks: http://prohackingtricks.blogspot.com

Appendix A

List of Acronyms

AES	Advanced Encryption Standard
AOSP	Android Open Source Project
API	Application Programming Interface
CD	Compact Disc
CRM	Customer Relationship Management
CRT	Cathode Ray Tube
DoS	Denial of Service
EDGE	Enhanced Data rates for GSM Evolution
EMS	Enhanced Messaging Service
GPS	Global Positioning System
GPRS	General Packet Radio Service
MMS	Multimedia Messaging Service
OEM	Original Equipment Manufacturer
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PIM	Personal Information Manager
PIN	Personal Identification Number
SMS	Short Message Service
USB	Universal Serial Bus
VPN	Virtual Private Network
WIFI	Wireless Fidelity