Mobile device security

Kevin Curran*, Vivian Maynes and
Declan Harkin

Faculty of Computing and Engineering,
University of Ulster,
Northern Ireland, UK
Email: kj.curran@ulster.ac.uk
Email: Maynes-v@email.ulster.ac.uk
Email: declanharkin@gmail.com
*Corresponding author

Abstract: None of the early internet designers has ever foreseen the pervasiveness of its involvement in everyday life. That is why we have so many security and privacy issues today. The landscape is moving all the time with new smartphones hitting the market and new features being rolled out almost weekly. The standard desktop operating system is quickly being overtaken by computing on mobile devices however many of us are unaware of the security vulnerabilities on mobile devices. This paper highlights the security mechanisms deployed to make mobile devices safe for use. Such mechanisms include the choice of mobile device by the user, encryption, authentication, remote wipe capabilities, lost phone hotline, firewalls, utilisation of third party software, intrusion prevention software, anti-virus software and finally Bluetooth.

Keywords: security; mobile security; mobile; network security; malware.

Reference to this paper should be made as follows: Curran, K., Maynes, V. and Harkin, D. (2015) 'Mobile device security', *Int. J. Information and Computer Security*, Vol. 7, No. 1, pp.1–13.

Biographical notes: Kevin Curran holds a BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM and FHEA. He is a Reader in Computer Science and Group Leader for the Ambient Intelligence Research Group. He has made significant contributions to advancing the knowledge of computer networking evidenced by over 800 published works. He is a regular contributor to BBC radio and TV news in the UK and quoted in trade and consumer IT magazines on a regular basis. He is an IEEE Technical Expert for Security and a member of the EPSRC Peer Review College.

Vivian Maynes is a graduate in Computer Science of the University of Ulster. She is currently working in the information technology industry with research interests including distributed systems, network security and internet technologies.

Declan Harkin is a graduate in Computer Science of the University of Ulster. He is currently working in industry. His research interests include security and programming languages.

1 Introduction

Most people do not take time to consider privacy on their mobile devices. It is a fact that only 50% of people put a lock code on their phone therefore any stolen phone can allow thieves to also burrow into their online accounts (*Information Week*, 2011). Most people store access codes in their e-mail account. A thief would easily siphon off passwords from that. Accessing your online bank account or PayPal can allow a thief to transfer money or buy an online anonymous currency like BitCoin and you will never see that money again. For the first time in our history, banks and other financial institutions are beginning to offload the blame for an account being hacked onto the customer. They are claiming that customers should have had greater protection mechanism in place. Securing your actual communications is a different matter. If you have a lot to lose by being snooped upon like a drug dealer or a spy then it is important. If you are the other 90% of the population then it can be harder to see the need for secure communications – especially voice communications. There is more of a need for secure messaging. Say you wish to talk movies with your friend and he is working and also using a corporate phone or iPad, then having a secure password protected app or program can simply prevent problems with his/her boss. It would also be important for people having affairs. There are smartphone messaging apps out there on the app market like SafeSlinger which claim to prevent even the NSA snooping.

No one mobile OS is inherently more secure than another. They each have strengths and quite often the more popular one can be more secure but due to popularity, that is where most hacker attacks are aimed. Basically it is a numbers game. But I will say at this time that Android needs to improve its app security. Apple has an easier time as they have a more stringent entry test to getting an app into their app store. Google by default allow most people to post an app to the store but they are trying to become better at identifying rogue apps. One could also say Windows phone is secure as most of the popular leading apps were either written by Microsoft or paid third parties! BlackBerry before its demise due to the BlackBerry messenger app was considered an excellent secure messaging system. We do know however that there is a global private key and we have to simply assume that the NSA know this key so no message anymore can be considered safe. In fact, BlackBerry themselves however in their BlackBerry solution technical overview document advise users to 'consider pin messages as scrambled, not encrypted'.

If you are paranoid, then do not use e-mail services such as yahoo, Gmail or Hotmail. In all likelihood the NSA have sent national security letters to each of those providers and got the keys (or more likely, installed wire taps upstream of their data centres and are recording all the traffic to later decrypt quite easily…..) There are products such as sold by Go-Trust Technology Inc. who sell and Android App which uses a hardware secure element embedded in a microSD to safeguard sensitive information by encrypting SMS text messages, photos, videos, data files and contacts. Hardware encryption can be effective. No real details have been released but there is every chance that a hardware-based solution like this can be quite secure. It is still recommended to select a proper VPN and/or TOR over this system however. It is not recommended to jailbreak a phone as it may leave that phone more vulnerable to attack. A jailbroken phone will not quite often get the necessary updates to protect it against new vulnerabilities. Downloading random apps is always a risk. Security suites on mobile phones are still limited. The proper assessment of their capabilities has not really been carried out. It is well known that phones have been compromised whilst a leading mobile 'security suite' has been loaded on the phone. Easiest way to protect is to simply install the leading well know apps and to steer clear of 'recent uploads'. A time stamp is important as most malware on phones is discovered but the first people to download it are the ones compromised.

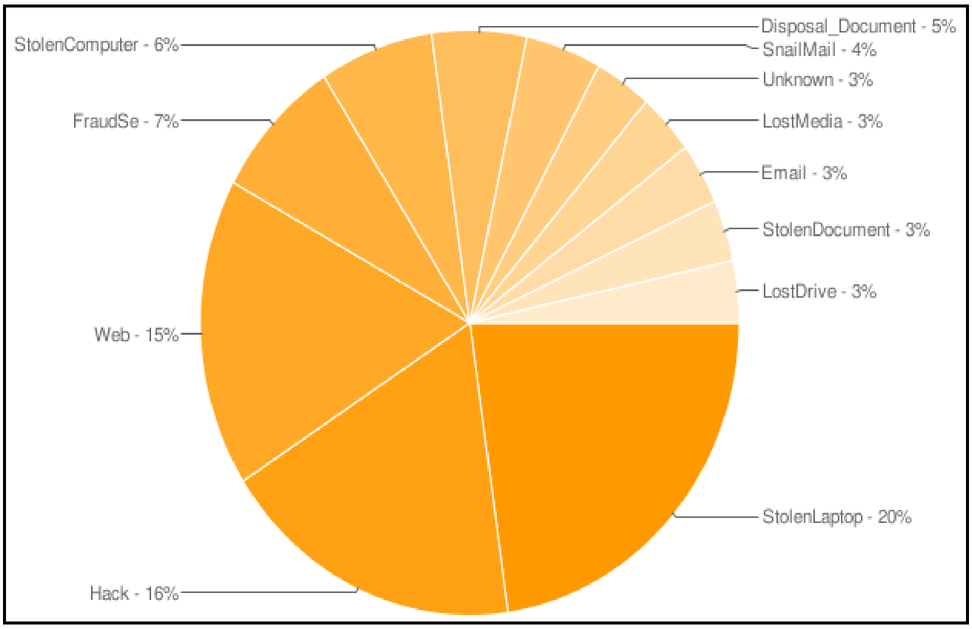
What follows is an outline of security mechanisms deployed to make mobile devices safe for use.

2 Mobile device security

A mobile device is a piece of equipment that can come in different forms. The data these devices hold could be photos or document files containing sensitive material (e.g., bank details, personal photos, credit card numbers even home address) (Fling, 2009; Holzer and Ondrus, 2009). The ranges of mobile devices that are available include mobile computers, personal digital assistants/enterprise digital assistants, pagers, personal navigation devices (PNDs), mobile phones and portable media players. More than half the global population now use a mobile phone (ITU, 2008). The advanced features of mobile devices that have made them so attractive to the end user include: internet web browsing, e-mailing, Bluetooth, wireless communication, digitising notes, file sharing and mobile field management capabilities. As mobile devices advance in terms of technology the security risk also increases (Chickowski, 2009). It is evident that the corporate organisations that fabricate the mobile device are not incorporating the correct security mechanisms within the equipment to minimise security risk (Hegarty et al., 2010; Wasserman, 2010; Jacobs, 2011).

There is different ways you can protect a mobile device, from placing it in your pocket to using encryption software. All of these devices have some type of security that restricts foreign bodies from obtaining their information. Data protection is crucial in today's world of technology. Even with the advancements in mobile devices such as card readers, chip and pin, and online payment security, data is still never 100% secure. Most or all mobile devices have the ability to enable a four-to-eight digit PIN in order to use the device. When the device is switched off onto standby, the pin security is enabled. So when you try to access the device again you will be a prompt for a pin request. If someone stole or came across your device and they seen that it was pin protected they probably would not try and hack it for the data but wipe it and sell it for a quick pound. Figure 1 presents breach statistics for 2008 on portable devices (Lingfen et al., 2010). Here we can see that more than 32% of data breaches were the result of a lost or stolen laptop, mobile phone, or other portable media device while only 14% of data breaches were the result of a hacking event. It may seem therefore that the actual problem lies with regards to data security…. outside the firewall.

Figure 1 Incidents by breach type (see online version for colours)



The starting point for protection for devices as mobile phones would be to introduce IT policies. This is a written agreement with the users of the devices and statement what can and cannot be used on them. Some examples of policies are acceptable use, password, backup, network access, incident response, remote access, virtual private network (VPN), guest access, wireless, third party connection, network security and encryption policies (ITU, 2008). BlackBerry mobiles are bound to some of these. They are pushed to their handhelds over the air during wireless activation. Through these policies employers can set their own security needs like passwords, timeouts on the device and have read only parameters; only permitting voice calls on locked handhelds for instance. They can even deactivate the Bluetooth and control how the data is encrypted. There also can be application policies. Letting the employer control third party applications and which resources they can access. All policy settings are synchronised and assigned to the BlackBerry smartphone over-the-air. As a result, BlackBerry Enterprise Server administrators who need to facilitate large deployments can easily change IT policies on a corporate level without requiring users to cradle their BlackBerry smartphones. This policy ensures that administrators can control each BlackBerry smartphone, An IT policies has digital signatures to ensure that only the designated BlackBerry Enterprise Server can send updates to a BlackBerry smartphone. When sending information through a wireless connection on the BlackBerry, the information is routed through BlackBerry's RIM infrastructure. The information is encrypted with either AES or 3DES and the keys are only known to the handheld or the BES. BES decrypts the information the sends it to the messaging server like Microsoft exchanged or Qmail which runs on Linux operating system. There are other types of encryption available like IPSec tunnelling to VPN and Wi-Fi data encryption using WPA/WPA2 and WEP keys. These methods are to stop people eavesdropping on messages during transfer (B'far, 2005; Burns, 2008).

The Symbian platform uses several algorithms, including data encryption standard (DES), 3DES, Rivest's Cipher 2 (RC2) 64 block cipher. The Symbian device will determine how the information should be encrypted and will furthermore select the required encrypted channel, if it wishes to send data. It will then use its built in functions to encrypt to the proper format for transfer. But the information on the device will not remain encrypted unless third party encryption software is installed and configured to do so. To protect data on Symbian devices they introduced a program called Symbian-signed. This is where software publishers could digitally sign applications that had been tested by Symbian. There are three different levels: Open-signed which is used for limited or internal use, Express-signed where it is self tested and certified-signed, this version is independently tested. These use the digital signatures to tie the software to publisher identities. Express and certified must use publisher Ids issued by TC trustCenter. The 'for Symbian OS' logo is awarded to applications that are Symbian Signed. Symbian Signed promotes best practice in the design of applications and content to run on Symbian OS-based phones. Symbian Signed is endorsed and supported by network operators, handset manufacturers and developers (Chickowski, 2009).

Windows-based devices are managed using Microsoft's System Centre Mobile Device Manager (SCMDM) 2008 on Windows Mobile 6.1 operating system. Just like the BlackBerry, this server is capable of over the air device activity for, policy enforcement, Software installation and monitoring/reporting. To create an account for WM6.1 the client will have to enter his or hers e-mail address and a unique PIN number. The device uses secure socket layer (SSL) to connect to the server. This gateway authenticates the user and completes the interacting with the management server. These SCMDM server functions can be distributed for instance using a separate Microsoft CA to issue device certificates. Once the device and the gateway are configured to each other they are protected by an auto-configured IPSec, 'mobile VPN' tunnel. SCMDM installs and enforces IT-defined active directory group policies. Once connected the device can be monitored centrally and up dated through SCMDM. If a mobile device is never lost or stolen, the SCMDM can be used to remotely wipe the device next time it connects to the enterprise network. A mobile device with WM6.1 installed can use 3G or WI-FI connectivity to automatically reconnect to the SCMDM from their mobile VPN tunnel (Dumaresq and Villenueve, 2010).

Google Android is a multi-tasking system. Each application runs in its own process. Most security between applications and the system is forced through standard Linux services. Their user and group IDs that are assigned to applications. The more advanced security features are provided through a 'permission' method that enforces restrictions on a task that a particular process can perform, and per-URI permissions for granting ad-hoc access to particular pieces of information. Android's security design is that it uses sandboxing. A protective mechanism that prevents a program from accessing or changing memory or disk space outside of its own permitted area. This is a security feature preventing programs from damaging the operating system. For example, a Java applet loaded from the World Wide Web runs in a sandbox where it is prohibited access to the hard disk on the browser's computer. Sandboxing are to ensure one application is protected from another. Say your PayPal application from the malware you just downloaded, using Windows XP's internet explorer. It protects the operating system from the application and to ensure one bad application cannot interfere with the good ones. Before they carry out a process the user will be prompted detailing the action to be taken. Or you could set the device on automatic, where it determines what the application is allowed to do by its certificates. Android also has application signing, similar to the Symbian OS signature on Nokia devices. However, on Android you can use self-signed certificates for your applications. This will open up the operating system to attacks from different methods. Conventional attacks uses buffer overflows and most harmful attacks rely on executing code in the memory.

The iPhone prevents malware or spyware trying to execute code on the stack or heap as it will cause an exception in the program. This is implemented by using the 'no execute bit' or NX bit. The NX bit makes areas of memory as non-executable, preventing the process from executing any code in those marked areas. Another protection the iPhone uses is a keychain which stores sensitive information. It can be used by iPhone applications to store, retrieve, and read sensitive information, such as passwords and certificates. Before granting permission the application will be verified it can use the Keychain by checking its signature. The Keychain takes care of all the key management issues, so the application just has to carry out its service. When an iPhone is backed up to a regular computer, all the data on the iPhone will be stored on the PC, except for data stored in the Keychain. If the application is not using the keychain, then the data will be shown on the computer in clear text.

Table 1 shows the difference between each operating system securities. The BlackBerry has quite an extensive range of security measures, but strangely does not have the buffer overload protection. They all possess the basic pin protection and application signing.

Table 1 Difference between each operating system security approaches

Feature	*BlackBerry*	*Windows mobile 6*	*iPhone*	*Google Android*
Pin	Yes	Yes	Yes	Yes
Remote wipe	Yes	Yes	Yes	No
Remote policy	Yes	Yes	Yes	No
Lojack	Third party	Third party	No	No
Local mail encryption	Yes	No	No	No
File encryption	Yes	No	No	No
Application sandbox	Yes	No	No	Yes
Application signing	Yes	Yes	Yes	Yes
Buffer overflow protection	N/A	GS stack protection	Non-executable heap and stack	Propolice, safe_iop, OpenBSD, malloc and calloc

Source: Dwivedi et al. (2009)

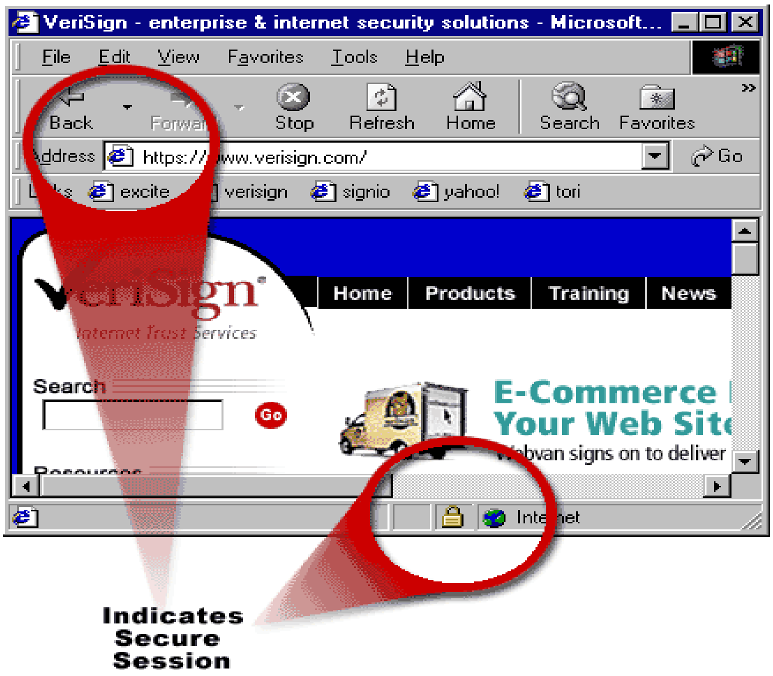
3 Authentication

There are several authentication mechanisms which can be incorporated in mobile devices including digital signatures. A digital signature is designed to assure recipients that the senders of messages are really who they claim to be and the messages have not been modified along the way (Ni and Zheng, 2006). The sender of a message signs a message via a digital signature just like the way a cheque is signed to authenticate it. Therefore it can be deemed that a digital signature authenticates a message and it ensures a message is genuine. The verification of digital signature endures a stringent process and involves two parties namely: the sender and the recipient. Firstly the sender constructs the message and the clear text is prepared for sending. A hash algorithm is then used so the data (message) is hashed which cannot be reversed. Then the digital signature is generated by using the sender's private key to encrypt the message. The final stage of the process is to attach the final signature to the message and then send the message off to the recipient. When the recipient receives the message the first stage is to decrypt the message using the sender's public key. The message body is then hashed by the hashing algorithm. The result of this is then compared with the decrypted message digest. If the two are the same it can be deemed the message has not been distorted and that it is still in its original state. The authentication process is now complete. This method of authentication is deemed full proof for if someone tries to mimic the sender, it is impossible as they do not have the sender's private key and therefore cannot generate a valid digital signature. If a hacker tries to intercept and distort a message, the hash code of the received message will differ from that carried in the digital signature. Therefore overall making use of digital signatures is an excellent method of authentication to ensure messages remain confidential and uphold their integrity (Kumar, 2007; Onias, 2003).

Passwords can be used to ensure unauthorised personnel do not gain access to data and information. In a networked computer system a user has a password to gain access to the system. When the user enters a password it must be authenticated against managed security tokens which are held on a log-in server. Passwords on the log-in server are usually hashed. If both sets of data match access is granted otherwise the user can not gain access to the system. Passwords should be changed on a regular basis to ensure their value and worth is obtained. When passwords are being created they must follow the creation guidelines to ensure a good, secure password is chosen. Often in the case of mobile phones a four digit PIN number acts as a means of identification.

A further mechanism which can be deployed is that of internet protocol security. The main purpose of this set of protocols and mechanisms is to provide message authentication, integrity and confidentiality to the IP layer. IP packets can be sent over the network in two ways, transport mode or tunnel mode. The encapsulating security payload protocol header is inserted after the original IP header, and the original IP payload is encrypted when utilising transport mode. Whereas with tunnel mode a new IP header is inserted, then an encapsulating security payload protocol header followed by the encrypted IP packet. With both modes an encapsulating security payload protocol field is inserted at the end of a packet consequently ensuring authentication and message integrity. Another mechanism which assists the security and authentication process on mobile devices is the SSL. The SSL and transport layer security (TLS) are network security protocols which work at the transport layer. The main function of SSL and TLS is to work with protocols especially hypertext transfer protocol (HTTPS) to certify there is communication between the web client and the web server. TLS is also used with other application protocols such as simple mail transfer protocol (SMPT) and Post Office Protocol 3 (POP3). The web client must obtain a public or private key and a digital certificate so SSL can be used to authenticate the web client. Users can know a website is secure when the padlock symbol is evident at the bottom of their screen (see Figure 2).

Figure 2 Secure internet session (see online version for colours)


VeriSign - enterprise & internet security solutions - Microsoft...
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
Address https://www.verisign.com/
Go
Links excite verisign signio yahoo! tori
VeriSign Internet Trust Services
Home Products Training News
Search
Go
Resources
E-Commerce Your Web Site
Webvan signs on to deliver
Internet
Indicates Secure Session

4 Preventing loss of information

Due to their size and portability, mobile devices can be lost or mislead. One mechanism which could be employed to resolve this issue is remote wipe capabilities. Remote wipe capabilities are enabled on the mobile device or the appropriate software installed. When a device goes missing the administration program can be run to view all devices. The lost device is then selected from the list and wipe or delete commands are sent. When the commands reach the device they are then executed resulting in the removal of the data. Google for instance is adding basic mobile device management capabilities to Google Apps that will let IT managers remotely wipe data from lost iPhones. The remote wipe and other management features are available to users of Google Apps and will work for iPhones, Nokia E series devices, and windows mobile smartphones (Gohring, 2010). In the case of business users it is not sufficient to set up and install the remote wipe capabilities without a lost phone/mobile device hotline. If an organisations IT department sets up a hotline and the IT department will then take the correct measures to ensure the data is wiped from the device. This process can also ensure data is not lost as the IT department can also perform a back up of the data before deletion. Overall the remote wipe capabilities are an excellent security mechanism but a lost device hotline needs to be set up to ensure full capacity of the mechanism is achieved.

Since mobile phones and devices are becoming more advanced and are online their vulnerability has been dramatically increased. Most mobile devices can have third party software applications installed on them. When a user downloads third party applications they are unsure of the security of the software, especially the novice user. In other cases users do not subconsciously install the software on their machine, installation takes place unknown to them. The main problem with unsigned software is that when it gains access to the mobile device it relinquishes control. What commonly happens is that a virus usually in the form of a Trojan horse is unleashed via the internet to gain access to the mobile devices' VPN, Wi-Fi or dial-up. If a mobile device is infected with a keystroke logger it can have a detrimental effect. Firstly, access credentials to the network can be stolen and transmitted to a server on the internet. One should not accept gimmicks, special offers, open uncertain e-mails or download unknown programs or data to a mobile device as these sources carry the most risk. However it is important to realise that even if the user is extremely cautious and deploys the recommended security precautions the third party software applications can still enter the mobile device via loop holes in the operating system.

One further element which should be highlighted is the fabrication of firewall policy. An organisation should implement a firewall policy if they know their employees will be accessing data especially that of sensitive data via mobile devices. Accessing data from mobile devices could pose a great security threat to company data. The firewall policy will allow access from mobile devices that they see fit otherwise access will be blocked. Intrusion prevention software is another mechanism which can be integrated into mobile devices to ensure they are secure. Intrusion prevention software can be articulated as a software program which runs on a mobile device to stop unauthorised personnel acquiring access. All the traffic penetrating the network is examined in turn to scrutinise its authenticity. If it is believed to be genuine material, access will be granted otherwise it will be blocked. The software can perform these actions unknowingly to the user or provide notification of actions. The user can configure the software accordingly to meet their needs and requirements. Intrusion prevention software is another avenue which should be explored by the user when considering security instruments for their mobile device.

5 Bluetooth vulnerabilities

Bluetooth technology in mobile devices is one of the features that has rapidly developed in recent years. Bluetooth can be denoted as a short range wireless technology used for exchanging data between mobile devices. Even though the Bluetooth signal can only travel a short distance it can still be susceptible to security risks. Security risks encompass of data confidentiality and authentication. The Bluetooth special interest group (SIG) was established to ensure the integration of a security architecture into the Bluetooth official specification. Therefore the SIG has defined a number of security policies to deal with potential security threats. When one mobile device wishes to connect with another, authentication comes into play. If device 1 wants to access device 2 then it must be authenticated by device 2. Device 2 sends a random number to device 1 and uses a secret key to compute a response. The response is then sent and received by device 2 where it performs computations and finally compares this result with the response. If both the result and response match then authentication can take place. The second Bluetooth baseband security mechanism is per-packet encryption. This policy works using the main encryption policy. Once again an encryption key is generated utilised an algorithm. The encryption process is then started with the master sending a random number to the slave. The slave then computes a keystream using yet another algorithm and ciphertext is produced. Since the mechanisms that can be incorporated into Bluetooth devices have been discussed it is no fitting to also discuss the loopholes and vulnerabilities of devices for attack. When two Bluetooth devices try to connect a PIN number or authorisation code is usually required. This information can be the gateway for a hacker to gain access to the mobile device. A hacker can eavesdrop on the communication channels between the two parties to snatch the clear text which contains random numbers. Then the hacker can perform the key algorithm which produces the users PIN code. The hacker can also gain the encryption key alongside the PIN code. With these two vital pieces of information the hacker can easily access the mobile device. A mobile device user can increase security by choosing a long PIN code, a PIN code can be up to 128 bits in length. The user can also disable or turn off Bluetooth capabilities when they are not using their mobile device to ensure security is maintained. Furthermore the user can conduct the communication process in a closed environment as opposed to a wireless environment.

Even though the Bluetooth specification has provided a firm foundation for security in Bluetooth mobile devices it has become apparent some of the mechanisms have not been well implemented nor taken into account. This leaves the device susceptible to attacks such as Bluesnarfing, Bluebugging, Bluejacking, Back-door attacks, Virus and battery draining. Bluesnarfing is known to take place as a result of an insecure mode in devices enabled by some manufactures. Hackers can launch an attack on the device using modified Bluetooth equipment which exposes all the data on the device. This is a very powerful method of attack and poses great threat. A Bluebugging attack is one in which a hacker controls a device remotely allowing interception and rerouting of the communication. This type of hacking is extremely difficult to trace. A user can ensure this does not happen with their mobile device by making sure the device mode is not set to discoverable. When in discoverable mode a device is in a very venerable state. Bluejacking takes place due to a weakness in the Bluetooth handshake protocol. The handshake protocol is used when two devices are communicating and authenticating. This leaves a vulnerability whereby the hacker can alter the device name and then send anonymous messages. This is not such a furious attack as the others detailed as the user still remains in control of the device and the data remains secure, the displaying of anonymous messages can alarm the user. With a back-door attack the hacker targets the pairing relationships that have been established between the two mobile devices. The hacker can take control of the device and monitor it remotely. Such control will enable the attacker to see and download all data on the device including pictures, e-mails, business cards and calendars. The hacker can also access applications on the device such as the camera, music player, internet, network connection and audio recorder. This attack is one which has the potential to cause most damage as the mobile device is left wide open and the user is not even aware it is happening.

The last forms of attacks are viruses and battery draining. Mobile Operating Systems have been tweaked and security heightened but there is still evidence they can be attacked for viruses especially worms. The worm scans devices to see if the Bluetooth feature is turned on and if so it sends itself to that device. Prompt messages are displayed on screen asking for the user's permission to install programs, the user usually clicks ok and does not actually read what they are installing. Therefore the virus has easily been installed on their device, in fact the user has actually agreed to it. When the worm has infected the device it then constantly scans for other devices which have Bluetooth switched on consequently draining the device battery extremely quickly. One type of worm that has been successful in infecting devices is the Cabir worm. To prevent this type of attack a user should be careful about messages displayed on screen and not agree to the installation of programs unless they are certain they know that it is. Also anti-virus software could be deployed to combat this. The best practice a user can follow regarding Bluetooth is only turn it on when transmitting data otherwise turn it off and keep it off, that way your device and its data will remain safe and secure.

6 Privacy

Smartphone security in general is a problem. There are over two billion smartphones in use worldwide, with the majority of consumers using their devices for both personal and business use. Smartphones are becoming the PC of yesteryear with the added problem of mobility which can lead to physical theft which can then lead to identity theft as more of use store important financial information on smartphones such as credit card and bank account information, e-mails, photos, notes, contacts and messages. The number of identity fraud incidents is increasing year on year. Smartphones running the Android operating system represent the majority of all new phone purchases. Unlike Apple iOS, RIM BlackBerry or Windows Phone, the phone manufacturer not the software vendor is responsible for providing Android software updates to their smartphone. Phone carriers also inject themselves into the mix by selling further customised models and sometimes charging data usage for software updates. This is a problem especially with Android as waiting for an Android phone to receive the latest release can be very frustrating.

Smartphone vulnerabilities include a large attack surface due to the actual number of communications protocols such WiFi, SMS, MMS, GPS, cell radio, e-mail, web, USB through which they are connected. And by default all smartphones are 'connected'. That is not the case with traditional desktops and laptop. It is also pretty difficult to reduce this attack surface, because the connections are what people expect to keep. Another problem leading to attacks are the malware on the online app stores. Apple are better at policing their store than Google. In addition, the tiny lower-accuracy keyboards on mobile devices can also have a negative impact on authentication. Entering a ten-character password that is easily entered on a desktop with 13 or so keystrokes can take 26 or more key-presses on a smartphone. The majority of vulnerable smartphones are Android. A reason is that many Android phones come to the market at least one major version behind the latest Android release, and they linger six months behind the update curve moving forward so a lot of over the air updates simply never make it to the phone leaving it in a vulnerable state. There are a number of ways people can better protect themselves from revealing sensitive information. The most obvious tip is to employ a pin code on the phone. Surprisingly, only 50% of people put a lock code on their phone therefore any stolen phone can allow thieves to also burrow into all information on the phone. For the first time in our history, banks and other financial institutions are beginning to offload the blame for an account being hacked onto the customer. They are claiming that customers should have had greater protection mechanism in place. For that reason alone, a pin is best practice. It is also possible to lock a SIM card.

To be ultra secure, you should encrypt a phone and place a pin on it to increase privacy. Try not to install anything on it apart from absolutely essential apps. Block all location activity, turn off GPS and uninstall all defacto apps not useful which are there from the start. Main thing is to turn off location update settings. I also place a piece of black tape over the front facing camera lens. Then install a VPN client such as proXPN or even Orbot. Orbot is an application that allows mobile phone users to access the web, instant messaging and e-mail without being monitored or blocked by their mobile internet service provider. Orbot brings the features and functionality of Tor to the Android mobile operating system. TOR is a way of browsing the web which leaves no trace and allows you to remain anonymous. Do not install any software which claims to be 'secure', snoop free which the community of security experts are not familiar with. Orbot is of course fine.

7 Conclusions

It is difficult to generate a common security structure which addresses all the vulnerabilities in the mobile device world. Therefore it is quite possible that no one lone solution will resolve all potential problems. Firstly the operators of the networks mainly wireless need to take responsibility for providing a secure, efficient mechanism of communication. Such communication channels need to encompass of strong authentication procedures to ensure the security of mobile devices is upheld. The mobile devices themselves need to incorporate system-level security to ensure they are not susceptible to attacks in both network and virus format. The manufactures of mobile device applications and services need to once again incorporate strong authentication, authorisation and accounting procedures. Even if all these mechanisms are deployed further issues that need addressing to ensure mobile devices are secure are political and cultural concerns, social engineering and business practices and policies. In summation no device will ever be 100% full proof but a user should follow the ten best practice guidelines and manufactures of both networks and devices should fulfil their role of providing safety and security for users.

Security features within Enterprise networks are different from one mobile operating system to the next. Some mobile operating systems are more equipped for the enterprises regarding security features, but each has its own benefits. Companies should not select which mobile devices have the best security settings and settle on that for the whole organisation but rather adopt a plan laid out for each mobile device that includes IT policies and application restrictions. For example, an organisation may decide that the Android device has the strongest OS for securities and therefore sanction it for the entire company. But there could be important people within the company using iPhone devices. Likewise, an organisation may think Symbian is the best platform, but their mobile application is available through the BlackBerry application store, therefore the Symbian device would need to support it also. Companies should be prepared for employees to use any of the four major mobile devices, or even a few more, and have a supported security solution for each of them. Although companies may choose a supported handset for the enterprise, employees may want a device that they are comfortable with, even if it is not the preferred solution. The refusal to have a security solution for each device expected in the enterprise may mean that corporate data is walking away in an unsupported and uncontrolled fashion, thus making the choice not to support a device much more risky.

References

B'far, R. (2005) *Mobile Computing Principles: Designing and Developing Mobile Applications*, Cambridge University Press, London, UK.

Burns, J. (2008) *Developing Secure Mobile Applications for Android*, iSec Partners, NY, USA.

Chickowski, E. (2009) 'Ten best practices for mobile security', *Baseline Magazine*, 26 February [online] http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/.

Dumaresq, T. and Villenueve, M. (2010) *Test Strategies for Smartphones and Mobile Devices*, Macadamian Technologies, London, UK.

Dwivedi, H., Clark, C. and Thiel, D. (2009) *Mobile Application Security*, McGraw Hill Professional, San Diego, USA, ISBN: 0071633561.

Fling, B. (2009) *Mobile Design and Development*, O'Reilly Publishers, Cambridge, MA, USA.

Gohring, N. (2010) 'Google Apps now can remote-wipe files from iPhones and Windows Mobile devices', *Infoworld*, February 4 [online] http://www.infoworld.com/d/mobilize/google-apps-now-can-remote-wipe-files-iphones-and-windows-mobile-devices-175?source=rss_infoworld_news.

Hegarty, R., Lunney, T., Curran, K. and Mulvenna, M. (2010) 'Ambient interface design (AID) for the ergonomically challenged', *International Journal of Ambient Computing and Intelligence*, April-June, Vol. 2, No. 2, pp.57–65, ISSN: 1941-6237, IGI Publishing.

Holzer, A. and Ondrus J. (2009) 'Trends in mobile application development', in C. Hesselman, C. Giannelli, O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari et al. (Eds.): *Mobile Wireless Middleware, Operating Systems, and Applications – Workshops*, Vol. 12, No. 2, pp.55–64, Springer Berlin Heidelberg.

Information Week (2011) 'Most consumers don't lock mobile phone Via PIN', April [online] http://www.darkreading.com/risk-management/most-consumers-dont-lock-mobile-phone-via-pin/d/d-id/1100508?.

International Telecommunications Union (ITU) (2008) *Market Information and Statistics* [online] http://www.itu.int/ITU-D/ict/statistics/.

Jacobs, M. (2011) 'Living on the edge of mobile development' [online] http://java.sys-con.com/node/1719019.

Jha, A.K. (2007) *A Risk Catalog for Mobile Applications*, Florida Institution of Technology, Florida, USA.

Kukkonen, H.O. (2003) *Developing Successful Mobile Applications*, Stanford University, California, USA.

Lingfen, C., Woods, D., Curran, K. and Doherty, J. (2010) 'Mobile development environments for electronic finance', *International Journal of Electronic Finance*, Vol. 4, No. 3, pp.20–28, ISSN: 1746-0079, Inderscience.

Ni, L.M. and Zheng, P (2006) *Smart Phone and next generation mobile computing*, Morgan Kaufmann Publishers, San Francisco.

Wasserman, A. (2010) Software Engineering Issues for Mobile Application Development, ACM Digital Library, NY, USA.