Managing Smart Phone Security Risks

Max Landman
Information Systems
Kennesaw State University
1000 Chastain Rd, MS 1101, Kennesaw, GA 30114
mlandman@students.kennesaw.edu

ABSTRACT
Smart phones, their operating systems and security characteristics have rapidly evolved as has the reliance upon them by organizations to conduct business. The unusual mix of personal and business use for smart phones as well as their unique combination of capabilities creates a number of challenges to managing their risk. This paper explores the types and nature of threats to the organization from the use of smart phones along with controls, available security software and tools. The current state of corporate smart phone security programs and policies is examined. Smart phone security policy considerations are discussed and recommendations are made for building a smart phone security program.

Categories and Subject Descriptors
C.2.0 [**Computer-communication Networks**]: General – *security and protection.*
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection (D.4.6 K.4.2) – *authentication, invasive software, unauthorized access.*

General Terms
Management, Security, Human Factors

Keywords
Smart phones, security policies

1. INTRODUCTION
The increasingly sophisticated capabilities of smart phones and the growing reliance upon them by organizations to conduct business are creating an ever more attractive target for criminal attacks. Vendors of security software are just beginning to develop products that are more than knockoffs of PC security software and deal with the new vulnerabilities posed by smart phones. Lagging further behind are the organizations that have yet to implement adequate controls for smart phones and the policies to guide their use. Managing the risk of smart phones requires specific policies to address their unique attributes and usage. Smart phone security must also be integrated into the enterprise security policy. Smart phones not only have different technical and connectivity attributes than PCs, but they engender a different attitude, one that undermines security policies and practices. The blur of personal and business perspectives towards smart phones makes the establishment and enforcement of security programs and policies particularly difficult.

InfoSecCD'10, October 1-2, 2010, Kennesaw, GA, USA.

The number of mobile workers is rapidly increasing and most mobile workers will be relying on their smart phones in the course of their work. So while to date malware has been far less of a threat to smart phones than PCs, there is every reason to expect that to change. Malware and rootkits have successfully infected every major smart phone on the market, but malicious code is not the only threat to smart phones in the enterprise. Phishing, social engineering and direct hacker attacks have already been conducted successfully as well. Intercepting communications from smart phones is relatively easy and lost, stolen and improperly disposed phones present a huge risk to organizations that increasingly have confidential data stored in and communicated with smart phones. But the greatest danger lies in inappropriate user behavior fed by the mixing of personal and business use. Users often do not distinguish between these uses or the security rules appropriate to each and they typically lack awareness of the threats and potential damage from smart phone attacks.

CIOs and CISOs can use security education training and awareness initiatives to prevent inappropriate user behavior and employ controls to protect device access, network access, data communication and stored data from attackers. To be effective these controls must take into account the distinct characteristics of the different smart phone operating systems and security attributes. Controls to protect access to devices and their data include authentication procedures and the use of intrusion detection, firewalls, context-aware access control, remote device management, digital certificates, sandboxing and encryption of stored data. Encryption of transmissions and appropriate connectivity restrictions can help secure communications over a Wireless Wide Area Network (WWAN), Wireless Local Area Network (WLAN) and a Bluetooth Personal Area Networks (PAN). In addition for a WWAN and a WLAN, the use of a Virtual Private Network (VPN) is essential.

Before controls can be safely deployed, a comprehensive security program with security policies specific to smart phones must be implemented and incorporated at a high level into the enterprise security policy. The National Institute of Standards (NIST) issued guidelines for handheld mobile device security in 2008 and many security experts have offered ideas and methodologies for getting a smart phone security program in place. However, recent surveys show an appalling lack of smart phone specific plans and policies in organizations underscored by a failure to appreciate

the serious threats to enterprise security from unsecured smart phone usage. This lack of awareness is particularly serious at top management levels, where support is needed for CIOs to implement smart phone security policies that may be unpopular with employees and seen as interfering with their jobs and personal lives. Achieving a balance between effective smart phone security policies and procedures, efficient business operations and employee acceptability is a serious dilemma for CIOs and security professionals today.

2. BACKGROUND

First easy access is provided and then security follows. This predictable pattern is being repeated again with smart phones which are increasingly being deployed in businesses but which are not included in conventional network security. Smart phones could soon be the most vulnerable point in corporate security. While so far there has only been a small amount of malware activity targeting smart phones compared to PCs, the rapid rise in the number of smart phones accompanied by their increased capabilities and use by corporations makes them attractive targets [9].

International Data Corporation (IDC) predicts there will be more than one billion mobile workers in 2011 and by 2012 three quarters of all workers globally will be mobile workers. The Ponemon Institute calculates that each breach of mobile security in the UK costs £47 and that 36% of these breaches are due to lost or stolen mobile phones. Over 80% of business executives are continually connected through their mobile handsets according to Korn/Ferry International. This growth of smart phones and corresponding growth in their applications and storage of sensitive data means perimeter security is increasingly being breached [12].

Yet in spite of this dramatic growth and increased threat inherent in smart phone use, security for smart phones significantly lags behind security for PCs. The complexity of securing smart phones that operate on multiple networks is a far greater challenge than securing PCs. While vendors of PC security software are now offering products targeting smart phones, simply moving PC controls over to smart phones will not be effective. In fact there are no widely accepted security standards for mobile phones with respect to controls such as communicating over VPNs, encrypting data stored on the phones, use of passwords to control access and shutting down the devices remotely [12].

Smart phones today store hefty amounts of data and operate over international cellular networks, WLANs and Bluetooth PANs. They run a diverse set of complex operating systems such as Symbian, iOS, Blackberry OS, Android and Windows Mobile. Most smart phones also support the Java platform for mobile devices, J2ME, with a variety of extensions. All this network connectivity and diverse rich code makes these devices more vulnerable than traditional PCs, which typically run standard operating systems for which many security products are readily available [21]

Smart phones lack many of the security capabilities of PCs. Some smart phones cannot read a Secure Sockets Layer (SSL) certificate or even attach a certificate from an organization's own certificate authority. Firewall capabilities and centralized management are just beginning to become available. On top of all this, rapid changes in the still largely consumer driven smart phone market mean that code is quickly written, deployed and replaced. Development platforms that support the writing of secure code are lacking for mobile devices, particularly the operating systems which are often written in C or other native languages leaving security totally to the discretion of the developer [21].

3. THREATS

Conventional viruses have not been the major threat to smart phones that they have been to PCs. More often the threat is simply rogue code or malfunctioning applications that are not addressed by anti-virus vendors focused on the more virulent and easily detectable PC viruses. The threat from accidental or malicious misuse by employees is a significant threat to business. Smart phones are frequently lost or stolen and individuals often use them to communicate sensitive data, even in violation of applicable security policies. Passwords and encryption are of no use in these cases. Administrators often cannot remotely audit the content of smart phones as mandated in the International Organization for Standardization (ISO) 27001 security requirements. They frequently do not know what information has been stored on the phone and may not be able to remotely delete data or kill the device [12].

3.1 Malware

Scott Totsky, Vice President of Product Security at Research in Motion, reported in May of 2010 that there are only about 400 malware occurrences per year on smart phones compared to 4 million on desktops. Totsky also noted that 43 companies had breaches in security from smart phones in 2008. However with the significant increase in smart phone usage, it is inevitable that a corresponding increase in malware attacks will follow. The increasing diversity of smart phones and the threats to them pose new and unique challenges to businesses and individuals responsible for information security. For example, security solutions can eat up the resources of smart phones and the effectiveness of these solutions is highly dependent on users to invoke the security applications on their phones [1].

The lack of sufficient computing power is a major reason that smart phones have not been attacked as much as PCs. However, that is changing rapidly. This same characteristic has made it difficult to provide security for them. Collecting diagnostics and the security technologies used in a PC can significantly degrade smart phone performance. Managing risk on smart phones is more expensive than managing risk on a PC and this high cost is exacerbated by the rapid changes in smart phone models and architectures. Yet some attack techniques cost little such as eavesdropping on a Global System for Mobile communications (GSM) signal [26].

Smart phones are quickly approaching PC capabilities and the same incentives exist for the hackers: Fraud, stealing personal and business information and extortion. Hackers are poised for attack with many different avenues available to spread malware some of which has multiplatform capabilities that can damage smart phones and PCs alike. The following brief review of smart phone malware shows that the malicious capabilities of the hackers have clearly been demonstrated [9].

Cabir, a worm that attacked mobile devices with Symbian OS came out in June of 2004 and now can be found in 40 countries.

Cabir spreads through Bluetooth, an easy and effective vector that subsequent malware such as Comwar, PBStealer, and Skuller among others also used. Mobile phone users frequently leave Bluetooth in discoverable mode, inviting malicious attacks and infections. In fact, research by Kapersky labs showed that 25% of users with devices in discovery mode accepted files sent via Bluetooth. Comwar uses Multimedia Messaging Service (MMS) to send enticing messages to run the code to all the contacts on an infected phone. Skuller replaced icons with skulls and crossbones and disabled the associated service [9].

Duts, a virus targeting Windows Mobile and Windows CE, appeared in 2006 followed by Brador the first Trojan targeting these devices and Flexspy, a Trojan targeting the Symbian OS. These Trojans with backdoor capability can easily steal the often unencrypted and sometimes not even password protected data stored on smart phones. The Trojan Mosquit used Short Message Service (SMS) to send messages without the user's knowledge. Lasco is a hybrid worm and virus and CXover is a Trojan that infects both Symbian OS smart phones and Windows PCs targeting Windows after it deletes files on the Symbian device and looking for Symbian devices once it is on the PC. The RedBrowser Trojan can spread to any phone running Java via Bluetooth [9]. This means most smart phones are vulnerable regardless of operating system. Blackberry devices have been targeted by BBproxy, Palm devices by Liberty.A, PALM Phage.A and PALM Vapor.A and Trojans attacking iPhones have been reported [11].

Malware embedded in three different applications for Windows Mobile phones was reported by *eWeek* on June 7, 2010. After lying dormant for three days the malicious dialer calls between four and six expensive international phone numbers. The malware then goes dormant again for a month before making another round of calls and then repeats every month. So after getting hit for potentially hundreds of dollars in phone bills it can be some time before the victim figures out what is happening. The offending applications, "3-D Anti-Terrorist", "PDA Poker Art", and a Codec Audio pack, can be obtained at websites offering legitimate applications. Another malware dialer known as the Terred Trojan had previously infected "3-D Anti Terrorist", Symantec reported last April. Neither malware affects the operation of the infected games. Fortunately the malware does not erase call history so a record of the calls exists. Smart phone users should keep their phones regularly updated with current antivirus software to protect against the ever increasing presence of malware [22].

Rootkits can infect mobile phones just as they can PCs, but they have new targets to damage on mobile phones. Not only can they install Trojans and disable firewalls and antivirus software, but they can attack the phone's voice, messaging, GPS and battery. In addition to logging key strokes as they do on PCs rootkits on smart phones can record conversations and even make a phone call. They can use the GPS to track the victim, with the perpetrator receiving regular updates of the victim's location. Rootkits can also quickly exhaust a mobile phone's battery by activating power hungry features. Rootkits can be sent through email or picked up on websites or through Bluetooth connections. Rootkits infect the kernel of the operating system and if they stay only in memory they can elude detection. Mobile phones are rebooted more frequently than PCs thus providing a memory only resident rootkit less time than on a PC. However, much damage can still be done [2].

3.2 Phishing & Social Engineering

The 2009 Cisco Midyear Security Report noted the increased use by hackers of social networks and SMS text messages to take advantage of mobile phone users. Two primary techniques used were phishing and inundation with unwanted advertising usually for drugs from fake pharmacies. Cisco reported that in 2009 new attacks started every couple of weeks. The attacks often took advantage of current events. For example, over 2 billion spam messages embodying a variety of scams went out following the death of Michael Jackson. The report states that mobile devices are "the new frontier for fraud irresistible to criminals" [14].

The Cisco report identified the increasing use of a new technique, smishing, a phishing attack using SMS messaging to send a fraudulent link to a smart phone. Most attacks with SMS messaging still direct the user to call a phony number rather than click on an embedded link. Once the fake number is called, typically a recorded voice will answer asking the victim to enter personal information through the touchtone phone. The report also notes the increased number of vulnerabilities that are being discovered in smart phone operating systems. The report concludes that the growth in usage of smart phones means that an increase in new attacks will certainly follow. [14].

3.3 Direct Hacker Attack

An example of a very recent vulnerability is with the iPhone. IT blogger Jim Mareinfeldt was able to bypass the 4 digit pin in the current O/S version of the iPhone, access almost all of the data stored on it and get out without leaving any sign that the iPhone had been hacked. This was reported to Apple, but as of June 7, 2010, no time line for a fix had been set. Users have assumed that the authentication protection provided by the Personal Identification Number (PIN) would protect them. This vulnerability is a serious issue for businesses because according to Ron Spears, CEO of AT&T Business Solutions, four out of ten iPhones are purchased by business users. One reason for the robust sales to business users is the iPhones reputation for strong security [16].

A number of direct attacks via Bluetooth can be used to gain access to and even control of smart phones. Bluebug and Bluesnarf allow the attacker access to contacts, text messages and other content without detection. Other direct attacks capture the PINs during pairing and use brute force techniques such as BT crack and btpincrack to reveal the PINs. A four digit PIN can be cracked in milliseconds while a sixteen digit PIN takes thousands of years, so PIN length is very important. Another way to get PINs is to simply guess. Many users never change the default PINs shipped with the device. Car-whisperer makes this easier by trying the most common PINs for Bluetooth devices, particularly headsets and hands free accessories [8].

3.4 Intercepting Communications

Man-in-the-middle attacks using public wireless local area networks are a significant threat to smart phone security. SMobile Systems tested the iPhone, an HTC phone running Android, an HTC phone running Windows Mobile and a Nokia phone. All succumbed to the attack in which SMobile used a laptop to intercept network traffic and get user names and

passwords. A number of tools were effective including Arpspoof which sends fake Address Resolution Protocol replies to redirect packets; SSLstrip which collects HTTP communications; Ettercap which sniffs, intercepts and logs; webspy which can open sniffed out web pages; and Wireshark a network analyzer used as a sniffer. All communications from the smart phones were rerouted through the attack laptop to the WLAN access point. Since the data is going through the hacker's machine unencrypted, usernames and passwords entered when the victim opens email and even bank accounts can easily be seen. While applications that employ encryption would prevent this attack, such applications are not commonly used. Antivirus software, firewalls and encryption are just as important for smart phones as for other corporate mobile computers [4].

Another man-in-the-middle attack takes advantage of the Bluetooth feature Just Works which is used to connect to a printer without authentication. The BT-SSP-Printer-NITM attack interrupts the connection with a denial of service attack. When the victim tries to reconnect, the attacker's device is disguised to look like both the sending device and the printer so it becomes a relay with full unencrypted access to the entire transmission [8].

3.5 Stolen and Lost Phones

Lost and stolen phones and mobile devices are a serious problem. In June of 2010 *CIO.com* reported that 31,544 smart phones had been left in New York City taxis in the last six months [1]. In 2005 Pointsec and the Licensed Taxi Drivers Association surveyed taxi drivers in London and other cities. London taxi drivers reported over 60,000 mobile phones along with 5,500 PDAs and 4,500 laptops were left in their cabs over a six month period. The smaller phones appear to be more likely to be left behind. In fact loss or theft of smart phones is more apt to result in financial damage to a company than malware attacks. Loss is a well documented security threat to smart phones but so is improper disposal. An example is an incident involving a Wall Street banker selling his supposedly non-functioning Blackberry upon leaving his employer resulting in the buyer getting hundreds of private emails and a huge detailed contact list after putting in new batteries [10].

3.6 User Behavior

Employee behavior often creates vulnerabilities. Employees may be careless, unaware of policy or deliberately violate policy for convenience and lack of appreciation for the risk involved. This is particularly true for smart phones where the lines between personal use and business use may not be clear or are ignored. Examples of vulnerabilities created by user behavior include turning off security applications such as antivirus software or firewalls, downloading infected applications from the web, using instant messaging or file sharing software in violation of policy, putting confidential information on removable storage devices, and putting confidential information in emails sent to unauthorized recipients. Surveys indicate that most employees are aware of information security policy violations and one-third of the employees surveyed said that they need to skirt policy in order to do their jobs. Malicious insiders also are a potential threat. They may be disgruntled employees out for revenge, former employees sharing confidential information with a future employer or an individual selling confidential information for personal profit. Smart phones make all of this easier. Viewed as a personal device, they are often taken by the employee with all the data on them when leaving the company [11].

4. CONTROLS

Effective enterprise smart phone security programs need to address user behavior, access to the phone and network, and communications and storage of data. Mobile devices by the very nature of their use invite lax security practices on the part of users. Encryption, firewalls, antivirus software, digital certificates, remote kill and remote data deletion can be used to protect access to devices and the data stored on them. VPNs can protect data while being communicated. Networks can be protected through the use of the Remote Authentication Dial In User Service (RADIUS) protocol and other security technologies while wireless networks can be guarded with Wireless Protected Access (WPA) and by modifying defaults [6].

Controls for networks can be applied to smart phones. Controlling remote access through authentication software and ensuring VPNs are properly configured can mitigate the damage from lost or stolen phones. WPA2 should be used for authentication and Advanced Encryption Standard (AES) 256 cipher used for encryption. Businesses must take the responsibility for controlling access to smart phones and not rely on the users for security. Password protection should be robust and two-factor authentication should be employed. The ability of the enterprise to monitor and control the data on smart phones is critical to its overall security [12].

Smart phone platforms have different inherent security characteristics. If at all possible, the organization should control the selection of smart phones and consider their security capabilities as a critical element in their selection. David Canon, Program manager of communications at IDC Australia, suggests that CIOs select phones with platforms that can be customized for employees, but acknowledges that CIO's may have difficulty restricting usage to phones they select [1].

4.1 Security Characteristics of Smart phones

Even if the organization has no control over platform selection, knowing the strengths and weaknesses of particular platforms is important to effective security management of smart phones. Oberheide & Jahanian [20] evaluated the Apple iPhone, Google Android, RIM Blackbery, Symbian OS and Windows Mobile platforms with respect to three security characteristics: Application delivery, trust levels and system isolation. As the following discussion of their work shows, the differences between the capabilities of the platforms have a significant impact on the management of their security.

Application delivery is the capability of the smart phone platform to validate the reliability of an application's source. Knowing where an application came from can be important in thwarting infection from malware. Balancing the restrictions imposed by application delivery mechanisms while ensuring an acceptable level of versatility and usability of the smart phone is a challenge for manufacturers. Some vendors provide for encoded signatures on applications and some restrict applications to a single controlled source while others have no restrictions on the source of an application. The iPhone's application delivery controls are very strong since all applications must be validated by Apple before being offered in the App Store. Not only that, but Apple can delist an application and remotely kill it after it has been

installed. While Android only allows applications to be sold through the Android Marketplace, an option to override this restriction is available which leaves Android phones wide open to malware infection. RIM uses encoded signatures, but these are easily available from RIM for a low cost and provide little genuine security as hackers can apply them to malware [20].

Trust levels can control the actions of an application. Applications are assigned a confidence value or receive a privilege. Trust levels may depend on the encoded signature of the application or they may be determined by the user. Granularity must be balanced. If trust levels are too detailed they may impact performance and usability. If they are too broad, they may provide inadequate protection. Android employs a straight forward easy to use scheme that presents an application profile to the user to select which capabilities to permit. Windows Mobile allows the user to place an application in a privileged category meaning there are no restrictions on the application; the normal category which restricts the application from certain pre-defined files and APIs; or the blocked category which prevents the application from running. The iPhone only allows a few restrictions and only minimally uses trust levels to provide protection [20].

System isolation refers to the ability to keep applications from affecting each other or the supporting platform. This capability referred to as sandboxing prevents vulnerability in one application from being used to damage the system or another application. Since the iPhone places most applications into a single privilege level, other applications can easily be affected by a rogue application and thus the iPhone has a weak sandboxing capability which is a serious security weakness. Android runs every application under a different user identifier (UID) providing effective sandboxing and keeping the operations of one application separate from the system and other applications [20].

4.2 Controlling User Behavior

The greatest challenge to mobile device security is not technology but user behavior. Organizations have limited ability to enforce security policies in the field, so user attitudes towards security are extremely important. A major issue is the way employees view their smart phones. Even if provided by the company, employees look upon them as personal devices to be used for their enjoyment as much as for business. This view shifts their attitude towards a less professional application of security practices. Security awareness is a serious problem for senior management as well. A global survey of executives conducted by the Economist Intelligence Unit for Symantec found that less than one third worldwide and one quarter in North America believed that their senior management fully appreciated the security risks of mobile devices. An AT&T study showed that senior managers often violate security policies such as opening email from senders they do not know and using passwords that are easily guessed [10].

While security awareness training is clearly needed, the Economist Intelligence Unit survey showed most executives believed this to be a significant challenge. Only one-third of respondents globally and one-quarter in North America were conducting security awareness training for mobile devices which corresponds exactly with senior management's understanding of the risks in mobile computing. Basic education regarding everything from theft and loss prevention, to malware to encryption is necessary. Employees must be made to accept personal responsibility for the security of their phones and data [10].

Smart phone web browsers are an attractive target for hackers. A survey of North American smart phone users conducted by F-Secure showed that 30% use their smart phones to access the internet and two-thirds of North American users have no security software on their mobile phone. Microsoft's Mobile Internet Explorer provides warnings when users leave an encrypted SSL site, but it is up to the user to notice and respond. Extended validation certificates are also recognized by Mobile Internet Explorer. This feature displays color codes to notify the user as to whether an SSL protected site is genuine or a suspected phishing site. Extended validation certificates are being deployed on desktops and only beginning to be implemented on smart phones [5].

Another problem is the use of web widgets which are code embedded in a web page and can be used in lieu of a browser to quickly get data from the internet. While the code may have a digital certificate, once downloaded it operates outside of host control. A famous example is the "Secret Crush" widget which was supposed to identify Facebook users with a crush on you, but in fact was a vector for adware. Organizations need to evaluate the security of their smart phones browser and operating system, encourage employees to adopt secure browsing practices and establish a smart phone management system [5].

4.3 Controlling Access

4.3.1 Authentication

Authentication is a way to make sure that only authorized individuals are granted access to a system or device. Three techniques are employed: What you know; who you are; what you have. What you know employs usernames, PINs and passwords. Who you are is represented by biometrics such as finger prints, facial identification and iris scans. What you have usually involves a token that generates a random number which the user must match. Two-factor authentication requires the use of two of these three techniques to grant access [24].

While the smart phone is typically in the possession of a single user and less likely to be shared, the aforementioned problems of theft and loss require a robust authentication scheme. Authentication on smart phones is customarily done using a PIN. A separate PIN may also be used on some operating systems such as Windows Mobile for protection of the Subscriber Identification Module (SIM). When this PIN protection is enabled, it controls access to the cellular network preventing the SIM from being removed from the phone and used to make calls in an unprotected phone. Many users do not realize that to control access to the device and the SIM requires two separate authentications [3].

In Windows Mobile the SIM can be protected by a four to six digit PIN, but phone access is configurable and a password may be used in lieu of a PIN. Also available is an authentication called PIN2 to protect network settings. Another Windows Mobile option is to use a standby PIN which requires re-authentication if the phone goes unused for a period of time. This technique is common on desktops, but a survey showed only 18% employed it on their smart phones. Since smart phones are often left on for extended periods, this creates a considerable vulnerability [3].

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.