Securing Mobile Devices: Be Smarter Than Your Smartphone

A Bird's Eye View

Duwane A. Brown

ITEC 6823

Information Security Management

Dr Phil Lunsford

OUTLINE

I. Introduction: The Evolution of Technology

II. Policy

III. Device Theft

IV. Passwords and Pins

V. Bluetooth

VI. Removable Media

VII. Viruses and Worms

VIII. Encryption

IX. Conclusion

Technology is forever changing. It has greatly changed how people communicate on a daily basis. Technology has also changed how we operate whether its home, business or school. Phone calls have gone from home phones to cell phones to Voice over IP. We no longer rely on using the United States Post Office Service as for mailing pictures, sending and receiving letters. Smart phones have greatly impacted the world with the ability to text message, take pictures and email are at our convenience. However some conveniences come with a price. It's not the value of the smart phone, which could have been expense, is what we hold in high regard. It's the information stored on the smart phone is what we truly treasure the most. Phone numbers, messages, email, addresses and pictures. All are and have been stored by us on smart phones and could be easily tampered by someone else. Whether it's considered personal or confidential, the information stored should be protected.

Most companies have supplied their work force with smart phones. The work force mainly consist of top executives to mid range managers. These individuals are in high demand and at times hard to reach. Therefore having smart phones available makes them easily accessible. They can now create or edit documents, presentations, email and hold meetings while mobile allowing them to multitask. But owning a smart phone does bring about additional rules that they have to abide by. The state of a company can be at risk based on the information stored on their smart phone. "The problem is, employees are using smartphones in their jobs, whether the security team is on board or not. In a July InformationWeek survey, 82% of smartphone owners said they use their devices to read business e-mail, 80% surfed corporate Web sites, and 61% accessed enterprise data". (Ginevan Feb 2008) A policy by the company must be set as for dos and don'ts while possessing a smart phone. The first step in creating the policy should be training. Most users are handed their device and unaware how to use them and

what risks are involved. The policy should be enforced by the user holding them accountable by signing a user agreement when they are issued a smart phone. A basic policy might include rules like these: Use the device for company purposes only; Always encrypt sensitive data; Never leave the device in a public place; Always lock the device when not in use; Use passwords and change them regularly; Sync and backup data regularly. (Thornberry, 2002)

The first real threat with a smart phone, believe or not, is one of the oldest risks know to man…theft. Every couple of months or so, new phones enter into the marketplace. The new innovations and sleeker designs make these phones attractive to previous and new smart phone users. The phones also attract those waiting for the user to turn his head for them to soon discover their phone now belongs to someone else. "Another challenge for IT managers is that the inherently small form factors of PDAs and smartphones make them more likely to be lost or stolen. Most users carry critical data on their devices such as e-mails, address books, meeting notes, and calendar appointments". (Hicks Feb 2006). The information on the phone may just have phone numbers, addresses and picture. It also may contain information that could be catastrophe to a company if it's leaked out. Keeping a watchful eye, out of plain sight and being password protected are some options are for safeguarding the phone. However these options are not the end all in protecting your phone. Blackberry has in one way found an approach to protect the information on a phone; even through the information is lost to the user as well. On Blackberry servers there is a way to actually kill the smart phone rendering it unusable to the thief and to the user if recovered. The method could be considered crude but very effective in regards to security.

Like all lock things, one must have a key to enter. A smart phone is used as mobile computer away from the office. In order to access your computer at work, a password is needed. A smart phone should not be treated any different. Most phones also have a pin to access them as well as being able to set a password for it. Password and pins should not be stored anywhere on the phone. It's like telling someone about the spare key hidden under the welcome mat. Passwords should at least have 8 characters (most companies are going up to ten) and should be change every 90 days. Strong passwords include two upper case, two lower case, two numbers and two special characters (symbols). A log should be kept to ensure you don't use the same password twice and one should think of using a paraphrase in a way to better remember the password that was set. "As you select PDA devices for your company, I recommend doing some homework regarding power-on passwords. However, don't rule out a device just because it only offers a four-digit PIN. Some of these devices use an incremental timer to prevent brute-force PIN cracks. For example, after the first time the PIN is entered incorrectly, there's a one-second delay before the user can try the password again. After the second attempt, there's a two-second delay. After the third attempt, there's a four-second delay. The delay time doubles after every incorrect guess. This makes it very difficult for someone to enter 10,000 possible PIN numbers in a brute-force crack attack." (Posey Mar 2004)

Most users love the luxury of being able to talk on their phones hands-free. This is either done enabling the device to become a speaker phone or using another device known as a Bluetooth. Bluetooth is actually a wireless protocol to create short distance communication between to devices creating a personal area network. In this case, the smart phone and the device use to hear the conversation…The Bluetooth. All networks need to be secured for the protection of the transmission of information between all points. Some agencies have gone to

the point of disenabling Bluetooth on their company smart phones to due to their fear of their transmission being intercepted. "Numerous hacks have been created to use Bluetooth as a vector for attack -- particularly against phones and PDAs that use Bluetooth to pair with hands-free headsets. Many take advantage of programming flaws and poor implementation choices associated with the Bluetooth Object Exchange (OBEX) protocol. For example:

- BlueBug lets an attacker make calls on another Bluetooth phone.
- BlueDump cracks PIN codes by watching Bluetooth devices bond (pair).
- BlueJack lets an attacker add contacts to a Bluetooth device's phonebook.
- BlueSmack crashes a Bluetooth device by sending a "ping-of-death" message.
- BlueSnarf lets an attacker retrieve contact and calendar data from Bluetooth devices.
- BlueStab uses badly formatted names to crash a device during Bluetooth discovery." (Phifer 2006)

Users normally communicate using their Bluetooth in a non-secure mode. However little do they know there are two additional modes. Mode 2 provides security which is determined by the application in use. The third mode secures the wireless connection in whole. "For best results, use mode 3 to enforce link authentication and encryption for all Bluetooth traffic, and discourage or ban business use of devices that support only mode 1." (Phifer Oct 2006) Along with passwords and pins as regards to Bluetooth on devices, users should power off their Bluetooths to avoid them from being linked to another device when they are not being used.

Information on smart phones can be tampered without theft or transmission inception. This is done by the use of removable media. Removable media is used as additional storage space for information that exceeds the amount of storage on our phone. The storage space at times is considered the source of all of our media. We must remember the compact flash card we are using as a flash drive or memory stick is in fact removable. The additional storage can easily be remove by anyone and once its remove the user is left at a lost. Like all data, a backup

is essential to recover any data which as be stolen or lost. Please safeguard all removable storage by securing them in another location besides the device's carry case or leaving in phones if they are easy accessible. "Recently, at the Microsoft Exchange Conference, I saw several next-generation flash cards that were in development for PDAs. One flash card contained 512 MB of storage, plus an integrated fingerprint scanner. Using this device requires users to enter the device's PIN, plus pass a fingerprint scan before they are given access to the data stored on the card" (Thornberry Oct 2002)

Just like any computer or network, smart phones are vulunable to viruses and worms. Information could be lost by a virus or worm due to removing a compact flash drive and inserting in it a computer or another untrusted source. Email being delivered to a smart phone with attachments can be just as fatal to the device just as to a computer. Instant messaging and downloading applications to the device can leave the device open to a security risk that could leave it not operational and rending useless with the its information completely irretrievable. Companies are now enforcing virus protection software on their issued device and blocking the ability to download third party software and instant messaging. Email could still be an issue but spam filters and blocking html content could help remedy the matter. "Mobile viruses can be a major threat, particularly with devices that have significant computational capabilities. Mobile devices, in general, are susceptible to viruses in several ways: Viruses can take advantage of security holes in applications or in the underlying operating system and cause damage; applications or applets downloaded to a mobile device can be as virus-prone as desktop applications; and, in some mobile OSs, malformed SMS messages can crash the device. The 911

virus caused 13 million i-mode users to automatically place a call to Japan's emergency phone number." (Guest Jul 2004)

There is really no one try solution to protect ones information on a smart phone. However, companies are making very difficult through the use of encryption. "The first line of defense is encryption, either of folders or the full device, including removable storage such as SD cards. There are tradeoffs here: Encrypting all device storage ensures that you won't miss any data, but it can negatively impact performance. Encrypting select folders leaves performance intact but requires continual asset classification to make sure the correct data is being encrypted. Because device speed is increasing and given that users may inadvertently store sensitive data in unencrypted folders, full disk encryption is best"(Given Feb 2008). Vendors are now keying on the untapped market of encryption for mobile device from software, security drives and even Bluetooth. Any sensitive information should not be broadcast on a wireless connection unless it's secured. "Encryption can cover a multitude of sins," says Paul Stamp, an analyst with Forrester Research. "Whether that is data that you encrypt to use again yourself, data you need to encrypt to someone else for use at a later time, or data you need to encrypt to send out across the Web, they can all present a different business problem, and it can be difficult or impossible to find a 'one size fits all' solution." (Dunn Aug 2007)

Mobile devices have allowed us freedom to move about and still be able to complete our assigned tasks. We can be at many places at once while giving each objective our full attention. However the freedom comes with a risk, information which can be stolen, changed or deleted. Like any other wireless network, personal area networks can be subjected to being hacked and transmission of information be intercepted. Virus and worms through downloading and email

attachments can destroy information and devices are prone for theft if a watchful eye is not keep. Even with a policy in place, strong passwords, safeguarding media, software and encryption, nothing is a 100 percent. When it comes to security, there is no such thing is safe enough.

BIBLIOGRAPHY

1. Posey, Brien. Address security problems with a solid PDA use policy 4 Mar 2003
http://articles.techrepublic.com.com/5100-10878_11-5034288.html?tag=rbxccnbtr1

2. Ginevan, Sean. Strategy: Securing Mobile Data Network Computing 11 Feb 2008
http://www.networkcomputing.com/channels/wireless/showArticle.jhtml?articleID=206401696

3. Thornberry, Suzanne. Strong PDA policies help secure data and prevent equipment loss 1 Oct 2007
http://articles.techrepublic.com.com/5100-10878_11-1053046.html?tag=rbxccnbtr1

4. Ginevan, Sean. Advances.For Mobile Security On The Horizon. Information Week. 11 Feb 2008
http://www.informationweek.com/news/mobility/security/showArticle.jhtml?articleID=206105248

5. Dunn, Darrell. How To Secure Mobile Devices. 14 Aug 2007 <
http://www.baselinemag.com/c/a/Intelligence/How-To-Secure-Mobile-Devices/

6. Hicks, Sarah. Best practices for securing mobile devices 1 Feb 2006
http://searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1163542,00.html

7. Phifer, Lisa. Taking the bite out of Bluetooth 31 Oct 2006
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151_tax310797,00.html

8. Guest Contributor. Identify and reduce mobile device security risks 19 Jul 2004
http://articles.techrepublic.com.com/5100-22_11-5274902.html