Do New Mobile Devices in Enterprises Pose A Serious Security Threat?

Ali A Altalbe

Deanship of e-Learning and Distance Education-King Abdulaziz University

Jeddah – Saudi Arabia

aaltalbi@kau.edu.sa

Abstract

The purpose of this paper is to introduce a research proposal designed to explore the network security issues concerning mobile devices protection. Many threats exist and they harm not only computers but handheld devices as well. The mobility of phones and their excessive use make them more vulnerable. The findings suggest a list of protections that can provide high level of security for new mobile devices.

Keywords: security, handheld devices, malware, wireless interfaces, cell phones.

I. INTRODUCTION

Technology is improving all the time and we rely on our cell phones and other handheld devices. We use them not just for making calls, but also sending emails, organizing meetings, and surfing the World Wide Web. Modern mobile devices can cope with all the functions that an average computer can do. However, there are many that can do some harm. According to statistics, in 2007 thieves worldwide stole around eight million handheld devices (Hoard, 2007). Their owners, moreover, were asked to pay large amounts of money if they wanted them returned. Even if a person's mobile device has not been stolen, there is still a threat to the information that is inside the phone. Bluetooth connection is an easy way transfer messages, memory and e-mails, and also viruses.

Currently, people tend to buy new mobile devices more and more. There are smart phones, tablets and other new technological devices combining the features of traditional cell-phones with many new features. When we purchase a PDA, for instance, we receive a large screen, many programs, large amounts of memory, etc. There are many models of smart phones and tablets choose from (Juniper Networks, 2010). These devices may perform various functions, but all in all they work according to common principles. This study looks at mobile devices, provides some background information on them and attempts to describe the best method of phone security.

II. HANDHELD DEVICES SECURITY THREATS AND METHODS TO PROTECT THEM

Most mobile phones have functions that can be found in tablets or smart phones. Our phonebook entries, different passwords, personal files, and other data can catch the attention of hackers. There is also another target – remote resources. Anyone can use his or her mobile device's communications to access a person's data. This information can be represented by services for cell phones, email storages, information and software on community networks, which can be easily accessed. People are now using their personal mobile devices to maintain corporate software and information. These gadgets are more mobile than computers, notebooks or netbooks. Modern mobile devices are capable to incorporate corporate features of a workplace. On the other hand, computers have far more protection capabilities than phones. The place of modern mobile devices is somewhere in between in the information infrastructure;

DOI : 10.5121/acij.2013.4106

yet it is difficult to administer them (Jansen and others, 2004) People who are aware of the risks apply particular security software and other means to protect their information.

There are countless threats to handheld devices and the list is increasing all the time. As far as they are portable, different handheld devises may pose various risks. Due to the fact that mobile devices are small and easily portable, they are easily lost or even stolen. What is more, people do not need much time to break into the protection software to obtain the data on your mobile device. Then it is “cleaned up” and probably sold to another person. Such an additional interface that Bluetooth provides may pose another risk to your device, such as sending malware to a phone.

Since the size of handheld devices is small, pickpockets can steal them. Having stolen the device, thieves sweep the data found in the memory of the phone, reset it and then sell it. The number of handheld devices that disappear during each year counts to several millions. Very few of them could are returned to their owners‟ hands. About eighty-six thousand mobile phones and twenty-one thousand other handheld devices were left in the taxi cabs of one Chicago firm over one half-year period (Hoard). Stolen phones are used not only to store data on, but also for placing charge and international calls. Furthermore the device itself may have been expensive in the first place.

Despite various means of protection, it is not hard to access a device and its information by typing in a correct personal identification number or code word. A bypass system may be applied to avoid it. As a rule, people use very simple PIN codes and passwords. A combination of digits may reflect their date of birth, or it may consist of the same digits. If we apply an improper configuration to a device, this may increase the level of risk. Motorola phones require the customer to go through two levels of its security system. The phone password is inserted and a security code rearranges the lock on the phone in case the owner changes his or her mind. Anybody may arrange a code to lock a phone, but he or she cannot change the security code because it is always default. Consequently, everyone can use this code to gain access, to rearrange or just turn off the lock system of their phone.

Some mobile devices may have a master pass code integrated into the security system and one that cannot be changed. This makes it possible for someone to ignore the phone lock and enter the phone. The master security code for overruling the phone security system can be pulled out of the values that identify the handheld device. Some situations exist where an individual is able to use a secret method of gaining partial or total control over the phone without entering any codes (Withers). There are many other means to outsmart integrated protection systems. It is possible to create a surrogate subscriber identity module for a particular phone model, so that it is treated as the original one.

Many enterprises integrate test programs into their products that might serve as a source of information leakage. Companies now support the Joint Test Automation Group standard – a general test of processor, memory, microchips and other hardware. With the help of special equipment one can set up a software communication system and observe the memory contents of any handheld device that is locked. It is not as hard for an experienced technician to break into phone security by heating the circuit board sufficiently to remove solder from its memory chips and access the contents by using a special memory chip reader (Willasen).

Mobile malware is a phenomenon present mostly in handheld devices with a software development kit. This tool is more usual for tablets, personal digital assistants and smartphones. Besides these, communication networks may also pose a risk of viruses and different forms of malware being delivered to our handheld devices. There is one particular feature of malware: they usually require your agreement to be installed. Malware can behave in various ways. It can overhear on user input, steal personal information or shred it, or put a phone out of action. Malicious software may also accumulate wireless connection fees and then user spends his or her money on some strange and expensive messages and calls that were sent or made from the account (McMillan). With the help of malware an individual can access data on the device, steal it by sending it from the phone or make the handheld device function faster.

Availability or steadfastness of a mobile device might be impacted on by malicious software. A person may not even notice when somebody else uses his/her mobile phone to access networks or uses it as a proxy for some web connections. Furthermore, some malicious software is able to propagate itself. Malware incidents have been growing steadily and are expected to continue to spread (Nakashima).

Not very long ago people began receiving so-called „spam‟ messages from advertisers. Mobile spam may persuade users to make calls or send messages to toll-free numbers that are in fact not free. Spam may also ask you to give details of your pass codes, financial accounts or other private information. The mobile phone user may also download malware attached to a message (Espiner).

Many mobile phone users usually try to go as far as possible from crowded places when they receive or make a call so that no one listens to their conversation. However, it is not necessary to be present physically near those people to hear their speech, but it is possible to eavesdrop on information that is being transferred. The easiest way to organize electronic eavesdropping is to install special software onto a particular phone and then deliver the information to another mobile device. Another method is to adjust a laptop to impersonate a legitimate access point for a public wireless hot spot.

Communications between a mobile phone and cell tower were originally designed with security in mind, but every secure point has its weak sides. South Korean researchers assembled equipment that could monitor a Code Division Multiple Access system (Dae Hyun Ryu, 218-227). At the same time, researchers in Israel and the United States Erica have found ways to crack the encoding system for Global System for Mobile Communications phone networks to make eavesdropping possible.

Software or data hosted on servers maintained by other parties are at the risk of exposing secret information. Typical examples are electronic mail and other communications solutions that keep information on a server operated by the network carrier. Unreliable employees who administer particular servers but who have technical skills can detect vulnerabilities in a server’s defenses. A well-known incident involving the T-Mobile account of a celebrity’s handheld device has been described (Roberts). All her personal information from the mobile device was saved onto a server for access through a Web portal. Unauthorized users managed to get access to this information and spread it all over the World Wide Web.

Some enterprises offer location tracking services for mobile devices which allows the location of the user to be known by friends and relatives. It is also possible to track employees‟ locations. These services periodically send the phone a notification for the user that controlling is taking place. Others do not provide an indication when registration is occurring. There is one early tracking service that is vulnerable to the possibility of secretly registering someone else’s phone for tracking without having possession of the mobile device (Pamplin).

In certain cases unique device identifiers of particular handheld device are reprogrammed into a different mobile phone; a clone is created that can act as the original technical device. For instance, displaying the radio wave transmissions of analog mobile phones allowed the factory-set Mobile Identification Number and Electronic Serial Number from those devices to be received easily and used to create clones (Cell Phone Fraud). Digital cell phone technology has an improved security during device authentication. It is, however, possible to clone some early generation handheld devices if one has physical access to a cell phone.

Problems may appear with third-party data resident on servers other than those of network carriers. For example, companies would show the current and past locations of a person who would then gain unauthorized access to the data maintained at Web servers, which could be operated by mobile device tracking.

Security issues for mobile phones range beyond those of other computer equipment. Much widespread protection software available for desktop computers is not easily obtainable most of the time for a huge range of handheld devices.

III. RECOMMENDATION

We need to rely not only on security software to provide protection, but also take active participation in this process. Mobile devices" owners should maintain proper configuration settings to protect equipment and themselves. It is advisable not to lend the phone to somebody because it can be misused, security settings might be changed (deliberately or not) and the device may be subjected to unauthorized activities. To protect our phone the first thing we need to do is enable user authentication, which means establishing necessary pass codes; they should be long, hard to guess and unique. Screen savers can sometimes be annoying, but to an extent they protect a lost, stolen, or misplaced phone until the owner recovers it.

We should never use a handheld device as a storage place for important information. It is better to back up data on the memory card in an alternative means of storage. Phone numbers and addresses can also be printed out and kept in a secure place. In cases where the presence of sensitive data is unavoidable, such information should be kept in a suitable encrypted form until required. Securing personal data on a device with encryption is an effective strategy, and appropriate for devices used for organizational goals. The Advanced Encryption Standard was developed for federal U.S. government departments and agencies to encrypt and decrypt such information (Advanced Encryption Standard).

Memory cards should also have a strong password consisting of up to eight characters. It helps to secure sensitive data kept separately from a handhold device, even in cases when encryption is applied. In cases where no procedure can be determined, the alternative is to physically destroy the memory slot.

People need to be careful when they see any suspicious alternative question on the screen of our mobile phones. Any messages or contacts received on a cell phone from an unknown number should be treated with suspicion. Such messages should be deleted without opening them. Malicious software attempting to enter your mobile device through Bluetooth usually cannot install itself without the user's approval.

The use of wireless interfaces should also be avoided. It is desirable to disable Bluetooth, Wi-Fi, infrared, and other wireless interfaces if they are not used at any particular moment. Such automatic connections to cellular data services as General Packet Radio Service or Enhanced Data Rates for GSM Evolution should be turned off as well. Phone users need to be very careful with Bluetooth and its settings. All connections should be limited and a strong password secured.

Minimized functions, features, and capabilities typically give rise to security issues.

However, it may sometimes have the opposite effect. Agreements on cellular services and their settings represent another way to reduce mobile phone performance (Pogue).

Users should keep compromised devices deactivated. They can do this by triggering the remote protection mechanism if it is available on the mobile device through the receipt of a message. This is contained in an in advance registered activation code if it is lost or stolen.

Another strategy to improve phone security is to add prevention and detection software, which adjusts additional security controls. This helps to prevent the handhold device from software attacks. In order to protect the phone or other mobile device, the following security software can be added: firewall, antivirus, or antispam. Phone owners should not forget about user authentication alternatives, device data and memory card encryption, intrusion detection, virtual private networking issues, and devices that will not erase important content.

Mobile phone users need to ensure that security and other configuration settings are correct and comply with policy. It is also advised to register one's mobile device, follow the policy rules, control the phone settings, create a secure and long password, limit the number of entry attempts, try to reset pass codes from time to time, restrict software downloads, keep an eye on infrared, Bluetooth, Wi-Fi, and other means of communication, take care of device content and removable media encryption, check Virtual Private Network, firewall, antivirus, and intrusion detection programs. A mobile phone user is also advised to refuse services offered by unknown or unregistered devices.

IV. CONCLUSION

It is clearly evident that mobile phone devices are now an integral part of our everyday lives. People use them to check their mail, visit social networks, play music, movies, take pictures, etc. They can perform various difficult tasks and help make life easier for us. However, in order to ensure all the tasks undertaken by mobile devices are safe and secure, and function properly, we need to provide it with maximum security. This study has investigated the necessity of taking into account all the possible up-to-date and known threats and suggested ways to protect against them. These strategies will increase the security of mobile devices dramatically, but hackers have always been a few steps ahead. It is a challenge to stop them breaking or bypassing mobile phone security systems.

V. REFERENCES

1) "Advanced Encryption Standard." Computer Security Division, National Institute of Standards and Technology, Jan. 28, 2002. Retrieved from: http://www.itglobalsecure.net/pdf/aes_encryption_standards.pdf

2) "Cell Phone Fraud, FCC Consumer Advisory." Federal Communications Commission, Consumer & Governmental Affairs Bureau, Sept. 26, 2005.

3) "Designing for On-Board Programming Using the IEEE 1149.1 (JTAG) Access Port." Intel, Application Note, Nov. 1996. Retrieved from: http://www.ece.auckland.ac.nz/archives/datasheets/geninfo/jtag.pdf

4) Dae Hyun Ryu, SeungJu Jang. "A Security Weakness of the CDMA (Code Division Multiple Access) Cellular Service." International Journal of Computer Science and Network Security, Vol. 6, No. 5, May 2006, pp. 218-227,

5) Espiner, Tom. "Phone Phishing Attack Hits US." ZDNet.co.uk, June 23, 2006.

6) Hoard, Bruce. "8M Cell Phones Will Be Lost in 2007 – how to back yours up," Computerworld. July 13, 2007.

7) Jansen, W., Wayne, A. "Towards a Unified Framework for Mobile Device Security." NIST, Nov. 18, 2004. Retrieved from: http://www.sigsac.org/SLIDES/ccs04-6.pdf

8) Juniper Networks. "Mobile device security in the enterprise." Oct. 18, 2010. Retrieved from: http://www.juniper.net/us/en/local/pdf/whitepapers/2000363-en.pdf

9) McMillan, Robert. "New RedBrowser Trojan First to Target J2ME." Computerworld, Feb. 26, 2006. Retrieved from: http://www.itworld.com/060228redbrowser

10) Nakashima, E. "Used Cellphones Hold Trove of Secrets That Can Be Hard to Erase." Washington Post, Oct. 21, 2006.

11) Pamplin, Jonathan. "How to Track Any UK GSM Cell Phone." 2600 Magazine, Vol. 22, No. 4, 2005.

12) Pogue, David. "How to Block Cellphone Spam." Pogue"s Posts, The New York Times, June 12, 2008. Retrieved from: http://pogue.blogs.nytimes.com/2008/06/12/how-to-block-cellphone-spam/

13) Roberts, Paul. "Paris Hilton may be victim of T-Mobile Web holes" IDG News Service, Mar. 01, 2005. Retrieved from: http://www.itworld.com/050301hilton

14) Ryder, Nathan. "GPS technology helps parents track teens." 14wfie, Feb. 10, 2010. Retrieved from: http://www.14wfie.com/story/11932039/gps-technology-helps-parents-track-teens

15) Willassen, Svein. "Forensic Analysis of Mobile Phone Internal Memory." Advances in Digital Forensics, Vol. 194, 2006.