Running head: MOBILE PHONE SECURITY

Mobile Phone Security

Benny C. Rayner

East Carolina University

Abstract

Phones are used in various ways. Majority of the people you see have a mobile phone. This comes as an advantage and a disadvantage. The advantage is the functionality and accessibility of the phone. Some are getting as powerful as laptops. With great power, however, comes great responsibility. The responsibility is the concern that a user should have of the security of their mobile phone. Numerous viruses are beginning to be made specifically to infect these phones. They are being targeted because of their vulnerability. Anything that is accessed via an open network is susceptible of being infected. Mobile phones are beginning to see that they are no different than their laptop counterpart. The variants that are being made can steal phonebooks or spread to other phones from the contacts that are stored in its host phone. The attacks are alarming and because of this many anti-virus companies are beginning to come together and protect the phones from the malicious variants.

One of the fastest growing technologies of our times is that of mobile phones. When one thinks of sources of communication, telephones would be one of the top sources. They have gone through many changes, going from the rotary phone, to the touch tone phone, to the cordless, and now to the mobile phone. With each advancement in technology comes more ways to exploit that technology. Since phones are the primary source of communication, an increase of exploitation of the advancement in technology has happened.

When mobile phones were first used, because of the lack of technology, there susceptibility of being exploited was rare. Mobile phones now have web browsers to browse the internet, e-mail, text messaging, picture messaging, and many other features. These phones have now known as smartphones. Because of this advancement in technology, hackers are more susceptible to exploit these features for valuable information. As the devices gain more power so that they are capable working with multi-media applications, they have also gained the ability to run all the malware found on PCs and notebooks (Korzeniowski, 2005). As a result, hackers are attacking cell phones. Cellular fraud is estimated to cost the telecommunications industry a million dollars a day (Wong, 2005). Attacks are proving to be successful because mobile phone operating system vendors had to contemplate adding new security functions to their operating systems versus making their devices large and bulky. In most cases, they decided not to trade system security for user ease-of use (Korzeniowski, 2005).

More than 100 viruses now target mobile phone operating systems from Microsoft Corp. (www.microsoft.com), PalmSource Inc. (www.palmsource.com), Researching Motion Ltd. (www.rim.com), and Symbian (www.symbian.com) to name a

few (Panettieri, 2006). Symbian OS is the most popular operating system for mobile phones, including those sold by market leader Nokia. Symbian has approximately 70 percent of the world market for all phones, and Microsoft Windows Mobile has approximately 10 percent, while the rest is a combination of lesser-used platforms (such as Palm OS) (Vamosi, 2006). Two-thirds of all mobile phones shipped in the third quarter of last year ran the Symbian OS, according to recent Gartner research (Evers, 2006). Mikko Hypponen, chief research officer at security company F-Secure, told attendees during a session at RSA's Conference that more than 150 viruses that target cell phones have been discovered since June 2004, and tens of thousands of infections have been reported worldwide (Evers, 2006). While there have been more than 150 cell phone viruses discovered since 2004, compared to over 150,000 Windows PC viruses, the count may seem low at this time, however, a widespread attack could surface by the end of next year (Zonk, 2006). These viruses could also cause a threat by infiltrating a Wi-Fi connection and spread from the mobile phone to school servers, desktops, and notebooks, contaminating critical data. Although there has not been many malware infections detected, any detection of malware is too many.

The Cabir worm was the first notable piece of malware seen on mobile phones. The Cabir worm targeted mobile phones that ran Symbian OS and Nokia's Series 60 (www.nokia.com) user interface (Panettieri, 2006). Once infected with this worm, Cabir uses Bluetooth (www.bluetooth.com) to send itself from one phone to another. The Cabir worm presents itself to users as the "Caribe Security Manager" and is installed as the CARIBE.SIS file.

Disguised as a security utility, Cabir can deliver other malicious codes, such as the Skulls Trojan horse, to other phones. The worm has been detected in several countries, including China, India, Turkey, the Philippines, and Finland, and spreads as people travel with infected phones (Keizer, 2004). The worm is considered benign for the primary effect of the worm is blocking normal Bluetooth connectivity and draining the infected phone's battery life for it continuously is seeking a Bluetooth connection. According to several anti-virus vendors, the source code for the Cabir worm is out and in the hands of those beyond the people whom created it, which is a Russian hacker gang (Keizer, 2004). Unfortunately this may lead to a lot of versions of the Cabir worm.

Helsinki-based security firm F-Secure noted that new copies of Cabir (Cabir.h and Cabir.i) are more efficient than their ancestors at spreading (Keizer, 2004). Cabir originally would only spread to one new phone per reboot, which explains why it so far has only managed to spread to eight countries. The new versions, however, can spread to an unlimited number of devices per reboot of the infected phone. As soon as a suitable target phone is seen, the worm sends itself and keeps sending itself to that phone while it is still in range. Once the target phone leaves the area, Cabir.h and Cabir.i will find a new target and continue spreading. In conditions where people move around and new phones come in contact with each other and Cabir.h and Cabir.i can spread rapidly.

Another example of a malware targeted for mobile phones is the CommWarrier, which use both Bluetooth and MMS (multimedia messaging service; www.mobilemms.com), to infect the phone. CommWarrior attempts to spread by sending messages via Bluetooth wireless connections and MMS, which is different from the Cabir worm, which only used Bluetooth to proliferate. This malware is similar to the

Cabir worm; however, for infection the worm uses MMS. The worm is able to read out the telephone numbers from the address book and send a MMS message with a malicious SIS file.

MMS, a mobile technology for sending text messages that can also include images, audio or video, is built into devices from Ericsson, Motorola and others. CommWarrior, however, only affects Nokia Series 60 phones. As MMS can be used to send text messages worldwide, it has a greater reach than the short-range Bluetooth and so could be forwarded more rapidly, researchers said (Hines, 2005). MMS viruses are more comparable to e-mail worms like Bagle, MyDoom, Sobig and others. An MMS threat can travel around the world in hours, so in that regard, it's much more dangerous.

CommWarrior infects the telephone directory software in the Nokia handsets. It randomly selects one directory profile at a time and sends a copy of itself to that person. It can be sent to any kind of wireless gadget or computer, but if that device does not run the Symbian Series 60 software, it will not be infected. Similar to the Cabir worm, recipients also have to accept and download CommWarrior in order for the Trojan to launch it. The Trojan uses more than 20 different messages to try to lure users into opening its file, including text designed to look like legitimate software updates from Symbian, or even pornographic photographs.

FlexiSpy is another mobile phone culprit that has become controversy of whether or not it is something that can be put to good use or if it is something that is acting as malicious code. The application’s true purpose is to capture call logs, text messages, and mobile Internet activity so that parents can monitor what their kids are doing. The data captured is sent to Vervata’s servers and is accessible to customers via a special website.

FlexiSpy has attracted a criticism from security company F-Secure, which has labeled the software as a Trojan, or a malicious program that disguises itself as something harmless (Evers, 2006). The application installs itself without any kind of indication as to what it is and hides itself from the user. FlexiSpy could be used by an offender as part of malicious software that targets phones. An attacker could try sending the program to phones via a Bluetooth connection and trust that there are enough curious people to install it.

FlexiSpy has defended themselves by saying that the product is not a Trojan horse, nor a virus. FlexiSpy further stated that it does not replicate itself and pretend to be something that it is not (Evers, 2006). Any product that does data capturing should not be taken lightly and should be left in hands of people whom know what the product is and how to use it. If not, the data that is captured could be exposed to the wrong people.

Cdropper, Pbstealer, Sendtool, and Booton are all variants targeted for mobile phones that were identified by Symantec (www.symantec.com). Pbstealer tries to send the user's address book, notepad content, calendar, and task list to other Bluetooth devices, while Cdropper attempts to install versions of the Cabir and Locknut viruses on the mobile device, according to Symantec (Evers, 2006). Booton can perhaps wreak the most havoc. It restarts the mobile device when executed, but the restart will fail because the Trojan also drops corrupted files on the system, Symantec said. Sendtool drops a tool that can be used to send malicious programs, such as other Trojans, to other Bluetooth-enabled devices.

Vulnerabilities of the Bluetooth technology is yet another way attackers can hack into mobile phones. There are many ready-made Bluetooth hacking tools that are easy to

download from the Internet. BlueStumbler is sniffing software that can monitor and log all Bluetooth devices and display their Bluetooth friendly name. Bluebrowse is another hacking tool that is equivalent to a port scanner and displays all the available services on devices. These tools allow the use of BlueJacking, which is the sending of anonymous messages to other Bluetooth machines (How Can Bluetooth ~, 2006). A Bluetooth phone creates a message as a contact entry in the address book, and then instructs the phone to send it via Bluetooth. The phone seeks out any other Bluetooth enabled phone within range and the message pops up on the other phone's screen. These can be in the form of adverts, SPAM, or simply nuisance messages. The use of these tools can violate user's locational privacy, so their movements can be tracked and recorded and subsequently sold commercially to potential advertisers (How Can Bluetooth ~, 2006).

A much more serious breach of security occurs with BlueSnarfing attacks. Devices are especially vulnerable to these forms of attacks if their mobile phone is left in discoverable mode. Downloadable tools allow access to data such as contacts, calendars, images, business cards, logs, and the IMEI (International Mobile Equipment Identity) and all this can be done without alerting the owner. Bluesnarfing attacks combined with various backdoor tools such as Bluebug and Gnokii allow disguised access to AT commands. Attackers can then initiate and send SMS messages, access the Internet, initiate calls to premium rate numbers, and monitor conversations in the phone's vicinity all without the owner's knowledge.

Bluetooth connectivity is the primary route for malware to infect mobile phones; however, it is not the only way of infection. Because of this there are unfortunately other potential routes by which malware might gain entry. There could be potential for future

infections to occur via Wi-Fi, which is already becoming a fairly standard feature on PDAs and high-end smartphones (Furnell, 2005). Perhaps the most obvious concern would appear to be the cellular air interface.

User intervention can be used to prevent a lot of the malware. For instance, the potential for infection for the Cabir worm was the explicitly acceptance of the application that contained the worm. As with users of instant messaging, if an IM message is sent to a user and the user knows not whom the person is and the user clicks on the link without second guessing what that link could be, infiltration of the malware is done which could have been prevented by the user.

If users also avoid leaving their mobile phones in discoverable mode, and exercise appropriate caution over what they agree to download, then the infection opportunities will effectively disappear. Most of these viruses are spread by Bluetooth and although Bluetooth has its geographic limitations, attackers have been able to leverage the technology to support malware.

Users are assigned default passwords, which they are supposed to change once they access the network. In many cases, they fail to take that step, which leaves their mail box open to intruders. Users also pick easy to remember passwords, such as their first name or simple numeric sequences, like 123456. If a password is simple for a user to remember, it is also simple for a hacker to crack (Korzeniowski, 2005).

Users also tend to be careless with their security checks. Mobile voicemail is the prime target for hacking because many people give their cell numbers, and even their passwords, to close friends, relatives, and colleagues. The carefree attitude of mobile phone users make hackers job that much easier to do their malicious work.

A hacker was able to break into Paris Hilton's mail box by duping a carrier's caller ID system. If a call comes from a user's phone number, the customer can change their password security options. A hacker found Hilton's phone number, mimicked it, changed the settings, accessed her personal information, and then shipped it to a variety of web sites. As a result, phone numbers and e-mail address for various celebrities became available to anyone with an internet connection (Korzeniowski, 2005).

Another option for hackers is to first mimic a valid phone number and then grab the token given to a user so they can reset their passwords. Also, flaws in the design of the reset feature allows hackers who know the URL of a carrier's password reset page to bypass the user authentication page and change an account's password without having to provide information that proves they are the account owner. A similar technique focuses on the databases where carriers store user password data. In an SQL injection attack, hackers rely on SQL database queries to inject unexpected commands into a password database, which allows them to manipulate the database's contents.

The increasing number of attacks shows that there's an interest building among the hacker community. As e-commerce becomes a bigger part of what people do with mobile phones, so to will attacks. Considering this, mobile phone manufactures can not close their eyes and hope that these attacks will go away because they never do. Manufactures are going to have to realize that the more mobile phones become Internet-connected data devices through IRDA, Bluetooth, and other forms of data communications, they become more susceptible to exploitation. It is like having a computer on the Internet without a firewall or anti-virus software.

Mobile phone manufactures should be held to the same standards to which operating vendors are held. Some cell phone vendors are reluctant to do that. Verizon Wireless, one of the top U.S. mobile networks, doesn't see a need for its customers to install antivirus software on cell phones. "At this point, that is absolutely not required by individual customers," spokesman Jeffrey Nelson said (Evers, 2006). Today, most middle-end mobile phones embed a Java runtime environment that can execute programs downloaded on the network by the user. This new functionality creates great opportunities for new services but also brings the full range of risks that existed on the personal computer to the phone (Alvarado, 2005). Developing a corporate mechanism for fixing, announcing, and distributing bug fixes to their users would elevate a lot of these malicious bugs (Graff, 2004). Maybe when mobile phones were seen as a luxury rather a necessity, this was not a problem. Now mobile phones are used to do everything and because of this advancement more hackers are going to be more interested in gaining control of the device because valuable information will be store on the device.

Approximately 812.5 million cell phones left factories last year, a 14 percent increase over the 713 million shipped in 2004, according to research firm iSuppli. That means that roughly one out of every six people on the globe bought a phone during the year (Kanellos, 2006). Considering the rise in mobile phone usage and the advancement of technology with mobile phones and the rise of viruses targeted toward them, AV manufacturers and some mobile phone vendors are beginning to realize that these targeted viruses could get worse if nothing is done about it.

Vendors are beginning to provide mobile phone manufactures with protection AV (anti-virus) software. Several leading AV vendors are already offering specific products

for mobile and handheld devices, with products available from Symantec, Kaspersky, F-Secure, McAfee, and many others (Furnell, 2005). Like their desktop counterparts, these can offer real-time protection, and can obtain automatic updates over the network.

McAfee has launched a new security suite built exclusively for mobile phones. The consumer side of the McAfee Mobile Security is an application that is available for both Symbian and Windows Mobile. McAfee VirusScan Mobile protects phones from software arriving via e-mail, instant message, downloads, SMS, MMS, and Bluetooth. McAfee has suggested also that the antivirus shield be administered by the service provider, which would therefore be responsible for maintain and updating the client component of the package.

Since Nokia's phones all run the same Symbian OS, they can all be infected with the same virus. Because of this Nokia has announced that F-Secure Mobile Anti-Virus will ship on several of its business oriented phones. The software will be on the memory card bundled with the N71 and will be in the catalog on E60, E61, and E70 devices.

Research In Motion has announced that BlackBerry e-mail will soon gain the ability to be secured by PGP. While there will be an extra cost associated with the service, PGP provides sender-to-recipient e-mail security in the form of high-grade public key encryption.

Bluefire Security Technologies (www.bluefiresecurity.com), a privately held firm in Baltimore, MD, is developing an integrated security suite for mobile phones. Bluefire's mobile security suite offers authentication, encryption, integrity monitoring, a firewall, VPN (virtual private network), and centralized management (Panettieri, 2006).

This would be good for the business workforces whom are constantly transacting business on mobile phones.

One of the fastest growing technologies of our times is that of mobile phones (Boretos, 2005). Why not start to work to protect them? First came the PC, then the PC was made smaller to become a laptop, and now the laptop has been made smaller to become everyone's mobile phone. If mobile phones are going to be made more in the light of portable PCs, let's think about their protection as well. We can do this by seeking out vulnerabilities in products. Acknowledging them honestly, fixing them aggressively, and feeding the lessons learned back into the production process so that real security can be built in at the design level in future versions (Graff, 2004).

References

* Alvarado, P. (2005). Improving the Security of Downloadable Java Applications With Static Analysis *Electronic Notes in Theoretical Computer Science, 2005, 129-144*

* Boretos, G. (2005). The Future of the Mobile Phone Business *Technological Forecasting and Social Change, 2005*

Evers, J. (2006, March 29). Retrieved April 12, 2006, from Spy program snoops on cell phones Web Site: http://news.zdnet.com/2100-1009_22-6055760.html

* Furnell, S. (2005). Handheld Hazards: The Rise of Malware on Mobile Devices. *Computer Fraud & Security, 2005, 4-8.*

Graff, M. (2004, February 19). Retrieved April 10, 2006, from It's time to talk mobile phone security Web Site: http://www.esecurityplanet.com/views/article.php/3315111

Hines, M. (2005, March 7). Retrieved April 12, 2006, from Trojan gets the cell phone message Web Site: http://news.zdnet.com/2100-1009_22-5602919.html?tag=nl

* How Can Bluetooth Services and Devices Be Effectively Secured? *Computer Fraud & Security, 2006, 4-7.*

* Hunter, P. (2004). New Threats This Year *Computer Fraud & Security, 2004, 12-13.*

Kanellos, M. (2006, February 10). Retrrieved April 12, 2006, from Mobile phone sales pass 800 million Web Site: http://news.zdnet.com/2100-1009_22-6037984.html?tag=zdnn.alert

Keizer, G. (2004, December 29). Retrieved April 10, 2006, from Phone Worm Source Code Out, Expect More Threats Web Site: http://www.techweb.com/wire/56700137

Korzeniowski, P. (2005, May 4). Retrieved April 10, 2006, from Why IT managers should pay attention to cell phone security Web Site: http://software.itmanagersjournal.com/print.pl?sid=05/04/29/0235223

Panettieri, J. ( ). Retrieved April 10, 2006, Don't be out'smart'ed Web Site: http://thejournal.com/the/learningcenters/center/?msid=10

Vamosi, R. (2006, February 17). Retrieved April 12, 2006, from Your smart phone has a dumb virus Web Site: http://reviews.cnet.com/4520-3513_7-6442087-1.html

* Wong, K. (1996). Mobile Phone Fraud – Are GSM Networks Secure? *Computer Fraud & Security, 1996, 11-18.*

Zonk (2006, February 24). Retrieved April 10, 2006, Anti-virus vendors eye cell phones Web Site: http://it.slashdot.org/article.pl?sid=06/02/24/1547253