Attacks against Smartphones

Adnan Waheed Muzammil Zareen Khan
Email: {adnwa060, muzkh007}@student.liu.se
Supervisor: Anna Vapen, {annva@ida.liu.se}
Project Report for Information Security Course
Linköpings universitet, Sweden

Abstract

With the rapid increase in usage of Smartphones the risk of attacks is respectively increasing. According to a survey [1] the number of Smartphone users is increasing to 125 million in 2009. In this report we are presenting some specific problems related to Smartphones, the threats which are affecting this emerging technology, how an attacker can attack Smartphones, related work in the field and at last mitigations and precautions to be taken to avoid and prevent these attacks.

1. Introduction to Smartphone

We are going to explore the following questions in our report. These are the most important questions which are being addressed in the report.

- What is a Smartphone?
- How does a Smartphone communicate using different networks?
- Which possible attacks against Smartphones are there and from which sources do they originated?
- How can attacks against Smartphones be mitigated?
- What is the state of the art research of different information security companies and concerning Smartphone hardware and software?

A Smartphone is a mobile phone offering advanced capabilities, often with PC like functionality [2]. According to Wikipedia there is no agreement on a standard definition of the term Smartphone, it is changing with the modification in technology.

A Smartphone is a telephone with information access; it provides digital voice services as well as any combination of email text messaging, pager, web access, voice recognition, still and or video camera, MP3, TV or video player and organizer [3].

Smartphones were introduced by IBM and Bellsouth in 1994 under the name "Simon" [4]. These Smartphones were very heavy and costly.

Smartphones use mostly used cellular networks like GSM, GPRS and 3GP. Smartphones have powerful capabilities; they can be used to threaten accounting and eliminating predictability by using subverting. There are different sources of attacks on Smartphones which include internet, PC to Smartphone data transfer and attacks during wireless connection to other devices, Infrared, Bluetooth etc. There are a number of existing malware and vulnerabilities which are discovered and reported by different security providers there detail will be presented in further sections. Some known threats from telecommunication networks to Smartphones and from Smartphones to telecommunication like DoS and DDoS attacks will be discussed in coming sections of the report. Anti-malware companies like Symantec and Fsecure are improving their products to also be affective against Smartphone malware. There should be awareness about Smartphone attacks among users as well as in companies providing facilities to Smartphones users like telecom operators etc. There should also be consensus between the telecom industry and internet service providers to provide proper solutions to Smartphone attacks.

2. Background of Smartphone attacks

Smartphones are end points to both telecom networks and the internet, it means that Smartphones are connected to both internet and telecommunication networks [6]. Following figure illustrate this fact.

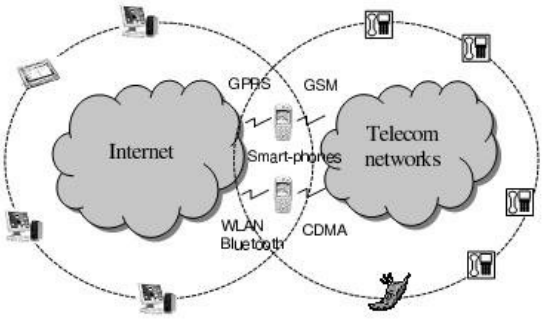

Fig: Smartphone endpoint between two networks [6]

Smartphones are having capabilities of normal computers and cellular phones, they are also portable devices. They contain different operating systems like Symbians, Microsoft Windows, Linux and Android etc. This makes it possible for an attacker to transfer a wide range of different malware from internet to telecommunication networks. This malware is a threat to

Smartphones and telecommunication networks. Malware which is transferred from internet or other networks to for example personal computers can then be transferred to a Smartphone for which it is harmful.

3. Telecom Networks for Smartphone

Smartphones can use different networks like GSM, GPRS and 3GP depending on the device.

4. Sources of attacks

There are different sources of attacks on Smartphones. These attacks do not only affect the Smartphones, but also influence telecommunication networks since Smartphones are endpoints between internet and telecommunication networks.

4.1 Internet

Internet is the main source of attacks on Smartphones. Examples of these attacks are spreading of viruses and hacking are possible attacks, normally Smartphones have WiFi connections - they are internet enabled. The number of WiFi access points is also increasing day by day at homes and organizations.

Modern Smartphones are coming with built-in WiFi connection support. WiFi is not properly secured. It can easily be hacked and misused. Smartphones having WiFi technology, the attackers can hide themselves and attack networks causing damage [7].

There are some aspects regarding the internet connection in Smartphone explained below.

- Personal data can be stolen e.g. saved passwords, PIN codes etc.
- Telecommunication networks can be hacked using Smartphones through internet.
- Illegal and copyright protected data can be downloaded using Smartphones.
- It can be possible that some one else is hacking or performing some wrong deeds and remain hidden while using another persons access point.
- Smartphones can be used to send malicious emails using unsecured WiFi connections.
- A traitor employee can steal sensitive data from his organization and later misuse it.
- Networks within a company can be disabled or misused by a person working in company by using Smartphones.

4.2 Desktop Computers

Smartphone users use their personal computers for data synchronization and data transfer. The connection can be wireless or wired. The relationship between Smartphones and PCs is a trust relation [6]. It is possible that the PC is infected with a virus and during data transfer or data synchronization the virus is transferred to the Smartphone, while using the Smartphone in a telecom network and the organization's networks infected data can be transferred to these networks infecting the entire network. Files can get infected by different causes such as the following

- Data transfer
- Data Synchronization
- Software installation through personal computer
- Allowing un verified applications to be installed on Smartphones
- Unsecured connection between PC and Smartphone can be interrupted by attackers and thus they can access the Smartphone and the PC

4.3 Hardware

A Smartphone contain components like microprocessor, main board, ROM, RAM, flash memory and a LCD display. Hardware can be under physical or logical attacks depending on the functionality for example if the ROM is an EPROM it can be altered. Hardware attacks are low level attacks but can be initiated by malware.

4.4 Connections

Smartphones uses different connections for data transfer, beside internet there are some more short range wireless connections used by Smartphones like infrared and Bluetooth that can be used for malware spreading and other attacks.

4.4.1 Bluetooth

The first ever detected Smartphone worm was Cabir which attacks Smartphones running the Symbian operating system. This worm detects other Smartphones with the same operating system and automatically spread via Bluetooth [8].

4.4.2 Infrared

Infrared is a very short range wireless connection. Someone using IR on his Smartphone should receive data only from trusted sources [9]. Because of the short distance it is easy to believe that the channel leads to the nearby device that you trust. Since users tend to trust IR, thinking the channel is trusted; infrared can be a channel for spreading malware.

5. Different Attacks on Smartphones

With the increase in use of Smartphones, security issues are also increasing. By attacking the Smartphone, the attacker can steal or damage following kinds of assets:

- Personal Information
- Sensitive data like IDs, personal notes, calendar, to-do list etc
- The user's internet connection
- Contacts / business cards
- Video or multimedia

5.1 Threats

Possible threats towards Smartphones can be malicious code that can destroy your Smartphone, in a sense that it stops functioning and can give the attacker access to information and data stored in your device, ffraudulent web page, e-mail or text message that entices the unwary to reveal passwords, financial details or other private data. [10]

Malware is malicious code that is being used to attack computing devices including Smartphones. Today there are more than 300 kinds of malware types aiming at Smartphones. Among them are worms, Trojan horses, viruses and spyware [10]. The major classifications of malware for Smartphones are:

- **Worms:** A worm is a small program or application designed to copy itself from one device to another automatically.
- **Virus:** A virus is a piece of code; may or may not be a complete program, attached to some other program. It usually depends on the execution of the host program [11]. Viruses can infect other files, but they cannot spread by themselves as worms do.
- **Trojans:** A program that purports to be useful but actually harbours hidden malicious code [10] or we can say that may appear to be legitimate, but in fact does something malicious [12].
- **Spyware:** Software that reveals private information about the user or a system [10]. Basically, a spyware is a hidden program installed on a device and collects and monitors the information and application data

The categorization of common malwares based on their functionality is as follows:

5.1.1 Bluetooth malware

- **Cabir:** June 2004. Connects to other Bluetooth devices and copies itself. Constant Bluetooth scanning drains phone's battery [10] [13].
- **CommWarrior:** March 2005. Replicates via Bluetooth; sends itself as an MMS file to numbers in phone's address book and in automatic replies to incoming SMS (text) and MMS messages; copies itself to the removable memory card and inserts itself into other program installation files on phone [10].
- **VeLasco:** replicates over Bluetooth connections and arrives as a file named *velasco.sis*. When the user clicks the *velasco.sis* and chooses to install the file, the worm activates and starts looking for new devices to infect over Bluetooth [14].

5.1.2 SMS/ MMS malware

- **Sexy View (SMS Worm):** is thought to be the first to spread via a text message, the worm manages to proliferate by sending an SMS to every contact in the device's address book inviting them to view some "sexy" pictures, hence the name [15].
- **RedBrowser:** February 2006. A Trojan surreptitiously sends a stream of text messages, at a premium rate of $5 each, to a phone number in Russia [16] [10].
- **Trojan.SymbOS.Mosquit:** is classified as a Trojan as it sends SMS messages to premium rated services without the knowledge of the user. The numbers which messages are sent to are coded into the program [16].

5.1.3 Malware attacks on System

- **Skulls:** November 21, 2004, Symbians OS, Trojan that replaces the system applications with non-functional versions, so that everything but the phone functionality will be disabled [14].
- **DoomBoot:** July 2005, a type of Trojan that prevents the phone from booting and installs Cabir and CommWarrior on the phone [10].
- **Trojan.SymbOS.Dampig:** is an OS vulnerability that replaces system applications [16].
- **Cardtrap:** September 20, 2005, Symbians OS, Trojan that spreads to users' PC through the phone's memory card [16].
- **Locknut (Gavno):** February 1, 2005, Symbians OS, replicates via download from Symbians patch sites that replaces a critical system binary, causing the phone to lock down so that no applications can be used [14].

5.1.4 Memory card malware

- **WinCE.Infomeiti:** A worm that spreads by copying itself to memory cards on compromised mobile devices. It may also send confidential information to a remote site and lowers security settings [17].
- **WinCE.PmCryptic.A:** is a worm that spreads by copying itself to memory cards on compromised mobile devices. It also attempts to dial premium-rate numbers [17].

5.1.5 Other malware

- **FlexiSpy:** March 2006. Spyware, Sends a log of phone calls and copies of text and MMS messages to a commercial Internet server for viewing by a third party [10].

5.2 Attacks

We may divide Smartphone attacks in these categories: [6] [18]

- **Attacks from Internet:** Internet is also a source to attack Smartphones, while browsing different websites there is a chance of malicious code to be downloaded.

- **Attacks originating from a local computer:** The Smartphone can be compromised by malware during the synchronization process with desktop PCs or laptops. First, the malware activates in PCs and then it is copied to the Smartphone and starts functioning.
- **Long range communication channel attacks:** Attackers are able to attack by sending malicious code via SMS or MMS to a Smartphone. Infected devices can also be used to send SMS to other contacts automatically.
- **Short range communication channel attacks:** Peer-to-peer connections or connectivity via Bluetooth or infrared can also be used to compromise Smartphone security. There are lots of malware that are being used by attackers to attack via Bluetooth.
- **DoS to base station:** DoS compromised smart-phones use up radio resource at a base station and can make phone calls easily using Microsoft Smart-phone SDK API "PhoneMake-Call" to phone numbers obtained from yellow pages etc.
- **Spamming:** Smartphones can be used to send spam messages even without the owner of the device knowing about it. Attackers can send marketing or junk messages via compromised Smartphone.
- **Identity theft and spoofing:** With compromised Smartphone, an attacker can use the identity of a Smartphone for any activity in the name of legitimate user.
- **Remote Wiretapping:** A compromised Smartphone can record any phone conversation and then send the recording to a malicious third party.
- **Physical Attacks:** Usually Smartphone contains a lot of secret information like personal files, contacts, pictures or business cards so that the stealth of Smartphone is a big lose.

6. Mitigation against Smartphone attacks

In 1970s the US department of defence created the Tiger Team; the mission of this team was to test the security of computers and operating systems [19]. It means even then when there was a little chance of computers being threatens there were precautions to handle the situations. With the passage of time there is an increase in hacking, Trojan horses, viruses, worms, vulnerabilities and threats, they are becoming challenge for the security minds and defenders to work against them and mitigate these threats to computers. With the development new Smartphone containing a powerful structure has been introduced. With the rapid use of this device attacks from internet, software and hardware are increasing with same speed. In this section we are going to explain some mitigations and preventions of different attacks from or to the Smartphones.

6.1 Software

Nowadays instead of upgrading hardware putting which is an expensive and time consuming process, newer versions of an existing product are upgraded through software. With the rapid software development come new vulnerabilities.

6.1.1 Operating System

Smartphone operating systems are not yet explored by malware writers but it could be an important area of mobile phone attackers to inject viruses and worms in to Smartphone OS. According to Marek Bialoglowy, an operating system vulnerability is found in Sony Ericsson P900 [14]. The vulnerability is not much dangerous but when sending a file to vulnerable phones it crashes the device. This vulnerability is explored by researchers, not malware writers, so there must be precaution to prevent it in other Smartphones also. Nokia 9500 also contains a similar kind of overflow problem, in this case when a user reads a vCard [14]. The vCard contains information like name, address, phone number etc. When the name field is longer than certain limit the text viewer crashes. This vulnerability can be used by attackers to inject their own code in to this Smartphone and cause it to overflow the buffer and then execute the attack code. The attack should be prevented by using advanced application designing tools in which security is considered to be the main part.

6.1.2 Internet side protection

The criteria which were designed for malware for internet side protection for personal computers can also be used for Smartphones, when it comes to defence against known vulnerabilities, but for unknown vulnerabilities internet service providers should ensure that the devices which is accessing their ISP is properly protected and patched, there should not be a possibility for an unprotected and unshielded device to access ISP and later spread its viruses on internet. For mitigation of such attacks the following measures should be taken

- The base stations of telecom networks should check if the device accessing them is protected or not and it is safe to access it
- If it is not safe, in some cases if it is possible, BS should make it protected

6.1.3 Phone Applications

Applications can be installed on Smartphones as on ordinary computers. These applications include games, organizers, converters, calculator etc. Many of these applications are not from reliable sources. There are a number of websites providing software for different brands of Smartphones, these small applications contain malware. They are not properly checked and should not be installed to Smartphones without verification.

Concerning the application development of Smartphone applications the following measures should be taken.

Software developers should understand what is to have mutually reinforced and independent software defense [8]. Software defense should make it complicated for attackers to perform any control dataflow analysis etc [8]. The executable version of the application should be so complex that no technology and technique should understand what program does. New tools are needed for application development and security.

6.1.4 Firewalls and intrusion detection system

There should be a proper firewall for protection of the Smartphone it's a suggestion not implemented in market. While deploying this firewall it should be kept in mind that firewall only protects from outside attacks. If a virus is already present in the phone the firewall will not be as useful so there should be proper precautions for it. Intrusion detection systems make the Smartphone protected from outside attacks such as hacking etc. A proper firewall should be there in the phone to protect in from external hackers attacks.

6.2 Hardware

Protection from for example malware attacks can be built into hardware directly thus making the Smartphone more of a trusted platform.

6.2.1 Bluetooth

Bluetooth is wireless communication system, the possibility of transmission to be jammed or intercepted and false information passing is very large. To attack Bluetooth devices powerful direction antennas can be used for scanning, eavesdropping and attacking on almost all kind of Bluetooth attacks. To mitigate such kind of attacks following measures should be taken.

- Bluetooth security is based on building a chain of events none of which shared provide meaningful information to eavesdropping [20].
- To make pairing of devices there must be PIN or passkey for trusted communication [20].
- As these keys can be guessed and cannot prevent eavesdropping fully, the keys should be made by using advance encryption techniques like SSP, Diffie-Hellman etc [20].

6.2.2 WiFi

For WiFi here is explanation for mitigation of different attacks

- **Interception:** Eavesdropping is possible through WiFi; to avoid this cryptography should be used properly.
- **Injection:** To avoid such kind of attacks MAC level could provide data source authentication for every transmitted frame by indentifying source as specific node[21]
- **Jamming:** Bluetooth can be jammed even from microwave oven, should be kept away from such devices.
- **Hijacking:** Spatial and frequency information should be included in victims authentication [21].

6.2.3 SIM Cards

Smartphones can be used for phone banking and stock transactions and the data, for example the PIN codes and keys, is kept on the SIM card. This data is kept without protection. An attacker can clone data on the SIM card, so there is a need for more efficient encryption techniques to make the data on the SIM card more protected [8].

6.2.4 Smartphone attack surface reduction

The security against such kind of attacks can be reduced by shutting down the internet portion while receiving or sending SMS and while using internet SMS applications should be shut down. This will reduce the attack surface [6].

6.2.5 Infrared

Attacks on infrared channels can be mitigated by using checks on the IR connection and keep using mutual authentication.

7. Companies developing anti-malware software

- **Fsecure:** "Once a malware gets into our Security Lab, it never gets out." F-Secure Corporation is providing security as a service through ISP's and mobile operators and offer security solutions to companies of different size [14].
- **Symantec:** Symantec provides anti viruses to protect from different kinds of attacks both for PCs and Smartphone also. Norton Smartphone Security is a valuable product of Symantec with key features including minimization of SMS spam, Blocks snoop-ware from turning on your camera and protects against viruses and other threats [17].
- **ESET Nod32:** ESET provides antivirus software with spyware and malware protection [22]. ESET has launched Mobile Antivirus for Smartphone that Detect and clean known and unknown mobile malware and also provides SMS anti-spamming [22].
- **Panda:** Panda Security also provides services and software to protect from different Smartphone malware. They have one of the best laboratories for analyzing [23].

8. Summary

In this paper we describe different kinds of attacks against Smartphones. The goal is to alert users and researchers to help them to find ways to avoid and

prevent these attacks. We have also presented possible mitigations to the attacks.

9. Conclusions

Smartphones are advanced computing and communication devices regarding mobility and their usage. Very little research is found on Smartphone attacks and their mitigations. We try to find countermeasures to many kinds of attacks and how to avoid them. We have discussed telecommunication networks, internet, software and hardware. Before launching new Smartphones on the market all the companies including both hardware and software developers should ensure that the product is secure in all ways.

References

[1] 3G Forums
http://www.3g.co.uk
Dated: 3rd March, 2009

[2] Silicon Driving Bussiness through silicon
http://networks.silicon.com
Dated: 5th March, 2009

[3] The Independent Guide of Technology
http://www.pcmag.com
Dated: 4th April,2009

[4] Schneidawind, J: "Big Blue unveiling", USA Today, November 23, 1992, page 2B
Dated: 25th, March, 2009

[5] http://news.zdnet.com

[6] Microsoft Research
http://research.microsoft.com/en-us/um/people/helenw/papers/smartphone.pdf
Dated: 6th march, 2009

[7] The Global Leader in wireless Security Solution
http://www.airtightnetworks.com
Date: 28th march, 2009

[8] Security Focus
http://www.securityfocus.com
Dated: 1st April, 2009

[9] Microsoft
http://www.microsoft.com
Dated: 3rd May, 2009

[10] Malware goes Mobile by Mikko Hypponen at Scientific America, Inc available at
www.sciam.com

[11] Malicious Software in Mobile Devices Chapter # 1 by Thomas M. Chen and Cyrus Peikari.

[12] Antivirus Software
http://antivirus.about.com

[13] Cnet NEWS
http://news.cnet.com

[14] Fsecure Antivirus solutions
http://www.f-secure.com

[15] Connecting Technology Professional
http://www.itwire.com

[16] All about internet security
http://www.viruslist.com

[17] Symantec Antivirus
http://www.symantec.com

[18] Mobile Malware: Threats and Prevention by Zhu Cheng available at
www.mcafee.com

[19] Industry Trends Sumit Ghosh, Stevens Institute of Technology
http://cs.uttyler.edu

[20] Keijo M.J. Haataja, Konstantin Hyppönen University of Kuopio
Man-In-The-Middle Attacks on Bluetooth: A Comparative Analysis, a Novel Attack, and Countermeasures

[21] IEEE Computer Society
http://www.computer.org

[22] We protect your digital word
http://www.eset.com/

[23] Panda Secuirty
http://www.pandasecurity.com