Research on Resolution of Security Issues in Smart Phones

Qutubuddin Shaikh, Yashwant Deore
Department Of MCA,
Mumbai University Maharashtra, India

Abstract: Smart phones are becoming enriched with confidential information due to their powerful computational capabilities and attractive communications features. The smart phone is one of the most widely used platforms by businesses and users alike. This is partially because smart phones use the free, open-source Linux as the underlying operating system, which allows development of applications by any software developer. This research study aims to explore the security damage caused by subverted smart-phones could range from privacy violation and identity theft to emergency call center DDoS attacks and national crises. We also propose techniques to generate solution space that includes smart-phone hardening approaches, Internet-side defense, telecom-side defense, and coordination mechanisms that may be needed between the Internet and telecom networks.

Keywords: Spamming, Identity Theft, Wiretapping, Internet, Telecommunication Side Protection, Vulnerability Malware, Smart phones, Hacker, Threats, Vulnerability.

1. INTRODUCTION

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

A smart phone is a mobile phone with an advanced mobile operating system. They typically combine the features of a cell phone with those of other popular mobile devices, such as personal digital assistant (PDA), media player and GPS navigation unit.

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.

Smartphones were introduced by IBM and Bellsouth in 1994 under the name “Simon” . 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.

We give guidelines and potential strategies on protecting the telecom infrastructure as well as smart-phones and discuss other interoperating devices and the causes for such 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 . Following figure illustrate this fact.

ISSN: 2278 – 1323

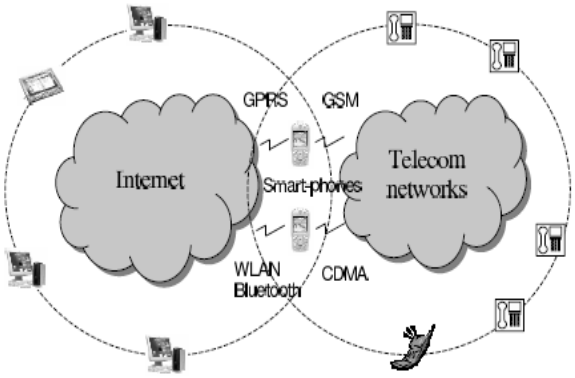

Fig: Smartphone endpoint between two networks

Although the detailed design and functionality vary among these OS vendors, all share the following features :

- Access to cellular network with various cellular standards such as GSM /CDMA and UMTS.
- Access to the Internet with various network interfaces such as infrared, Bluetooth, GPRS/CDMA1X, and 802.11; and use standard TCP/IP protocol stack to connect to the Internet.
- Multi-tasking for running multiple applications simultaneously.
- Data synchronization with desktop PCs.
- Open APIs for application development.

3. SOURCE OF SMART-PHONE ATTACKS

a) Internet:

Internet is the main source of attacks on Smartphones.

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.

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
- Networks within a company can be disabled or misused by a person working in company by using Smartphones.

b) 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.

c) Spamming:

As the popularity of mobile phones surged in the early 2000s, frequent users of text messaging began to see an increase in the number of unsolicited (and generally unwanted) commercial advertisements being sent to their telephones through text messaging. This can be particularly annoying for the recipient because, unlike in email, some recipients may be charged a fee for every message received, including spam.

d) 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.

e) 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.

f) Infection from compromised PC during data synchronization:

ISSN: 2278 – 1323

Smart-phone users typically synchronize their e-mails, calendar, or other data with their desktop PCs through synchronization software like ActiveSync. There exists trust relationships between smart-phones and their respective synchronization PCs. Therefore, to ultimately infect a smartphone, attackers can first infect its synchronization PC, and then the smart-phone will be infected at the next synchronization time

g) Peer smart-phone attack or infection:

A compromised smart-phone can actively scan and infect peer smart-phones through its Wireless Personal Area Networks (WPAN) interface such as Bluetooth or UWB (ultra wideband). Since smart-phones are mobile devices, they can infect new victims at different locations. The first smart-phone worm, Cabir, uses this method.

4. 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.

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. The major classifications of malware for Smartphones are:

a) Worms:

A worm is a small program or application designed to copy itself from one device to another automatically.

b) 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 . Viruses can infect other files, but they cannot spread by themselves as worms do.

c) Spyware:

Software that reveals private information about the user or a system . Basically, a spyware is a hidden program installed on a device and collects and monitors the information and application data.

d) Trojans:

A program that purports to be useful but actually harbours hidden malicious code or we can say that may appear to be legitimate, but in fact does something malicious

5. DEFENSE

a) Internet side protection:

Protection techniques like more intensive software patching and vulnerability-driven network traffic shielding will definitely be useful protection for smartphones against well-Known vulnerabilities. It would be desired for smartphone Internet service providers to guarantee that devices which access them are shielded or patched. It means that unshielded devices should not be granted access to the Internet.

b) Hardening the Smartphones:

Smartphone hardening is one of the recommended solutions to make smartphones less vulnerable. Some techniques can be:

i. Operating system hardening(OS hardening):

Some security issues can be enforced by Smartphone operating systems like always showing the callee's phone number and also brighten LCD display when dialing. This can be achieved by only

ISSN: 2278 – 1323

using security modified APIs to applications. There are also further policies for hardening operating systems such as using security patches and bug patches to software and limiting user privileges and disabling unnecessary processor

ii. Hardware hardening:

Smartphone already has an embedded smart-card(the SIM card)which has evolved to incorporate the use of the SIM Toolkit (STK) 1. STK allows the mobile operator to provide services by loading them into the SIM card without modification of the GSM handset .One intriguing method is merging the STK card and TCG‟s Trusted Platform Module (TPM) for smartphone hardware hardening without additional security chips.

iii. Feature reduction:

One simple protection technique is to reduce inactive features as much as possible. Although Smartphones are always on, most of their features are not necessary to be active. For instance, Bluetooth and WiFi should be turned off when not in use.

c) Telecom side protection:

In order to detect the smartphone attacks described, analyzing the following information from telecom networks can be helpful for telecom carriers: • Anomalous blocking rate of a base station or a switch: Commonly the call blocking rate must be under a threshold (< 0.01%). So a sharp increase in the blocking rate can be a conspicuous sign of an ongoing attack. • Call center load information: if a call center experiences a sudden flash crowd and user behaviors are anomalous then the call center is susceptible to attack. • End user's misbehavior: A normal behavior such as connected calls with no voice traffic; lengthy data packet transmission from a single user or to a single user and transmitting the same message to many different users (spamming).

d) Protection against spoofing:

A simple defense technique that only works for simple ARP spoofing attacks is the use of static IP-MAC mappings. In order to be protected against IP spoofing, the solution is to apply ingress filtering and have all internal routers to disable source routing. It can be further prevented by educating users to be conscious about the address window in a web browser that shows the web address they are directed to. In addition, DNS spoofing can be prevented by securing the DNS servers and by adding anti-spoofing measures to the filter-list to check site ratings for URLs by their name and IP address. DNS lookups are supported to filter-list information for improved IP address lookups.

6. CONCLUSION

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 counter measures 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. We have outlined a number of defense strategies, many of which demand much further research.

REFERENCES

[1] 3G Forums http://www.3g.co.uk

[2] Silicon Driving Bussiness through silicon http://networks.silicon.com

[3] The Independent Guide of Technology http://www.pcmag.com

[4] Microsoft Research http://research.microsoft.com/enus/um/people/helenw/papers/smartphone.pdf

ISSN: 2278 – 1323

[5] Security Focus http://www.securityfocus.com

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

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

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

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

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

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

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

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

AUTHORS PROFILE

Qutubuddin Shaikh currently pursuing MCA from IMCOST Thane affiliated by Mumbai University.

Yashwant Deore currently pursuing MCA from IMCOST Thane affiliated by Mumbai University.

ISSN: 2278 – 1323