ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

Research on Different Types of Attacks in Smart Phones

Vasundhara Varade
Department Of MCA,
Mumbai University Maharashtra, India

Abstract **- Smart phones are becoming improve 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. personal and business information now stored on smart- phones This research study aims to explore the types of attacks in smart-phones. I also propose effects of attackers on smart-phones as well as give some information about Threats. I have discuss coordination mechanisms that may be needed between the Internet and telecom networks.**

Keywords **- Spamming, Identity Theft, Internet, Internet and Telecommunication Network, Threats, Consequences.**

I. 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 Smartphone
- How can attacks against Smartphones be mitigated?
- What is the state of the art research of different information security companies
  and concerning Smartphone and Software?

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

A Smartphone is a electronic device with information access; it provides digital voice services as well as any combination of email text messaging, 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.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. First we give some background on Smartphones. 2.In section 3, we describe source of smartphones

II. BACKGROUND OF SMARTPHONE ATTACKS

Smart-phone is the unified communications which integrate telecom and Internet services onto a single device because it has combined the portability of cell-phones with the computing and networking power of PCs. 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.

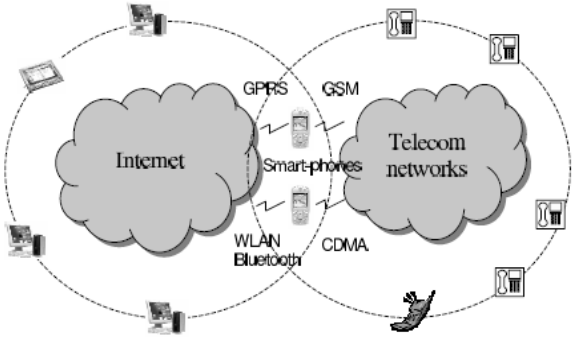


Fig: Smartphone endpoint between two networks

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.

III. SOURCE OF SMART-PHONE ATTACKS

3.1 *Internet:*

Internet is the main source of attacks on Smartphones.

Internet is an important aspect of smartphones. Modern Smartphones provide built-in WiFi service. Wifi is not completely secured. It can easily be hacked and misused using password. Smartphones having WiFi technology, the attackers can hide themselves and attack networks causing damage.

There are some problems 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

3.2 Hardware:

A Smartphone contain hardware components like microprocessor, main board, ROM, RAM, memory cards, memory, and screen Hardware contain two types of attacks i.e physical attack and logical attack

3.2.1 logical attack

Browser: In addition to the usual browser vulnerabilities (Web standards processing), smartphones offer further targets due to the interaction between browser and phone. For example, the user identity connected to the SIM card may be abused.

Remote Maintenance: Disabled automatic updates or an insecure configuration may promote attacks just as much as insufficiently protected interfaces to the remote device management.

3.2.2 physical attack

Wireless Interfaces: When an attacker is located in the

immediate vicinity of a device, manipulated data can be sent allowing vulnerabilities in radio communication (Bluetooth, NFC, WiFi, etc.) to be taken advantage of in order to obtain user data and passwords illegally.

Memory Cards: Data on external storage media is frequently unprotected. An attacker may be able to read the data directly if a smartphone ends up in his hands. When an attacker is able to store manipulated data on the memory card, the smartphone's vulnerabilities can be taken advantage of. If a manipulated smartphone is hooked up to the company's PC, the attackers may use it as a host for infections and attack the computer during synchronization and beyond that the overall enterprise network as well.

3.3 Spamming:

Attackers can manipulate smart-phone to send junk through SMS. compromised smart-phone can spam for "free"; and therefore its owner may not even notice its bad behaviour. Free SMS spamming gives attackers good incentives to compromise smart-phones..

3.4 *Bluetooth:*

Bluetooth is wirless device. Now a days Bluetooth is in-build in smartphones This wireless device spread worm automatically.

3.5 Infrared:

Infrared is also a type of wireless device. It provide very short range. Someone using IR on his Smartphone should receive data only from trusted sources. 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 spread malware using channels.

3.6 Infection from compromised PC during data synchronization:

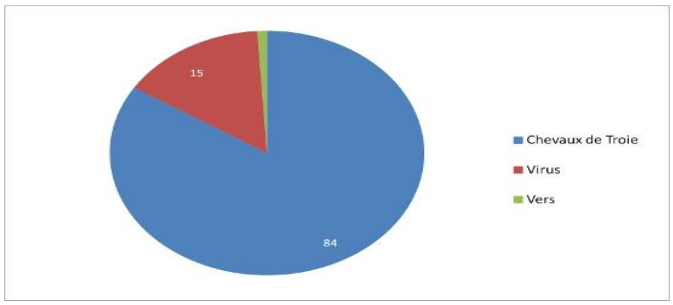
Smart-phone users typically synchronize their e-mails, calendar, or other data with their desktop PCs through synchronization software like ActiveSync. There exists trust relationships between smart-phones and their respective synchronization PCs. Therefore, to ultimately infect a smart-phone, attackers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

IV. THREATS

Threats can be malicious code to the smartphones that can destroy or damage your Smartphone, that means it can stops functioning and

give the chance to the attacker to access the information and data which is stored in your device.

Malware means malicious code. It is a computer program that aims to harm the system in which it resides. that means it used to attack to the computing devices including Smart phones. Today there are more than 300 types of malware which is aiming at Smart phones. worms, Trojan, viruses and spyware this are some types of Threads . The major classifications of malware for Smart phones are:



4.1 Worms:

A worm is a small program or application designed to copy itself from one device to another automatically in another words a worm is a program that reproduces on multiple computers across a network.

4.2 Virus:

A virus is a piece of software that can infect other programs by modifying them. The modification includes a copy of the virus program, which can then go on to infect other programs. A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. once a virus is executing, it can perform any function ,such as erasing files and programs.

4.3 Spyware:

Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. Spyware is mostly classified into four types: system monitors, Trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers ,may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. Keyloggers are sometimes part of malware packages downloaded onto computers without the owners' knowledge. Some keyloggers software is freely available on the internet while others are commercial or private applications. A spyware program is rarely alone on a computer: an affected machine usually has multiple infections.Users frequently notice unwanted behavior and degradation of system performance. A spyware infestation can create significant unwanted CPU activity, disk usage, and network traffic.

4.4 Trojans:

Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Trojans are a class of malware that take their name from the way they infect computers. Trojans hide themselves within seemingly harmless programs or try to trick you into installing them. Trojans do not replicate by infecting other files or computers. Instead, Trojans survive by going unnoticed: they may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Some of the more common actions that Trojans take are:

4.4.1 Creating backdoors:

some Trojans will makes changes to your security system so that your data and device can be accessed by their controller.

4.4.2 Spying:

some Trojans are designed to wait until you access your online accounts or enter your credit card details, and then send your data back to whoever is in control.

4.4.3 Steal your passwords:

some Trojans are made to steal your passwords of your most important online accounts.

4.4.4 Turn your computer into a Zombie:

Some Trojans just want to use your computer as a slave in a network controlled by a single hacker.

4.4.5 Send costly SMS messages:

Even smartphones get Trojans, and the most common way for criminals to make money is by using them tomake your phone send costly SMS messages to premium numbers.

V. CONSEQUENCES

When a smartphone is infected by an attacker, the attacker can attempt several things:

- The attacker can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email.

- The attacker can easily force the smart phone to make phone calls. For example, one can use the API (library that contains the basic functions not present in the smart phone) Phone Make Call by Microsoft, which collects telephone numbers from any source such as yellow pages, and then call them. But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone. It is also very dangerous because the smartphone could call emergency services and thus disrupt those services.

- A compromised smartphone can record conversations between the user and others and send them to a third party. This can cause user privacy and industrial security problems.
- An attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner.
- The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user

VI. TYPES OF ATTACKS

6.1 Attacks based on Communication:

6.1.1 Attack based on SMS

A study on the safety of the SMS infrastructure revealed that SMS messages sent from the Internet can be used to perform a distributed denial of service (DDoS) attack against the mobile telecommunications infrastructure of a big city. The attack exploits the delays in the delivery of messages to overload the network.

6.1.2 Attack based on MMS

Another potential attack could begin with a phone that sends an MMS to other phones, with an attachment. This attachment is infected with a virus. Upon receipt of the MMS, the user can choose to open the attachment. If it is opened, the phone is infected, and the virus sends an MMS with an infected attachment to all the contacts in the address book.

6.1.3 Attacks based on the GSM networks:

tracing of mobile terminals is difficult since each time the mobile terminal is accessing or being accessed by the network, a new temporary identity (TMSI) is allocated to the mobile terminal. The TSMI is used as identity of the mobile terminal the next time it accesses the network. The TMSI is sent to the mobile terminal in encrypted messages.

Once the encryption algorithm of GSM is broken, the attacker can intercept all unencrypted communications made by the victim's smartphone.

6.1.4 Attacks based on Wi-Fi:

As with GSM, if the attacker succeeds in breaking the identification key, it will be possible to attack not only the phone but also the entire network it is connected to.

Many smartphones for wireless LANs remember they are already connected, and this mechanism prevents the user from having to re-identify with each connection. However, an attacker could create a WIFI access point twin with the same parameters and characteristics as the real network. Using the fact that some smartphones remember the networks, they could confuse the two networks and connect to the network of the attacker who can intercept data if it does not transmit its data in encrypted form.

Lasco is a worm that initially infects a remote device using the SIS file format. SIS file format (Software Installation Script) is a script file that can be executed by the system without user interaction. The smartphone thus believes the file to come from a trusted source and downloads it, infecting the machine.

6.2 Attacks based on Software application:

6.2.1 Web browser

The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, mobile web browsers are extended from pure web navigation with widgets and plug-ins, or are completely native mobile browsers. Smartphones are also victims of classic piracy related to the web:malicious websites, etc. The big difference is that smartphones do not yet have strong antivirus software available.

VII. 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.

ACKNOLEDMENT

We thank our colleagues from IMCOST who provided insight and expertise that greatly assisted the research ,although they

may not agree with all of the interpretations/conclusions of this paper.

We thank Mrs.Trupti Deshmukh for assistance us by providing proper IEEE formats all faculties for guiding us.

REFERENCES

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

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

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

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

[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 Security http://www.pandasecurity.com

AUTHORS PROFILE

Vasundhara Varade currently pursuing MCA from IMCOST Thane affiliated by Mumbai University.