International Journal of Innovative and Emerging Research in Engineering
Volume 3, Special Issue 1, ICSTSD 2016

A Study on Security for Mobile Devices From Mobile Malware and It's Attacks

Ajay Gopichand Barsagade
M.E (Pursuing)
Computer Science and Engineering
PRMIT&R, Badnera., Amravati, India
ajaybarsagade32@gmail.com

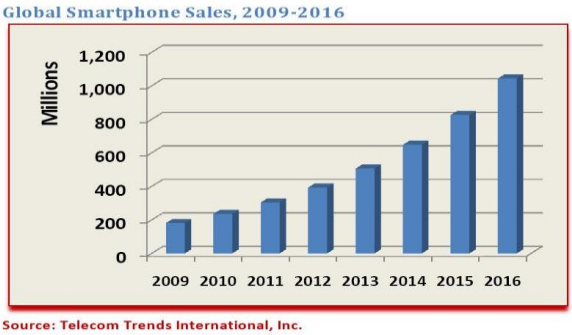
Ms. R.R. Tuteja
Professor
Computer Science and Engineering
PRMIT&R, Badnera., Amravati, India
rrtuteja@mitra.ac.in

***Abstract*—Now a days smartphones plays an vital role in today's day to day living. They enable us to freedom for doing variety of different work from any place. These devices not only provide voice communication but now they have to develop powerful platform for computing. Due to Smartphone's increasing popularity raises several privacy and security issues. Their central information and privacy database makes them very easy targets for hackers. Nowadays main use of smartphones in online shopping, net banking like all money related task may now represent a perfect target for malware maker. In this review paper we like to introduce you to all types of threats and their security solution with their Structured and comprehensive overview of the research on mobile malware is explored up to the period 2016, with their high-level attacks.**

I. INTRODUCTION

Now, there is a very small difference between Smart-phones, Personal Computers and other new emerged devices like laptops, tabs, and notebooks as all are now connected by verity of different connectivity options like Wi-Fi, Sharing apps, Bluetooth,, GPRS, UMTS, EDGE, 3G, 4G, HSDPA, HSPA (plus) and LTE.. Due to various services like Whatsapp, FaceBook, ShareIt and many online gaming provided by smart-phones with the help of applications, these are try to gain some private information from mobile-devices. This online network of cellphones has exposed them to the unsecured due to Malware and viruses designed for mobile phone environment. The security threat caused by these Malware and viruses are so severe that a time would soon come that the hackers could infect mobile phones with malicious software that will try to gain your private data or can run up a victim s phone bill by making toll calls. All these can lead to overload in mobile networks, which can eventually lead them to crash and then the financial data stealing which poises risk factors for smart phones. Due to this growing skill-set of cyber-criminals who device their own algorithms for stealing privacy, embarrassing service-provider and bring difficulties to the users. So, it requires special tool to secure these privacy of devices from virus and malwares with the help of anti-developed techniques and algorithms for detection.

Still if global sales of Smartphone's will pass 420 million devices in 2011 (according to a recent report by IMS research [10]). Worldwide sales of Smartphone's to end users totaled 968 million units in 2013 an rise of 42.3 percent from previous year (see fig a) as per view of a Gartner, Inc. Sales of Smartphone's accounted for 53.6 percent of over mobile sale in 2015 and increases annual sales of SMART phones for the very first time. Smartphone sales are still on track to high pick during the next few years and will exceed up to 2016 by one billion, IMS Research said in a new report. The quantity of mobile malware is still weak as compared to that of PC virus and malware [6]. In the next upcoming years we are going to face a larger variety and quantity of virus and malware.



The paper is categorized as follows. That is Section 2. Describes various types of mobile malware. In section 3. Discusses Mobile Malware attacks on Smartphone's Section 4. Mobile Malware Symptoms and Tips for safe computing. Section 5 we will present security solutions. Finally, in Section 6 we give some conclusions

II. MOBILE MALWARE

The amount and variety of mobile malware programs targeting Mobile phone and tab users is definitely growing at an alarming rate. We will explain the common types of malicious programs targeting mobile computing platforms, and give a brief description of each.

In this section we offer a comprehensive summary of latest mobile malware, symptoms of them and few tips for safe computing.

2.1 What is Mobile Malware?

Mobile malware first introduce in early 2004 attacking the Symbian OS, but exploded in 2011 when computer security pros reported a new attack on the Android computing platform every few weeks. These nefarious programs either install themselves or are installed on the device by unknowely mobile

users, and then perform functions without user knowledge or permission. Malicious mobile apps are often designed as legitimate applications. They can be distributed through the internet via mobile browsers, installed from Google play stores or even installed via device messaging functions. The insidious objectives of mobile malware range from hacking to stealing, from text messaging to phishing, from unwanted marketing to outright fraud. There is various malware out there attacking every mobile platform – from Apple iOS to WinMobile to Blackberry – yet today are the large variety of mobile malware programs today target Google Android users. Some researchers report a rate of infection too high percent, due to Google's open app development and distribution model. There are four broad classifications of mobile malware:

2.1.1 Spyware and Adware

Spyware secretly gathers confidential information about the mobile user and then spread this data to hackers. In variety of cases these may be publish like advertise or marketing data firms, which is why spyware is sometimes name as "adware". It is mostly download without user consent by disguising itself as a legitimate app (say, a simple app) or by attacking its payload on a designated app. Spyware uses the victim's mobile connection to relay private information such as contact list, present location, chatting habits, browser history and user preferences or downloads. Spyware that collect device information such as product ID, OS version, International Mobile Subscriber Identity (IMSI) number, International Mobile Equipment Identity (IMEI) number, and can be used for future attacks.

2.1.2 Trojans and Viruses

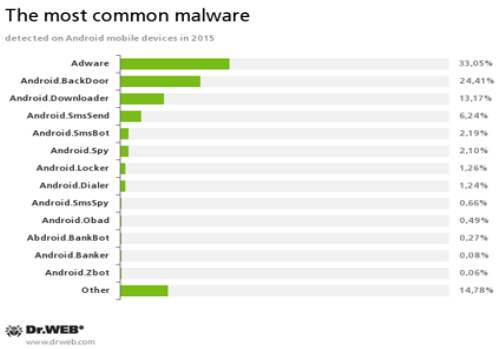
Mobile Trojans infect user mobile by sticking themselves to harmless or designate programs, are download with the program and then try to do malicious actions. Such programs have been known to hijack the browser, due to this the mobile to directly send unauthorized premium rate texts, or capture user login information from other apps such as mobile net banking. Trojans are much related to mobile viruses, which can become installed on the device by many ways and do variety of effects that range from simply annoying to highly-destructive and irreparable. Malicious parties can largely use mobile threats and viruses to root the device and gain access to files and flash memory.

2.1.3 Phishing Apps

Mobile internet browsing is growing with smartphone and tablet penetration. Just as with desktop computing, fraudsters are designing mobile phishing sites that very much look like a legitimate service but may steal user credentials or worse. The small screen size of mobile devices is making malicious phishing techniques easier to hide from users which less fit on mobile devices than PCs. Some phishing schemes use rogue mobile apps, programs which can be considered "trojanized", give their true presence as a system update, marketing offer or game. Others infect legitimate apps with malicious program that's only known to the user after installing.

2.1.4 Bot Processes

Mobile malware is getting more designated with programs that can operate in the background on the user mobile device, concealing themselves and creating a wait for certain operation like an online banking session to strike. Hidden processes can execute completely invisible to the user, run executable code or contact botmasters list for new instructions. The next wave is expected to be even more advanced, with botnet hibit to actually hijack and control infected devices.



III. METHODOLOGY OF ATTACKS ON MOBILE PHONES

All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from variety of communication technique like Short Message Service (SMS, aka text messaging),Multimedia Messaging Service (MMS), Wi-Fi Networks and many apps like ShareIt, Zappya etc., the de facto global standard for mobile communications. There are also attacks to destroy software vulnerabilities from both the web browser and operating system. Finally, there are kind of malicious software that used the weak knowledge of most of users.

3.1 Attacks based on communication

3.1.1 Attack based on SMS and MMS

Some mobile phone models have problems in managing SMS messages. It is done by sending an ill-formed block, to cause the phone to restart, show that denial of service attacks. If a user of mobile received a text message containing a Chinese character, it will be a denial of service. In some other case, while the standard requires that the maximum size of a Mail address is 32 characters, some phones did not verify this standard, so if a user enters an email address over 32 characters, that leads to complete dysfunction of the e-mail handler and puts it out of commission. This attack is called "curse of silence". A study on the safety of the messaging infrastructure referred that SMS messages sent from the Internet can be work to do a distributed denial of service (DDoS) attack against the mobile communications infrastructure. The attack work as a delay in the delivery of messages to overload the network. Another potential attack done by sending an MMS to other phones, with an attachment. This attachment is contains virus. After receipt of the MMS, the user can choose to open the attachment. If it is opened, the phone gets infected, and the virus starts sending an MMS with

an infected attachment to all the contacts in the address book.. Then, the virus began to send messages to recipients taken from the address book.

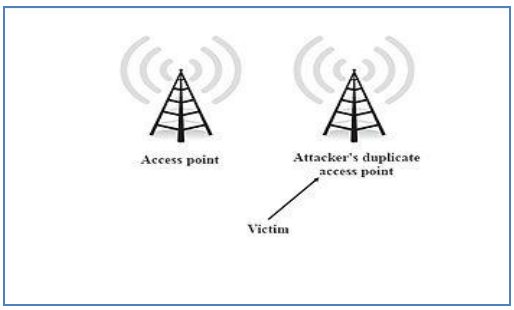
3.2 Attacks based on communication networks

3.2.1 Attacks based on the GSM networks

The attacker may try to break the GSM network encryption of the mobile. This algorithm belongs to the family of algorithms called A5. Due to the policy of security through obscurity it has not been possible to openly test the robustness of these algorithms. This has two version of the algorithm: A5/1 and A5/2 (stream ciphers), where the former was designed to be very strong, and the previous was designed to be weak on purpose to allow easy cryptanalysis and eavesdropping. The 3GPP approved a change request to prohibit the implementation of A5/2 in any new mobile phones. Stronger public algorithms have been added to the GSM standard, the A5/3 and A5/4, otherwise known as KASUMI or UEA1[22] published by the ETSI. Even in case mobile phones are able to use stronger 3G or 4G which have too stronger encryption than 2G GSM, the base station can downgrade the radio communication to 2G GSM and specify A5/0 (no encryption) .[20] This is the basis for eavesdropping attacks on mobile radio networks commonly called an IMSI catcher.

In addition, tracing of mobile terminals is difficult since every time the mobile device is accessed by the mobile network, a new identity for some time (TMSI) is allocated to the mobile device. The TSMI is used as identity of the mobile terminal the next time it accesses the network. The TMSI is sent to the mobile device in encrypted mix messages. Once the encryption algorithm of GSM is broken, the attacker can get all original messages made by the victim's smartphone.

3.2.2 Attacks based on Wi-Fi



An attacker can try to access on Wi-Fi communications to derive information (e.g. username, password). This is not a common type of attack, but they are very vulnerable to these attacks because very often the Wi-Fi is the only way to access the internet. The security of wireless networks (WLAN) is very necessary. Initially wireless networks were secured by WEP keys. The weakness of WEP is a short secrete key is the common for all connected devices. Now, most wireless networks are protected by the WPA security protocol. WPA is based on the "Temporal Key Integrity Protocol (TKIP)" which was designed to allow migration from WEP to WPA on the device. The major improvements in security are the dynamic encryption keys. For small networks, the WPA is a "pre-shared key" where encryption can be vulnerable if the length of the key is small. With very small chance for input (i.e. only the numeric keypad) mobile phone users might define short encryption keys that contain only numeric. This increases the likelihood that an attacker succeeds with a brute-force attack. The higher of WPA is called WPA2, and it is safe enough to withstand a brute force attack.

As with GSM, if the attacker gets access to identification key then it not only attack on mobile phone but also its network to. Many smartphones for wireless LANs remember they are already connected, and this technique disallow user from getting re-identify with each connection. However, an attacker could create a WIFI access point exactly same as the real network. Using the fact that some smartphones remember the networks, it may be possible to connect the network of the attacker who can intercept data if it does not transmit its data in encrypted form.

For example Lasco is a worm that initially infects a remote device by SIS file format.

3.2.3 Principle of Bluetooth-based attacks

Security issues related to Bluetooth on mobile devices have been studied and have shown numerous problems on different phones. One easy to exploit vulnerability: unregistered services do not require authorization and its virtual serial port used to control the phone. An attacker only gets access to that port to get full control of the device.[20] Another example: a phone Bluetooth in discovery phase. The attacker sends a file via Bluetooth. If the recipient accepts, a virus is transmitted. The virus searches for nearby phones with Bluetooth in discoverable phase and sends itself automatically to the target device. The user must accept the incoming file then it automatically installs the viral program. After installing, the virus(worm) get infects the machine.

3.3 Attacks based on vulnerabilities in software applications

Other attacks are based on flaws in the OS or applications on the phone.

3.3.1 Web browser

The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, mobile web browsers are have all widgets and plug-ins. Jailbreaking the iPhone with firmware 1.1.1 was based entirely on vulnerabilities on the web browser. As it described here underlines the importance of the Web browser as an attack vector for mobile devices. Here it based on a stack-based buffer overflow in a library of web browser.

Smartphones are also victims of classic piracy related to the web: phishing, malicious websites, etc.

3.3.2 Operating system

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. These attacks are difficult. In 2004, vulnerabilities in virtual machines running on certain devices were revealed. It is easy to pass the bytecode verifier and get access the native of operating *system*. The firmware security of Nokia's Symbian Platform

Security Architecture (PSA) is based on a central configuration file. In 2008 it was possible to manipulate the Nokia firmware before it is installed, and it's some version are human readable, so it can be modify the firmware. This vulnerability has been solved by an update from Nokia.

In some systems it was possible to overwrite a file with a file of the same name. In the Windows OS, it was possible to change a pointer from a general config file to an editable file.

When any application is installed first time, this application is verified by a series of certificates. Any hacker can create a valid signature without using a valid certificate and add it to the list.

3.4 Attacks based on hardware vulnerabilities

3.4.1 Electromagnetic Waveforms

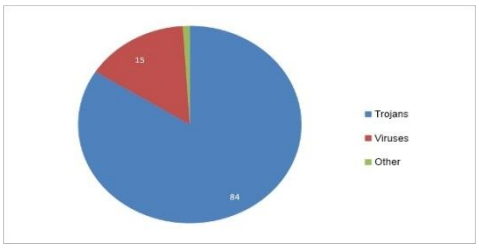
In 2015, researchers at the French government agency ANSSI demonstrated the capability to trigger the voice interface of certain smartphones remotely by using "specific electromagnetic waveforms".To took advantage headphone wires while plugged into the audio-output jacks of the smartphones and effectively spoofed audio input to inject commands via the audio interface.

3.4.2 Juice Jacking

Juice Jacking is a method of a hardware vulnerability specific to mobile platforms. Get by the dual purpose of the USB charge port, many devices have been susceptible to having data ex-filtrated from, or malware installed on to a mobile device by utilizing malicious charging kiosks set up in public places, or hidden in normal charge adapters.

3.4.4 Malicious software (malware)

A smartphones can easily access internet as computers with malware. A computer program means malware that aims to harm the system in which it resides. Malware includes all Trojans, worms and viruses. However, it must be said that the malware are far less numerous and important to smartphones as they are to computers.



Nonetheless, recent studies show that the evolution of malware in smartphones have rocketed in the last few years posing a threat to analysis and detection.

Depending on the type of malware, if you have it, the performance of your device could suffer, your personal information could be stolen, or intruders could gain access to your accounts. Those are just some of the potential consequences.

IV. MOBILE MALWARE SYMPTOMS AND SOME TIPS

4.1 Mobile Malware Symptoms

While all types of mobile malware distinguish by how they spread and infect devices, they all can produce some common symptoms. The symptoms of a malware infection in which unwanted behaviors and degradation of device performance. Stability issues such as hanging apps, fail to reboot and also get difficulty connecting to the network are also common. Mobile malware can decrease a battery suddenly or processing power, take control over the browser, send unauthorized SMS messages, freeze or brick the device entirely.. Android malware is becoming harder to detect for the average smartphone user who pays little, if any, attention to security. Fortunately, most malware creators are not rocket scientists, and a user does not have to be a computer scientist to combat them.

The following clues provide the presence of malware:

4.1.1 Bad Battery Life

Android users who don't perform too many activities to keep long their battery should last. Malware can mysteriously drain battery quicker than usual. That's usually due to adware, spam-like malware that shows app users of ads. Continuously displaying aggressive adware will impact heavily on battery life.

Whether the malware is hiding or trying to stay hidden from the user but mysteriously battery droping can often give away the presence of an Android infection.

4.1.2 Dropped Calls And Disruptions

Mobile malware can also perform some action on ongoing or incoming calls. Dropped calls or strange disruptions during a conversation could give the presence of malware in device. If you can't blame your mobile1 carrier, then some strand of mobile malware could be the culprit and it is possible that someone or something is trying to eavesdrop on conversations to perform some suspicious activities.

4.1.3 Inordinately Large Phone Bills

Android malware often infects devices and starts sending SMS (text) messages to premium-rated numbers. While these effects are easily seen in your phone bill, not all malware programs do the same and only send an SMS message just once a month to avoid suspicions. Whether you use a monthly plan or a pay-as-you-go subscription, just by checking bill can give you the presence of malware.

4.1.4 Data Plan Spikes

Malware that smuggles data from your device to a third-party can often be detected by an examination mobile data charges. Automatic variation in your download or upload patterns could be a sign that someone or something has browsing over your device.

4.1.5 Clogged Performance

Depending on device hardware specifications, malware infestation may cause serious performance problems as it tries to read, write or broadcast data from your smartphone. Anybody that has ever had a PC infected with malware should be familiar with this. Sometime your device restart several times a day due to background-running malware consumes too much processing power. Power as well as Performance and

task clogging are yet another sign that malware might be present on your device. Checking RAM or checking CPU load could reveal the presence of malware that's actively running on the device.

4.2 Tips for safe computing

Mobile users can follow number of practices to prevent mobile malware infections. In the fact most of mobile user in our free mobile security eBook. Some malware need some special treatment than others, but following these recommendations will allows user to increase security of mobile devices. Smartphones and tablets are common devices to mainstream consumer gadgets. As mobile devices become a ubiquitous part of the mainstream culture, malware developers are concentrating to exploit the fertile new territory.

To protect against malware you need to keep five general things in in your when buying or downloading apps for your mobile devices:

4.2.1 Be Aware

Now a days window's mobile malware work same as PC malware…yet. Malware developers aren't looking for a challenge. They will develop malware for the platforms and devices that have the largest chance of potential victims, and those that are easiest to exploit. Be aware is the first step in protecting yourself that the threat exists.

4.2.2 Do Your Homework

Think before you download. Just as it makes sense to take reviews before testing out a new restaurant or read some reviews of an app before you take into your device. General word is that you can get advice from your social networking friends and family you trust--before downloading an app.

4.2.3 Check Your Sources

Not all third-party sources of apps are bad, but the different is much higher. For a platform like iOS, you have to go out of your way to jailbreak the device in order to use apps such things never approved by Apple. If you have taken such drastic measures, you are hopefully already care about risk.

Android users may not be as conscious of the threat because third-party app repositories are common for that device. Then only, the safest source of Android apps is the official Google Android Market. To avoid shady apps, you should deselect the "Unknown sources" option of setting available in the Android Applications Developer Settings mode.

4.2.4 Watch the Permissions

Mobile operating systems have enough security option for to request permission to access core functions and services of the device. Just think about the type of permissions you are granting before you installing and blindly accept them. Does that Arrow game really need access to your contacts, camera function, and location information?

4.2.5 Use Antimalware

As per the mobile market grows, and the malware developers trying to target it, the security vendors like Antivirus companies are working to step ahead of the malware attacks with security tools and software.

Following the first four tips general way to avoid malware, but antimalware software can help detect and identify any threats that slip past your defenses.

V. SECURITY SOLUTIONS FOR MOBILE DEVICES

In this section we survey existing mechanisms that are developed to prevent different type of threats for smartphones. We present, first of all, intrusion detection systems for smartphones. They classified on the basis of their working area and behavior (distributed or local), reaction (active or passive), collected data (OS event, keystrokes), and OS.[14]

A. Intrusion Detection Systems

In this section, we present the state of the art of models and tools that implement Intrusion Detection Systems (IDSes) on smartphones. IDSes can differentiate on basis of their approaches:

1) prevention-based approaches:
using cryptographic algorithms, digital signatures, hash functions, important properties such as confidentiality, authentication or integrity can be assured; in this approach IDSec should be running on real time.

2) detection-based approaches:
IDSes serve as a first line of defense by effectively identifying malicious activities. Furthermore, there are two main types of detection:

a) *anomaly-based* (alternative names: anomaly detection, behavior-based), which compares the "normal" behavior with the "real" one;

b) *signature-based* (alternative names: signature detection, misuse-based, knowledge based, detection by appearance), also well-known pattern of attack.. There exist also hybrid approaches which combine the aforementioned types of detection. With signature-based approaches, the advantage is the false alarm rate that is usually very low. The disadvantage is that they only prevent the known attacks.. On the other hand, with an anomaly-based IDS we can detect various types of known as well as unknown attacks, but the amount of false alarms is usually quite high. Some of the metrics used to measure their effectiveness are true positive rate, accuracy and response time. In the following, we partition existing IDS solutions using these features:

- ***detection principles*:**
  - anomaly detection:
    - machine learning;
    - power consumption.
  - signature-based:
    - automatically-defined;
    - manually.
- architecture:
  - distributed;
  - local.
- reaction:
  - active;
  - passive.
- collected data:
  - system calls;

– CPU, RAM;
– keystrokes;
– SMS, MMS.
• OS:
– Symbian;
– Android;
– Windows Mobile;
– Apple iOS.

First of all, we combine all mobile IDSes basis on detection principles used to find anomalies: anomaly detection (which includes machine learning and power consumption), signature-based (automatically or manually defined) and runtime policy enforcement. Then, we consider both local and distributed architectures. Next, we distinguish tools that perform any kind of reaction from which only obser the anomalies. We next observe IDSes by considering what kind of data are used as input and used by the OS. By considering all features, all the solutions discussed are presented in chronological order.

Detection Principles: We partition existing IDSes using the following principles

• anomaly detection;
• signature-based;
• run-time policy enforcement.

2. Detection based pproaches:

IDSes provide a first line of defense by effectively recognize malicious activities. Furthermore, there are some main types of detection:

(1) *Anomaly Detection*: An anomaly detection system compares the normal behavior of the Smartphone with the real behavior. The best solutions included in this section is either monitor various activities on the mobile, e.g. WiFi services, SMS services, Bluetooth connections, or analyses the power consumption model of the phone to discover anomalies.

(2) *Signature-Based:* In this mechanisms that find anomaly on Smartphone using signatures. The signature-based approach checks if every signature derived from an application matches any signature in a malware database. The database of malware signature can be automatically or manually outlined.

(3) *Measurements:* A collection of measurements includes several performance indicators of a Smartphone, like CPU activity, file I/O activity, memory consumption and network I/O activity. Therefore, we can extract activity profiles and use them for comparison with normal behaviors in order to discover anomalies. Some of these features such that RAM free, user inactivity time, count of process, send SMS which are used for anomaly detection.

(4) *Keystrokes:* Some solutions exploit keystroke logging (key logging) techniques to discover anomalies. These techniques track the keys affected on a keyboard to watch the actions of the user. Typically, the logging is provided in a covert manner in order that user is unaware of the observance. This is a standard technique of behavior-based anomaly detection.

VI. CONCLUSIONS

In this work, first of all we have mentioned the introduction of all mobile malware, by summarizing its classification, along with some notable examples. We have also classified known attacks against Smartphone's and focusing on how the attack is done by malware. We identify some symptoms of malware and give some suggestion of security. Finally, we have reviewed current security solutions for Smartphone's focusing on existing mechanisms based upon intrusion detection and trusted mobile platforms. Many Smartphone's focusing on previous mechanisms based upon intrusion detection.

References

[1] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?" Computer, vol. 41, pp. 12–14, May 2008.

[2] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra IEEE Communication Survey and Tutorial, "A Survey on Security for Mobile Devices" by VOL. 15, NO. 1, FIRST QUARTER 2013.

[3] M.Chandramohan and Hee Beng Kuan Tan, "Detection of Mobile Malware in Wide", Sep2012.

[4] M. Hypponen, "Mobile Security Review September 2010,"F-Secure Labs, HelsinkiFinland, Tech. Rep. September 2010.

[5] P. Traynor, M. Lin, M. Ongtang, V. Rao, T.Jaeger, P. McDaniel, and T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp.223–234.

[6] Q. Yan, Y. Li, T. Li, and R. Deng, "Insights into Malware: Detection and Prevention on Mobile Phones," in Security Technology, D. ´Slzak, T.-h. Kim, W.-C. Fang, and K. P. Arnett, Eds. Springer Berlin Heidelberg, 2009, vol. 58, ch.30, pp. 242–249.

[7] S. Coorporation, "Symantec Internet Security Threat Report Volume XVI," Whitepaper, vol.16, Apr 2011.

[8] Yong Wang, Kevin Streff, and Sonell Raman, IEEE Journal, "Smartphone Security Challenge", December 2012.

[9] "Bluetooth-Worm:SymbOS/Cabir," Jun 2004. [Online]. Available: http://www.f-secure.com/v- descs/ cabir.shtml

[10] IMS Research, "Global Smartphone's Sales Will Top 420 Million Devices in 2011, Taking 28Percent of all Handsets, According to IMS Research," July 2011. [Online]. Available: http://imsresearch.com/ press-release/Global Smartphone's Sales Will Top 420 Million Devices in 2011 Taking 28 Percent of all Handsets According to IMS Research.

[11] http://www.gartner.com/newsroom/id/2665715

[12] http://www.clove.co.uk/viewtechnicalinformation.aspx?content=3B2BD491-6465-4C70-ABDB-5A12A06C3D8D

[13] http://www.webopedia.com/TERM/B/botnet.htm l

[14] Zameshkumar J. Balhare "A Study on Security for Mobile Devices" , International Journal of Research in Advent Technology, Vol.2, No.4, April 2014 E-ISSN: 2321-9637 .

[15] http://www.pcworld.com/article/243782/five_tips_to_avoid_malware_in_mobile_apps.html

[16] Wilkinson, Glenn (25 September 2012) Snoopy: A distributed tracking and profiling frameworkSensepost, Retrieved 29 March 2014

[17] Jøsang, Audun; Miralabé, Laurent; Dallot, Léonard (2015). It's not a bug, it's a feature: 25 years of mobile network insecurity (PDF). European Conference on Cyber Warfare and Security (ECCWS 2015).

[18] https://en.wikipedia.org/wiki/Mobile_security#CITEREFJ.C3.B8sangMiralab.C3.A9Dallot2015

[19] Kasmi C, Lopes Esteves J (13 August 2015)."IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones".IEEE Transactions on Electromagnetic Compatibility

[20] https://en.wikipedia.org/wiki/Mobile_security#cite_note-FOOTNOTEJ.C3.B8sangMiralab.C3.A9Dallot2015-15