IJCSMS (International Journal of Computer Science & Management Studies) Vol. 15, Issue 04
Publishing Month: April 2015
An Indexed and Referred Journal with ISSN (Online): 2231 –5268
www.ijcsms.com

Today's Security Threats on Android Operating System

Marin Aranitasi[1], Gent Daci[2] and Igli Tafa[3]

[1]Center for R&D on IT, Polytechnic University of Tirana
Tirana, Albania
maranitasi@fti.edu.al

[2]Department of Computer Engineering, Polytechnic University of Tirana
Tirana, Albania
ggdaci@fti.edu.al

[3]Department of Computer Engineering, Polytechnic University of Tirana
Tirana, Albania
itafaj@gmail.com

Abstract

In the last years the use of intelligent mobile devices (also called smartphones) has increased dramatically. Everyone can have a smart phone and use it for its needs. Because the firms that produce the mobile devices are more concern to make them as much user friendly as they can, every mobile client think that can use such devices easily. The increased usage of smatphones can bring these devices and their users into the attention of persons with not good intentions. The number of malware writers has increased exponentially. This paper reviews the latest techniques of attacks on mobile operating systems. We categorize and analyze each of them using different resources. We show also the differences between normal attacks and mobile attacks by evidencing the specifics of mobile devices.

Keywords: *Mobile, Attacks, Smartphones, Review.*

1. Introduction

Mobile technology is fast on the rise with current Smartphone's boasting very powerful processing components and high capacity storages, some can go as far as being classed as mini computers, capable of web browsing, shopping, social networking, business, banking, and much more. This growing popularity in mobile technology has giving malware developers a new playground to exploit. A Smartphone is defined as a mobile phone that allows the user to download and run third-party applications from the Internet. Contrasted with feature phones, which provide enhanced functionality fixed by the device manufacturer or service provider, smartphones enable the user to decide how to extend a phone's functionally based on available applications. An appication store (or app marketplace) is a type of digital distribution platform for mobile apps. In the recent years the heterogeneity of mobile operating systems has increased. We have Apple's IOS, Linux-based Android OS, Windows Phone and BlackBerry OS. Table 1 provide an overview of market share for mobile operating systems for the third quarters from 2011 to 2014. As we can see clearly Android OS is the absolute lied. When we talk about mobile handsets according to [2] the mobile handset market is highly competitive with market leader Samsung holding 23% of the global handset market volume in Q3. This compares to 12% of Nokia/Microsoft and 9% for Apple. Chinese brands Xiaomi, TCL-Alcatel and Huawei as well as LG rounded out the top 7 brands with approximately 4% market share respectively.

Table 1 Market share of mobile operating system for third quarter of 2011 – 2014 [1]

Period	Android	IOS	Win. Phone	Blackberry
Q3 2014	84.4%	11.7%	2.9%	0.5%
Q3 2013	81.2%	12.8%	3.6%	1.7%
Q3 2012	74.9%	14.4%	2.0%	4.1%
Q3 2011	57.4%	13.8%	1.2%	9.6%

With this huge penetration of smartphones in our everyday live many researchers are expecting more security incidents with increased processing power and memory, increased data transmission capabilities of the mobile phone networks, and with open and third-party extensible operating systems, phones become an interesting target for attackers. This is confirmed even by Symantec

Corporation in their Threat Report [3]. The key findings of this report are as follows:

- 91% increase in targeted attacks campaigns in 2013
- 62% increase in the number of breaches in 2013
- Over 552M identities were exposed via breaches in 2013
- 23 zero-day vulnerabilities discovered
- 38% of mobile users have experienced mobile cybercrime in past 12 months
- Spam volume dropped to 66% of all email traffic
- 1 in 392 emails contain a phishing attacks
- 1 in 8 legitimate websites have a critical vulnerability

So nearly 40% of mobile users have experienced a cybercrime in the last year. But in the same trend there has been an increase in attention to security from security researchers even if Bontchev [4] says that today operating systems are sufficient secure. According to McAfee Labs [5] in just one year, the total number of mobile malware samples has grown by 167%. Figure 1 and 2 shows how fast is the "malware world" grouing up.

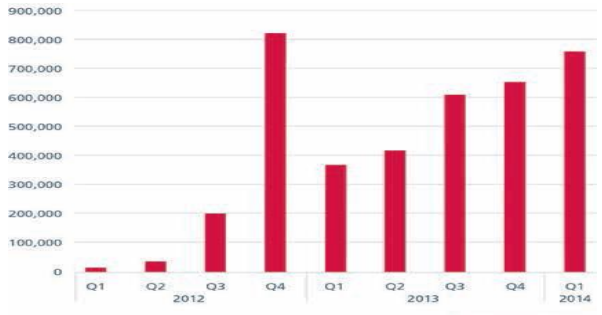

Fig. 1 New Mobile Malware

Fig. 2 Total Mobile Malware

In this paper we review the area of smartphone security and especially the threats that could harm mobile devices. Many articles about this topic are published [6] – [11]. The paper is organized as follows. Section 2 presents an overview of the mobile threats. This section is divided in 2 subsections. In the first subsection we give some examples of mobile malware and in the second subsection we present the history of the evolution of mobile threats. Section 3 shows related works that have been done in this area. Section 4 discusses the specifics of mobile security and section 5 analyzes the different kind of attacks on the mobile devices.

2. Mobile Threats

Malware refers to software programs designed to damage or do other unwanted actions on a computer system. [14] Malware is often distributed as a spam within a malicious attachment or a link in an infected websites. Malware can be grouped in the following main categories, according to its features[15]:

- Virus;
- Worm;
- Trojan;
- Rootkits;
- Botnet.

A *virus* is a piece of code that can replicate itself. Different replica of a virus can infect other programs, boot sector, or files by inserting or attaching itself to them.
A *worm* is a program that makes copies of itself, typically from one device to another one, using different transport mechanisms through an existing network without any user intervention. Usually, a worm does not attach to existing programs of the infected host but it may damage and compromise the security of the device or consume network bandwidth. Malware can also come packaged as a *Trojan*, a software that appears to provide some functionalities but, instead, contains a malicious program.
Rootkits achieve their malicious goal by infecting the OS: usually, they hide malicious user-space processes and files or install Trojans, disable firewalls and anti-virus. Rootkits can operate stealthily since they directly apply changes to the OS and, hence, can retain longer control over the infected devices.
Finally, a *botnet* is a set of devices that are infected by a virus that gives an attacker the ability to remotely control them. Botnets represent a serious security threat on the Internet and most of them are developed for organized crime doing attacks to gain money. Example of such attacks are sending spam, Denial-of-Service (DoS) or collecting information that can be exploited for illegal

purposes Mobile malware can spread through several and distinct vectors, such as an SMS containing a link to a site where a user can download the malicious code, an MMS with infected attachments, or infected programs received via Bluetooth. The main goals of malware targeted at smartphones include theft of personal data stored in the phone or the user's credit.

2.1 Malware Examples

Kaspersky Lab [16] shows a Trojan for Android smartphones named TrojanSMS.AndroidOS.FakePlayer.b, which appears as a media player and requires the user to install it. This fake application is downloaded from an infected webpage in order to view adult videos. During the installation the application asks the user permissions to send SMS messages. Once the installation has finished, if the user launches the fake application, the Trojan begins sending SMS messages to a premium rate number without the user's knowledge. These messages result in costly sums being transferred from the user's account to that of the cybercriminals.

Damopoulos et al. [17] created an airborne and stealth malware called as iSAM [18] to wirelessly infect and self-propagate to iPhone devices. The goal of the malware is to expose the possible vulnerabilities of modern mobile devices and OS. The iSAM malware besides supporting six malware mechanisms illustrated below connects to an iSAM bot master server and updates its programming logic or obeys commands for a synchronized attack. The iSAM architecture has following malware techniques:

a) *Propagation*: Wirelessly propagates to other iPhone devices
b) *Botnet Update:* To update and control the new version of the malware
c) *Data Collection*: Collects stealthily confidential information
d) *Leak*: Sends stealthily a large number of malicious SMS messages
e) *Availability*: Denial of Application Services in the iPhone
f) *Availability*: Denial of Network Services of the iPhone

[19] develops a kernel-level Android rootkit in the form of a loadable kernel module that can open a shell for the attacker, using a reverse TCP connection over 3G/Wi-Fi, upon the reception of an incoming call from a trigger number. This results in full root access on the Android device. In this way, an attacker can read all SMS messages on the device, incur the owner with long-distance costs or even potentially pinpoint the mobile device's exact GPS location.

[20] analyzes three sample rootkits. A smartphone rootkit can access several distinctive interfaces and information that are unique to smartphones, such as GPS, battery, voice and messaging, which provide rootkit writers with new attack vectors to compromise either the privacy or the security of end users. The first proposed sample rootkit allows a remote attacker to stealthily listen into (or record) confidential GSM conversation using the user's infected smartphone.

The second attack aims at the victim's location privacy by requiring the infected smartphone to send a text message to the remote attacker including the user's current GPS location. The final sample attack exploits powerintensive smartphone services, such as those offered by GPS and Bluetooth, to exhaust the battery on the smartphone.

2.2 Malware History

The first smartphone virus was identified in 2004. It wa called CABIR (or Caribe) [21]. Its most notable outbreak was at the 2005 World Championships in Athletics [22]. More interestingly, Cabir did not exploit any vulnerabilities. It operated entirely within the security parameters of both its infected host (Symbian OS) and Bluetooth. Instead, it leveraged flaws in the user interface. While a victim is in range, Cabir continually sends file transfer requests. When the user chooses "no," another request promptly appears, frustrating the user who subsequently answers "yes" repeatedly in an effort to use the phone [23].

Cabir was followed by a series of viruses and Trojans targeting the Symbian Series 60 platform, each increasing in complexity and features. Lasco [24] additionally infects all available software package (SIS) files residing on the phone on the assumption that the user might share them. Commwarrior [25] added MMS propagation in addition to Bluetooth. Skulls [26] Trojan provided one of the first destructive payloads. When installed, Skulls writes non-functioning versions of all applications to the c: drive, overriding identically named files in the firmware ROM z: drive. All applications are rendered useless and their icons are replaced with a skull and crossbones. Other Trojans, e.g., Drever [27], fight back by disabling Antivirus software. The Cardblock [28] Trojan embeds itself within a pirated copy of InstantSis (a utility to extract SIS software packages from a phone). Cardblock sets a random password on the phone's removable memory card, making the user's data inaccessible. While malware for other early smartphone operating systems such as Windows Mobile also appeared, smartphone malware little new malware was discovered after 2006 until recently [29].

Symantenc[30] in january 2012, has identified Android.Counterclank - a Trojan horse for Android devices that steals user information. This Trojan can be found in many applications in the official Android market. The download figures of all the malicious applications suggest that Android.Counterclank has the highest distribution of any malware identified so far this year. *Zeus In The Mobile* (Zitmo) [31] is an example of malware that can attack Two Factor Authentication system. Zitmo is a heterogeneous Trojan that infects Symbian, BlackBerry, Windows Mobile, and Android devices. Milligan [32] analyzed the business risk, threat and countermeasures in using mobile phones. Following are some of the risks illustrated in the paper:

- Intentional or unintentional data leakage.
- Data theft
- Business and financial malware attacks
- Network spoofing attacks
- Network congestion by spamming

3. Related work

This section provides an overview of some important surveys related to mobile threats. Peikari presents an overview of Windows Mobile and Symbian OS malware [33]. Shevchenko in his work [34] shows the evolution of mobile threats. Eren and Detken lists known malware samples, surveys the weaknesses of mobile operating systems, and describes much of the mobile and the mobile device security knowledge [35]. Tyssy and Helenius list infection routes and some examples of malware, but their focus is on countermeasures and media perception of mobile malware [36]. Bontchev talks about mobile malware classification problems and focuses on Symbian OS malware[37]. A survey of mobile malware is presented by Hypponen [10]. McAfee published a study in 2014 as a result of surveying mobile network operators [38]. McAfee finds that privacy-invading apps dominate the landscape, some containing malware, and many leveraging ad libraries. As they analyzed the behavior and permissions of thousands of Android apps, they found that 82% of apps track you, and 80% of apps collect location information. Another work on this topic is by Oberheide and Jahanian [13]. Felt [39] analyzed 46 pieces of iOS, Android, and Symbian malware that spread in the wild from 2009 to 2011. La Polla [15] surveys the state of the art on threats, vulnerabilities and security solutions over the period 2004-2011, by focusing on high-level attacks. This paper carries further research and illustrates latest malwares, detection and defense techniques by referring several papers, blog posts, vendor specifications and tech talks.

4. Mobile Security Features

Even if normal PCs and mobile devices both have similar hardware and software running inside there are some specific aspects that are unique to mobile Becher[40] explained the specific characteristics of mobile security. Figure 3 shows the specifics of mobile security.

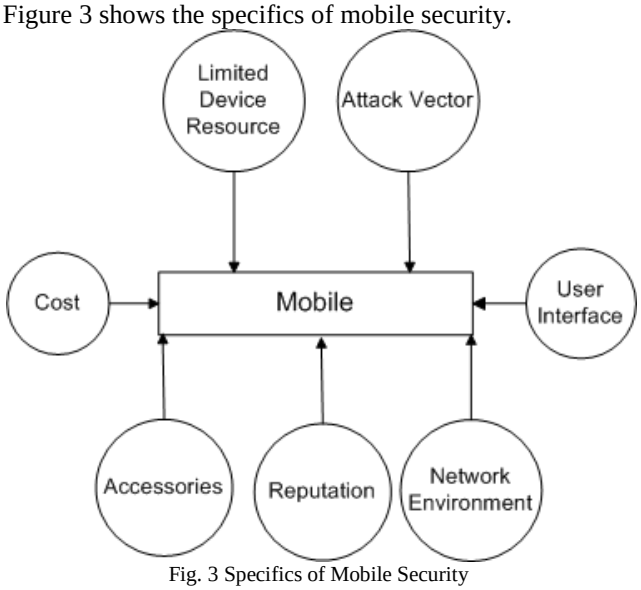

Fig. 3 Specifics of Mobile Security

The differences between Mobile and computer security consist of :

a) *Creation of Costs:* One of the motivations for attackers is to create costs for the user and profit from this situation. Attackers use mobile network operator's services like calls, messages, in payment systems like being trustworthy channels as part of the authorization process and incur costs for the user. Jamaluddin[41] made a comparison of the effects of a malware in computers and in a mobile device. In PC world Trojan horses impact the speed and performance of the network world, however in mobile world Trojan horses could inflict heavy financial penalty on the consumer. They developed a Trojan application that sits inside an application sending SMS or MMS messages, at a cost to the user.

b) *Limited Device Resources.* This is the most obvious difference between computer and mobile devices. Even if in the past few years, the computational power of smartphones has

increased, when compared with computers, they lose the competition. The main factors that limit the performance of a smarthphone are the CPU and the RAM. A unique factor of limitation for smartphones is the battery. Software applications that run in a computer that need high computational power may not run in a mobile due to the above constraints. Malware knows this situation and can attack the mobile device by consuming most of the resource and thereby causing denial of service. These limitations can make the defense from malware more difficult..

c) *Attack methodology:* Unlike traditional attack *methodology* related to Desktop PC, mobile devices have some special ways which can use SMS, MMS, Bluetooth and traditional IP-based applications.

d) *User interface*: Felt [42] illustrate that limitations in mobile user interface makes it easy for attacker to conduct phishing attack than in desktop browsers. Mobile devices are also different from the desktop PCs in size. Hence, the security mechanisms applied for PCs like visual indicators in browsers, URL bars, may not be directly applicable to mobile device. Hence, the may be a need to redesign for smaller screens to suit mobile devices..

e) *Network Environment*: we are talking about the environment between the mobile device and mobile network operator (MNO). The Network Environment plays a major role in smartphones. This consist of three aspects Strong Connection, Firmware updates process and remote device management. This strong influence of MNO over the device brings a new dimension of attack at both the ends. Firmware keeps updating. Due to frequent releases firmware updates are not done locally anymore. It requires MNO to update mobile device with latest firmware. Also the MNO or the corporate IT department can perform remote management. The user notices the new features changes as updates for example when MMS or WAP settings are pushed to the device.

f) *Reputation*: In case of mobile devices, the reputation of MNO is very fragile. When a mobile phone is infected by malware, it can be used by the that malware to do bad things. However, mobile network operator will charge for every everything regardless of whether the action is taken from the user or from the malicious software. However, from the user's perspective, it is the MNO who charges and not the malicious attacker. This can impact the reputation of the system.

g) *Other Capabilities*: Mobile phones are vulnerable to unauthorized intrusion on its sensors. In the case of PCs, sensors are add-on's whereas in mobile phones these are essential part of its structure. In the case of PC, attacks primarily focus on accessing private data and sniffing on user activities while interacting with the PC like key loggers. These attacks can be effectively controlled by proper file system access control. However, in the case of mobile phones, access control on sensors depends on the context, thus making it challenging to defend on privacy attacks. Schlegel [43] illustrated a malware that could capture the voice calls and record conversation in built-in microphones

5. Attacks on Mobile Operating Systems

In this section we are going to discuss several kinds of attacks on smartphones.

5.1 Attack vector Classes

According to [44] mobile device threats are classified as follows:

- ***Hardware attacks*** are related to physical attacks on the device. Even though they are suited to attack the mobile device for example to steal personal data using forensic analysis, they cannot be used easily by attackers , because they need to physical access to the mobile device. Removing SIM lock of the iPhone and man in the middle attack are some of the examples for hardware centric attack
- ***Device-independent attacks*** are independent of the device such as on infrastructure. Global System for Mobile Communications (GSM) have lot vulnerabilities like immature asymmetric crypto system, no network authentication etc. Another example is eavesdropping on the wireless connection or leaking mirrored personal data on back end systems both steal user's personal data.
- **Software attacks.** These attacks are focused on the software running on the mobile devices. Some of the software centric attacks using:
    - SMS communication channels
    - MMS communication channels
    - Attacks via mobile web browsers

- Rootkit attacks

- **User layer attacks** are related to trick the user and to override the normal security. Many of today's mobile threats are not focused on technical vulnerability, but how to trick the user into overriding technical security mechanisms [10]. This is an important class of vulnerabilities, even if not of technical nature.

5.2 Methodologies of the Attacks

Another way to classify the mobile attacks is given in La Polla's work [15]. According to her work we have the following classes:

- wireless;
- break-in;
- infrastructure-based;
- worm-based;
- botnet;
- user-based

Now we are going to detail these possible methodologies and possibly give an example for each of them.

1. **Wireless Attacks.** There are different kinds of wireless attacks against mobile devices. One of the most used attack is eavesdropping on wireless transmissions to extract user confidential information, such as usernames and passwords. Wireless attacks can also abuse the unique hardware identification (e.g., wireless MAC address) for identifying the owner of the device. Bluetooth is the preferred medium to speed up the propagation of the malware. [45] discusses security problems in wireless environments. A review of Bluetooth attacks affecting mobile devices can be found in [46]. Other studies about this topic are proposed in [47, 48, 49].
2. ***Break-in Attacks:*** In this kind of attacks, the attacker gets control of the mobile device by detecting programming errors for example to causing buffer overflows, or format string vulnerabilities. Typically, these attacks are used as a first step for performing further attacks, such as overbilling attacks or data/identity theft. Some studies for preventing this class of attacks are proposed in [50, 51].
3. ***Infrastructure-based Attacks:*** [52] discusses the social and the economic impact of these kind of attacks. The basis for mobile device functionalities are placing/receiving calls, SMS and e-mail services according to the authors the impact can be very large if the right measures are not taken. [53] evaluates the security impact of the SMS interface on the availability of the cellular phone network. For example, if an attacker simultaneously sends messages through the several available portals into the SMS network, the result in load can saturate the control channels and, therefore, block voice and SMS communications. In this paper is demonstrated that an attacker that injects text messages from the Internet can deny voice service in a metropolitan area using hit-lists containing as few as 2,500 targets with little more than a cable modem.
4. ***Worm-Based Attacks :*** The main features that characterize attacks based upon worms are:
   - transmission channel;
   - spreading parameters;
   - user mobility models.
5. ***Botnets:*** Some years ago, mobile networks have been relatively isolated from the Internet, so there was no need for protecting them against attackers trying to create botnets. However, this situation has rapidly changed since mobile networks are now well integrated with the Internet. Hence, threats on the Internet will migrate over the mobile networks, including botnets, since mobile devices can be infected by malware so they can be turned into a botclient very easily [54].
6. ***User as an Attack Vector:*** User-based attacks contain everything that is not of technical nature. This is an important class of vulnerabilities and several studies have been performed to evaluate the security knowledge of the average user. In particular they focus on the security mechanisms implemented by the mobile devices and analyze if the normal user does not understand them. Quite often, if the user clearly understands how to use one specific mechanism, she might find it difficult to understand another, possibly new and updated, mechanism. Very often social engineering attacks trick a user to override technical security mechanisms. [44] They abuse of trust relationships, which might happen when a malware access the address book of the victim and send itself to the contacts that trust the infected user. In another scenario, a user cannot distinguish if a feature is a legitimate functionality or an imitated one, e.g. in case of a Bluetooth message with malicious content. A survey conducted by Sophos [55] asked users whether their smartphone was encrypted: 26% percent of users replied that their data was encrypted, 50% said they were not protected in

the event of theft or loss of the device, and 24% of users were not sure whether their smartphone was encrypted. These results show that further education on the security dangers of smartphones is required

6. Android OS Features

In this section we are going to show some of the characteristics of the Android Operating System.

6.1 Android Sensitive data

The Android operating system contains many security-sensitive pieces of data that identify the user's identification information and user specific settings [56]. The most sensitive pieces of data are described below:

- International Mobile Equipment Identity (IMEI)
- International Mobile Subscriber Identity (IMSI)
- Android ID
- Mobile Subscriber Integrated Services Digital Network Number (MSISDN, phone number)
- Contacts list
- Contents of external SD card (user _les, application data)

With the combination of the IMEI, IMSI, and Android ID, an Android mobile phone can be uniquely identified down to the physical device and the subscriber. The IMEI is a unique number that identifies the cell physical phone device. The number is used by the GSM, Global System for Mobile Communications, to identify valid phones in its cellular network. The IMSI is a unique number securely stored inside the phone's SIM (subscriber identification module). The number is sent from the phone to the network and identifies the user's mobile subscription and provider. The Android ID uniquely identifies an Android device with a 64 bit hex string that is randomly generated on the device's first boot and normally remains constant for the lifetime of the device. The phone number is stored securely as the MSISDN of the mobile and uniquely identifies the subscription of the phone inside the mobile network. The contacts list of the phone identifies all contacts stored by the user which may include, names, phone numbers, addresses, emails, etc. The contents of the SD card (external storage) may contain personal files of the user, including: photos, music files, and document files. The card may also contain application data that is stored by applications as a temporary location or settings location. The information contained in these is dependent on the application.

6.2 Android OS Permissions

In Android, access to sensitive resources is controlled by permissions. Each application bundle includes an XML manifest file that lists the permissions requested by the application. When an application is installed, the permissions in the applications manifest are shown to the user, who then decides whether to proceed with the installation (i.e., grant the permissions), or to cancel it. No additional permissions may be acquired when an application runs, and an application is killed if it tries to access a resource for which it does not have permission.
Below are some of the most important permissions of the Android operating system that define what an application has access to. Currently, Android's security model does not protect against misuses of these permissions. Once a permission is granted, it is up to the developer of the application to ensure that the data is being used in a safe manner [57]. Here we present some of the most used permissions by the android developers:

- Access Fine Location, Access Coarse Location
- Call Phone
- Read SMS, Send SMS
- Read Phone State
- Internet
- Read Contacts, Write Contacts
- Write External Storage

7. Malwares on Android OS

In this section we are going to analyze some android malwares that we have discovered from several articles and especially from the thread reports of the most used antiviruses. [58] collects a dataset of 1260 samples. By manually analyzing malware samples in this collection, we categorize existing ways Android malware use to install onto user phones and generalize them into three main social engineering-based techniques, i.e., *repackaging*, *update attack*, and *drive-by download*.

1) **Repackaging** is one of the most common techniques malware authors use to piggyback malicious payloads into popular applications (or simply apps). In essence, malware authors may locate and download popular apps, disassemble them, enclose malicious payloads, and then re-assemble and submit the new apps to official and/or alternative Android Markets. Users could be vulnerable by being enticed to download and install these infected apps. To quantify the use of repackaging technique among our collection, we take the following approach: if a sample shares

the same package name with an app in the official Android Market, we then download the official app (if free) and manually compare the difference, which typically contains the malicious payload added by malware authors. If the original app is not available, we choose to disassemble the malware sample and manually determine whether the malicious payload is a natural part of the main functionality of the host app. If not, it is considered as repackaged app. In total, among the 1260 malware samples, 1083 of them (or 86.0%) are repackaged. By further classifying them based on each individual family , we find that within the total 49 families in our collection, 25 of them infect users by these repackaged apps while 25 of them are standalone apps where most of them are designed to be spyware in the first place.

2) **Update Attack** The first technique typically piggybacks the entire malicious payloads into host apps, which could potentially expose their presence. The second technique makes it difficult for detection. Specifically, it may still repackage popular apps. But instead of enclosing the payload as a whole, it only includes an update component that will fetch or download the malicious payloads at runtime. As a result, a static scanning of host apps may fail to capture the malicious payloads. In our dataset, there are four malware families, i.e., BaseBridge, DroidKungFuUpdate, AnserverBot, and Plankton, that adopt this attack
3) **Drive-by Download** The third technique applies the traditional drive-by download attacks to mobile space. Though they are not directly exploiting mobile browser vulnerabilities, they are essentially enticing users to download "interesting" or "feature-rich" apps. In our collection, we have four such malware families, i.e., GGTracker, Jifake, Spitmo and ZitMo. The last two are designed to steal user's sensitive banking information.
4) **Others.** In this group are all the other malwares that do not fit with the first three groups. Here we categorize them into 4 subgroups.

a. The first group is considered spyware as claimed by themselves – they intend to be installed to victim's phones on purpose. That probably explains why attackers have no motivations or the need to lure victim for installation.
b. The second group includes those fake apps that masquerade as the legitimate apps but stealthily perform malicious actions, such as stealing users' credentials or sending background SMS messages.
c. The third group contains apps that also intentionally include malicious functionality (e.g., sending unauthorized SMS messages or subscribing to some value-added service automatically). But the difference from the second group is that they are not fake ones. Instead, they can provide the functionality they claimed. But unknown to users, they also include certain malicious functionality.
d. The last group includes those apps that rely on the root privilege to function well. However, without asking the user to grant the root privilege to these apps, they leverage known root exploits to escape from the built-in security sandbox. Though these apps may not clearly demonstrate malicious intents the fact of using root exploits without user permission seems cross the line.

8. Conclusions

In this paper we gave an overview of the current level of mobile attacks that can harm smartphone devices. As the years pass smartphone features increase, so do the number of mobile malware. In section 1 we demonstrate using the latest data such as those presented in Kaspersky Lab report or McAfee threat report 2014 that the level of mobile threats is increasing very fast and the need for immediate reaction is becoming an everyday issue. Differently from normal PC, the smartphones have to deal with many limitations such as the power and the processing unit, as me metioned in section 4, but they are closing the gap rapidly. In section 5 we presented the methodology that attackers use to penetrate smartphones. We analyzed and categorized each of them and gave an example of malwares that have been already discovered for some of the categories. We also analyze a dataset of 1260 malwares. Around one third (36.7%) of the collected malware samples leverage root-level exploits to fully compromise the Android security, posing the highest level of threats to users' security and privacy. More than 90% turn the compromised phones into a botnet controlled through network or short messages. Among the 49 malware families, 28 of them (with 571 or 45.3% samples) have the built-in support of sending out background short messages (to premium-rate numbers) or making phone calls without user awareness. 27 malware families (with 644 or 51.1% samples) are harvesting user's information, including user accounts and short messages stored on the phones.

We think that we are on the beginning of the era of mobile attacks and we think that security of the mobile operating

systems will be a very interesting area to discover in the years to come.

References

[1] International Data Corporation (IDS) http://www.idc.com/prodserv/smartphone-os-market-share.js
[2] HIS Technology "https://technology.ihs.com/522734/apples-record-iphone-results-prove-no-mobile-market-leaders-position-is-ever-secure"
[3] Symantec Corporation "Internet Security Threat Report 2014 volume 19". http://www.symantec.com/security_response/publications/threatreport.jsp
[4] V. Bontchev, "Virusability of Modern Mobile Environments" in Virus Bulletin Conference, Sep. 2007
[5] McAfee Lab Threats Report 2014 http://www.mcafee.com/in/resources/reports/rp-quarterly-threat-q3-2014.pdf
[6] N. Leavitt, "Malicious Code Moves to Mobile Devices", IEEE Computer, vol. 33, no. 12, 2000.
[7] S. N. Foley and R. Dumigan, "Are Handheld Viruses a Significant Threat?" Commun. ACM, vol. 44, no. 1, 2001.
[8] D. Dagon et al., "Mobile Phones as Computing Devices: The Viruses are Coming!" IEEE Pervasive Computing, vol. 3, no.4, 2004
[9] N. Leavitt, "Mobile Phones: The Next Frontier for Hackers?" IEEE Computer, vol. 38, no. 4, 2005.
[10] M. Hypponen, "State of Cell Phone Malware in 2007," http://www.usenix.org/events/sec07/tech/hypponen.pdf.
[11] J. Kleinberg, "The Wireless Epidemic," Nature, vol. 449, no. 20, Sep. 2007.
[12] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?" IEEE Computer, vol. 41, no. 5, 2008.
[13] J. Oberheide and F. Jahanian, "When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments," in Workshop on Mobile Computing Systems and Applications (HotMobile), February 2010.
[14] http://techterms.com/definitions/malware
[15] M. La Polla, F.Martinelli, D. Sgandurra "A Survey on Security on mobile devices" IEEE Communications Surveys &Tutorials 2012.
[16] Kasperksy Lab, "Popular Porn Sites Distribute a New Trojan Targeting Android Smartphones," 2010. [Online]. Available: http: //www.kaspersky.com/news?id=207576175
[17] Damopoulos, D., Kambourakis, G., and Gritzalis, S. 2011. iSAM: An iPhone Stealth Airborne Malware. In Future Challenges in Security and Privacy for Academia and Industry, J. Camenisch, S. Fischer-H•ubner, Y. Murayama, A Portmann, and C. Rieder, Eds. IFIP Advances in Information and Communication Technology vol. 354 Springer Boston, Chapter 2, 17-28
[18] iSAM: An iPhone Stealth Airborne Malware http://www.icsd.aegean.gr/postgraduates/ddamop/iSAM/iSAM.pdf
[19] C. Papathanasiou and N. J. Percoco, "This is not the droid you're looking for..." in *DEFCON 18*, July 2010.
[20] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L.Iftode "Rootkits on smart phones: attacks, implications and opportunities," in *Proceedings of the Eleventh* Workshop on Mobile Computing Systems & Applications, ser. HotMobile '10. New York, NY, USA: ACM, 2010, pp. 49–54
[21] F-Secure, "Bluetooth-Worm:SymbOS/Cabir," http://www.f-secure.com/v-descs/cabir.shtml".
[22] "TeliaSonera Finland and F-Secure united against mobile viruses: Cabir spreads at the World Championships," http://www.f-secure.com/en_EMEA/about-us/pressroom/news/2005/fs_news_20050811_1_eng.html.
[23] Hypp¨onen, M. (2007), "Mobile Malware," USENIX Security Symposium, invited Talk.
[24] F-Secure Corporation, "Virus Description: Lasco.A," http://www.f-secure. com/v-descs/lasco_a.shtml accessed February 2015
[25] "Virus Description: Commwarrior," http://www.f-secure.com/v-descs/commwarrior.shtml accessed February 2015
[26] "Virus Description: Skulls.A," http://www.f-secure.com/v-descs/skulls.shtml accessed February 2015.
[27] "Virus Description: Drever.A," http://www.f-secure.com/v-descs/drever_a.shtml accessed February 2015
[28] "Virus Description: Cardblock.A," http://www.f-secure.com/v-descs/cardblock_a.shtml accessed February 2009
[29] Schmidt, A.-D., H.-G. Schmidt, L. Batyuk, J. H. Clausen, S.A. Camtepe, and S. Albayrak (2009) " Smartphone Malware Evolution Revisited: Android Next Target?" in Proceedings of the 4th International Conference on Malicious and Unwanted Software (MALWARE).
[30] Android.Counterclank Found in Official Android Market

http://www.symantec.com/connect/fr/blogs/androidcounterclank, found-official-android-market, 2012

[31] Axelle Apvrille, Senior antivirus analyst and researcher, "Zitmo hits Android", July, 2011 @ http://blog.fortinet.com/zitmo-hits-android/

[32] Milligan, P. M. and Hutcheson, D. 2007. Business risks and security assessment for mobile devices. In MCBE'07: Proceedings of the 8th Conference on 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics. World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, 189-193

[33] C. Peikari, "PDA Attacks, Part 2: Airborne Viruses – Evolution of the Latest Threats," (IN) Secure Magazine, vol. 4, Oct. 2005.

[34] A. Shevchenko, "An Overview of Mobile Device Security" Sep. 2005, http://www.viruslist.com/en/analysis?pubid=170773606

[35] E. Eren and K.-O. Detken, Mobile Security. Hanser, 2006.

[36] S. T¨oyssy and M. Helenius, "About Malicious Software in Smartphones." Journal in Computer Virology, vol. 2, no. 2, 2006.

[37] V. Bontchev, "SymbOS Malware Classification Problems," in Virus Bulletin Conference, Aug. 2006

[38] McAfee Mobile Security Report 2014 http://www.mcafee.com/in/resources/reports/rp-mobile-security-consumer-trends.pdf

[39] Adrienne Porter Felt , Matthew Finifter , Erika Chin , Steve Hanna , David Wagner, "A survey of mobile malware in the wild", Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, October 17-17, 2011, Chicago, Illinois, USA

[40] Becher, M.; Freiling, F.C.; Hoffmann, J.; Holz, T.; Uellenbeck, S.; Wolf, C.; , "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Security and Privacy (SP), 2011 IEEE Symposium on , vol., no., pp.96-111, 22-25 May 2011

[41] Jazilah Jamaluddin, Nikoletta Zotou, Reuben Edwards. Member, IEEE, and Paul Coulton, Member, IEEE; "Mobile Phone Vulnerabilities: A New Generation of Malware" 10 January 2005

[42] A. P. Felt and D. Wagner. "Phishing on Mobile Devices" In W2SP Conference, 2011

[43] R. Schlegel et al., "Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones," in Network and Distributed System Security Symposium (NDSS), Feb. 2011.

[44] M. Becher, "Security of smartphones at the dawn of their ubiquitousness," Ph.D. dissertation, University of Mannheim, Oct. 2009

[45] A. Makhlouf and N. Boudriga, "Intrusion and anomaly detection in wireless networks," in Handbook of Researchon Wireless Security, Y. Zhan, J. Zheng, and M. Ma, Eds. Information Science Publishing, 2008.

[46] K. Haataja, "Security threats and countermeasures in Bluetoothenabled systems," Ph.D. dissertation, Department of Computer Science, University of Kuopio, 2009

[47] Y. L. Ho and S.-H. Heng, "Mobile and ubiquitous malware," in MoMM '09: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia. NewYork,NY, USA: ACM, 2009, pp. 559–563

[48] A. Bose, X. Hu, K. G. Shin, and T. Park, "Behavioral detection of malware on mobile handsets," in MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services. New York, NY, USA: ACM, 2008, pp. 225–238.

[49] A.-D. Schmidt, F. Peters, F. Lamour, C. Scheel, S. A. C¸ amtepe, and S. Albayrak, "Monitoring smartphones for anomaly detection," Mob. Netw. Appl., vol. 14, no. 1, pp. 92–106, 2009.

[50] L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu, "pBMDS: a behavior based malware detection system for cellphone devices," in Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24, 2010. ACM, 2010, pp. 37–48.

[51] M. Becher and F. C. Freiling, "Towards Dynamic Malware Analysis to Increase Mobile Device Security," in Sicherheit 2008: Sicherheit, Schutz und Zuverl¨assigkeit. Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft f¨ur Informatik e.V. (GI), 2.- 4. April 2008 im Saarbr¨ucker Schloss, ser. LNI, vol. 128. GI, 2008, pp. 423–433.

[52] 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.

[53] W. Enck, P. Traynor, P. McDaniel, and T. La Porta, "Exploiting open functionality in SMS-capable cellular networks," in Proceedings of the 12th ACM conference on Computer and communications security, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 393–404.

[54] A. R. Flø and A. Jøsang, "Consequences of botnets spreading to mobile devices," in 14th Nordic Conference on Secure IT Systems, 2009, pp. 37–43.

[55] Sophos, "Security Threat Report," 2010. [Online]. Available: http://www.sophos.com/sophos/docs/eng/ papers/ sophos-security-threat-report-jan-2010 wpna.pdf
[56] Gomez, Neamitiu "A Characterization of Malicious Android Applications" University of California, Riverside june 2011
[57] Google Inc. Android Developers. http://developer.android.com/reference/android/ Manifest.permission.html
[58] Yajin Zhou Xuxian Jiang "Dissecting Android Malware: Characterization and Evolution" North Carolina 2012