A Systematic Mapping on Security Threats in Mobile Devices

Anselmo Lacerda
Center of Informatics
Federal University of Pernambuco - UFPE
Recife, Brazil
alg@cin.ufpe.br
anselmo.gomes@upe.br

Ruy de Queiroz
Center of Informatics
Federal University of Pernambuco - UFPE
Recife, Brazil
ruy@cin.ufpe.br

Márcio Barbosa
Center of Informatics
Federal University of Pernambuco - UFPE
Recife, Brazil
mbof@cin.ufpe.br

Abstract—**The increase in the use of mobile devices and the large amount of sensitive information that they store make them valuable targets for cybercriminals. In this work, we use the systematic mapping methodology to identify what are the main security incidents targeting mobile devices and what are their main causes. Finally, this research aims to propose some guidelines to avoid or minimize the extent of the damages provoked by these incidents.**

Keywords—mobile malware behaviour; privacy; digital identity theft; systematic mapping;

I. Introduction

We are experiencing a great expansion in the mobile device usage nowadays. According to an estimate released by [1], 2.2 billion of these devices were sold worldwide in 2014. This huge demand generates a growing consumption of mobile apps. In addition, there are several categories of such apps, like social networks, games and banking applications [2].

The diversity of apps brings a great concern about security. This comes from the fact that the mobile devices are handling more sensitive information, making them valuable targets for cybercrimals. Not only personal data, and banking passwords are important, but other information such as localization and navigation history can also be targets of attackers.

There are many ways of carrying out an attack against a mobile device. For instance, there exist reported cases of sophisticated man-in-the-middle attacks, as in [3], commercialization of botnets [4] and distribution of malicious softwares to exploit flaws in the operating system and in other apps running in the target device.

In order to protect mobile devices from attacks and security flaws, their operating systems usually adopt several techniques such as sandboxing, and permission-based access control. Additionally, virtual stores, that make apps available online, adopt measures to constantly classify and update their products, as well to remove identified malicious software. Nevertheless, most part of the security of the device and its data depends upon the user behaviour. For instance, the jailbreaking operation allows for the user to have more control over the device, breaking several operating system native protections and, as a side effect, making malicious apps even more disastrous. Other examples of bad behaviours related to the device security are the granting of too many permissions to apps, the use of a default root password, and the non-utilization of antivirus. According to the authors of [4] in 2017, 75% of mobile device data thefts will be due to the bad configuration of apps. Additionally, according to the authors of [3], 20% of mobile devices victims of attacks targeting banking apps did not use any antivirus protection.

Another important component to the mobile device security is the quality in the development of the well intentioned apps. That is, the developers must be always aware of the fact that their applications will be executed in an unknown environment, will share resources with other applications and will be constantly connected to the Internet. Flaws in the design or in the implementation of sensitive parts of the application, like the data transmission and storage, constitute a threat to the user privacy and anonymity [5, 6].

The first goal of this work is to present the main categories of mobile security incidents, gathering data from technical reports and other research papers. With this information, we will point out some causes for these security threats. Finally, we will present a list of guidelines, in several levels, aiming to minimize the malware infections and their effects.

II. Related Work

The scientific research on the field of mobile security has increased because of the rise in the number of known mobile threats. Several works have tried to summarize and classify these threats, while others have proposed techniques for detecting them and preventing their spread. In this section we will reference some of these works that are related to ours, either because of their goals or their methodology.

We can find in [7] an attempt to classify the mobile threats into categories, namely malware, grayware and spyware. The main contribution of this work, however, is the review of terms related to malware detection algorithms. The authors divided these algorithms according to their use of static analysis, dynamic analysis and permission-based analysis while identifying malicious behaviours. After a careful definition of these categories, the authors try to design general guidelines for developing new malware detection algorithms. These guidelines, however, are too broad and it is not clear how they were designed.

The work in [9] divides the fight against malwares into analysis, classification, detection, and containment. The detection techniques, in turn, are divided according to whether they are based on signature matching, specification of rules, behaviour monitoring, data mining and cloud services. The last one is defined with the example of Google Play. The classifications of malware detection algorithms given in [7] and [9] are different but, in the end, they specify the same set of techniques, yet in different granularities.

Still on the matter of fighting against mobile threats, the work in [8] proposes an algorithm based on anomaly-detection for preventing the spread of malwares. The objective of the work is to use dynamic analysis to detect and block actions not generated by the user. With the idea similar to a firewall, the authors intend to block the most common channels of malware dissemination. It is important to notice that the assumptions made to select these channels might be outdated. For instance, the access to the web is considered less dangerous than other ways of malware dissemination (e.g, the use of infrared), and as consequence, is not covered in the work.

The work in [10] proposed a general mobile malware model using a hybrid approach, i.e, collecting data from both dynamic and static analysis, to capture key features that can identify malicious behaviour. With a similar goal, the work in [11] designed a self-learning mobile malware detection. The detection was based on the behaviour extracted by a Bayesian classifier from the network data generated by the mobile device. To train this classifier, it was used network data coming from both known malicious activities and legit applications.

The behaviour of malwares is also studied in [12]. This work created a tool called DroidGraph to collect information of Android applications from their APK file. The DroidGraph constructs hierarchical behaviour graphs to grasp the semantics of an application, based on its Android API calls. DroidGraph is the result of a set of systematic procedures proposed in [13] to analyze typical malware behaviours on the popular mobile operating system Android.

It is worth to mention that the dynamic analysis, used for example by the works [8, 10, 11], is a good way to get around the techniques employed by the malwares to evolve, like code obfuscation or junk code injection. These techniques trick strategies solely based on static data by changing the binary representation of the malware.

Some tools for detecting and analyzing mobile malwares are freely available online. One of them is Anubis [15], a service for analyzing APK files. Anubis gives an extensive report on the interactions the APK makes while executing, focusing on those who might represent security issues. Anubis accepts also the submission of Windows executables. Another online tool is VirusTotal [16]. It analyzes files and URLs using an extensive list of antivirus, facilitating the quick detection of viruses, worms, trojans, and other kinds of malware.

III. Research Questions

This work was based on the orientations in [17] for preparing research questions. They were designed according to the previous literature investigation and the points mentioned in the foregoing sections. They are the following:

- **Research Question 1 (RQ1):** What are the main security incidents in mobile devices?
- **Research Question 2 (RQ2):** What factors cause the security threats in mobile device?
- **Research Question 3 (RQ3):** What contributions classified as solution and categorized as method, technique or tool/architecture were the most recommended in the polls?

IV. Using Data Extraction and Mapping Process

A. Search Strategy

To define a search strategy for the detection of primary studies, it is necessary to determine the keywords to search for and where these searches will be carried out [17]. We defined as primary sources for searching the ACM Digital Library, specifically the ACM Transactions on Information and System Security (TISSEC), and IEEE Xplore. We also used technical reports from antivirus companies such BitDefender, Alcatel-Lucent's Motive Security Labs, Kaspersky Lab and Symantec.

We expected the data coming from technical reports to be more up-to-date and, therefore, more likely to cover the newer techniques employed by the cybercriminals. On the other hand, the academic sources were expected to contain a more systematic approach of the subject, providing us with a sound theoretical ground for conducting our research.

The search string was used for searching on different data sources, and was designed according to the approach in [17], which creates it by composing search terms using AND and OR operators. Our research string, used in the mapping study, was "*mobile malware behaviour*".

B. Study Protocol

The systematic mapping study was conducted using a pre-defined protocol that uses the research questions, the string search and the criteria for inclusion and exclusion of papers and technical reports.

C. Inclusion Criteria

First, we started this process considering the following inclusion criteria:

- Papers that have security threats in mobile devices as their main theme;
- Studies about malwares in mobile devices;
- Publication with details about security threats in mobile applications;
- Papers and technical reports that have some kind of proposal solution, with statistical data, tests, etc;

D. Exclusion Criteria

- Papers without a proposal of solution or publications containing only revision or approach;
- Data source not accessible online;
- Studies that did not report empirical findings or literature that was only available in the form of abstracts or PowerPoint presentations.

V. Analysis and Results

After the inclusion and exclusion steps are completed, the data is ready to be more deeply analyzed. This chapter describes the results obtained in the systematic mapping study of the publications collected and aims to answer the research questions previously determined.

A. Answer for Research Question 1 – RQ1

According to the data extracted using the mapping process, it was possible to answer the RQ1 by creating a list with the main security incidents reported in mobile devices.

a) ***Malwares****. These malicious softwares can have several behaviours, like making calls without the user notice; sending, recording and receiving SMS messages; reading contacts data; tracking by geolocalization, and many others. In some cases, the malware can obtain root access and, consequently, control completely the mobile device, including the management of sensitive information. Infecting mobile devices with malwares gives to the attackers the ability of retrieving information from its targets nearly in real time, contrasting to other types of devices which might not have the same online availability.*

b) ***Ransomwares****. This type of malware prevents the user from accessing some functionalities or files, requiring a payment in order to unblock the access to them [18]. Fake antivirus applications that block the device claiming an infection and demand the purchase of premium services can also be considered ransomwares. The number of ransomware infections in mobile devices is expected to grow mainly due to the lack of basic protection of the mobile devices, like antivirus and periodic backup, and the large amount of sensitive data that these devices store.*

c) ***Cryptoransomwares.*** *It refers to a class of ransomwares that encrypts targeted files with specific extensions and demands payment before providing the key to decrypt them [18].*

d) ***Phishing pages****. This type of threat, common to desktop users, is also developed for mobile devices. The pages can be hosted on standard websites, and simply designed in such a manner to lend themselves to mobile devices - smaller images, less text, and so on [19].*

e) ***Botnets****. A device that belongs to a botnet can provide several services, like anonymous proxy web browsing; restricted foreign content access and many illicit activities. This can consume large amounts of bandwidth and airtime, impacting in the user experience of the device [20]. Mobile devices are becoming more attractive to botnet masters because of the increasing in their computational power and their high availability.*

f) ***Spyware****. This traditional threat consists of software designed to spy on the phone's owner. It can track the phone's location and monitor ingoing and outgoing calls and text messages. These are functions that are unique to the mobile environment [20].*

g) ***Scareware****. This is a broad class of mobile threats that try to extort money from the user. They threaten the user with the encryption or removal of private data or even with denouncing crimes allegedly committed by the user [20].*

h) ***Identity theft****. It's the theft of information that can lead the thief to somehow assume the victim's identity. This includes the theft of email, banking, network or business credentials, for example [20]. The mobile devices are interesting targets for this kind of threat because of the large amount of private data stored there by the user, specially credentials, passwords, and emails. Additionally, this sensitive data might be accessed through insecure means, like public networks.*

i) ***Trojan****. This type of malware can offer a legit service to the user, or at least present itself as a legit application. Once installed, however, the trojan will silently perform other activities, like monitoring the device and stealing sensitive data. The trojans are common in mobile devices mainly because most of these devices lack basic protection, store sensitive data and are highly available.*

j) ***Grayware.*** *It is a general term used for applications that are undesirable or an noying, but that are not as harmful as viruses, for example. This class of applications includes, for instance, spywares, adwares, dialers and joke programs [20].*

k) ***Madware.*** *It is refers to apps that use aggressive advertisement libraries [22]. These libraries might leak sensitive information collected from the user, and might exhibit annoying behaviour, like changing browser bookmarks.*

l) ***Social engineering.*** *It is a broad term used to refer to many possibilities of manipulating someone to give up private information or to carry out any other action. For example, an* *attacker pretending to be from a legit company may induce the user to install a malicious app; to access a false page in the web or even to reveal information like the device's IMEI - a code that uniquely identify the device. Revealing informations that identifies the device can be as dangerous as a malware infection. They might be used to send specific advertisement and to track the user [23].*

The mobile devices are at a higher risk than other electronic devices because they are constantly connected to the Internet and a malware infection can open the possibilities for further infections.

In the following table, we present some information about malwares that infected a huge number of mobile devices worldwide. They gained great repercussion not only for their power of dissemination in global scale, but also because of the different strategies employed to infect their targets. They are present in several technical reports of security and antivirus companies, and their behaviour was useful for helping answering our research questions.

TABLE I. MOBILE MALWARE BEHAVIOUR

Malware	Mobile Malware Behaviour	
	Description	*Prevention/Solution*
Waller.A[1, 2]	Android/Waller.A was installed as an Adobe Flash update. This malware exploited the monetary transfer protocol used by Visa QIWI Wallet to steal money from the user.	The users are advised not to activate "developer mode" or the "install applications form third-party sources" options on their smartphones. In addition, users are advised to install antivirus software on their devices, and only download apps from trusted sources.
Obad [1]	It uses a mobile botnet to spread, sending messages containing malicious links to the user contact list. The botnets arise from a malware infection that allows for the attacker remote controlling the infected device.	The Android vulnerability that allows the Trojan to gain DeviceAdministrator rights has been patched by Google in Android 4.3.
Svpeng[3]	It displayed messages saying the phone was blocked and demanding several hundred dollars to unblock it. The malware checks a user's phone for a list of certain financial applications, probably for future usage, when it starts stealing login/password of online banking.	Install security software on all mobile devices. Avoid downloading apps from third parties. Never perform banking activities over public Wi-Fi networks. Install antivirus software.
BadLepricon[3]	It uses the power of the infected devices to mine Bitcoins. These devices overheated and had their battery drained.	Install security software on all mobile devices. Avoid downloading apps from third parties. Android devices do not allow installs from unknown sources.
Simplocker[3]	It encrypts users files and demanded a payment in order to decrypt them. It infected more than 20.000 unique users.	Install security software on all mobile devices. Avoid downloading apps from third parties. Android devices do not allow installs from unknown sources.
Flappy Bird's[2]	The Flappy Birds requests a larger number of permissions, including to read and send text messages.	Removed from the official store
Baloon Pop 2 [2]	The Balloon Pop 2 game is advertised as a program that can be used to back up WhatsApp conversations.	Removed from the official store
WireLurker[1]	The vulnerability that allows an infected Mac OS-X computer to install applications on any iPhone that connects to it via a USB connection.	Removed from the official store. Install security software on all mobile devices.
Android.Fake defender[1, 2]	A fake security software ran a scan, warned the user of non-existent threats that the software found on the device. Then, attempted to coerce the user into paying for the fake app in order to remove them.	Install antivirus software.
BadInst.A[2]	App abuses app store account authentication and authorization to automatically download, install, and launch other apps without user permission.	Blocked the apps. Install security software on all mobile devices.

[1] Ransomware [2] Spyware [3] Crypto-Ransomware

B. *Answer for Research Question 2 – RQ2*

The existence of independent stores, that have few if any control over the available apps, makes easier the spread of trojans. Even the Android official store does not apply a rigid policy to its content, allowing, for instance, apps signed by self-signed certificates. In addition to the ease of distribution, other important factor to the spread of trojans in Android is that the permissions granted by the users to the apps that they install. These permissions are part of a more complex native security system, and their goal is to limit the applications' behaviours, preventing them from having access to resources not expressly authorized by the user during the installation. One problem of the Android permission system is its granularity: either the user grants all the permissions required by an application or the installation can't proceed. This can stimulate the user to always accept all demands from the apps. In a similar way, Android doesn't offer any mechanism to revoke permissions, even temporarily. Another interesting event in the spread of trojans is related with downloading or executing applications from untrusted sources without cares.

a) ***Protocol Vulnerabilities***. Some application protocols have issues that contribute to the rise of other vulnerabilities. The use of SMS messages, which do not provide adequate level of authentication, is an example of such an issue.

Malwares can also use a version resultant of reverse engineering to take actions not intended by the user.

b) ***Third-party stores***. There are many non-official stores from which is possible to download apps, specially for Android devices. This is a dangerous practice, since these stores might not have a good control of the provided apps or might even distribute malwares intentionally. The existence of such unofficial stores can also cause the appearance of *clones* of legit applications carrying malwares in disguise.

c) ***Lack of control in official stores***. Even though the official stores are more concerned with the security of the published apps, some adopted policies make easier malware distribution. Allowing self-signed certificates to sign apps, for example, makes impossible to trace the developer of an app.

d) ***Affiliate Programs***. Affiliate programs are a very common way of delivering malware. Typically these programs are created by cybercriminals which then invite Internet users to be accomplices. Each user creates a landing page to distribute a slightly different version of the malware, and the objective is to maximize the number of access to this page. To do that, the criminals might resort to several techniques, including attracting users with pornography and free games, for instance. About 38% of the access to these pages result in the download of the malicious apps, and 5% of the downloads are installed. [18]

e) ***The spread of the usage of mobile devices***. The number of mobile devices' users grew in 2013, as well as their lack of awareness of basic security measures. The called *later adopters* tend to be less digitally literate, less aware of security risks, and, therefore, more susceptible to security threats [19].

f) ***Email and SMS***. One popular method for spreading malicious apps is sending emails to be read in mobile devices. These emails provide a link and ask users to download and install an application. If installed, informations like contact details are gathered from the device and the message is spammed out to other users in the recipient's address book. The same can be carried out through SMS messages [18].

g) ***Legit application flaws***. As in other environments, vulnerabilities in legit mobile applications and in the underlying operating system may be exploited and turn a device completely vulnerable. A flaw in the certificate verification in Android, for instance, allowed applications to carry out privilege escalation [20].

C. Answer for Research Question 3 - RQ3

The RQ3 will be answered with a list of guidelines, in several levels, that aim to prevent or at least minimize the effects of the issues brought up by the answer of RQ2.

a) ***Not downloading or executing applications from untrusted sources*** [18]. It relates mainly to the answer (b) given for RQ2.

b) ***Changes in legislation*** aiming, among other things, to reduce SMS fraud. For instance, the Advice of Charge (AoC) mechanism notifies the customer about costs, and requests additional confirmation every time the customer tries to send an SMS to a premium number [18]. This kind of effort tries to minimize the user's monetary loss due to malware infections. In addition, as noticed in [18], anti-fraud measures, even when taken in a single country, can have a beneficial effect in the whole world. This is mostly related to the answer (d) and (f) given to RQ2.

c) ***Individual users should protect their devices with secure passwords*** to prevent attackers from accessing personal data in a stolen device by brute-forcing the password. This relates to answer (e) given for RQ2.

d) ***Not enabling the installation of apps from third-party sources***. In general, official channels for distribution of apps, like Google Play and Apple Store, carefully verifies the software it distributes. If for some reason this kind of installation was necessary, it should be turned off as soon as possible [20]. This guideline chiefly relates to answers (b) and (f) for RQ2.

e) ***Using a security solution on the device and making sure it scans files*** as they are downloaded and protects the device from other types of Internet attacks. Often the antivirus software also include applications designed to test devices for newly-discovered vulnerabilities. Using these solutions and keeping them updated might help to address problems like the ones in the answers (d), (e), (f) and (g) for RQ2.

f) ***Using two-factor authentication whenever possible***, especially when conducting sensitive operations, like banking transactions. Ideally, temporary codes used in these authentications should be sent to a different phone from the one from which you are trying to authenticate. Using simple devices with no smartphone features for this purpose is recommended, since this minimizes the chances of these devices being infected with a malware. This kind of attitude might help to prevent the problems discussed in the answers (a) and (g) given for RQ2.

g) ***Using encryption*** when storing any valuable information (financial, personal or work-related) on the device. With this precaution, even if the device is stolen, the attackers will not be able to access the encrypted data [18]. This is an important guideline, and is related to the answers (a), (b), (e), (f) and (g) given for RQ2.

h) ***Quickly contact law enforcement and expert organizations in the event of a cybercrime***. This helps the entire society to keep track of organizations and people involved in the incident. Additionally, in most countries, creating and distributing malware or stealing personal information is a crime that is investigated by dedicated law enforcement agencies [18]. This is a very general guideline and can be related to every answer given for RQ2.

Corporations should have a security solution, with mobile device management capabilities, including encryption and remotely wiping of data from smartphones, especially when adopting the Bring Your Own Device approach. Also, it is important to train the employees to handle properly business data and how to proceed in case of a security incident [18].

This guideline helps to prevent the problems discussed in every answer for RQ2 to happen in the corporation environment.

VI. Conclusion

This paper presented a study on mobile security threats based on the systematic mapping methodology. During this research, we found that the increasing use of mobile applications, along with characteristics like high availability, contributes to estimulate the growing in the number of malwares that targets mobile devices. We also noticed that not only malwares, but also flaws in protocols, bad design of applications and permissive policies in the official stores can be very dangerous to the integrity and security of user data in mobile devices.

Our RQ3 lead us to the conclusion that the majority of the issues brought up in the RQ2 are caused by downloading and executing applications from untrusted sources; the lack of basic protections in the devices, like antivirus software and a strong password; the lack of encryption for transmitting and receiving data; and also by the flaws in design and distribution of legit software.

Another conclusion from this work is that the security of mobile applications is implemented in several levels. The owners of the official app stores, developers of applications, and the devices users, for instance, they all hold a share of the responsibility. So, in a future work, we intend to focus on one of this levels and study, for instance, how exploit kits are used for finding and exploiting security holes in mobile applications.

The growth in the use of mobile devices, their importance and computing power should keep growing, as well as the diversity of security threats for these devices. Because of that, it is expected that researches like this one become even more relevant.

References

[1] Gartner, “Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration”, May 2014, Available from: http://www.gartner.com/newsroom/id/2753017

[2] Thawte, "The rising costs of mobile data breaches", May 2014, Available from: https://www.thawte.com/about/news/?story=452627

[3] Theregister, "Attackers raid SWISS BANKS with DNS and malware bombs", Jul 2014, Available from:http://www.theregister.co.uk/2014/07/23/ruskie_vxers_change_dns_nuke_malware_in_swiss_bank_raids/

[4] McAfee, "McAfee Labs Threats Report", February 2015. Available: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf

[5] TIME, "Snapchat Weakness Would Reportedly Allow Phone Numbers to Be Matched to User Accounts", July 2014. Available: http://techland.time.com/2013/12/27/snapchat-weakness-would-reportedly-allow-phone-numbers-to-be-matched-to-user-accounts/

[6] L. Jedrzejczyk and B. A. Price and A. K. Bandara and B. Nuseibeh, "I Know What You Did Last Summer: risks of location data leakage in mobile and social computing.", July 2014. Available: http://computing-reports.open.ac.uk/2009/TR2009-11.pdf

[7] Dua, Lovi, and Divya Bansal. "TAXONOMY: MOBILE MALWARE THREATS AND DETECTION TECHNIQUES." International Journal of Computer Science & Information Technology 6.4 (2014).

[8] Yean Li Ho and Swee-Huay Heng. 2009. "Mobile and ubiquitous malware.” In Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09). ACM, New York, NY, USA, 559-563.

[9] Mohata, Vinit B., Dhananjay M. Dakhane, and Ravindra L. Pardhi. "Mobile Malware Detection Techniques." International Journal of Computer Science & Engineering Technology (IJCSET) 4.04 (2013): 2229-3345.

[10] Mas'ud, M.Z.; Sahib, S.; Abdollah, M.F.; Selamat, S.R.; Yusof, R.; Ahmad, R., "Profiling mobile malware behaviour through hybrid malware analysis approach," Information Assurance and Security (IAS), 2013 9th International Conference on, vol., no., pp.78,84, 4-6 Dec. 2013.

[11] Guo, Dai-Fei, et al. "Behavior Classification based Self-learning Mobile malware detection." Journal of Computers 9.4 (2014): 851-858.

[12] Jonghoon Kwon; Jihwan Jeong; Jehyun Lee; Heejo Lee, "DroidGraph: discovering Android malware by analyzing semantic behavior," Communications and Network Security (CNS), 2014 IEEE Conference on, vol., no., pp.498,499, 29-31 Oct. 2014.

[13] Juanru Li; Dawu Gu; Yuhao Luo, "Android Malware Forensics: Reconstruction of Malicious Events," Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, vol., no., pp.552,558, 18-21 June 2012.

[14] He, D.; Chan, S.; Guizani, M., "Mobile application security: malware threats and defenses," Wireless Communications, IEEE, vol.22, no.1, pp.138,144, February 2015.

[15] Andrubis. “Andrubis: A tool for analyzing unknown android applications”. July 2014. Available: http://anubis.iseclab.org/.

[16] VirusTotal. “VirusTotal - free online virus, malware and url scanner.” July 2014. Available: https://www.virustotal.com/en/

[17] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattson. “Systematic mapping studies in software engineering.” In Proceedings of the 12th internacional conference on Evalutation and Assesment in Software Engineering, EASE´08, pages 68-77, Swinton, UK, UK, 2008, British Computer Society, 29.

[18] Mobile Cyber Threats. Kaspersky Lab & INTERPOL Joint Report. Fev, 2015. Available: http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf

[19] Internet Security Threat Report 2014. Vol. 19. 2013 Trends, Volume 19, Published April 2014. Jan, 2015. Available:http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[20] Dua, Lovi, and Divya Bansal. "Taxonomy: mobile malware threats and detection techniques." International Journal of Computer Science & Information Technology 6.4 (2014).

[21] Icloak. “Cryptoware: A Ransomware Trojan You Should Avoid at All Costs.” Fev, 2015. Available: https://icloak.org/cryptoware-a-ransomware-trojan-you-should-avoid-at-all-costs/

[22] Uscilowski, B.: Mobile Adware and Malware Analysis. Tech. rep., Symantec October 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf

[23] Grzonkowski, S.; Mosquera, A.; Aouad, L.; Morss, D., "Smartphone Security: An overview of emerging threats.," Consumer Electronics Magazine, IEEE , vol.3, no.4, pp.40,44, Oct. 2014