Management, Enterprise and Benchmarking in the 21st Century
Budapest, 2017

Smartphone Security Threats

Esmeralda Kadëna, Ph.D Student

Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Hungary

kadenaesmeralda@gmail.com

Abstract: Nowadays the use of smartphones have become an inevitable part of our lives. The mobile revolution offers new ways of working, increasing efficiency and responsiveness of users in different environments. The concern is that with comfort and convenience also come security risks. Security is a key component in any mobile device management strategy. What might be convenient for users, might be convenient for attackers. Here the focus is on the human factor as the weakest link in this field. To develop this work I am concentrated in these research questions: "How users contribute to smartphone security threats?" and "How can we help on minimizing the risks that the use of smartphone brings?". The aim is to provide an easy and concise view of different threats and possible solutions. I am based on reviewing literature to find the most common threats, to see how users contribute on them and how their solutions are introduced. By analyzing the findings there are given some estimations of the possible threats and suggestions for average users and enterprises to improve the security of daily life operations.

Keywords: Smartphone, Security, Threats, Human factor.

1 Introduction

In recent years, the smartphone usage raised significantly. Thus because smartphones provide users with a wide range of services like phone calls, Internet services, sharing and keeping data, on/off-line games and some entertaining applications. Due to these services, a smartphone is faced with some challenges like security and privacy as well. Actually the dawn of the planet of the smartphones came in January 2007, when Steve Jobs, Apple's chief executive, presented an object of plastic, metal and silicon in front of the Apple audience. He promised: "This will change everything" [1].

But before speaking about smartphones, is very important to understand mobile computing. This term is defined as the use of transportable computing devices with mobile communication technologies [2]. Mobile computing is a technology that

allows for the transmission of data, voice, and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link [3]. Connecting to a network is made of different methods such as internet, intranet, WAN, LAN, WLAN, and a number of other related methods.

The beginning of wireless and mobile computing technology is marked in 1894 when Guglielmo Marconi, the father of radio, produced radio waves over long distances. In 1958 was completed the first wireless network in Germany. In 1983 came Motorola, the first personal cellular phone in the world and he entered the mobile computing industry [3]. This invention simultaneously marked the creation of the commercial cellular service market.

A smartphone contains an MNO[1] [4] smartcard with a connection to a mobile network. Moreover, it has an open operating system that can be extended with third-party software. Since most of the operations smartphones perform are on the Internet, so it is necessary to ensure security and safety of data and information. We can use as authentication, a pattern like password, code password, PIN password, face/finger unlock [5]. Actually these are penetrated methods with such as brute forcing and guessing. A lot of Malware, Viruses and Trojans have been developed based on smartphones APIs (application program interface). Critically most of them look like safe software and some reliable applications (Gmail, Facebook, etc.) with GPS service in smartphone, collect information about the user such as location without his knowledge [6].

There are many smartphone operating systems available, such as Android, iOS, Microsoft Window Phones, Symbian and BlackBerry [5]. The most widely used smartphone OS is Android. According to Schulz and Plohmann in 2012, Android is the widely used smartphone operating system with better performance compared to other smartphone operating systems. Android OS is based on Linux OS architecture. The desktop operating systems and the versions of smartphone of such operating systems differ, especially in user interfaces and architecture of the system. Smartphone is nearly used for every kind of communication, to store a lot of personal and sensitive details like contacts, emails, credentials, to browse data/information from the World Wide Web [7].

Now, smartphones pair mobile phones with other devices such as PDAs, HD camera, media player, GPS navigation units and other data storage and processing devices. Even before mobile devices came with 3G and 4G compatibilities; but now such devices transformed into mobile computers with smart options like touch screen and laptop capabilities and easily can browse the Internet using wireless network and third party applications. Strategy Analytics expects that in 2020 will become available in Japan and South Korea, the first commercial 5G handsets. Then

[1] An MNO smartcard is a smartcard inside the mobile device that is controlled by a mobile network operator (MNO).

it can be followed by the US and China in 2021. It is also expected that by 2025, 7% of worldwide mobile connections will be 5G [8]. So it is obvious that the rapid advancement in smartphone technology and the growth of the number of this devices make the security one of the biggest problems as the cybercriminals have "desire" for these devices as well. In the Symantec Internet Security Threat Report (ISTR) is presented that in 2013, 38 % of smartphone users have been victims of cybercrime [9].

But while talking about the security on this field we have to put human- factor in the first line. The user can influence over the mobile device. In most cases he can harm or prevent from harming himself. For an average user it is very important to understand some basics regarding the security solutions of his mobile device. Most of security mechanisms like application frameworks (i.e., the Java framework J2ME) and signature schemes for different trust levels might not be understood by the average user. An example is a phone that was locked for third-party software. And below we can see that in such cases they prefer to open the doors and skip the security mechanisms.

There are given some examples from Denning [10] and Anderson [11] of weak password use, documenting low security awareness, because the relationship between guessable passwords, successful attacks, and the role of the user is often unclear to users. Many security awareness are shown when they choose a password on mobile devices, short, especially consisting only in numbers. Moreover it has to be mentioned that the appreciation of the mobile device is lower than for desktop PCs, and that it is more seen as a disposable item [12]. Regarding their mobile devices, the security awareness can be considered lower than for PCs as well.

2 Related news/work

Nielsen has reported that when looking at smartphone users by age, the highest percentage belongs to age 18-24, 98% of whom own smartphones, age 25-34 with a 97% ownership rate, followed by the group of 35-44 at 96%, making smartphones nearly used by everyone [13].

Based on past researches, privacy and security play roles in users' installation decisions. The result from the interviewed people was that they were cautious when installing new software because of malware concerns [14]. In an experiment realized by Good et al., was found that people preferred applications with better privacy policies if the privacy is included in the cost of application functionality [15].

The beginning of the smartphone era can be called as the new millennium. There are a lot of articles written about smartphone security and the considerable threats on smartphones. Lot of them try to give a prediction on the future through a

statement, for example “The wireless epidemic” [16], in 2008 “Is it finally time to worry about mobile malware?” [17], “Planet of the phones” in 2015 [18], etc. Based on the latest news, Check Point, the cybersecurity company discovered a “severe infection” in 38 new Android smartphones and which is more the malware were not downloaded into the devices but they arrived with pre-installed malware. Actually they belong to two companies which were not named [19].

Obviously these mean that more and more incidents are expected ever since these devices are gaining so popularity since started to become more powerful in terms of: increased processing power and memory increased data transmission capabilities of the mobile phone networks, and with open and third party extensible operating systems.

In 2010, IDC reported that for the first time smartphone sales surpassed PC sales [20]. Faced by this onslaught of devices and recognizing the productivity and cost benefits, organizations are increasingly implementing policies of bring-your-own device (BYOD). J. Gold Associates reports that about 25%-35% of enterprises have a BYOD policy, and they expect that to grow to over 50% over the next two years [21]. 40% of U.S. employees in large enterprises use their personal devices for work [22]. This makes sense as mobility evolves from a nice-to-have capability to a business advantage.

According to eMarketer, by 2020 the number of mobile phone users will climb to 4.78 billion while the user growth is slowing [8]. You can see below:

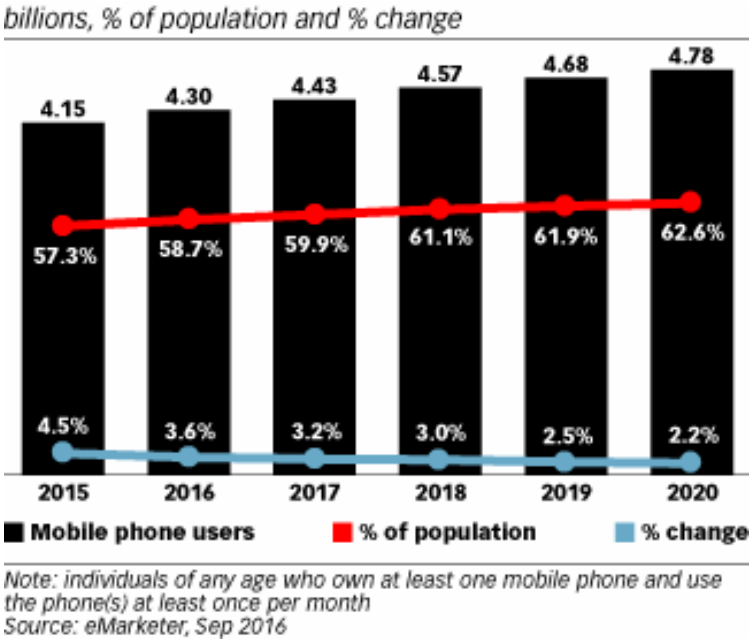

Figure 1

Mobile Phone users and penetration worldwide, 2015-2020

The top manufacturer on a global level is Samsung [8]. Apple controls a significant share of the market in wealthy, digitally developed countries. Chinese smartphone brands have made strong headway as well, especially in Southeast Asia [8]. North America boasts the highest share of 4G mobile connections overall, some of the most reliable 4G networks are found in Japan, Singapore and South Korea [8].

3 Smartphones and Security

Mobile devices always have on hand all the information and personal contacts with interest for us through multiple channels of communication that we can use anywhere relying on audio networks and wireless data. As a result, smartphones became the gateway of personal details both local and those who are delivered to a third party "in the cloud". But in inevitable way, they lead tracks, not only details regarding the owner of the phone but also of his friends and colleagues, their contacts, messages, appointments, notes and locations.

As the security is and will remain one of the biggest issues in our era, is very important to have a clear view on the most common problems regarding

smartphones. On the other hand, there is not a complete security model and it is not said that a unique possible model can give the flexibility of the medium and multiple configurable scenarios. Anyway there are settled some assumptions, policy and common mechanisms in commercial platforms proposed from Apple, Google, Microsoft and Research in Motion.

The owner of smartphone is considered as the partial administrator because usually some implemented security policies and relative mechanisms limit the proper owner. A second indirect assumption found on mayor part of the market players offers is that the supplier of the platform and potential partner are closely connected such as in some cases where telephone operators came as reliable and present "power", capabilities in areas of the administrator. Shared assumptions between different platforms lead to similar security mechanisms although with many differences and characteristics such as the use of virtual environments for the abstraction of resources and application sandboxing mechanisms with a pronounced separation of privileges; a push towards the development of managed code, by compiling in the intermediate languages in Java and .NET environment to try to limit some of the problems resulting from programming errors; the explicit exposure of the resources required by applications and their run-time imposition by the system; the use of cryptographic protocols to ensure the origin of the installed applications and mechanisms for their installation.

When talking about privacy, is very important to define the concepts of Confidentiality, Integrity and Availability in relation with the characteristics of the smartphones and their operation systems, containing present the described view. Confidentiality is about preventing unauthorized disclosure of information, integrity is about preventing of unauthorized modification of information, and availability is about preventing unauthorized withholding of information or resources [23].

3.1 Data protection and Privacy

There are made a lot of studies regarding data protection and privacy with focus on users' behaviors/practices. Boshmaf et al., analyzed the users' need for protection and privacy in smartphones. They outlined the types of data that users want to protect and investigated users' behavior in the protection of such of data. The result from 22 interviewed participants showed that users want to protect their data on smartphone but is not convenient to do it in practice [24]. Muslokhlove presents the problems of data protection against physical threats and possibility to conquer weak authentication. He resulted from the survey, that to increase the confidence of user and safety of smartphones a good solution might be upgrading the lock screen system in support of authentication and user's accessibility and providing suitable security [25].

Another study comes from Ghosh et al. They worked on user data, privacy and protection regarding semantic reasoning and user context modeling. The authors state that the privacy of users and smartphone under this framework are protected using embedded semantic policies based on the user's privacy and settings [26]. To execute the privacy policies on smartphone and to protect the data on an enterprise, Kodeswaran et al. showed a framework [27]. The authors defined their privacy policies of acceptable information flow on mobile devices. This flow of information is depended on the object involved in conforming IPC (Inter-Process Communication) and its data. Their framework design is based on policies for Android platform and the presented results measuring were executed by the framework.

The research of Onwubiko and Owens shows that employees compliance with security policies and guidelines is taken for granted in many companies. Instead they prefer a formalistic approach of the security [28]. Actually these provides some directives on where to extra resources should be used to improve the employees (regarding security awareness) as the most important line of the defense. Information security should be integrated into all processes of the business. Considering “Pareto Principle”, known as 80%-20% rule that states that 80% of the effects/output comes from the 20% of the investment/input [29]. In this case, maybe 20% is invested in technical security measures and formal controls to protect 80% of the undesirable effects that are threats. Whereas the human-factor is remaining the weakest link in security.

3.2 Security threats

There are several threats to the smartphones using mobile operating system. The malicious software industry is also growing in terms of technology and structure. We will see these threats discussed in three main categories as it is shown in figure below: Malware, Vulnerabilities and Attacks [30].

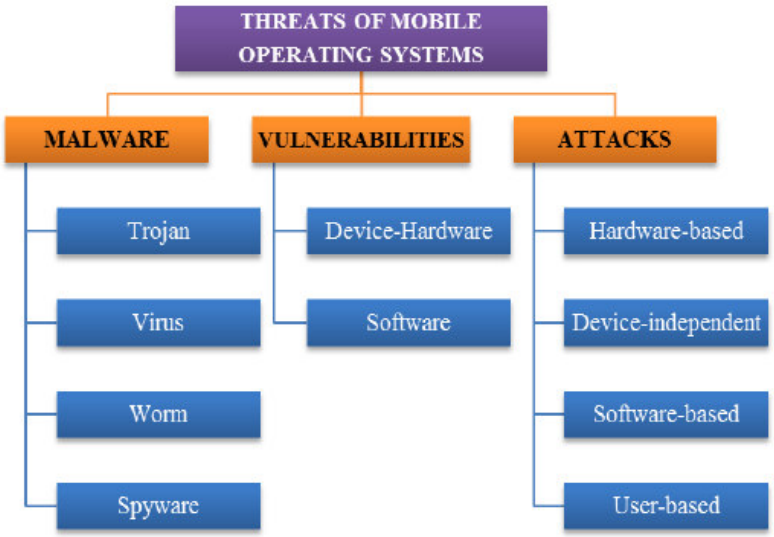

Figure 2

Threats of Mobile Operating Systems

3.2.1 Malware

Malicious Software (Malware) tend to disturb users by entering at private specific information, they may cause breakdown of the device and lead to stolen or to become unusable the information/documents of the users [31]. These illegal software installed not by the user are used for all attacks that came from the outside taking advantage of the vulnerabilities in the device/system. Thanks to its closed system, Apple is more protected against OS malware software. While Android OS becomes the most target of Malware attacks. That because the applications can be taken from many secure-insecure sources. The major ones of these software are Trojans, Worms, Virus and Spyware.

The current platforms ask users to make the decision about access. For example, iOS asks users to decide whether an application may access a feature such as

location, and Android asks them to agree to an install-time manifest of permissions requested by an application.

Unfortunately, these permission-granting approaches place too much obstacle on users. Most of them are often ignored or not understood by users [32] and permission prompts are disruptive to the user's experience, teaching users to ignore and click through them [33]. As a consequence users unintentionally grant applications too many permissions and become vulnerable to applications that use the permissions in malicious or questionable ways (i.e., secretly sending SMS messages or leaking location information).

- Trojan

Trojan software aims not to spread themselves but to seize the management and the information of the device [34]. Here they differ from worms and viruses. Keyloggers are the most widely used spyware. It is transmitted under the cover of a file and the user can unintendedly activate. In that moment it has the entirely device in the background under control and not noticed by the user. For this reason, while downloading an application necessary for the smart devices, it is of big importance to search before it and to check if is a reliable software.

- Worm

Imagine you are at the airport/coffee bar/hotel and you want to find the free Wi-Fi. By scanning, your smartphone is going to show the Wi-Fi access points. Actually that is an easy channel for a hacker to inject malicious worm code into your smartphone. Worm is a kind of virus but does not require user interaction to reproduce itself. Worms are designed to spread through the network [34]. Transmitting forms: by SMS, MMS and activated by clicking on a file or opening a plug-in sent by e-mail, i.e social engineering. Worm penetrates using this vulnerability and integrates itself into a service running in the OS. Then it can act as a spy inside the device, send the required information to the center that is managed from itself, through creating an unnecessary data flow can cause clogging and slowing down in the Internet bandwidth and reduce the performance of the device. So, users tend to be careless and not pay attention.

- Virus

A malicious software which can penetrate into documents and send them elsewhere, distort their contents or making them unusable and making the hardware elements to slow down [34]. Infected programs should also be installed in other devices. In 2010 in China, a virus named "Zombie" infected more than 1 million smartphones by causing a loss amounting to $300,000 per day. This was followed also by data loss, data leakage and even disruption of the conversation [35]

- Spyware

They are used to collect information and data regarding a target subject. They specify that their usage is for advertising and promotional purposes (adware) or to

offer better service to users (cookies), while what they do is collecting information about a person/organization and send to someone else without their permission (here works like a Trojan) [34]. It can be caused by malicious people and aimed at taking control of the devices infected.

According to McAfee mobile threat report [36], for iOS, the biggest threat in 2016 were as a result of applications with very aggressive adware while Google Play saw a number of applications infected with malware. In considerable studies by security firms, it is seen that malware software are not only used by hackers but also created by some profit-oriented "teams", i.e. in an incident in the year 2013, the Trojan "botnet Trojan-SMS.AndroidOS.Opfake.a" enabled the spread of the malware software "Backdoor.AndroidOS.Obad.a". It send a spam containing the malware to its victim list [37]. CISCO published the top malware categories as it is shown in the figure below [38]:

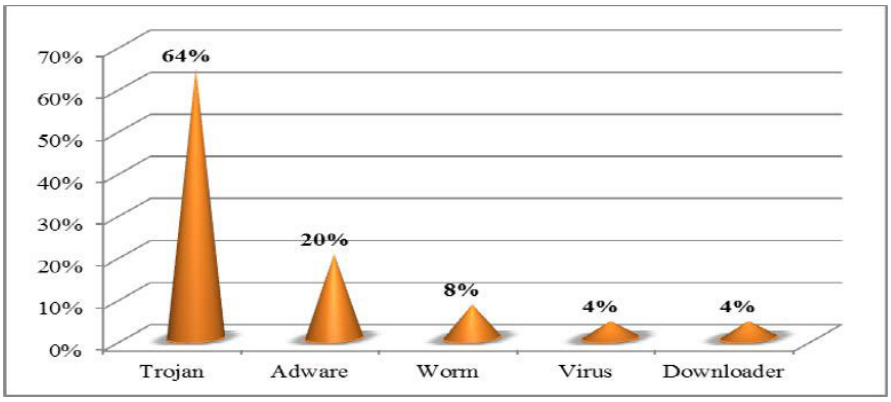

Figure 3

Rates of Malware Software affecting Mobile Operating Systems

As it is shown, Trojan software are represented with the highest rate, 64%.

3.2.2 Vulnerabilities

Vulnerabilities refers to the weaknesses occurring in the system security procedures, internal controls, design and applications among the security vulnerabilities in the device [34]. These vulnerabilities can be grouped under several headings but in this work they are classified in two major categories: Device-Hardware and Software.

- Device-Hardware

Here we can see two critical points. The first issue is when the smartphone may not receive the latest security updates. This came from the age of the device. The manufactures do not support those who are manufactured before a certain date.

The second issue, however, is the disability of the mobile devices to ensure the safety of the ports they use while connecting to a network or the Internet. The fact that the mobile devices are have no limit to navigate in the Internet and there is not any firewall to control this is an important vulnerability. An intruder can easily access to the mobile devices through this unsecure port and in such cases must be used "firewall" to protect these ports. As a consequence, while connecting to the mobile device, the user will be asked for a permission and will be able to see it. Taking in consider unauthorized changes ("jailbreaking" or " rooting") on the mobile devices which are not using a firewall. Jailbreaking is the method used for obtaining an application that does not belong to Apple or due to some restrictions from any other source cannot be downloaded. Through this method allows to have access to the OS of the mobile and as a result creates a vulnerability. Furthermore these devices do not receive the necessary security updates and become vulnerable to threats [39].

- Software

If the mobile OS is out of date it can lead to vulnerability also. Usually users don't pay attention on messages to update their mobile OS. Another issue is related with downloading from the third party applications. Deficient API[2] management is responsible for many malicious code infections. APIs are classified into Open APIs, third party application development and control APIs; used to remote maintenance. Controlled APIs have specific higher privileges to update system, file destruction, and information fetching. If attackers gain the APIs control, could easily initiate attacks and use the privileges of the APIs [40, 41].

Another important vulnerability come from the shared open source common components such as WebKit and Linux kernel. In order to reduce the costs (a common practice in large open systems, i.e., Android) these components have a reusable structure. A vulnerability has been discovered in WebKit or Linux, however, a patch was released in order to use in solving this problem. While in Apple's iPhone-like WebKit and BSD kernel derivative (Darwin) constitutes the common software components. At this point, the problem is not its reuse but where it is employed. According to this, Android put the patch model into practice with a little delay [42].

3.2.3 Attacks

Attacks are the interventions made from outside using a variety of vulnerabilities. The term "attacks" generally stands for the attacks made by the hackers to obtaining users' private information without their knowledge. Figure below shows Kaspersky

[2] API- "Application Programming Interface": a set of commands, functions, protocols, and objects that can be used from programmers to create software or interact with an external system. They are available for both desktop and mobile operating systems [54].

Lab findings against Android users, the number of Android threats, and the number of attacks between the 2nd quarter of 2012 and 3rd quarter of 2014 [43].

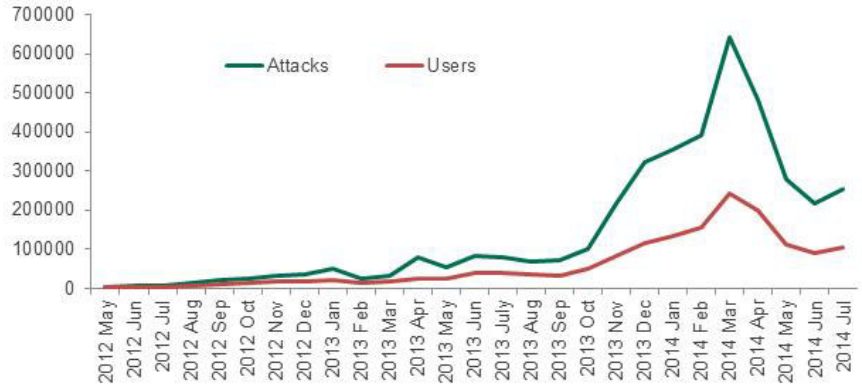

Figure 4
The relationship between the smartphone users and the number of attacks (May 2012-July 2014)

Two researchers (Vincenzo Iozzo and Ralf Philipp Weinmann) in March 2010 made the first real attack against smartphones in order to steal a database from a phone via SMS. They realized this by looking at an error in the Safari Browser on iPhone 3GS and aimed to upload the file sent by SMS to the server [44]. In November 2010, an attack was directed to the browser in the Android OS using a common vulnerability [45]. It has been introduced again by Weinmann the first -over-the-air attack for GSM software which will lead to memory corruption. [46]. Furthermore were identified by Oberheide and Lanier, a range of different attack vectors for the iTunes App Store [47].

According to classification in terms of attacks there are many. In this work I am referred to Becher which groups the attacks towards mobile devices in following mentioned categories [30].

- Hardware-based

With a broad perspective, hardware-based attacks constitute a mobile security element. Even if the smartphone has any vulnerability, it cannot easily reach to the user information, however, there is an access to the device.

- Device independent

Wireless connection is not safe and through it, many attack independent from the device, can violate the privacy of the target user.

- Software-based

These attacks are an important part of the technical vulnerabilities on smartphones. The increase in the number of mobile web browsers has led to an increase in the vulnerabilities used in this field.

- User-based

There are such attacks not technical. They are made through cheating without using malicious software which are direct to the smartphone users. These attacks made through "social engineering" and aimed at reaching to private information are very common today [48]. Anderson also discusses this topic in his book "Security Engineering" [11]. Social engineering becomes most important when there are no more technical vulnerabilities to exploit. So security depends on the user and the technical security mechanisms are effective and sufficient.

- Phishing Attacks: This kind of attack is formed by combining the words "Password" and "Fishing". This method is independent from OS and can be used in every type of devices. Attacks are made by directing the user to a false (imitation) website in order to steal private information (credentials, credit card information, user name or password). There are some varieties of this attack such as Similarity attack, Forwarding attack, Background attack and Notification attack [49].

- SSL Proxy Attacks: Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption is a protocol that assures users and provides data security when implemented correctly. Today it is used in many applications such as internet banking. If it is not implemented correctly, applications may be threatened and unintended vulnerabilities occur. If this code is left uncontrolled, the settings can be changed undesirably and the information which were supposed to be safe and transmitted can be stolen through the path of communication [50].

- Camera based Vulnerabilities and Attacks: All smartphones have certain features like camera and touchscreen but also these functions can lead to attacks on smartphones. Users go to third party applications from the "app stores" or traditional websites. As the source application is a problem, users are at risk of installing malicious programs. As a result they can steal personal information or gain root access to their device [51, 52].

4 Suggestions

It is very important for everyone to know how to use properly the smartphone and to create some basic security habits in order not to expose yourself. For an average user it is difficult to understand practical security mechanisms but some theoretical and basic knowledge is almost enough to be protected from the threats. The education and training form is the most important measure that should be used. Average users cannot be security experts at all, because it is the task of the security experts to protect the common user. What everyone should keep in mind is that these vulnerabilities and attacks will always exist, no matter what operating system you use. Here it is important the way you use it and what privacy layers you enforce.

Firstly when talking to security, trust is something that must be neglected. We must maintain physical control of the device, it can be loosen or stolen especially in public places. To keep intruders away screen lock should be activated. It is also important in case you lose or someone steal it, even you are careful with your things, there is no guarantee. A strong password for authentication also should be used. A long one, mixed chars number and letters is secure enough.

Do not "root" or "jailbreak" the mobile device, you must be careful with third party applications. Always use official application stores to download and install an application. You can disable the option to allow installation of third party apps. Be choosy when selecting and installing apps. A little research on apps before installing is very useful. The permissions for the installed apps should be checked and if something looks out of order then deny them access. Do not forget to make a spring cleanup of your apps. Have time to take a look over your apps and remove the ones you do not use anymore. Another thing that you can do is to update you apps. As we saw, the apps that remain out of date make your mobile device is more exposed to threats.

Beware of phishing. Do not trust on such as spam emails, link from an ad, messages from your friend's social account that got hacked, etc., because by clicking on a link it will redirect you to an infected website. So is very important to not click on short, suspicious links for which you did not request. Attackers can use phishing techniques to steal your money, your identity and open credit card accounts in your name and much more. Even the strongest antivirus will protect you from phishing and malware. Take in consider to be sure that you are connecting only in secure wireless connection. That means to not use free or public Wi-Fi, especially when you are accessing sensitive data. Information sent via public networks can be accessed by they who know how to view it.

Conclusions

In this work some theoretical and practical background was introduced with regard to security on the smartphones. Here the threats were categorized in three major groups: Malware, Vulnerabilities and Attacks. Both the number of threats and users were represented as a growing risk. As the users are the weakest link in the internet, they can influence on this concern. When it comes to the question who is responsible for the security of mobile devices, here is the main response. Based on the literature, some results were presented to this question. But yet the response is open.

The IT risks management entities in an organization have to put a special emphasis on the education of employees. Maybe the numerous security mechanisms are useful but when the user does not understand them it become a critical point. The first and most important thing is education from IT teachers and experts. Data privacy and threats are the major open issues of security. All users want to protect their data and they must beware to take measures for themselves. So, human factor is and will remain one of the biggest problems to the field of security.

Thinking that the future belongs to IoT (Internet of Things) where all the devices are interconnected, the security will become more and more in risk. With the rapidly growing field where development occurs at large scale it is hard to achieve 100% security, but the careful habits of smartphone users associated with learning and education can put them on the safe side.

And do not forget, be suspicious!

References

[1] Leaders, "Planet of the phones - The smartphone is ubiquitous, addictive and transformative," *TheEconomist,* 2015.

[2] M. Rouse, "Nomadic Computing (Mobile Computing)," May 2007. [Online]. Available: http://searchmobilecomputing.techtarget.com/definition/nomadic-computing.

[3] D. Livingston, "Introduction & History of Mobile Computing," LinkedIn Corporation, 2013.

[4] techopedia, "What is a MNO? - definiton from techopedia," [Online]. Available: https://www.techopedia.com/definition/27804/mobile-network-operator-mno.

[5] N. Yildirim, R. Das and A. Varol, "A Research on Software Security Vulnerabilities of New Generation Smart Mobile Phones," in 2nd International Symposium on Digital Forensics and Security (ISDFS'14), 2014.

[6] A. Agrawal and A. Patidar, "Smart Authentication for Smart Phones," International Journal of Computer Science and Information Technologies, vol. 5, no. 4, pp. 4839-4843, 2014.

[7] P. Schulz and D. Plohmann, "Android Security - Common Attack Vectors," Institute of Computer Science: Rheinische Friedrich-Wilhelms-Universitat Bönn, Bönn, 2012.

[8] eMarketer, "Mobile Phone, Smartphone Usage Varies Globally," eMarketer, 23 November 2016.

[9] Symantec Corporation, "Internet Security Threat Report 2014," Symantec, 2014.

[10] D. E. Denning, Information Warfare and Security, New York: Addison-Wesley Professional , 1999.

[11] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., Indiana: Wiley Publishing, Inc., 2008.

[12] E. Chin, A. P. Felt, V. Sekary and W. David, "Measuring User Confidence in Smartphone Security and Privacy," in Symposium on Usable Privacy and Security (SOUPS) 2012, Washington, DC, 2012.

[13] Nielsen Mobile Insight, "Millenials are top smartphone users," The Nielsen Company (US), LLC, 2016.

[14] R. Wash, "Folk Models of Home Computer Security," in Proc. of the Symposium on Usable Privacy and Security (SOUPS), 2010.

[15] N. Good, R. Dhamija, J. Grossklags, S. Aronovitz, D. Thaw, D. Mulligan and J. Konstan, "Stopping spyware at the gate: A user study of privacy, notice and spyware.," in Proc. of the Symposium On Usable Privacy and Security (SOUPS), 2005.

[16] J. Kleinberg, "The wireless epidemic," Nature, p. 287–288, 2007.

[17] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?," 2008.

[18] Leaders, "Planet of the phones," The Economist, 2015.

[19] A. Mamiit, "New Android Smartphones Found To Be Already Infected By Malware: Are You At Risk?," Tech Times, 2017.

[20] C. Albanesius, "Smartphone Shipments Surpass PCs for First Time. What's Next?," PCmag, 2011.

[21] J. E. Gold, "Mobile device strategy bypassed as enterprises face tablet invasion," TechTarget, 2011.

[22] Gartner, "Gartner Says 40 Percent of U.S. Employees of Large Enterprises Use Personally Owned Devices for Work," Gartner.com, 21 October 2014.

[23] M. E. Whitman and H. Mattord, Principles of Information Security, Boston, MA: Course Technology, 2003.

[24] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester and K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," in IEEE 28th International Conference on Data Engineering Workshops, 2012.

[25] I. Muslokhlove, "Survey: Data Protection in Smartphones Against Physical Threats," University of British Columbia, Canada, 2012.

[26] D. Ghosh, A. Joshi, T. Finin and P. Jagtap, "Privacy Control in Smart Phones Using Semantically Rich Reasoning and Context Modeling," in IEEE Symposium on Security and Privacy Workshops, 2012.

[27] P. Kodeswaran, V. Nandakumar, S. Kapoor, P. Kamaraju, A. Joshi and S. Mukherjea, "Securing Enterprise Data on Smartphones Using Run Time Information Flow Control," in IEEE 13th International Conference on Mobile Data Management.

[28] C. Onwubiko and T. J. Owens, "Situational Awareness in Computer Network Defence: Principles, Methods and Applications," IGI Global, 2012.

[29] G. Muzea, The Vital Few Versus the Trivial Many : Invest With the Insiders, Not the Masses, New Jersey: John Wiley & Sons, Inc., 2005.

[30] M. Becher, "Security of smartphones at the dawn of their ubiquitousness," University of Manheim, Cleves, 2009.

[31] A. Felt, M. Finifter, E. Chin, S. Hanna and D. Wagner, "A survey of mobile malware in the wild," in Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2011.

[32] E. Ha, A. P. Felt, S. Egelman, A. Haney, E. Chin and D. Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Washington DC, 2012.

[33] S. Motiee, K. Hawkey and K. Beznosov, "Do Windows users follow the principle of least privilege? Investigating user account control practices.," in Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS), New York, 2010.

[34] H. Bidgoli, "Volume III: Threats, Vulnerabilities, Prevention, Detection and Management," in Handbook of Information Security, New Jersey, John Wiley & Sons, Inc., 2006, pp. 146-165.

[35] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," in IEEE Transactions on Mobile Computing, 2013.

[36] McAfee, "Mobile Threat Report 2016," McAfee.com, 2016.

[37] R. Unuchek and V. Chebyshev, "Mobile Malware Evolution: 2013," 2014.

[38] CISCO, "Cisco Annual Security Report," Cisco Systems, Inc. , 2014.

[39] P. Ruggiero and J. Foote, "Cyber Threats to Mobile Phones," United States Computer Emergency Readiness Team (US-CERT), 2011.

[40] R. Prodanovic´ and D. Simic´, "Survey of Wireless Security," Journal of Computing and Information Technology, vol. 15, no. 3, p. 237–255, 2007.

[41] A. Kataria, T. Anjali and R. Venkat, "Quantifying smartphone vulnerabilities," in 2014 International Conference on Signal Processing and Integrated Networks (SPIN), 2014.

[42] T. Vidas, D. Votipka and N. Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks," in In Proceedings of the Fifth USENIX Conference on Offensive Technologies, Berkeley, CA, 2011.

[43] Kaspersky & INTERPOL, "Mobile Cyber Threats: Kaspersky Lab & INTERPOL Joint Report," media.kaspersky.com, 2014.

[44] A. Portnoy, "Pwn2Own wrap up and analysis," Journal Network Security, vol. 2010, no. 4, pp. 4-5, April 2010.

[45] M. Keith, "Google Android 2.0 < 2.1 - Reverse Shell Exploit".

[46] R. P. Weinmann, "All Your Baseband Are Belong to Us," Laboratory for Algorithmics, Cryptology & Computer Security- University of Luxembourg, Luxembourg, 2010.

[47] E. Mills, "Google pulls app that revealed Android flaw, issues fix," cnet.com, 2010.

[48] Symantec, "2016 Internet Security Threat Report," Symantec Website Security, 2016.

[49] C. Marforio, R. J. Masti, C. Soriente, K. Kostiainen and S. Capkun, "Personalized security indicators to detect application phishing attacks in mobile platforms," arXiv preprint arXiv:1502.06824, 24 February 2015.

[50] J. Hubbard, K. Weimer and Y. A. Chen, "Study of SSL Proxy attacks on Android and iOS mobile applications," in Consumer Communications and Networking Conference (CCNC), 2014.

[51] A. Pore and M. Bartere, "A Review on Camera Based Attacks on," International Journal of Computer Science and Technology, vol. 6, no. 1, pp. 88-92, January-March 2015.

[52] M. Bartere and A. Pore, "Preventions and Features of Camera Based Attacks on Smart Phones," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 4, no. 4, p. 4846–4853, July - August 2015.

[53] Information Systems Audit and Control Association (ISACA), "Securing Mobile Devices," 2010. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx.

[54] TechTerms.com, "API (Application Programming Interface) Definiton," [Online]. Available: https://techterms.com/definition/api.