Smartphones and IoT Security

Ioan ADĂSCĂLIȚEI
Bucharest University of Economic Studies, Romania
ioan.adascalitei@ie.ase.ro

Mobile devices (smartphones or IoT devices) threats are all over and come in many ways. Nowadays the number of mobile devices is extremely high and we use them to cover many personal needs like ordering food, buying plane tickets, controlling our home from distance (using IoT devices) and so on. But all of this comes with a cost and that cost is that we have to give personal data to some devices which lead to threats. This paper contains a classification for the threats and vulnerabilities for smartphones and tablets and a short one for IoT devices. Here are described some attack scenarios for IoT and a few representative attacks. As method of research was used a qualitative one by documenting from articles related to this theme, reports realized by companies which operates in this field and other resources.

Keywords: mobile devices, IoT, attacks, malware, ransomware

1 Introduction

Nowadays mobile devices capture more and more areas and are used in many activities [1] like administration, health, construction, tourism and many others. But the usage it is not limited to different areas of expertise, every person in the world who possess a smart device has used it for personal needs other than calling or texting. We use these devices to do shopping for us or to buy tickets to a spectacle or any other kind of event but many of this people don't know that these facilities comes with a cost, and that cost is our privacy and the fact that we give our personal data to them. The problem is that these devices are not very secured and they can be attacked in different ways.

A threat refers to anything that has the potential to cause serious harm to a mobile system. A threat is something that may or may not happen, but has the potential to cause serious damage.

When someone breaks into a mobile system, that person takes advantage of multiple factors like technology, lapses in procedures or management (or some combination of them), allowing unauthorized access or actions. The specific failure of the controls is called a vulnerability or security flaw [2].

When we talk about any newly discovered incident that can harm a mobile device we talk about mobile security threats and when we talk about vulnerabilities we talk about some already known weakness of an asset which can be exploited by attackers [3].

The usage of mobile devices (smartphones, tablets, wearables or IoT) have increased a lot in the past years. Over the last 5 years, their numbers have grown significantly and are expected to grow even further over the next 5 years.

As we see in Figure 1, the number of IoT connected devices is nearly double in 2019 compared to 2015, it will double in 2020 and will be 5 times higher over 6 years, in 2025. This enormous increase it happens in only then years, and this only for the IoT devices which are just a part of the mobile devices. For example, if we will look at the numbers of the smartphone users from 2014 until 2020 from Figure 2 we will see that within 6 years the number is almost double.

DOI: 10.12948/issn14531305/23.2.2019.06

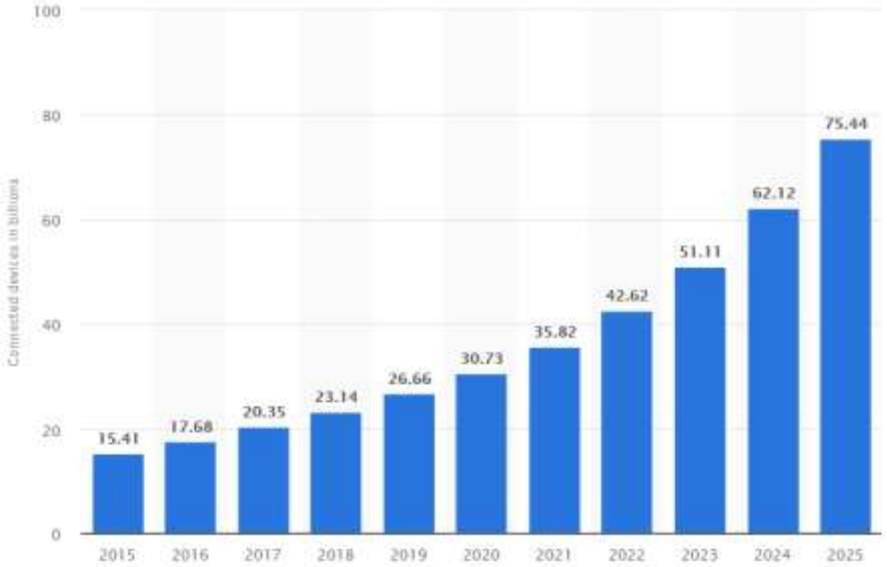

Fig. 1. IoT connected devices installed base worldwide from 2015 to 2025 [4]

As presented in figure 2, about 3 billion people, one third of the people in the world, have a smartphone[4].

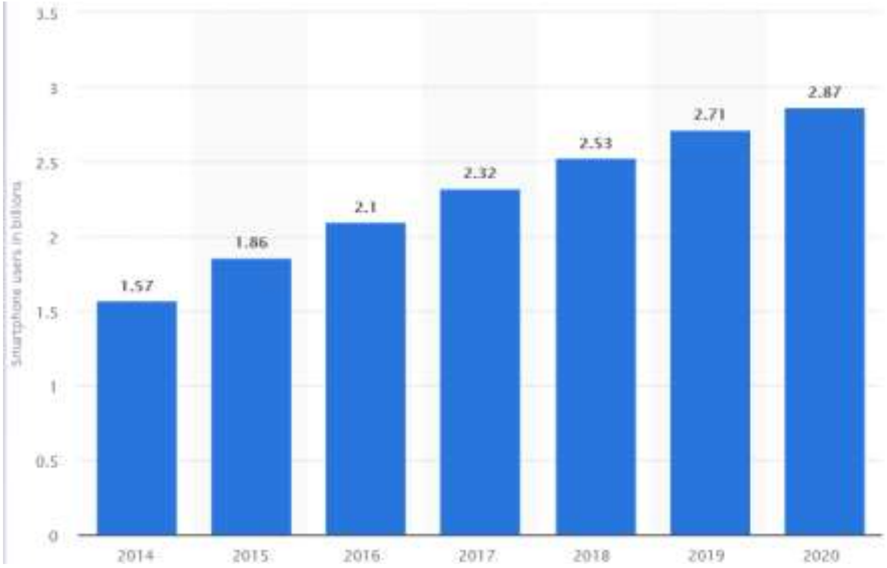

Fig. 2. Number of smartphone users worldwide from 2014 to 2020 [4]

The reason these smart devices appeared was the need for people to connect to the Internet more easily and from multiple places. Today, however, they do much more than just connect to the Internet and even more than monitor heartbeat or sleep time [5]. We use these devices to connect with people everywhere, to pay bills, shop, rent cars or houses, take a ticket to the theater or a plane ticket, we connect to our bank accounts via those devices and much more. The usage of IoT is way wider from the old and know smart home to the smart car, smart farming, smart city and smart anything [6].

As we seen the number of mobile devices greater and keeps growing, the possibilities are huge and everything comes with a price, the price of people safety [5]. But what exactly are those threats? How they appear? Are all the threats the same? How these vulnerabilities occurred? Can we prevent them? Nick Dawson, global director of

DOI: 10.12948/issn14531305/23.2.2019.06

enterprise business of Samsung Electronics said: “mobile security has never been a more urgent concern than it is today, and the threat defense landscape continues to evolve at an accelerating peace”.

The paper is structured as follows. The second part is an overview of the mobile threats and vulnerabilities. The focus here is on smartphones and tablets but it is presented a classification for the IoT threats too, a detailed one is planned to be made in the future. The third section presents a comparison between Android and iOS threats. The fourth section will present an overview of the IoT devices and a top 10 security issues viewed by OWASP. The fifth section presents in detail a few types of attacks and threats. The paper ends with conclusion that will leave us with some questions and some plans for future work.

2 Mobile and IoT threats and vulnerabilities

2.1 Mobile devices

These threats are not only software based, they are also physical. As we mentioned above these mobile devices are used more and more for a lot of activities from which a part of them require users personal data like personal bank account and many others [7]. All of this data and the fact that, at least in case of the smartphones, there are much complex functions that a mobile device is capable, which come with a pretty much financial cost, make these devices very valuable targets and they are easy to be stolen or lost [8]. Mobile device vulnerabilities exist in the wireless connection, the device itself, a user’s personal practices the organization infrastructure and wireless peripherals (keyboard, printers, mouse) which contains software, an OS and data storage device [9].

So far we can group these mobile threats as physical threats and software-based threats.

Physical threats and vulnerabilities include lost device, damaged device and stolen device or how the user use it. Physical threats have a simple resolve but very hard to put in practice. To eliminate much of this kind of threat, we need to educate ourselves and those around us that we are no longer so greedy.

Software-based threats and vulnerabilities occur at the application level, network level or device level (or OS threats) [11]. For example, at the application level, a device can be attacked through a SMS Trojan and the attacker can get money from it, or when the device it is connected to some unsecured Wi-Fi, it can leak medical results or other important data. A vulnerable Wi-Fi connection is an unencrypted one, which become a “secure” way to leak data. The point here is that exists many ways through which attackers can get from devices data like credit card details, transactions, different accounts, call logs and many others without the user’s permission in order to harm him or to use that data for personal benefits [10]. At the application level can be a more vulnerabilities like incorrect permission settings, potential functionalities that can access user personal resources and many others [9].

DOI: 10.12948/issn14531305/23.2.2019.06

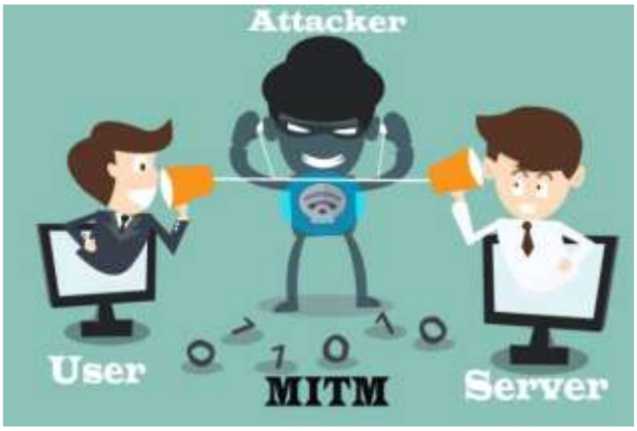

Fig. 3. Man in the Middle Attack

When we talk about threats at the network level we talk about man-in-the-middle or phishing/smishing or rogue cell tower or others. Man in the middle appear when a third entity alters a communication between other 2 entities (see Figure 3) and this usually happens through unprotected Wi-Fi hotspots [11].

Rogue cell towers is a cell tower operated by some rogue individuals who can trick the mobile devices making them believe that the tower is trusted and secured. Once the device is connected to the rogue tower they have access at the data sent via network, at SMS or calls [11].

Phishing/smishing were attacking only PC's until a year or two ago, but now they widen their targets and the number of attacks is increasing at a high speed. The users are trapped in this kind of threat when they click on untrusted and/or malicious links, pop-ups or e-mails that were spoofed as shown in Figure 4. The number of this attack is rising because the cost for the cybercriminal is low and it is very effective [11].

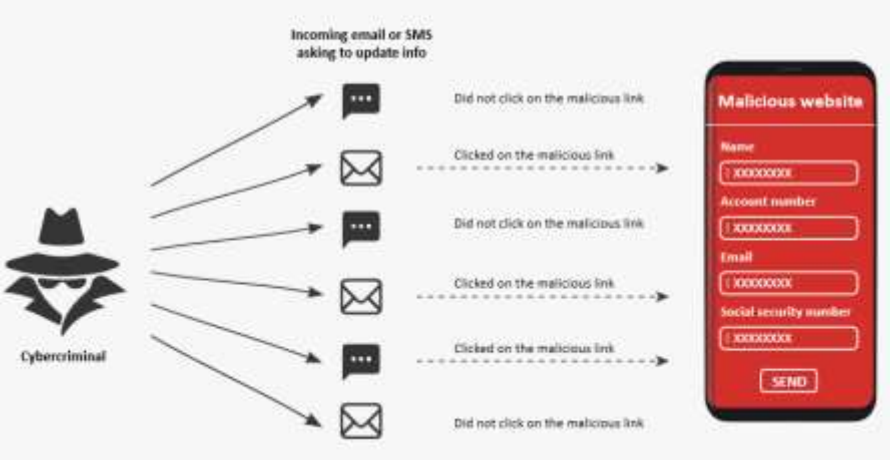
Incoming email or SMS asking to update info
Cybercriminal
Did not click on the malicious link
Clicked on the malicious link
Did not click on the malicious link
Clicked on the malicious link
Clicked on the malicious link
Did not click on the malicious link
Malicious website
Name
XXXXXXXX
Account number
XXXXXXXX
Email
XXXXXXXX
Social security number
XXXXXXXX
SEND

Fig. 4. Fishing threats [11]

At the device level we can talk about OS vulnerabilities exploit, or jailbroken device exploit or unmanaged/malicious profile or others. An unmanaged profile can lead to exposing the data through a network very easy, jailbreak will remove the device security checks and limitations and this way will ease the access to the data. OS security vulnerabilities are some holes discovered by some malicious entities which will use it for personal benefits [12]

2.2 IoT systems

An IoT system is formed from many

DOI: 10.12948/issn14531305/23.2.2019.06

components at many levels (see Figure 6), but the most important ones are sensors/devices, connectivity, data processing and user interface. The main responsibility of sensors is to collect data, data that can came in different form, from temperature to a video feed. A device can have one or more sensors which can "work" together to do more than just sense things. For example, the smartphone has a GPS sensor, an accelerometer sensor that can be used to get data about distance and speed. Now that we collected the data we have to send it to the cloud so it can be processed. The possibilities of connecting the sensors to the cloud are multiple, like via Wi-Fi, Bluetooth, cellular/satellite networks or WAN and etc., but every possibility comes with his pluses and minuses so we should choose wisely. Once the collected data gets to the cloud it need to be processed. How the data is processed depends on its type, for example if it is about temperature it only need to be read. Once the data is processed, it has to be displayed to the user. The user can be announced about modifications through triggers, alarms or any other ways [13].

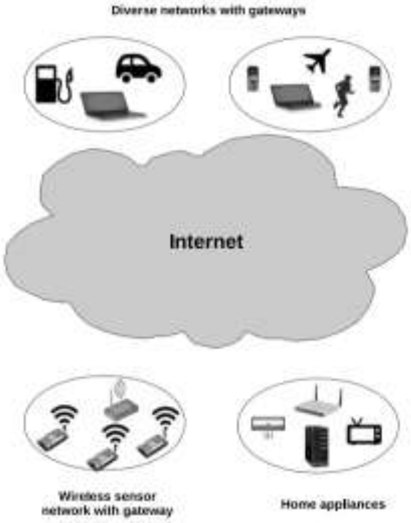
Diverse networks with gateways
Internet
Wireless sensor network with gateway
Home appliances

Fig. 6. IoT elements [14]

Based on this specific architecture of IoT systems, we could talk about three categories of security issues [14]:

- Low-level security issues
- Intermediate-level security issues
- High-level security issues

The low-level security issues occur at the hardware level and data and link layers of communication. Some of these threats are insecure initialization and insecure physical interface. The intermediate-level security issues appear at network and transport layers and affect the communication, routing and session management while the high-level security issues are mainly concerned with the applications executing on IoT [14].

3 Case Study: Android vs iOS

The Android system is more exposed to threats than iOS system because there are way more devices on Android than on iOS. Also the iOS system is built to be more restrictive and secure than the Android system. As we see in Figure 7 the rate of threats is higher on Android for all those 4 commences, as expected. Data leakage appears in both platforms, on Android with a proportion of 61% that is almost double of the proportion that appears on iOS. When we talk about network exploits the Apple platform is obviously more secure than the one from Google with only 1% of attacks compared to the 13% of the Android system, but here we must not forget the numbers of user's on those two platforms. Overall, from the figure bellow results that the iOS platform is more secure.

The software-based threats have a very high occurrence at the application level as we seen in the Figure 8.

DOI: 10.12948/issn14531305/23.2.2019.06

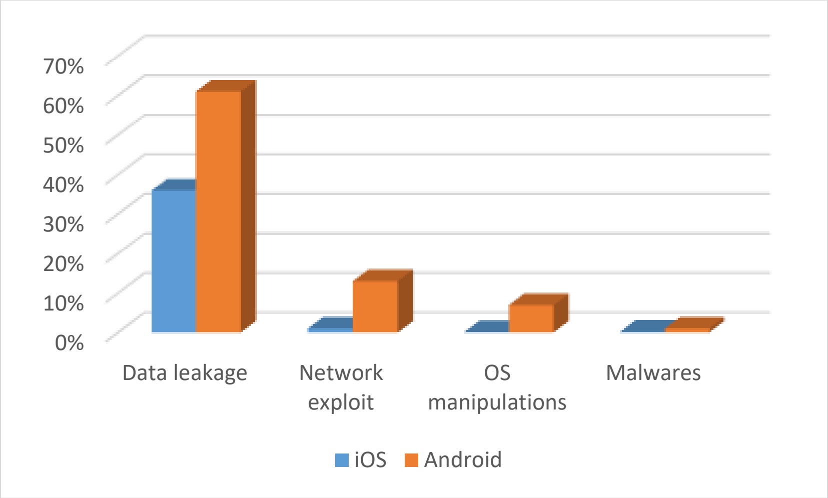

Fig. 7. Threats percentage on Android vs iOS [11]

Data exfiltration is the most common threat at the application level in the last 2 years, but let us not forgot about malwares, which even their number decreased, they are still extremely dangerous [12]. Therefore, the most harmful are the leaky applications and malwares.

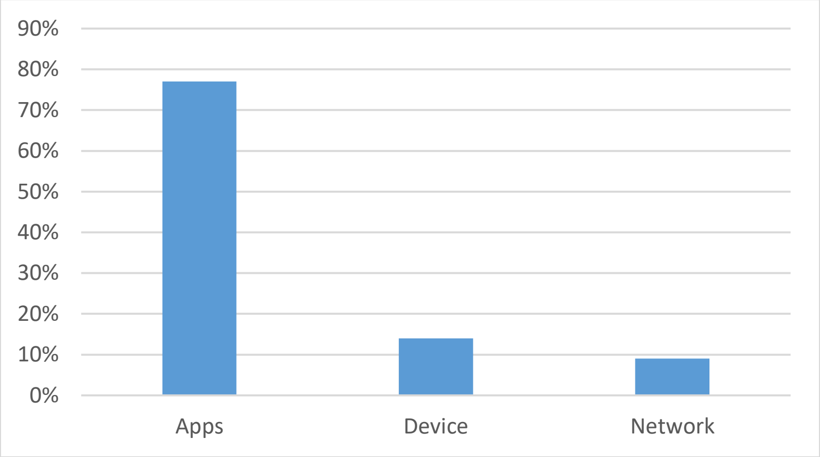

Fig. 8. The mobile attack surface [12]

Now let us see the percentage of hacks on free vs paid apps on those two platforms (see Figure 9). Despite the platform, either Android either iOS, both have allowed application that can be hacked. Again, the higher proportion of attacks is registered by the Android platform, but in this case the difference it is not big, it is 10% for the paid apps and only 5% for the free apps. It is understandable why paid apps are more attacked than the free ones; a paid app has a higher chance to contain card details or data regarding bank accounts than the others.

For example, Pegasus is a spyware discovered in an iOS system version that was used for tracking calls, collecting information from application, tracking device location, collecting passwords and other actions harmful for the user.

DOI: 10.12948/issn14531305/23.2.2019.06

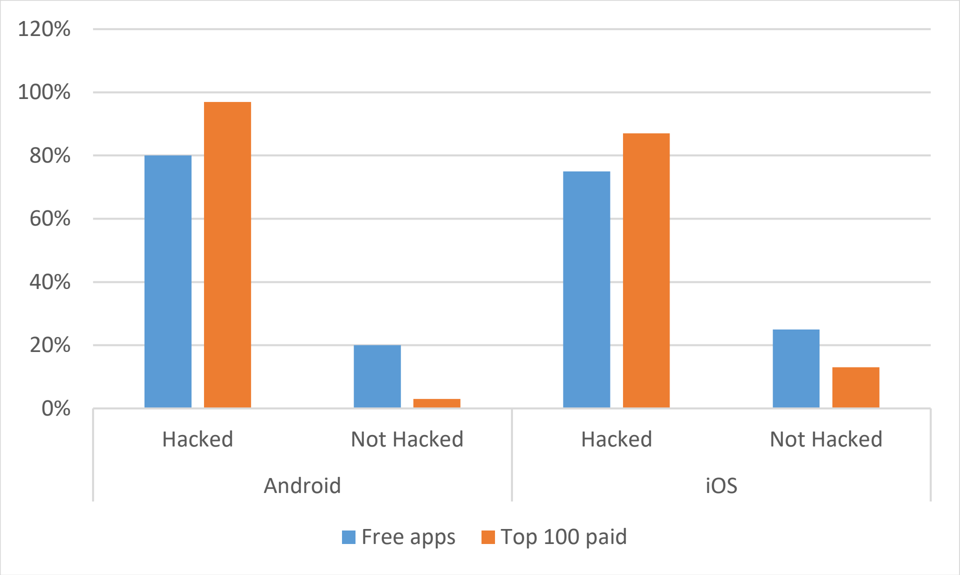

Fig. 9. Percent of hacks free vs paid apps [15]

As we seen in Figure 7 and 9 there are vulnerabilities, even if they are in different proportions still they exist, in both systems. Yes, the iOS system is rumored to be more secured than Android but it also has threats and that it is not something we as users want.

Table 1. Android vs iOS Threats comparison

Threat	Android	iOS
Accidental Data Leakage	X	X
Monetary Theft	X	X
Data Exfiltration	X	X
Network Exploit	X	X
Malwares	X	X
OS Exploits	X	X
Hardware vulnerabilities	X	X
Jailbreak		X
Hidden Root	X	

Table 1 presents some of the present threats in our days in order to see which of those two systems have or have not one of these vulnerabilities. From what we see, none of the system is threat free, and the worst part is that both are vulnerable to multiple kinds of attacks. We can say that the iOS system may be more secured than the Android system or vice versa but the real problem is that neither of them is 100% secure.

4 IoT Security Issues

The Internet of Things is a paradigm that changes the technology approach, expanding the surface of attack. IoT devices are already everywhere and for this reason the IT industry has to take account of security and confidentiality issues. A recent study by security firm Veracode has highlighted the fact that home IoT devices expose users to a wide range of threats, including data theft and sabotage, and the proliferation of IoT devices will have a major impact on human behavior. IoT devices will influence the movement of individuals in urban areas based on atmospheric parameters or traffic congestion in specific areas [16].

Unfortunately, in most cases, IoT devices have poor security protection at design stage, with the biggest concern being low perceptions of cyber threats. Cybercriminals, state-hacked hackers, and cyber-terrorists can exploit flaws in the IoT architecture and cause extensive damage to any industry. Experts estimate that the number of cyber-attacks against intelligent objects will grow rapidly in the years to come [17].

IoT enemies - means and motivation

To protect IOT devices it is important to identify the main actors of the threats and their motivations. Let's begin by analyzing the categories of attacks that threaten IoT architectures. Unfortunately, there are a lot of "bad guys" threatening to implement the paradigm, including cyber criminals, government entities, and politically motivated hackers. All of these actors are primarily interested in the huge amounts of data that IoTs administer, but we cannot underestimate the risks of cyber-sabotage attacks. Design errors on the fundamental principles of IoT securitization can expose users to sabotage, hacker attacks (eg man-in-the-middle attacks, take control of the network), data theft and misappropriation of products. Cybercriminals may be interested in stealing sensitive information managed by IoT platforms, or may be interested in compromising intelligent objects and using them in illegal activities such as attacking third entities or Bitcoin mining.

Security companies have already detected cybercriminals that use botnets made up of millions of infected IoT devices running cyber-attacks against private companies. Typically, "bad boys" infect or compromise inappropriately configured smart objects such as routers, SOHO devices, SmartTVs and other IoT devices. Similarly, Intelligence agencies are interested in exploiting intelligent devices to run large-scale espionage campaigns that use routers, game consoles, and smartphones to spy on the target people. Cybernetic terrorists and hackers may also be interested in compromising IoT devices to steal sensitive information or to cause extensive damage.

What are the main cyber threats for IoT devices?

Symantec specialists published an interesting study about the main cyber threats for IoT, grouping them into the following categories [18]:

- **Denial of service - DDoS** attacks can target all the points of a work scenario, causing serious problems in the smart grid and paralyzing the service they provide. Keep in mind that elements belonging to an IoT network are the target of attacks that interfere with the operation and communication between devices.
- **Botnets and malware** - Probably this is the most common and most dangerous scenario, IoT devices are compromised by attackers who abuse their resources. As a rule, attackers use specialized code to compromise software running on IoT devices. Malicious code can be used to infect computers used to control the smart grid or compromise software running on them. In the second scenario, attackers can exploit the presence of some firmware malfunctions running on these devices and run their arbitrary code to hijack IoT components for unplanned operation. In November 2013, Symantec experts discovered a new Linux, Linux.Darlloz worm, specifically designed to attack IoT Intel x86 devices running Linux [19]. Attackers have compromised IoT devices to build a botnet that was used for illegal activities, including sending Spam, generating costly SMS messages, or running DDoS attacks. Another possibility for attackers is to exploit improperly configured devices, for example, if you know the factory settings of a router, you may have access to its management console and modify the parameters that control its behavior.
- **Data breaches** - data breaches are another serious risk for adopting IoT devices. Organizations need to be aware of the potential unplanned consequences of IO usage situations. Attackers can spy the communications between IoT devices and collect information about the services they

DOI: 10.12948/issn14531305/23.2.2019.06

implement. Data accessed through IoT devices may be used for cyber spying purposes or by an Intelligence agency or by a private company for commercial purposes. Data breaches represent a serious threat to organizations or people using smart devices.

- **Accidental Breaches** - Data management in an architecture that includes IoT devices is a critical aspect. Sensitive information can be exposed not only to a cyber-attack but can also be exposed or lost accidentally. Symantec gives the example of transmitting the coordinates of a CEO's car, but the reality is that more sensitive information may flow from the business environment.
- **Lost perimeters** - the lack of safety measures at design stage may cause loosening of the perimeter. By exploiting a malfunction in our SmartTV, the attacker can access the home network and disable any anti-theft system implemented for physical security.

OWASP Top 10 security issues for IoT

The Open Web Application Security Project (OWASP) has as primary purpose the dissemination of best practices that will improve software security. It is natural to also analyze the top 10 security issues for this popular paradigm [20]:

1. *Unsafe web interface*: Almost any device has a webserver implemented for maintenance purposes, but in most cases the internal server interfaces are not secure. Poor authentication, CSRF, XSS, and SQL injection are the most common vulnerabilities affecting web servers.
2. *Insufficient Authentication / Authorization*: Security experts need to carefully check the adoption of strong passwords and avoid hard-coded credentials. Another aspect is checking common vulnerabilities (e.g., sqli) for authentication / authorization processes.
3. *Unsafe network services*: SSH, SFTP, and other services must be properly deployed. A common error in these situations is the hard coding of service credentials.
4. *Lack of Data Encryption*: Credentials and data must be encrypted. Adopting PKIs should help administrators implement effective information security processes.
5. *Confidentiality issues*: It is important to analyze all aspects of IoT architecture that could expose unencrypted sensitive data.
6. *Uncertain cloud interface*: IoT devices can be integrated with cloud services for data sharing. The cloud services interface must be properly deployed and designed to avoid the presence of critical vulnerabilities.
7. *Unsafe mobile interface*: Many smart devices provide a "Wireless Access Point" functionality, such as smart TVs, and a strong encryption algorithm and security best practices (such as disabling SSIDs) need to be adopted.
8. *Insufficient security configuration*: IO devices must provide the ability to configure the main security features required by security policy compliance.
9. *Software / Firmware Uncertain*: Make sure that firmware and software running on devices can be upgraded and that upgrades are done by secured processes that avoid changing / replacing. Avoid software / firmware that has hard-coded credentials and good practice is software validation by digitally signing the source code.
10. *Low Physical Security*: Check the physical security of smart devices by protecting access to all exposed ports. Usually manufacturers give external access for maintenance purposes. An attacker can exploit one of these access points to inject malicious code, filter data, or sabotage the smart object. It is suggested to encrypt data stored in the device's memory and physically protect USB ports and any other port by disabling unnecessary access.

Attack scenarios

Security firms have seen an escalation of cyber-attacks against global IoT devices. The most common scenario is the use of botnets made up of thousands of IoT devices which are used to send spam messages or to coordinate DDoS attacks. Summing up a thingbot can be used to:

- send spam.
- to coordinate an attack on a critical infrastructure.
- to provide malware.
- function as a point of entry into a company's network.

The main security firms confirm an increase in the number of attacks against smart objects, including routers, SmartTVs, devices. NAS (network-attached storage), game consoles and various types of set-top boxes. One of the first large-scale attacks was reported by Symantec researchers in November 2013 when a worm called Linux.Darlloz infected many of the Intel x86 devices running Linux by exploiting the various vulnerabilities in PHP [19]. The worm has been able to compromise home-based x86-powered home kits, exploit and extend the infection. Malicious code has compromised global network equipment, as described by Symantec in a detailed report. Although the worm has been designed to compromise Linux-powered x86 devices, Symantec experts have found that there is also a Darlloz compiled to run on ARM and MIPS devices. Darlloz managed to spread quietly and partially delete files stored on IoT devices.

The attack technique was simple and efficient, the malicious code generated random IP addresses and tried to use credentials commonly used to log in to target machines. If the malware identifies a vulnerable device, it accesses and downloads the worms from a server. Once the IoT device was infected, the malware started looking for other targets by running a web server and PHP [19].

5 Attack types

Malware is a type of software designed intentionally to damage or infect a computer, and / or damage or infiltration across computer networks without the consent of the owner [21]. The notion is generally used by computer scientists to designate any hostile, intrusive, or troublesome form of software or program code. Malware varies depending on their purpose, how they infect a computer, how it is repeated, and the security or security risks it presents. Malware is present in all Windows, Mac OS, Unix-like, Linux or Android operating systems. Windows is still the main operating system for most users and will therefore always be the main target for malware [22]. Harmful software damages after it is implanted or introduced in some way into a target computer and can take the form of executables, scripts, active content, and other software. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware and scareware among other terms. Malware has a malicious intention, acting against the interest of the computer user - and thus does not include software that causes unintended damage due to deficiencies, which is usually a software bug. Almost every malware threat has the ability to block legitimate security software. In addition, they can update themselves to download additional malware or cause breaches in the security of the affected system.

Ransomware is malicious software that, when installed on the victim's device (computer, smartphone), encrypts the victim's data by holding them "hostage" or blackmailing the victim, who threatens to publish his data if he does not pay a “ransom”. Most of the time, the ransomware fools the victim, telling him that there has been illegal activity on the device and that he has to pay a sum of money. In most cases, when the victim has paid the requested amount, the victim has not escaped the ransomware. WannaCry Ransomware infects devices based on the vulnerability of SMBv1. If your computer has SMBv2 or SMBv3 enabled, Wanna Cry cannot attack.

A DoS-type cyber-attack (from Denial of Service) or ***DDoS*** (Distributed Denial of Service) is a fraudulent attempt to disable or block the resources of a computer. Although the means and the goals to perform this attack are very diverse, generally this attack is the effect of intense efforts by one (or more) people to prevent a website or Internet services from functioning efficiently, temporarily or unlimited. The authors of these attacks typically target sites or services hosted on high-demand servers, such as banks, credit card gateways, and even servers in their entirety.

A traditional attack method causes the target computer to "saturate" with external communication requests so that it can no longer respond to legitimate Internet traffic or even become unavailable. In general terms, DoS attacks are carried out in several ways:

- causing a forced reset of computers,
- consuming the available resources of a server so that it can no longer provide services,
- blocking communications between well-intentioned users and the victim's computer so that they can no longer communicate properly.

Denial of Service attacks are considered Internet Architecture Board (IAB) violations of the Internet's Right Internet Usage Policy. These attacks are also often violations of the law in that country. There are two main types of attack: via wired networks and wireless wired networks.

Attacks through wired networks require a lot of computing power, sometimes the distribution method is also available. Attacks on this type of network do not require additional network cards and do not even need a broadband connection. Attacks over wireless networks require advanced network cards and usually high performance external antennas to increase their broadcasting power and coverage. Attacks on virtual private servers at short VPS, it requires a special script.

A botnet is a computer network that, being infected with malware, is interconnected, and as soon as there is an Internet connection, it can react to the remote controls of cyber attackers. Independent computers are known as bots or zombies. The Internet connection and local resources of infected computers are used by cybercriminals for a variety of purposes without the knowledge of the computer owner. In this way, a private computer can be used to send undetected spam, but a DDoS attack or a scam attack can also be executed in order to access personal information and passwords. Botnet network operators aim to capture as many computers as possible to increase the number of available resources. The botnet network self-sustains and grows by spreading malware and infecting other computers. It is estimated that up to a quarter of computers in the world are part of a botnet network. Germany is in the top 10 because it has good Internet infrastructure available. Botnet networks act as a basis for Internet crime and are one of the biggest sources of illegal Internet revenue [23].

Phishing is a form of criminal activity that involves obtaining confidential data such as access data for banking applications, e-commerce applications (such as eBay or PayPal), or credit card information using manipulation techniques identity data of a person or an institution. An electronic fraud is typically the sending of an electronic message by the attacker using instant messaging or telephone programs where the user is advised to give confidential data to win certain prizes or is informed that they are due to technical errors that led to the loss of original data. The e-mail is usually also indicated by a web address that contains a clone of the financial institution's website or trading website. Most phishers use this method to get bank data.

6 Conclusion

Mobile threats appear in many ways, because of different reasons, reasons according with each platform or system either Android, or iOS or IoT or other system. It is important to know what they do and how they appear so we can find ways to prevent them or as the last instance to destroy them if possible. We discussed about a classification on multiple layers and from two points of view, the physical one and the system-based one. We how this threats attack, but I think we should go this research to the smallest level possible. This classification can be taken to an even more granular level for each system. This will be a subject for future work along with analyses regarding some of the most critical threats. It has been exposed how the IoT devices can make human lives easier and in the same time harder if their security is weak.

It was presented a top 10 security issues that affect these devices and also five types of attacks which can happen to smartphones.

Acknowledgements
Parts of this research have been published in the Proceedings of the 18th International Conference on Informatics in Economy, IE 2019 [10].

References

[1] I. Adascalitei and M. I. C. Baltoi, "The influence of Augmented Reality in Construction and Integration into Smart City," Informatica Economica, vol. 22, no. 2, pp. 55-67, 2018.

[2] M. Bishop, Introduction to computer security, Boston: Pearson Education, Inc, 2004.

[3] S. Watts, "https://www.bmc.com," bmc, 21 June 2017. [Online]. Available: https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/. [Accessed 12 March 2019].

[4] Statista, "https://www.statista.com," Statista, 2008. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed 26 February 2019].

[5] P. Abhishek and W. Zhiwei, "Introduction to the Special Section on Challanges and Solutions in Mobile Systems Security," Computers & Electrical Engineering, no. 59, pp. 201-203, 2017.

[6] R. Margaret, R. Linda, S. Sharon and W. Ivy, "https://internetofthingsagenda.techtarget.com," IoTAgenda, 2016. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed 26 February 2019].

[7] F. Stroud, "https://www.webopedia.com," Webopedia, [Online]. Available: https://www.webopedia.com/TERM/M/mobile_security_threats.html. [Accessed 228 February 2019].

[8] R. Paul and F. Jon , "Cyber Threats to Mobile Phones," Carnegie Mellon University, Pittsburgh, 2011.

[9] L. G. Wlosinski, "Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous," *ISACA*, vol. 4, no. 1, pp. 1-5, 2016.

[10] I. Adascalitei, "Mobile systems security," in *The 18th International Conference of Informatics in Economy*, Bucharest, 2019.

[11] Pradeo Lab, "iOS Security Report," Pradeo, 2018.

[12] Pradeo Lab, "Mobile threat report," Pradeo, 2018.

[13] Dataflair team, "https://data-flair.training," Dataflair team, 1 June 2018. [Online]. Available: https://data-flair.training/blogs/how-iot-works/. [Accessed 8 April 2019].

[14] A. K. Minhaj and S. Khaled, "IoT security: Review, blockchain solutions and open challenges,*" Future Generation Computer Systems*, no. 82, pp. 395-411, 2018.

[15] N. Agarwal, "Android vs iOS: Which Platform is More Secure in 2018," 1 February 2018. [Online]. Available: https://appinventiv.com/blog/android-vs-ios-which-platform-is-more-secure-in-2018. [Accessed 25 March 2019].

[16] P. Paganini, "https://www.veracode.com," Veracode, 30 July 2015. [Online]. Available: https://www.veracode.com/blog/2015/06/smart-devices-pose-many-challenges-iot-security-your-company-challenge-sw. [Accessed 20 June 2019].

[17] T. Dr. Hugh and T. Steve , "https://www.symantec.com," Symantec, November 28 2018. [Online]. Available: https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond. [25 March 2019].

[18] Symantec, "Internet Security Threat Report," Symantec, 2019.

[19] P. Paganini, "https://www.cyberdefensemagazine.com," Cyberdefensemagazine, 20 November 2013. [Online]. Available:

DOI: 10.12948/issn14531305/23.2.2019.06

https://www.cyberdefensemagazine.com/internet-of-things-symantec-has-discovered-a-new-linux-worm/. [Accessed 25 March 2019].

[20] OWASP, "Internet of Things Top Ten OWASP," 2014.

[21] Avira, "https://www.avira.com," Avira, [Online]. Available: https://www.avira.com/en/support-about-malware. [Accessed 25 March 2019].

[22] A. ZACKS, "https://www.safetydetective.com," SafetyDetective, 28 October 2018. [Online]. Available: https://www.safetydetective.com/blog/malware-statistics/. [Accessed 25 March 2019].

[23] botfree, "http://www.botfree.ro," botfree, [Online]. Available: http://www.botfree.ro/inform.html. [Accessed 20 June 2019].

[24] B. Heater, "https://techcrunch.com," TechCrunch, 2016. [Online]. Available: https://techcrunch.com/2016/06/09/lenovo-smart-shoes/?guccounter=1. [Accessed 26 February 2019].

[25] Pradeo Lab, "Mobile Security Report," Pradeo, 2019.

Ioan ADĂSCĂLIȚEI is a PhD Student at the Economic Informatics Doctoral School and his theme is “Security of mobile-based systems”. Currently he is Android Programmer at mReady. He is interested in Mobile Development, including Android and iOS and mobile Security.

DOI: 10.12948/issn14531305/23.2.2019.06