Vulnerabilities in Mobile Devices

Sulaiman Al amro *samro@qu.edu.sa*
Computer Science (CS) Department
Qassim University,
Buraydah, Qassim, 51452, KSA

Abstract

Mobile devices are no longer just dedicated communication devices and have even exceeded the limits of such, and have become an essential part of our life; they are indispensable. It is through the memory that you can store images and videos and can also connect to social networking; it can also be played by linking to bank accounts. However, we must bear in mind that there are people in this world who are trying, day and night, to get to your private information, to steal from you and either exploit the user or simply to steal his/her money. These people are called hackers, as will be named through our topic for today. We will put in your hands the most important points that make sure that he is spying on your mobile and the mobile penetrative. The biggest obstacle to these investigators, whether spies or hackers' encryption is "full device encryption" or "full data" to be encrypted, and here we must distinguish between the two things, not confusing them. This paper will explain the vulnerabilities of mobile devices and how they can be avoided.

Keywords: Mobile Devices, Vulnerabilities, Encryption, Operating Systems, Applications.

1. INTRODUCTION

Smartphones today are no longer just devices to conduct cross-GSM networks calls, but are considered "a treasure trove of information" and gold mines for hackers, security agencies and intelligence services, as well as for criminal investigations into the Interior Ministries of the world's departments, so the mobile phone has become the first thing that investigators will "confiscate"; then they start diving into the depths, not so as to pass a few hours, but the accused has become naked from the digital side; everything has been revealed and all the evidence has been classified. is no longer for its hardness and undeniable sense of concern .. and will collapse rapidly as soon as the development of digital ones on the table and face the evidence.

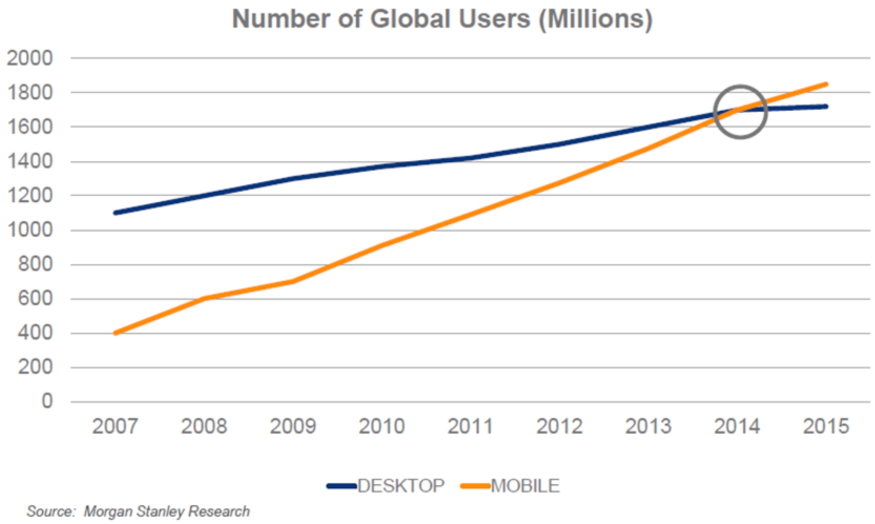
Investigators used advanced tools to extract information from Android Android devices and the iPhone, BlackBerry, Nokia and others, and most of these programs are only sold to the forces of law enforcement LE interior ministries and defence, some of which is sold to centres for criminal investigations, such as companies, including the Saybrkov company that provides criminal investigations into the crimes of computer service companies and institutions, to detect and analyse successful and failed attempts to hack.

However, not only the security agencies and investigators are keen to have access to your computer, but hackers and spies are also targeting devices to deploy spyware and viruses, not only by forged links and sites, but also through direct access to the device and by planting espionage applications inside, and it does not take them even five private minutes to do it, with the advent of "flash memory" with two entrances, USB and MicroUSB, where it is easy to store any malicious APK, then plant the device quickly and without the knowledge of its owner, especially for Android devices, and does so often in shops for mobile phones and maintenance, which is very dangerous [4].

The security and intelligence agencies also do the same thing in "black bags", especially when monitoring "the suspect" who is cautious in his movements and public in his calls, so they resort to breaking into homes in the absence of their owners, or deceive the suspect in any way in order to gain access to his computer, even for just a few minutes.

2. MOBILE TECHNOLOGY

Next is the natural evolution of smartphones as personal computers, which have contributed significantly to the popularity of these devices being cut after decades of dominance, and pushing the development of tablet PCs, which is a compromise between a smartphone and a personal computer. A smartphone differs from a traditional phone in that it provides a number of functions and advanced computing capabilities, as well as advanced communication, along with other traditional phone functions.The integration of the first smartphones was between traditional phone capabilities and the benefits of other popular consumer devices, such as a personal digital assistant (PDA), media player, digital camera and the global positioning system (GPS). According to Morgan Stanley Research, in 2015, the number of global mobile users exceeded the number of global desktop users by almost 200 million and this trend is increasing, as shown in Figure 1.



Source: Morgan Stanley Research

FIGURE 1: Number of Global User [10].

The current smartphones support more advanced additional features, such as touchscreens resistant to scratches, compact cameras and high-resolution imaging; we have begun to see smartphones with cameras which are, more precisely, 16 Megapixels, twenty Megapixels and some have the unprecedented accuracy of 41 Megapixels, like camera Nokia 808. Smartphones have features, as well as being strong with equipment, such as bilateral and Quartet processor cores, so we can find smartphones with processors of eight cores, as well as smartphones which include special processors for graphics which allow for the operation of three-dimensional games, when RAM is sufficient and there is an area of suitable storage [3].

Besides this gear, most smartphones are characterized by the possibility of downloading many third-party applications online, like private gaming applications that will attract many smartphone users. It must also be that smartphones are supported by many wireless communication capabilities, such as "Wi-Fi" that allows the phone user to surf the Internet, and the technology, "Bluetooth," which allows him to communicate with other phones and share files, and technology "NFC" that allows file sharing with another phone that supports the technology, once there is communication between them, along with GPS.

However, the highlight is what should be enjoyed by the ease with which it must be offered for use in communicating with others and sharing whatever he wants with them via the many social networking services, such as Facebook and Twitter, YouTube, Instagram and others. A set of traditional phones to the Finnish company Nokia (Getty). Besides those qualities, the smartphone is able to work as a reader to write a letter, especially after becoming relatively large in the measurements of those phone screens, and also being capable of recording video at high resolution and reviewing images in an attractive way.

The smartphone is also characterized by its ability to share its screen with larger screens, such as high-definition TVs, or computers and tablet PCs, as well as the ability to exchange files between it and personal computers and work being synchronized between them. Although there is significant progress in the field of smartphones and cloud services, it has become imperative for any smartphone these days to have the potential to work with synchronised media files being saved upon it with the user's account in the cloud’s storage services, as well as wireless printing to printers that support this feature.

Smartphones evolve day after day, with their capacities and capabilities increasing spectacularly, becoming some of those phones that use fingerprints, for example, as a kind of safety net to lift the phone lock (as in iPhone mobile 5 S, Galaxy S5, HTC One (M-8), and others), and, as used by some, eye tracking movements to surf Internet technologies or review images with the Once aerobic pointing hand. In contrast to all of this, the traditional phone leads in the main goal, which was to be designed to make phone calls and send text messages, with a limited capacity in the potential of photography and the sharing of files via Bluetooth; this class of phones gradually began disappearing with the advent of smartphones from the world-class being integrated with some of the advantages of the previous top tier phones. Also, the lead giants of the Google cross-operating system "Android" and Apple over the "EOS" system smartphone operating system have the market share of up to about 90% in the world, followed by a run of other enterprise systems, such as the system "Windows Phone," Microsoft Corporation of America and the system of "BlackBerry " by the Canadian company, BlackBerry.

3. DISCUSSION

3.1 Sim Cards

It was announced by researchers that the security and protection of the discovery of a very serious loophole in some telecom SIM cards allows for the penetration of phones and access to important information and control, such calls; within two minutes, just by sending two letters by SMS consecutively contains some information on it from the telecommunications company to the reverse action in a breakthrough key code length 56-bit, which encrypts the DES type (data encryption standard data encryption standard), with the knowledge that the process needs to hack a normal computer [5]. The reason for the gap is a continuation in some of the companies in the use of SIM cards which operate legacy encryption system 56 along the bit a DES. This standard has existed since 1977 and has been used for a long time in the Telecom mobile GSM until it was replaced by algorithms of the latest encryption, such as AES in some companies, but more information Read DES data encryption is standard.

According to [6], the DES encryption that uses the first two types is the normal standard DES. This exhibition of penetration by this gap could lead to a breakthrough in more than 750 million devices, and Type II Triple DES in any standard triple data encryption will be stronger on the grounds that it is later than the normal Ohz, the updated N encryption, to penetrate this gap. However, tinkering with this loophole should replace the cards that use standard DES encryption, by telecommunication companies, as well as media companies. SIM cards that work on the latest algorithms are working on longer encryption keys to make encrypting harder to break through. Finally, gaps in operating systems, such as loopholes which have been discovered in the Android or other smart-phone operating systems are not the only ones that lead to hacking. The gap in some contact SIM cards may be of greater risk because they do not differ between a smartphone or an ordinary phone because the SIM card contacts were originally infected and vulnerable to penetration, regardless of the operating system.

3.2 Vulnerabilities in Mobile Operating Systems

Serious loopholes in the regulations were detected in "Apple" Mac computers and iOS systems for mobiles and tablets and this gap may make them vulnerable to any breach of the company's security apparatus after skipping tests. This was revealed by a security researcher from the company "SentinelOne" Vilosa [7], who pointed out that this loophole enables the modification of the power of the mobile, in addition to skipping all the security tests, except for the possibility of the establishment code damaging the machine and thus will not be back to the user who can control it. Vilosa has been able to penetrate the SIP protection of a safety feature which sets out the powers of the user account access to certain sensitive areas in the system, and this loophole has been exploited by programs that use the powers of the user account, in order to do some updates on the button of the mobile system. He informed Vilosa "Apple" of this gap and said that the intelligence agencies and security forces may have used them before; here it is referred to that Apple has released an update to close this gap in the system iOS 9.3 and Mac OS X El Capitan, 10.11.4.

New research from NowSecure [8] pointed to a critical flaw in Samsung devices, which could put an estimated $600 million of its organs at risk of the penetration process in simple piracy.This is not the first time that there have been news' reports of security flaws in Samsung devices this year, but this imbalance may be considered one of the most serious problems faced by the company, due to the porosity of the machine on the way. The NowSecure company explained that the gap exists when applying the keyboard SwiftKey, which comes preinstalled on the set of the Samsung smartphones which have been launched over the last few years. The security company revealed that the phone models affected were Vulnerability "Galaxy S 6", put forward by Samsung this year, in addition to "the Galaxy S 5" phones. He spoke of the Ooualemhklh gap in the virtual keyboard SwiftKey when examining the new languages; this may result in mobile penetration and create a connection between him and the penetrator. In turn, the SwiftKey company issued a statement stating that the gap exists only in versions with pre-installed Samsung Galaxy phones, stressing that their applications, which are available on my shop, "Google Play" and "App Store", are devoid of this gap.

The NowSecure security company reported that there is a dangerous loophole, allowing the hackers to penetrate phones remotely, without the user's knowledge, where they can target the phones when they relate to public Wi-Fi networks, or through malicious updates. Hackers can and after the injury phone user control over some of the internal components, such as the camera or microphone, or install malicious applications without the user's knowledge, or eavesdrop on calls and read messages. The security company confirmed that the flaw also allows hackers, after penetrating the phone, access to basic information about the user, such as images, messages and personal information stored on his computer. NowSecure stressed that what is a more serious flaw is the lack of the user's ability to delete infected panel application keys, even though it is Mstamla by default in the machine. The company informed Google and Samsung Vulnerability, and the latter provided some telecom operators to dissolve it, but NowSecure noticed they have not put this update out to users yet. Samsung has commented on this matter; an update will be issued via the "Samsung Knox" for all users and all devices in the coming period of services [8].

A loophole in the program is placed in a smartphone to allow control and to remotely manage the device by the service provider or device manufacturer, as revealed by the research presented at the sixth month of August through being dedicated to data security in the city of Las Vegas's "Black Hat" conference. Since the disclosure of the program, Prism, and eavesdropping and spying widespread carried out by "US National Security Agency", as well as various information about the countries with monitoring and spying on smartphones, the subject of smartphone mobile security is one of the leading topics of concern for information security experts researching in their search to bridge the rear doors of confidential information in the software and handsets that allow intelligence agencies to eavesdrop on calls and monitor the data in those devices.

In this context, revealed by both Matthew and Mark Sulenak Blanchot [2], two researchers at the Information Security Laboratory Accuvant Labs, the existence of a gap in the smartphone features of more than two billion smartphones in the world are at risk of breaking-in and piracy. The reason for this gap is the program established by the smartphone service provider or phone manufacturer in the device to allow it to be controlled and administered remotely. These weaknesses were unveiled through the work of the famous "Black Hat" conferences held in several cities around the world, including Las Vegas, where the researchers showed how to exploit the weakness of this tool and pointed out that it requires accurate and in-depth knowledge of the work of the cellular network and Maiarmenzmh Open Mobile Alliance, which means to adjust the open standards for the mobile phone industry and therefore the ability to use a cellular transmitter fake Rogue Base Station or Femtocell device which devices use to strengthen Send, a cellular phone network in the home, where the network is difficult to pick up signals.

After the experiments which lasted two months, Sulenak Matthew and Mark Blanchot were able to detect and exploit this loophole in the software provided by the company Red Bend Software; this is a program that is installed in more than 70 to 90 percent of the world's smartphones. Note that some manufacturers of smartphones are developing this tool by cable and secret doors. This tool allows the service providers’ devices to be remotely managed and exploited; for example, to publish updates or prevent the machine from working on certain cellular networks or adjusting smartphone settings to serve the “Roaming” for use outside the country of the user, to establish or adjust the volume service settings through wireless connectivity Wi-Fi Voice - over WiFi - and there is a large group of jobs added by the service provider to meet the requirements of the services performed by sackcloth remote data or restore factory settings, or change the definition of a PIN code or identify the wireless networks nearby and other things, such as transferring phone calls or activating and deactivating certain applications.

Detection Test, as well as Matthew and Mark Sulenak Blanchot, reported that some systems can monitor the main page browsing program and, in some cases, the extraction of the list of contacts. Sulenak revealed that shortcut numbers added by the service provider to facilitate contact of its services, can also be used for programming the launch of certain applications and all this without the user's knowledge. Remote control of this tool authorises all the privileges to control smartphones, posing a significant risk in the event that the pirates take control; it opens the doors to all the possibilities of piracy, to install malicious programs, eavesdropping and carrying out extortion threats to data privacy and information critical to people and also to institutions. So the company, Red Bend Software, updated their tools to bridge this gap; many of the service providers have not yet installed this in the phones of their clients. The experts determined that the operating systems Android and BlackBerry are most vulnerable to this gap. As for your iPhone, when you are using Apple's tool developed by the customers themselves, the American service provider Sprint can be exposed to this gap, in cases where they do not update the operating system to the latest version [2].

Experts have not yet studied Windows’ Phone system to make sure of the existence of this vulnerability in Microsoft's systems. Experts pointed out in their report that the Blackberry Z10 and HTC ONE M7 are the devices most susceptible to the risk of breaking through by this tool. Given the gravity of this gap and the possibility of exploiting this loophole by pirates, some providers of phone service system code and systems provide safer added. However, the expert Accurant Labs were able to breach all the protection systems but Matthew and Mark Sulenak Blanchot emphasised that, so far, they have not been exploiting this loophole. It is important to make Smartphone users aware of the need to review their service providers on this issue and carry out renovations on their phones’ systems quickly and periodically.

3.3 Stagefright

Zimperium Team [9] has revealed specialised studies on digital protection on portable devices’ companies, for a serious loophole called “Stagefright” and it’s described by experts as the most serious loophole in the history of mobile phones. The gap is present in the vast majority of Android phones and is exploited by sending videos via MMS containing malicious software running on the phone without the user's knowledge, which implements things like turning on the camera and microphone in the phone to spy on the user. Worse is that the user does not even need to put pressure on the video or view it in order to activate the gap on his phone, but it could not carry out the attack upon the arrival of the MMS message to a phone without the user even knowing of their arrival and being unnoticed. Google has already begun sending an update to the official Nexus series of phones to repair the gap, and the rest of the companies will send a similar renovation to its phones in the coming days but until then, receiving updates on a mobile phone, you can now be sure of its existence in your phone and protect yourself from them.

First of all, you can be sure of its existence in the phone by downloading the application “Stagefright Detector App” from the PlayStation Store and play it. This application is developed by Zimperium, the same company that discovered the flaw, which unfortunately does not close the gap in your phone, but his mission is only to alert of the presence of the gap. After running the application, it will scan your phone and inform you of the existence of the gap or not. The biggest possibility is that the gap exists and will have actually learned through the colour red warning message that bears the word “Vulnerable” which will appear to you after the screening process is finished.

However, do not worry; there is an easy trick you can follow to protect your phone from the gap, which requires disabling the automatic downloading of multimedia messaging and MMS messages from the application that you use in your phone settings. In this case, even with a malicious link in an MMS message, your phone will not automatically be injured. They can get to your phone only if you download the video and watch it manually, so we do not advise you to download any video via an MMS received, even if the letter is from your hand, on a reliable connection, so only until your phone receives an update that resolves the problem. To stop the automatic download feature for multimedia messages is a very easy process, but varies according to the messaging application that you use in your phone. In general, you will need to log in to the application settings and search for MMS and disable the automatic download setting for multimedia messages’ option; the option name varies, depending upon the application, according to your language, which can sometimes be called "automatic recovery for multimedia messages" or "auto-loading".

3.4 Full disk encryption

It is known that Android’s own company Google platform has adopted a number of encryption system features as well as on the devices. In recent years, there has been a significant improvement in a lot of things that are still far from perfect; security researcher, Gal Beniamini, made the discovery of a new security flaw which the property Full Disk Encryption is prone to break through [1]. Gal Beniamini added that this gap affects hundreds of millions of Android devices, but the real surprise is that the devices that use Qualcomm processors are the most vulnerable. It is clear that the source of this new vulnerability that has been discovered is that there are a lot of flaws in the system kernel “Android kernel” and “chips Qualcomm”, so any smartphone running Android 5.0 or onwards, and which use encryption full part property (full disk encryption), are more vulnerable to penetration and, what makes the situation even worse, is that each of the two Google and Qualcomm have issued to address this problem before. It came in the Beniamini report that there are still some gaps that are to be fixed without new hardware.

It is known that encryption, like full feature disk encryption, is the property that you can save all data on the device safely and make this data unreadable without special encryption and unique entry. It is worth mentioning here that it is the basis of the legal battle between Apple and the Federal Bureau of Investigation (FBI), because Apple made it impossible for anyone to access the user encryption keys except for the company itself, but Beniamini said that, regretfully on the android system, this feature does not include full safety and possibly came through a security hole for the attackers to penetrate clients’ data with ease. It is worth mentioning here that Beniamini is working with Google Inc. and Qualcomm to find a solution, and it is still highly unlikely that hackers exploit these vulnerabilities for most Android users because hackers still need to enter a password, otherwise the encryption key here is not working. The importance of knowing this news lies in the fact that the full disk encryption feature on the Android system is not quite as secure as a lot of users think, and also, in order to avoid companies manufacturing processors which repeat these errors and defects again.

4. RECOMMENDATIONS

4.1 Encryption

The biggest obstacle to these investigators, whether spies or hackers, encryption is "full device encryption" or "full data" which will be encrypted, and here we must distinguish between the two things which are often confused, namely:

1. Protected with a password Password Protection
2- Data Encryption Data Encryption

The former is just a "thin layer" of protection which can stop a person from entering content, such as placing a secret number for the Android or Windows' system but which can be circumvented by them and then bypassing the PIN number, or delivering targeted particularly to a device so a criminal investigation can upload data directly, even without knowing the PIN. The use of "data encryption" by Data Encryption, by contrast, is data which is itself encrypted and cannot be read, even if it was to circumvent and overcome the PIN and was not "broken" or taken by a copy image of the encrypted device's content. The data can be read and analysed, but knowing the encryption key and long, and kind. Here we will explain how to do encryption for both iPhone or Android so that all the information will be encrypted, secure and very difficult to withdraw or analyse, especially with the access "physicist" of the device and attempt to inspect its contents or analysis. However, the same device must also be protected, otherwise you will not benefit if the encryption is on the device or an espionage virus program as well.

4.1.1 Encryption for iPhone Devices

An advantage enjoyed by the iPhone devices is a special encryption chip; each device has an "Encryption Chip". It is through keeping an encryption certificate and key to your encryption, through which you can access the entire contents of your device's encryption; when you delete or destroy this key, you will not be able to access data, and this certification "encryption key" is the device that makes the data unreadable after you enter the PIN number.

4.1.2 Encryption in Android devices

Android devices do not enjoy encryption. Default is not an independent chip encryption; as in Allaifun, encryption which is optional and was previously unknown can cause slowness in the machine, but in modern appliances, and evolution, has become so that it does not affect the performance of the device at hand. In this section, we will explain how to activate the full data encryption feature with some important security tips for each user. Note: The preferred back-up for your device, before you begin the process of one of the famous encryption solutions, is such as Titanium Backup.

4.2 Applications for mobile phone security

There are many applications available that help protect your mobile phone devices, such as those that are used to protect computers, but no program can close all the loopholes and threats to these phones. If you are new to using mobile phones, you can start using the application Sophos Sophos which is free and available for phones that run the Android operating system. This application contains a number of tools that protect the information in the phone, as in checking for viruses and malicious files, and tools that give tips on how to protect your data and your privacy. After downloading this application and the inauguration through Google App Store (Google Play Store), or if the site is blocked, we can download the application from here. After running, the application will appear on four optional screens that will describe it separately.

5. CONCLUSION AND FUTURE RESEARCH

The time that used to be, when the use of mobile phones was just to make voice calls, are long over, and have been replaced by smartphones, which have turned into small computers during the past few years, and for many people these devices are becoming their basic access to the Internet gateway. However, because of the suddenness of this development, the subject of the safety of these devices is not taken seriously, to the same extent that is being dealt with by security devices. Discovering the occasional new security flaws in the operation of various smartphone systems, this is very normal in the world of technology and software by virtue of the presence of a 100% secure product which can be considered, as they are copied from fiction in general. Once, the talk about new loopholes even began to start panicking attacks for a limited period of time, ending with a screening device, making sure that it is free from the exploitation of a loophole, or with the release of a new update to the operating system. It remains the most important question; what is the party that stands behind this gap? Discovering the gap is usually associated with the discovery of security or the institutions of views has exploited for a long period of time without telling one. Strangely enough, also those actors are dying to talk about it after a period of time, as if nothing had happened. This paper has explained the vulnerabilities in mobile devices and how they can be avoided.

Future work would collect and analyze a number of mobile devices with different operating systems installed on them. After that, it will start the second phase to revise and validate a framework by comparing these mobile devices.

6. REFERENCES

[1] Westlake, A., (2016). Qualcomm-powered Android devices found to have faulty full disk encryption. Retrieved Feb 28, 2017 from https://www.slashgear.com/qualcomm-powered-android-devices-found-to-have-faulty-full-disk-encryption-02446903/ .

[2] Solnik, M. and Blanchou, M., (2014). Cellular exploitation on a global scale: The rise and fall of the control protocol. Black Hat USA. Vancouver.

[3] Goggin, G., (2012). Cell phone culture: Mobile technology in everyday life. Routledge.

[4] Doherty, J., (2014). Wireless and mobile device security. Jones & Bartlett .

[5] Oteri, O.M., Kibet, L.P. and Ndung'u Edward, N., (2015). Mobile subscription, penetration and coverage trends in Kenya's telecommunication sector. (IJARAI) International Journal of Advanced Research in Artificial Intelligence.

[6] Duckett, C., (2015). DES encryption leaves SIM cards vulnerable to exploitation. Retrieved Nov., 12, 2016, from http://www.zdnet.com/article/des-encryption-leaves-sim-cards-vulnerable-to-exploitation/

[7] Vilaça, P., (2015). A loophole in "Apple" Mac computers and iOS system. Retrieved Mar. 22, 2016, from https://sentinelone.com/events/sentinelone-apple-security-expert-to-present-at-syscan360/

[8] NowSecure, (2015). Samsung keyboard security risk disclosed: Over 600M+ devices worldwide impacted. Retrieved Dec. 13, 2016, from https://www.nowsecure.com/blog/2015/06/16/samsung-keyboard-security-risk-disclosed-600m-devices-worldwide-impacted/.

[9] Zimperium Team, (2015). Experts found a unicorn in the heart of android. Retrieved Oct. 6, 2016, from https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/ .

[10] Stanley, M., (2009). The mobile internet report. Morgan Stanley research. Retrieved Dec. 13, 2015, from http://www.morganstanley.com/institutional/techresearch/pdfs/mobile_internet_report.pdf.