Mobile Systems and Corresponding Intractable Security Issues

23

23.1 Introduction

In the previous two chapters, 18 and 19, we dealt with wireless communication but restricted our discussion to sensor networks, wireless communication networks, and cellular networks. We discussed a good number of communication devices and their communication protocols. We also discussed the security problems and we propose solutions in some cases. What we did not do is actually put all these devices and technologies together to create the current phenomenal mobile communication devices, and the technology is currently driving computing and communication. We are going to do this in this chapter and more. The last two decades have witnessed a revolution of sorts in communication spearheaded by the rapidly evolving technologies in both software and hardware. A mobile communication system consists of two or more of the following devices, running specifically developed software to sustain, for a period of time, a wireless communication link between them: mobile telephone, broadly construed here to include devices based on code division multiple access (CDMA), time division multiple access (TDMA), Global System for Mobile Communications (GSM), and wireless personal digital assistant (WPDA) digital technologies and follow-ons, as well as satellite telephones and e-mail appliances. Mobile communication systems are revolutionizing the world today, shrinking the world to between two or more small handheld mobile devices. The rapid changes in communication technologies, the revolutionary changes in software, and the growth of large powerful communication network technologies all have eased communication and brought it to large swaths of the globe. The high-end competition between the mobile telecommunication operators resulting in plummeting device prices, the quickly developing smartphone technology, and the growing number of undersea cables and cheaper satellite technologies are bringing Internet access to almost every one of the global rural poor faster than many had anticipated.

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_23

23.2 Current Major Mobile Operating Systems

Perhaps none has contributed more handsomely to the global digital communication revolution than the mobile operating system technology. The mobile operating system, commonly called the mobile OS, or just mOS, is an operating system that is specifically designed to run on mobile devices such as mobile phones, smartphones, PDAs, tablet computers, and other handheld devices. The mobile operating system is the software platform on top of which other programs, called application programs, can run on mobile devices. The mOS performs the same functionalities like its bigger brother that runs laptops and PCs. The differences, however, are in the size of memory that an ordinary and modern operating system will need to perform those functions. In the case of mOS, we are talking small sizes for everything. In additional to running in limited everything, modern mOSs must combine the required features of a personal computer with touch screen, cellular, Bluetooth, Wi-Fi, GPS navigation, camera, video camera, speech recognition, voice recorder, music player, near-field communication, personal digital assistant (PDA), and others.

Mobile operating systems are as crucial and central to the running and security of the mobile device as they are in the bigger less mobile devices like PCs and laptops. When it comes to security-related issues, the mobile device is as secure as its operating system. So every mobile device integrates as in its operating systems as much security as it can possibly carry without sacrificing speed, ease of use, and functionalities expected by the consumers. Since most mobile operating systems are similar in a number of ways to their older brothers, the operating systems in the PCs and laptops, which seem and continue to see a growing problems with security like backdoors, spyware, worms, Trojans, and a growing list of others, mOS developers and other application third parties should not wait and solve these security problems using a knee-jack reactions like was the case with PCs and laptop security. Probably quick preemptive measure could help safeguard the mobile device a lot faster.

At the writing of this chapter, the most popular mOSs are Google Android, Apple iOS, Research in Motion's BlackBerry OS, and Windows Phone OS. Of course there are many others. Table 23.1 shows some of the most popular mOS (as of September 2016).[1]

23.3 Security in the Mobile Ecosystems

As mobile devices, more importantly smart devices that can do almost everything a computer can do and more, become ubiquitous, the risk for using them is increasing. They are increasingly holding and storing more private data like personal and

[1]Wikipedia > Mobile Operating Systems. https://en.wikipedia.org/wiki/Mobile_operating_system#Tizen

Table 23.1 Major mobile operating systems (as of September 2016)

mOS	Owner	Properties	Mobile devices
Android	Google	Largest in market share. Based on the Linux kernel	Smartphones and tablets
iOS	Apple	Second largest in market share	Smartphones, tablets, in-vehicle infotainment (IVI) devices, and smart TV
BlackBerry OS 10	Research in Motion	Fourth largest in market share. Based on the QNX OS	Phones and tablets manufactured by Blackberry
Sailfish OS	Jolla—Finland	Linux-based operating systems. Partly open source and OS version releases are named after Finnish lakes adopt GPL	Smartphones, tablets, in-vehicle infotainment (IVI) devices
Firefox OS	Mozilla	Open source and is released under the Mozilla Public License. The OS is built on the Android Linux kernel, using Android drivers, but does not use any of the Java-like code of Android	Smartphones and tablets
Ubuntu Touch	Ubuntu	Open source and uses the GPL license	Smartphones and tablets
Tizen	Linux Foundation	Fourth largest in market share	Smartphones, tablets, in-vehicle infotainment (IVI) devices, and smart TV
Windows Phone 7, 8, 10	Microsoft	Closed source and proprietary. Integrated with Microsoft services such as OneDrive and Office, Xbox Music, Xbox Video, Xbox Live games and Bing	Smartphones as well as tablets with screen size under 8 inches

business, and they are roaming in public spaces on public networks with limited security and cryptographic protocols to protect the data. In fact the kind of security threats toward these devices is similar and probably more than that experienced by PCs and laptops in their heydays. The security threats to these mobile devices are comparable if not more than those facing servers in that these devices can remain on without user attention and are always connected to a network. Also because of the fact that these devices have the ability to roam on several networks, there is a wider sphere of attack beset by geographical, legal, and moral differences. Because of the high demand for global connectivity, especially in developing countries, service providers are responding with a zeal to consolidate networks and standardize communication protocols, thus making it easier for these devices to roam in large spaces and networks, creating fertile ground for attackers. The penetration trend of these smart mobile devices is not limited to faraway rural places, but more scaring is their rapid penetration on enterprise IT spaces where security is paramount for any device. This extension of smart devices into the enterprise IT spaces is a result

of their popularity as they slowly eat away the enterprise laptop as the enterprise mobile device. This in turn is increasingly causing enterprise management to start focusing on their security issues. Although antivirus client applications have been available and security best practices have been in place for most high-level operating systems, this is not the case with small mobile devices. In his article, "New Security Flaws Detected in Mobile Devices," Byron Acohido [1] reports the two recent examinations by Cryptography Research, the company that did the research, of mobile devices that revealed gaping security flaws. In one study, Cryptography Research showed how it's possible to eavesdrop on any smartphone or tablet as it is being used to make a purchase, conduct online banking, or access a company's virtual private network. Also, McAfee, an antivirus software company and a division of Intel, showed ways to remotely hack into Apple iOS and steal secret keys and passwords and pilfer sensitive data, including call histories, e-mail, and text messages. What is more worrying is the reported fact that the device under attack would not in any way show that an attack is underway. Almost every mobile system user, security experts, and law enforcement officials are all anticipating that cyber gangs will accelerate attacks as consumers and companies begin to rely more heavily on mobile devices for shopping, banking, and working. So there is an urgent need for a broader array of security awareness of the community and actions by community to assist in providing all users the highest level of protection.

In its security report titled "Lookout Mobile Threat Report 2011," the Lookout Mobile Security, a smartphone security company [2], discusses security threats to mobile devices under four major areas: application, Web-based access, network, and physical environments. Major threats are encountered by mobile devices on a daily basis.

23.3.1 Application-Based Threats

For every mobile device, the biggest appealing feature is the ability to run thousands of applications (apps) to accomplish a variety of tasks. These applications are written by really unknown people with limited to no allegiance to anybody and taking no command from anyone. The applications archiving companies like the Apple Store really have any security standards for these applications and rely, if at all, check for security requirements. Do downloadable applications present the greatest security issues for any mobile device that is capable of downloading software? Application-based threats, therefore, generally fit into one or more of the following categories [2]:

- *Malware*—software designed with the intent to engage in malicious behavior on a device. As we will see later, malware can be used in a variety of ways including identity theft and stealing of personal information from a mobile device.
- *Spyware* is designed with the intent to collect or use data without a user's knowledge or approval. We will discuss this more later in Sect. 23.5.

- *Functionality features*—these are the device's normal functionality features that reveal or threaten an individual's privacy. These features include the GPS's location identification.
- *Vulnerable application* is a software that may have vulnerabilities that can be exploited for malicious purposes. Such software include the device's operating system.

23.3.2 Web-Based Threats

Mobile devices, once on, are continuously roaming in public spaces on public networks with limited security and cryptographic protocols to protect them. In many cases, they are often constantly connected to the Internet for normal Web-based services. Under such circumstances, they are exposed to Web-based threats such as [2]:

- *Phishing scams*—in this case intruders use Web-based services to launch attacks on those devices connected to the Web to acquire information such as usernames, passwords, and credit card details and other private data of the device owner by the intruder masquerading as a trustworthy friend in an electronic communication like e-mail and text.
- *Drive-by downloads*—these are like pop-ups written by scammers to automatically begin uploading treacherous application as soon as the device visits a Web page.
- *Other Web exploits*—anyone of the many Web exploits discussed in Sect. 23.5 below is possible. This is possible because scammers take advantage of vulnerabilities in a Web browser or software that can be launched via a Web browser to attack the mobile device.
- *Direct exploitation* is a threat to mobile browsers, some of them as code bases on mobile devices that malicious Web pages can target, including the browser itself and image viewers, Flash, PDF readers, and more [2].

23.3.3 Network Threats

As we stated above, once mobile devices are on, they immediately start looking for networks to connect on either cellular networks or the Internet. As we will see in Sect. 23.5 below, there are a number of threats that originate from these networks [2]:

- *Network exploits*—recall that mobile devices always network once on. Each one of these networks, including the Internet and Bluetooth, has their own exploits. See more of this discussion in Sect. 23.5 below.

23.3.4 Physical Threats

While all the different classes of threats we have discussed so far are based on the nature and the functionality of the mobile device itself, the physical threats are based on the size and the owner of the mobile device:

- *Lost or stolen devices*—the miniaturization of mobile devices while afford more convenience for the use, the small sizes make them more susceptible to theft and getting lost from the user. While there are ways to remote wipe the device, still very few users can think of it immediately giving enough time to the robbers to acquire the data on it. In fact there are more mobile devices prone to these kinds of threats than any other we have seen so far.

23.3.5 Operating System-Based Threats

The last major category of mobile devices is that category based on the device's operating system. As has been observed by many security experts, while the threats originating from the device's operating systems are many, there are so far two Windows opportunities: one is that we have learned a lot from operating system security and vulnerabilities from their bigger brothers the PC and the laptops, and the other is that so far the domain is still relatively safer than the domain of the PCs and laptops either because many would-be attackers have not yet acquired the script programming skills needed to develop and launch attacks or that since most attacks in the PC and laptop domains are repeat attacks supported by large archives of malware and viruses, the mobile device domain has yet to develop extensive archives of these malware and viruses. So far, it is lack of expertise that is still helping. Also most operating system threats are specific to the brand. So in our discussion, we will make specific mention of the brand whenever possible:

- KDataAtruct—This is a Windows Mobile (WM) operating system problem based on the vulnerability that in WM Microsoft placed all main system functions in one coredll.dll file so that developers do not have to include the code for functions in their own programs. They just call the coredll addresses of all the APIs it uses into memory space it is allocated. In so doing an address to the list of modules is provided so that the address of the coredll can be determined. From here, one can search through memory looking for the virtual address of the API wanted. This can open up the device for exploitation. This vulnerability is exploited by the virus WinCE.Duts.A.
- Pocket IE—another Windows vulnerability found in the small Internet Explorer, commonly known as Pocket IE (PIE), default Web browser for the WM Oss. The PIE has all the vulnerabilities found in the standard IE for the big brothers PC and laptops. See all these vulnerabilities in Sect. 23.5 below.
- Jailbreaking—is a process a user can alter the phone's operating system to gain full access (or root access) to the operating system and allow applications not officially vetted by the Apple's review policies. For example, JailbreakMe 3.0

for iOS devices is a nonmalicious Web page that exploits two vulnerabilities to jailbreak a device [3].
- DroidDream—is an Android malware that utilizes two exploits, Exploid and Rage Against The Cage to break out of the Android security sandbox, gain root control of the operating system, and install applications without user intervention [4].
- Update attacks—there is a growing problem of using application updates as an attack method in the Android Market. A malware writer first releases a legitimate application containing no malware. Once they have a large enough user base, the malware writer updates the application with a malicious version [2].
- Malvertising—is malicious advertising where an attacker lures victims into downloading malware, especially on the Android Market. They rely on the fact that developers commonly use in-app advertisements to gain more users, so people are used to downloading apps via advertisements [2].
- Other threats include flowed shell model (iOS), root account (iOS), static addressing (iOS), static systems (iOS), and reuse of code (iOS).

23.4 General Mobile Devices Attack Types

Most mobile system attacks are launched against specific mobile devices or operating systems or applications. Most of these attack techniques are carryovers from the computer and computer networks. So they are not generally new into the arsenal of attacks. Over the years, we have learned specific methodologies the attackers use to success in their quest. The most common attack chancels and techniques are [2, 5]:

Denial of Service (DDoS)
This technique is meant to cause system disruptions so that the device, the service, or the network on which the device operates cannot complete the operation under way.

Phone Hacking
This is a technique used to intercept phone calls or voicemail messages, either by accessing the voicemail or text messages of a mobile phone without the knowledge or consent of the phone's owner. You may recall the *News of The World* phone-hacking stories in the United Kingdom.

Mobile Malware/Virus
A mobile malware or virus is software that deliberately targets mobile phones or wireless-enabled PDAs.

Spyware
Spyware is a type of malware that automatically installs itself or in some cases is installed manually on computers so that it continuously or periodically collects information about a range or one event, user, or application without the owner's knowledge.

Exploit
An exploit is software code that takes advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated consequences to occur on computer software, hardware, or something electronic.

Everything Blue
This is a collection of malwares and spywares that take advantage of Bluetooth technology. Just like in any other wireless network, Bluetooth, with its ability to automatically connect with other Bluetooth-enabled wireless devices, has a number of security problems that are exploited. Bluetooth is now basic feature of mobile devices. All mobile devices now all have this feature embedded in them. Before Bluetooth, infrared technology was used to transfer data and communication between any two wireless devices as long as they were within the line of sight. But infrared hindered meaningful mobility of the devices. So Bluetooth technology came in to solve that problem. Many Bluetooth offered the needed communication and mobility within the unlicensed band of radio waves without having to be in line of sight. Because of this, Bluetooth applications have emerged that allow peering of users with false security. Because this unlicensed radio band is under no regulation, it is more vulnerable to an array of security issues. Mobile devices operating within the Bluetooth range can be compromised easily as hackers can have easy access to data into these devices even commanding them to do anything the hacker wants. Without exhausting them all, let us look into the different categories of how hackers can infiltrate user's mobile devices using Bluetooth, and then we will discuss their mechanism briefly to make the end user aware of how vulnerable the user can be [6]:

- Bluejacking—this is similar to spamming but in Bluetooth by sending unsolicited messages to victim device which opens up communication between the paired devices. This can lead to the attacker gaining access to the victim device.
- Bluesnarfing—a form of Bluetooth hacking which can allow a hacker to gain access to the victim's device's contact list, text messages, e-mails, and other vital information. The hacker can even use brute force attack even if the device is invisible to guess the victims MAC address.
- Bluebugging—is the type of attack, like a Trojan horse, where the hacker uses sophisticated attack techniques to gain control of victim's mobile device. Once in control, the attacker can do anything with the mobile device.
- Bluetoothing—this is social engineering in Bluetooth where a hacker can use traditional social engineering tricks to masquerade as the legitimate user of the mobile device.
- BlueBumping—is an attack involving two mobile devices pairing up setting communication; the attacking device gets the victim to accept a connection for a trivial data exchange such as a picture and then uses that pairing to attack other services. While the connection is still open, the attacker requests for a link key regeneration which it uses later to gain access to the victim device and thus gets full access to any of the services on the victim device.
- BlueChopping—is an attack that targets Bluetooth piconet (an ad hoc Bluetooth network linking other Bluetooth devices. It allows one *master* device to

interconnect with many other active *slave* devices), for disruption by spoofing one of the participating piconet slaves leading to confusion of the master's internal state and thus disrupting the piconet.

- BlueDumping—is the act of sniffing a Bluetooth device's key exchange by forcing the Bluetooth victim mobile device to dump its stored link key. Before the sniff, the attacker needs to know the *BDADDR* of a set of paired devices. To get this, the attacker spoofs the address of one of the devices and connects to the other. Since the attacker has no link key, when the target device requests authentication, the attacker's device will respond with an "HCI_Link_Key_Request_Negative_Reply," which will, in some cases, cause the target device to delete its own link key and go into pairing mode [7].
- BlueSmucking—is a Bluetooth denial-of-service attack that knocks out some Bluetooth-enabled devices immediately. It is carried out using the old "ping of death" but transforms to work in Bluetooth. On the L2CAP (echo request) layer, there is the possibility to request an echo from another Bluetooth peer, to check connectivity, and to measure round-trip time on the established link. This is possible in Bluetooth because the **l2ping** in BlueZ utils allows the user to specify a packet length that is sent to the respective peer. This is done by means of the **-s** < **num** > option [7].
- BlueSniffing—is a Bluetooth version of war driving.

Phishing
Phishing in Bluetooth devices takes the same attempting techniques just like in their big brothers the PC and laptops in that it is intended to acquire information such as usernames, passwords, and credit card details and other private data of the device owner by the intruder masquerading as a trustworthy friend in an electronic communication like e-mail and text.

Smishing
Smishing is social engineering crime like phishing in that it uses the mobile devices and texts as baits to pull in the mobile device owner to divulge private and sometimes personal information.

Vishing
Vishing is another criminal practice in the social engineering class just like the last two. It mostly uses the mobile device phone features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing.

23.5 Mitigation of Mobile Devices Attacks

More and more people are now using some form of a data-carrying mobile device. The data on these devices is either personal or work related. Either way, this trend is growing. What is growing even faster and more worrying is the trend where a

growing number of employers are increasingly using unmanaged personal devices to access sensitive enterprise resources and then connecting these devices to third-party services outside of the enterprise security controls. This potentially exposes the enterprise-sensitive data to possible attackers. This is creating a growing security headache for sometimes underfunded and overworked security staff. The enterprise security team has to deal with a plethora of different devices running different operating systems or different versions of an operating system. According to the report "Mobile Devices Expose Company Data To Severe Vulnerabilities" by Mobilisafe, a Seattle-based mobile risk management company and small and midsized business (SMB) are more affected by this growing move. The report found that [8]:

- SMBs are exposed to high-severity vulnerabilities from the increasing levels of mobile devices used to access and download company data.
- SMB IT managers cannot keep up with the rate of discovery of severe vulnerabilities these devices bring to their corporate network.
- SMB IT departments lack a standardized approach to mitigate the risks from different types of mobile devices, as they do with laptops, desktops, and servers.
- Even though they feel exposed to mobile device security risk, SMBs do not feel they have adequate tools to assess and mitigate these risks at a granular level.

So what needs to be done? There are several security protocols and best practices that can come in handy to situations like this. According to Michael Brandenberg quoting Clint Adams [9], the "holy trinity of mobile device management," there are three security components that must form the minimum security requirements for any mobile security management. These components are hardware encryption, remote wiping, and the ability to set a passcode policy. Therefore, those responsible for security in any enterprise that is intending to use mobile devices as one form of communication and corporate data access must pay attention to these three components of security. One good thing is that mobile device manufacturers and operating system developers have been paying increasing attention to these tenants at least the first two. Because of the rather large pool of mobile device makers and mobile operating system developers, the task of ensuring that these three security tenants are adhered to by all in the company can be daunting. To sort of lessen this task for a variety of companies and individuals, a new industry has sprung up. The mobile device management (MDM) system is a platform either from third-party or original mobile device manufacturers to support and help enterprises set up and enforce mobile security policies centrally. The mobile device management (MDM) software secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers, and enterprises. MDM functionality typically includes over-the-air distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, and others [10].

23.5.1 Mobile Device Encryption

So it is important and probably a must that on either personal or business mobile devices where sensitive data is carried, such devices must be encrypted. Encrypting a mobile device is meant to protect such data as the power-on and screensaver password, the SIM card, passwords to open apps, or certain functions within apps such as logging into an e-commerce retailer account, confidential e-mail, instant messages, SMS messages, and confidential data and medical files [11].

There are two different ways mobile device encryption can be done, and these are application and hardware encryption.

Application Encryption
In securing mobile devices using applications, encryption protects the mobile device from attacks made on the host device, as well as across network connections end to end. There are many vendor solutions for this kind of encryption.

Hardware Encryption
Hardware encryption are encryption protocols embedded into the hardware by either the original mobile hardware manufacturer. For example, Research in Motion (RIM), the manufacturer of BlackBerry, is well known and indeed currently takes first place in hardware encryption of the BlackBerry phones. On the BlackBerry, RIM combines strong Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) encryption with a strong mobile device management platform to provide a strong security stance for enterprise BlackBerrys. Its BlackBerry Enterprise Server (BES) and the BlackBerry devices provide a strong solution that can deliver encryption, remote wipe, and passcode policy enforcement [12]. Similarly other mobile device manufacturers like Apple, Google, Microsoft, and others have corresponding embedded encryptions either in their device operating systems, embedded SIM cards, or movable encryption SIM cards.

23.5.2 Mobile Remote Wiping

To remotely wipe data from a mobile device is one of the security techniques in the mobile device security bag of tricks. It offers the security IT managers the basic mobile device management capabilities to remotely wipe data from lost mobile device. The remote wipe and other management features are both mobile device manufacturer and third-party developed. Many are cross-platform like the Google's Apps Premier and Education Edition which works for iPhones, Nokia E series devices, and Windows Mobile smartphones.

23.5.3 Mobile Passcode Policy

Because there is a plethora of different devices running different operating systems or different versions of an operating system, it is hard for the IT team to keep abreast of the many mobile device manufacturers and third-party vendor mobile security solutions. To cope with these problems, a security policy targeting the mobile devices in use is required.

A complete mobile security solution should include [13]:

- A firewall to secure the device from attacks and malicious code
- A VPN to allow flexible means to ensure secure communications for any wireless data traffic
- An authentication mechanism to ensure that unauthorized persons are not accessing the device if it is lost or stolen
- Data encryption on the device to ensure that information is not stolen, either physically or electronically
- Antivirus software to protect the device from viruses and malware

23.6 Users Role in Securing Mobile Devices

Although we are living in a time when mobile devices are inevitable to do without in day-to-day personal communication and personal access to data, users must be aware that there are risks to the convenience afforded by mobile devices. It is important to know that mobile computing devices can store large amounts of personal and sometimes sensitive data whose loss may cause problems to the owner or user. It is also important to know that it is easy to steal or lose that data. Furthermore, it is important to know that unless precautions are taken, an unauthorized person can gain access to the information stored on these mobile devices or gain access through these devices to other devices or data because these devices may provide access to other services that store or display nonpublic data. This access may be enabled because the mobile device contains passwords or security certificates and other information that may help to identify the device, its user, or its content. So our role as users is to be vigilant and security aware.

Exercises

1. Discuss the steps you would take to protect your mobile device.
2. Search the Internet to find a company's security policy for its mobile devices. Suggest what you would change in that security policy to enhance security.
3. Study three remote wiping solutions and compare them.
4. Comment on the reasons for the rapid growth of the Android operating system.
5. Recently Apple's iOS4 encryption was hacked by a Russian company. Discuss the weaknesses in the iOS4 disclosed by the Russian company.

Advanced Exercises

1. Study the mobile device management platforms and discuss the solutions it offered.
2. What does a typical MDM solution include?
3. List and discuss vendors of MDM.
4. Discuss the Windows Mobile security model, authentication services, Credential Manager, cryptography, and LASS application development and programming elements.
5. Discuss the IPhone Mobile Authentication system.

References

1. Acohido B. New security flaws detected in mobile devices, USA Today. http://www.enterprise-security-today.com/news/Mobile-Devices-Vulnerable-to-Attack/story.xhtml?story_id=0010003FAI65, April 10, 2012 9:50AM
2. Lookout Mobile Threat Report, 2011. Lookout mobile security. https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf
3. Jean. Analysis of the jailbreakme v3 font exploit, Segeti ESEC Lab. http://esec-lab.sogeti.com/posts/2011/07/16/analysis-of-the-jailbreakme-v3-font-exploit.html
4. C-Skills (July23, 2010) http://c-skills.blogspot.com/search?q=exploid
5. Wikipe4dia. Mobile security. https://en.wikipedia.org/wiki/Mobile_security
6. Types Of Bluetooth Hacks And Its Security Issues, HubPages. http://hubpages.com/technology/Types-Of-Bluetooth-Hacks-And-Its-Security-Issues
7. Wikipedia. Bluetooth. https://en.wikipedia.org/wiki/Bluetooth#Security
8. Mobilifesafe. Mobile devices expose company data to severe vulnerabilities, PR Newswire. April 9, 2012. http://www.prnewswire.com/news-releases/mobilisafe-study-details-vulnerability-risk-to-company-data-for-smbs-146647805.html
9. Brandenberg M. Mobile device security overview. TechTarget. http://searchconsumerization.techtarget.com/tutorial/Mobile-device-security-overview
10. Wekipedia. http://en.wikipedia.org/wiki/Mobile_device_management
11. Adhikari R. Encryption on the Go, Part 1, TechNewsWorld. http://www.technewsworld.com/story/75245.html
12. http://trifinite.org/trifinite_stuff_bluedump.html
13. Komisky M. Mobile device security II: handheld operating systems, Bluefire. http://www.datamation.com/mowi/article.php/3575316/Mobile-Device-Security-II-Handheld-Operating-Systems.htm