International Journal of Advance Research, IJOAR .org
Volume 4, Issue 4, April 2016, Online: ISSN 2320-9194

MOBILE SECURITY

Reem Fairak

ABSTRACT

In recent years, smartphone becomes the most popular device people use in their daily live. It combines the functionality of mobile phone and provide some computer-based services, such as media player, Wi-Fi, and web browser. Mobile security has gathered a significant interest in research, industry, and normal people society due to the popularity of the smartphones. This paper analyzes some of the security challenges and concerns associated with mobile phone, which included, hardware-based mobile security, mobile network security, Application-based threats, and Web-based threats.

KeyWords
Application base threats, hardware, malware, network security mobile, security, SIM card security, web base threats.

Introduction

Smartphones offer a level of convenience that the world has never known before. In fact, 44% of smartphone users' sleep with their devices next to their beds to avoid missing a call, SMS, or any update during the night. Regrettably, people and organizations are not the only ones shift to mobile devices. Hackers and identity thieves are following close behind. Organizations and people are more likely pay attention to mobile security after they've been stolen, lost, or infected, than before. Moreover, despite the fact that smartphones are now just as risky as computers when it's come to security, many business and people don't hold the same precautions as they do for computers. The poor usability of the built-in security tools in the smartphones, may be because of their complexity, make the problem even bigger. Many people expect that iPhone or Android devices are secure by default. Security experts are finding a growing number of viruses, worms, Trojan horses, and attackers that target mobile phones. In fact, the number of unique mobile threats grew by 261% in just the last two quarters of 2012, [1] according to ABI Research. Hackers could inject mobile phones with malicious software that deletes user's data, runs up the phone bill by making calls, or overload mobile networks.

1. Hardware-based mobile security

1.1Root of Trust (ROTs):

One of the most difficult topics to discuss in the mobile security field is the hardware-based mobile security because the data is never secure without secure hardware. Moreover, hardware security is the first line of defense in the battle to protect mobile device data. The existing security mechanisms applied in the hardware-based mobiles are basically designed for PCs. They limited support mobile security because of the different hardware architecture between mobiles and computers, and due to the limited resources of battery, CPU, and memory for mobiles. In addition, many mobile devices are unable to provide strong security guaranties Due to lack of root of trust in mobile hardware-based. The standards-based Root of trust (ROTs) is just one of the big challenges faced by mobile companies, and the most important factor the current mobiles are missing.

[2]Mobile architectures are composed of hardware, firmware, and software interact with each other. Figure 1 obviously shows that each levels, which level provides services for the higher must trust the lower levels to be trustworthy.

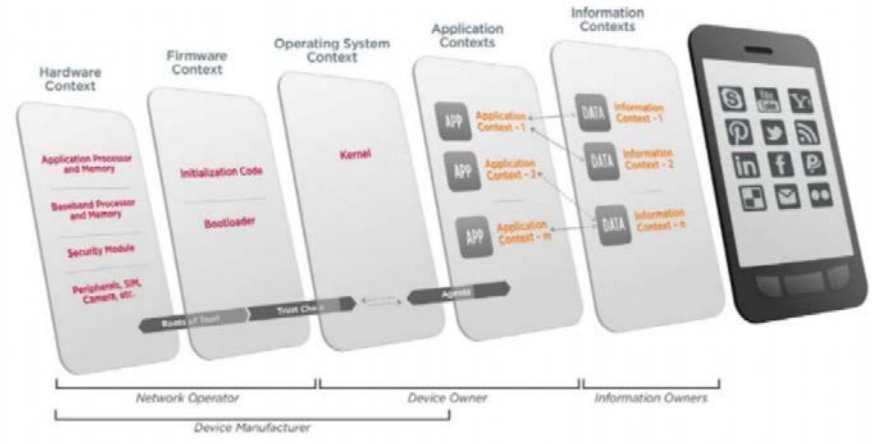

Figure 1: Mobile architecture

Root of trust, or RoTs are the hardware, software, and firmware levels that provide a set of trusted, and security-critical function. Because their misbehavior can't be detected, these components should behave consistently and in an expected way. It is always preferable to use and focus on hardware ROTs, and then find software ROTs capable because they inclined to be more reliable, and they have a smaller attack surface. Moreover, the hardware level represent the lowest level which provide services for all the higher levels in the mobile architecture. In addition, mobile hardware-based approaches typically rely on a Root of Trust. Smartphones lack the hardware-based root of trust features that are built for laptops and other hosts. There are several types of ROTs that provide different degrees of protection to the mobile environment include:

- Root of Trust for Storage (RTS): provides a secure warehouse to store the critical security parameters and manage the cryptographic keys. It is preferable to implement RTS in a trusted hardware with a protected interface to manage the data protected by RTS more than in an untrusted Hardware.

- Root of Trust for Verification (RTV): this part provides a protected machine which used to verify the digital signature using the public key stored in RTS and by executing the signature verification algorithm.

- Root of Trust for Integrity (RTI): this part store the assertions in a protected interface which protect the integrity as well.

- Root of Trust for Reporting (RTR): this part control the identities and the sign assertions by providing a protected interface and environment.

- Root of Trust for Measurement (RTM): this part helps the assertions which are protected by RTI and attested by the RTR to make the system measurement.

1.1.1 Trusted Execution Environment (TEE):

[3]Mobile manufactures usually establish a Root of Trust at the time of manufacturing. Appling the Root of Trust on mobiles hardware provides a trusted execution environment (TEE). The TEE is a secure area located in the mobile processor. By separating the hardware from the mobile operating system, the TEE make sure that sensitive data is processed and stored in a trusted environment. Trusted execution environment has the ability to provide a safe execution for authorized software (trusted applications), which built by the mobile makers or installed by the users. These applications have a full access to the device's memory and main processor. The hardware isolation feature provide a protection from the applications running in the main operating system, which offers a level of protected against some software attacks. As a result, by separating the unsecure operating system area, the device will provides a much greater degree of security. Furthermore, by enforcing integrity, data access rights, protection, and confidentiality, TEE enables the trusted applications to provide end-to-end security.

1.1.2 Trusted Platform Module (TPM):

[4]Root of trust can offer a Trusted Platform Module (TPM) as well. TPM is a micro-controller that can store passwords, encryption algorithms keys, and certificates that provide authentication for the platform. Trusted Platform Module has a built- in RSA engine - perform up to 2048-bit encryption /decryption- which uses in the key wrapping operations and digital signing. Moreover, it can be used to store the platform measurement that make sure the platform stay trustworthy. In security, cost and security must be balanced against each other. To provide the balance between them, Root of Trust can be applied as a combination of hardware and software. For Example, Trusted Platform Module provides Root of Trust for Reporting (RTR), trusted execution environment provides Root of Trust for Storage (RTS), and BIOS provide Root of Trust for Measurement (RTM).

[5]At the end of 2013, the hardware-based mobile security was represents %20 of the total global mobile security market. That percentage will go down to %17 by 2018, said Michela Menting, ABI's senior analyst in cybersecurity.

2. Mobile Network security

To understand the risks associated with mobile networks, it is necessary to take a look at the mobile network communication standards. There are two popular radio systems used in cell phone for communication, which are the Code Division Multiple Access (CDMA) and the Global System for Mobile (GSM).

This paper will focus on GSM technology from security perspective because most of the world's countries use GSM. The major difference between the two technologies is that the mobile identification is programmed in to it in CDMA. On the other hand, GSM uses SIM cards.

2.1 SIM Card security

SIM card (Subscriber Identity Module) considered as mobile identifier which placed in the phone to identify it on the network. Not only does the SIM card provide identification for mobiles, but it also authenticate the software sent by the mobile operator. In addition, it saves user's SMS, contact list, and all data associated with applications that use mobile number to verify the user, such as Google, WhatsApp, and Facebook. Many SIM cards use DES encryption algorithm when communicating with the operator, [6] said Karsten Nohl, an expert cryptographer with Security Research Labs, according to research posted on his company's blog. DES considered a weak encryption algorithm which allow the attackers to crack the SIM cards. By compromising the shared key between the SIM card and the service provider, the attacker can pretend and trick the SIM card to think that he is the service provider (man-in-the-middle-attack). The attacker can send a message for the SIM Card in order to open it up using the cracked key. Once the SIM card opened up, the attacker can listen to the user's calls, send SMS, and steal all data stored in the SIM card, known as remote cloning. To avoid these kinds of attacks, SIM card companies started to use triple DES encryption algorithm rather than DES because it's much stronger.

2.2 GSM security

Although the attacker can spying on conversation through the mobile SIM card, he can also reach his target by spoofing the cell phone towers (GSM towers). [7] An attacker can use IMSI catcher, an eavesdropping cell phone device, to intercept mobile calls traffic, performing a man-in-the-middle attack. Essentially, IMSI catcher is a small GSM base station that force the victim's mobile to use it rather than the real network.

IMSI, International Mobile Subscriber Identity, is an electronic identity associated with the SIM card that uses to identify the user's call at any point in the telephone network,

Once the attacker force the victim to use his station instead of the real one, he can directly Eavesdrop on calls. Moreover, he can enable/ disable the phone service, and face SMS messages from and to the phone. [8][9]GSMK is the first CryptoPhone available for Android phones that allow users to know whenever a rogue cell tower is connecting to their mobiles. GSMK's CryptoPhone compare the cell tower ID, which it connected to, and signal strength with the neighboring towers. Furthermore, the firewall will alert the user once the mobile network switched to 2G network, a less secure network which doesn't authenticate the cell towers, or the network encryption turned off. By using the IMSI catchers, the attacker can force the mobile to use 2G network, even if the 3G or 4G is available. When this occurs, the CryptoPhone firewall will alert the users.

2.3 Mobile Bluetooth security

Unlike Internet connection, mobile users don't consider Bluetooth as potentially risky technology. However, keeping mobile Bluetooth in "open" or "discovery" mood could allow the attacker to eavesdrop on the user. Even worse, not only can the attacker eavesdrop on the user's calls and personal information, but also he can crash the user's device, and block the mobile from receiving mobile calls using Denial of service attack. [10] Moreover, the attacker can attack the device battery by draining it, which called "sleep deprivation attack". Sleep deprivation try to exploit the power management system in order to prevent the device's ability to switch into reduced power states. Sleep deprivation can be divided into three basic categories: malignant power, benign, and service requesting attacks. A malignant power attack attempts to change some mobile programs to consume more power that they need. A benign power attack succeeds at start a component operation which drain the mobile battery rapidly. A service requesting power attack tries to request from the mobile device a genuine service requests in order to drain the device's battery. To prevent attackers from attack the mobile using the mobile's Bluetooth is to make sure that the Bluetooth configured to be "undiscoverable" or "hidden" in order to prevent the mobile from public broadcasting. If the mobile user doesn't use the Bluetooth, he should power it off. Moreover, people should make sure that the sensitive information broadcasting over Bluetooth are encrypted.

2.4 Mobile Internet security

Spoofing the GSM towers and cloning the SIM cards aren't the only threats the mobile network can be faced, however. By connecting to a public Wi-Fi, attacker can easily sniff people's packets because most of the public hotspots are open networks that don't encrypt data. Even worse, most mobile devices don't have strong security features against Wi-Fi threats. As a result, public Wi-Fi vulnerable to security breaches. In fact, almost the same risk applies to users' home wireless router if it isn't encrypted with WPA2, WEP, or WEP security. By using free tools which are available online, such as, Firesheep, SniffPass, and EffeTech Sniffer, attackers can capture users' login credentials to unsecure sites. More badly, attackers can capture and reassemble the webpages users' are browse. The Evil Twin hotspot is another way in which the attacker can eavesdrop on network traffic and insert themselves in between the user and the server. Basically, Evil Twin is a Wi-Fi access point set up by a hacker to mimic a legitimate access point provided by places for free. Once the users connected to this Wi-Fi, the attacker who own this access point will be able to steal user's login credentials, credit cards number, and redirect him to malware sites. The first line of defense people can apply against Wi-Fi eavesdroppers is to make sure the website they are connected to, is secured using SSL encryption. Moreover, by using a Virtual Private Network (VPN) on both cell data connection and Wi-Fi, people can make sure that they are connecting securely to the internet.

Data communication over mobile networks may experience security threats since there is a lack of mechanisms that can provide advanced security service to the traffic. Furthermore, special attention has to be considered in the GSM, SIM cards security. Security is a primary concern in the mobile networks. Security is required by the different types of traffic within the mobile.

3. Application-Based Threats

Downloadable applications for mobile devices can occur many security issues. According to FSecure [11], there are already more than 400 mobile viruses in circulation. These mobile application-based threats can be categorized as: (1) malware, which includes backdoor, Trojan, and worm; (2) and potentially unwanted application (PUA) which has spyware and trackware as its subcategories.

3.1 Malware

The definition of malware for mobile devices can be driven form the master definition of malware, which is software that is intended to damage or disable computers and computer systems, [12].

As for mobile device (such as tablets or smartphones), malware is software that performs malicious actions while installed on the device, [13]. It is mainly designed to target the system of the mobile device to damage it or disrupt it. For example, without your knowledge, malware give a malicious user control over the device, and allow the attacker to steal the stored personal information. It also could make charges to the phone bill and send to the contact list unsolicited mass messages.

Malware includes: backdoor, Trojan, and worm.

3.1.1 Backdoor

According to Techopedia [14], backdoor is a program that provides unauthorized remote access to the device. It is also known as a trapdoor. This program is written by the programmer, who created its code and he is often the only one who knows it. Which makes backdoor a potential security risk.

Coolpad, Chinese smartphone maker and the sixth largest smartphones manufacturer in the world, has included a backdoor to the installed software on many of Coolpad's Android devices.

Although Ryan Olson, intelligence director of Unit 42, Palo Alto Networks, said, "we expect Android manufacturers to pre-install software onto devices that provide features and keep their applications up to date," the CoolReaper backdoor goes beyond these expectations.

The CoolReaper backdoor that was built and operated by Coolpad, give them complete control over these devices. CoolReaper also allows them to track users by uploading the device information, location, application usage, and the history of calling and SMS to a Coolpad server. In addition, without users consent or notification, this malware (CoolReaper backdoor) can download, install/uninstall, or activate/disable any Android application. It also can serve users unwanted advertisements. Moreover, Coolpad has made modifications for the Android OS, which hide CoolReaper components from both users and other applications operating on the device, such as antivirus programs, [15].

3.1.2 Trojan

Trojan is a malicious program that performs actions that have not been authorized by the user, [16]. The Trojan appears as fun or important file on the mobile device, but when the user runs that file it will perform unwanted actions such as deleting, blocking, modifying, or copying data. It also can disrupt the device performance.

According to the type of action they take, Trojans may be subdivided as: Trojan-downloader, Trojan-dropper, Trojan-spy, and Trojan-SMS.

Let's talk about Trojan-SMS, they are programs that can cost user money and they will send text messages from the user's mobile device to premium rate phone numbers. They recently appear in more and more countries. Trojan-SMS.AndroidOS.Stealer.a, for instance, can send short messages to premium-rate numbers in 14 countries around the world. In February 2013, Kaspersky Lab detected Trojan-SMS.AndroidOS.FakeInst.ef, and since then 14 various versions of it have emerged and targets users in 66 countries, including the US [17].

3.1.3 Worm

The malware worm is a type of malicious software that self-replicates and distributes copies of itself to its network to infect other devices [18]. What makes the worms extremely dangerous is the fact that they are independent viruses, which can replicate and spread on their own and infect other devises without the mobile user's knowledge.

Selfmite is a new version of an Android worm that has the possibility to increase huge SMS charges for victims while spreading to as many devices as possible [18]. Thousands of spam text messages have been sent from infected devices because of Selfmite and it has spread to 16 countries. Generating money through pay-per-install schemes is the main reason of creating this worm.

Although security researchers were able to quickly disrupt the distribution of Selfmite that discovered in June 2014, researchers from security firm AdaptiveMobile have found recently a new version of that warm (Selfmite.b) which has a similar, yet much more aggressive spreading system [10]. The way of spreading in the first version of Selfmite differs from the new one in terms of the number of the receivers. In the first version, the first 20 contacts in every victim's address book will receive text messages with links to a malicious Android Package. While in the new one, all contacts in a victim's address book will receive text messages with rogue links and continue in a loop. According to Denis Maslennikov, a security analyst at AdaptiveMobile, that from more than 100 infected devices, Selfmite.b has send over 150k messages during the past 10 days [18].

After illustrating some types of malware, the following content will explain the second category of mobile application-based threats, which is potentially unwanted application (PUA) and some of its types.

3.2 Potentially Unwanted Application (PUA)

Potentially unwanted application (PUA) is an application or component that may install additional unwanted software, change the behavior of the mobile device, or perform activities not approved or expected by the user [19]. They may introduce privacy or security risks. In fact, sometimes the user is aware of the implied risk in these applications he or she still elects to install and use the application.

PUA can be subcategorized as: spyware and trackware.

3.2.1 Spyware

Spyware is designed to collect or use private data without your knowledge or approval. Those data are then send to the Spyware creators. Those programs invade the user privacy and profit from their data by selling it to a third party, [12].
According to European Union agency for network and information security [20], a study of 48,694 applications in the Android market found that one of every five application request permission to information that can be used for malicious purpose. Some of the application has the ability to make calls without the user authorization. Moreover, in iOS all apps are allowed to access the address book. This means that the user phone number is also accessible. All those information can be used for a marking purposes.

3.2.2 Trackware

It is a program that collect information that could be used identify or track a user or a device. Android.Monitor.Gizmo.A is an Android app that gives a complete remote phone tracking and monitoring system. The app allows the attacker to track all SMS, MMS, calls and GPS location [19].

4. Web-Based Threats

Web-based threats raise constant issues for mobile devices since mobile devices are constantly connected to the Internet and used to access web-based services. These issues can represented in phishing scams and drive-by downloads.

4.1 Phishing Scams

The simplest explanation of Phishing is that it is the act of using email, text messages, Facebook, and Twitter to send links to websites their sole purpose is to trick user in giving a way personal information like username, password, and credit card information and so on. By doing so attacker can use the information for malicious purposes like stealing money and more dangers stealing identity.
Indiana University defines Phishing scams as “fraudulent email messages appearing to come from legitimate enterprises. These messages usually direct you to a spoofed website or otherwise get you to divulge private information. The perpetrators then use this private information to commit identity theft” [21].
A typical scenario for a phishing scam is an email message form (Amzon.com) stating that there are some suspicion activity on the victim account. Then the user “victim” is ask to click on a link to verify his/her information. The link will be a replicate of Amazon login page, the victim will type in the username and password and perhaps the credit card information. Now, the attacker have all he need to buy anything using the victim information.
PC and mobile devices users are vulnerable for phishing scams. According to a post by Mickey Boodaei, CEO of Trusteer, mobile phones users are three times more likely to become victims of phishing attacks than desktop users [22]. There are two main reasons for that. First, user are always on. Users are most likely to read an email a soon as it arrives on their phones. On the other hand, PC users can check their emails when they have access to a device. The second reason is that it is more difficult to identify a phishing site on a mobile device than on a computer. The difficulty is due the limitation of mobile phone.
The post by Mickey Boodaei compare the phishing process in Blackberry and iPhones. In Blackberry, when the user receive an email only the sender’s name appears not the full email address. Most user do not click to check to see the full email address. For example, by seeing amazon as the sender’s name, most users may believe that amazon send this email. When the user click on the spoof link, the BlackBerry shows the following message: “Continue to” with the real address appended. Due to the size screen the full URL may not show. This may be shown www.amazon.com, but the full URL could be something like this www.amazon.com.hdh.dddj//dhsj. Once the Blackberry switch to the browser the real address is not presented instead the website name crated by the attacker appears.
The iPhone present a similar process but here the phone switch to the browser without asking the user if he want to continue. Contrary to Blackberry, iPhone browser have an address bar but the screen size problem airs again. In any phone if the user is not carful and does not checks the details he can be easily trick.

4.2 Drive By Downloads

Drive by download is a malicious program downloaded in the background to the victim device without the user knowledge. The download is trigger by only visiting a website. What usually happens is that the malicious website will contain different types of malicious code, hoping that at least one of them will be successful in taking advantage of the weakness in the browser, app, or the operating system, [12].
NotCompatible is a malicious code design for devices running Android operation system. "This threat does not currently appear to cause any direct harm to a target device, but could potentially be used to gain illicit access to private networks by turning an infected Android device into a proxy," Lookout said [23]. This can be very dangerous, the attacker can gain access to normally protected information or systems.
When the user visit the effected website, the NotCompatible application will being downloading automatically. An update patch called Update.apk is download. Then the user is asked if he want to install the “update”. The installation can be completed only if

the “Unknown sources” setting is enabled. An uneducated user may believe that this is really an update and allow the installation.

Conclusion

In the past years mobile security have been an emerging problem. People are now realizing that their mobile devices are under attack. This paper had discuss four major aspect of mobile security. The first aspect was the Hardware-based mobile security which is really the first line of defense.

ROTs are the hardware, software, and firmware levels that provide a set of trusted, and security-critical function. Although the importance of ROTs is obvious, Smartphones lack the hardware-based root of trust features that are built for laptops and other hosts.

The second aspect is Mobile Network security. Spoofing the GSM towers and cloning the SIM cards are major threats in mobile security. Solution for these threats has been proposed and deployed. Application-Based Threats and Web-Based Threats the final two aspect of mobile security mentioned here. Wither the user download the malicious code himself or it has been download automatically, users must be careful art all times. At the end, the security of mobile devices is not certain. No one party should be blamed for this lack of security. The paper had showed that.

References

[1] BYOD and Increased Malware Threats Help Driving Billion Dollar Mobile Security Services Market in 2013. (2013, March 29). Retrieved April 26, 2015, from https://www.abiresearch.com/press/byod-and-increased-malware-threats-help-driving-bi/

[2] Chen, L., Franklin, J., & Regenscheid, A. (2012, October 1). Guidelines on HardwareRooted Security in Mobile Devices (Draft). Retrieved April 26, 2015, from http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf

[3] GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide. (n.d.). Retrieved April 26, 2015, from https://www.globalplatform.org/mediaguidetee.asp

[4] Trusted Computing Group. (n.d.). Retrieved April 26, 2015, from http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

[5] Robinson, B. (2014, February 10). Hardware-based mobile security market heats up. Retrieved April 26, 2015, from http://gcn.com/articles/2014/02/10/mobile-hardware-security.aspx

[6] Rooting SIM cards. (n.d.). Retrieved April 26, 2015, from https://srlabs.de/rooting-sim-cards/

[7] Active GSM Interception. (n.d.). Retrieved April 26, 2015, from http://www.cryptophone.de/en/background/gsm-insecurity/active-gsm-interception/

[8] Trustworthy Voice and Message Encryption. (n.d.). Retrieved April 26, 2015, from http://www.cryptophone.de/

[9] ZETTER, K. (2014, September 3). Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls. Retrieved April 26, 2015, from http://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers/

[10] Buennemeyer,, T., Munshi, F., Marchany, R., & Tront, J. (2007). Retrieved April 26, 2015, from http://www.hicss.hawaii.edu/hicss_40/decisionbp/07_09_02.pdf

[11] Knowing the Mobile App Security Threats & How to Prevent Them. (2013, Apr 16).Retrieved April 26, 2015, from http://www.itexico.com/blog/bid/92948/Knowing-the-Mobile-App-Security-Threats-How-to-Prevent-Them

[12] What Is a Mobile Threat? (n.d.). Retrieved April 26, 2015, from https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat

[13] Viruses, Spyware, and Malware. (n.d.). Retrieved April 26, 2015, from https://ist.mit.edu/security/malware

[14] Backdoor. (n.d.). Retrieved April 26, 2015, from http://www.techopedia.com/definition/3743/backdoor

[15] Xiao, C. & Olson, R. (2014, December 17). CoolReaper Revealed: A Backdoor in Coolpad Android Devices. Retrieved April 26, 2015, from http://researchcenter.paloaltonetworks.com/2014/12/coolreaper-revealed-backdoorcoolpad-android-devices/

[16] What is a Trojan Virus? . (n.d.). Retrieved April 26, 2015, from http://usa.kaspersky.com/internet-security-center/threats/trojans#.VUcHdJTF92c

[17] Chebyshev, V. (2014, April 17). New threat: Trojan-SMS.AndroidOS.Stealer.a. Retrieved April 26, 2015, from https://securelist.com/blog/incidents/59384/new-threat-trojan-sms-androidos-stealer-a/

[18] Constantin, L. (2014, Jun 27). Self-propagating SMS worm Selfmite targets Android devices. Retrieved April 26, 2015, from http://www.computerworld.com/article/2491339/malware-vulnerabilities/self-propagating-sms-worm-selfmite-targets-android-devices.html

[19] Mobile Threat Report. (2013, September). Retrieved April 26, 2015, from https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q3_2013.pdf

[20] Spyware attacks. (n.d.). Retrieved April 26, 2015, from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/spyware-attacks

[21] What are phishing scams and how can I avoid them? (n.d.). Retrieved April 26, 2015, from https://kb.iu.edu/d/arsf

[22] Boodaei, M. (2011, January 4). Mobile Users 3 Times More Vulnerable to Phishing Attacks. Retrieved April 26, 2015, from http://securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/#.VUdPxpTF92c

[23] Strazzere, T. (2014, November 19). The new NotCompatible: Sophisticated and evasive threat harbors the potential to compromise enterprise networks. Retrieved April 26, 2015, from https://blog.lookout.com/blog/2014/11/19/notcompatible/