CHALMERS

Security Issues in Smartphones and their effects on the Telecom Networks

Master of Science Thesis in the program Networks and Distributed Systems

SAGHAR KHADEM
Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, August 2010

Security Issues in Smartphones and their effects on the Telecom Networks

SAGHAR KHADEM

Examiner: TOMAS OLOVSSON

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden August 2010

Abstract

Smartphones have become so popular these days because of their extra services and their extraordinary features compared to regular phones. They are very similar to PCs and laptops; therefore they encounter almost the same security problems and even worse with respect to memory and space limitations. Since the manufacturers focus on development of new features and fast release of new services more than security issues, security in smartphones is usually neglected. Smartphones as opposed to ordinary mobile phones use different technologies, so they are more exposed to different attacks. In addition, they are interoperating devices which work between the Internet and telecom networks, so they can bring Internet security threats to the telecom networks and cause serious damages and endanger critical call centers.

In this thesis security issues and different attacks against smartphones are presented and some countermeasures against the different types of attacks are introduced. In addition, certain security threats that Internet compromised smartphones have brought to the telecom networks and some solutions in order to make these threats ineffective are discussed.

Preface

This is a graduation thesis for Master of Science degree in Network and Distributed Systems. The examiner is Tomas Olovsson in the computer security group at Department of Computer Science and Engineering, Chalmers University of Technology. This thesis work is performed by Saghar Khadem during the period March 2010 to August 2010. I would like to thank my examiner Tomas Olovsson for invaluable support, pointers and discussions.

Table of Contents

Table of Figures

1. Introduction

Smartphones have been permeating everywhere these days because of their special extra services, advanced technology and their functionality compared to regular phones. These advantages give us an opportunity to have remote access and be in control of information and communication anywhere and anytime. On the other hand, the rapid development of technology in miniaturization and computing, particularly in wireless mobile networks, brings a new dimension to security threats.

Since these portable cell-phones with limited memory have been accompanied with the computing and networking power of PCs/laptops and they are also involved with various network technologies such as 3G, Bluetooth, infrared and WLAN (IEEE 802.11), they become extremely vulnerable to different attacks. Denial of service (DoS) attacks and flooding attacks are major security threats to Internet communication as they disrupt communication over the network and leave servers inaccessible to legitimate users. It has been reported that wireless networks such as smartphones are more susceptible to these types of attacks than wired networks [1].

All smartphones have lots of features in common. However based on their types they use different operating systems with different design, functionality and network stack architecture which could be attacked through WLAN. Besides they could be threatened via universal serial bus (USB), infrared and Bluetooth.

In addition, smartphones are interoperable devices which may be applied as conduits to connect to different networks. For example they can operate between the Internet and the Telecom networks becoming possible bridges for bringing Internet security problems to the telecom networks. They can cause serious damages such as privacy violation, Distributed denial of service attack (DDoS) against call centers and bandwidth exhaustion attacks against 3G and 4G networks [10]. Therefore, as these devices become so popular among the users which benefits from 3G/wireless communications, there is a need to put more emphasis on security problems existed in Smartphones and also the possible paths from which the Internet compromised smartphones transfer Internet security threats to the telecom networks.

1.1. Scope

The scope of this work is to conduct a survey about security vulnerabilities in smartphones and investigating various attacks which have been launched against them via different gateways such as WLAN, Bluetooth, 3G and infrared. This work also focuses on analyzing the impact of these types of attacks and proposes the feasible solutions to minimize or eliminate their damages. From another perspective, attacks which have been launched against the telecom networks through Internet compromised smartphones and defense techniques in order to protect them are also mentioned.

2. Background

2.1. General Attacks

In general, malicious users can exploit vulnerabilities in Operating systems, software, protocols and network interface. It is interesting that regardless of how well the system of the victim is secured, its susceptibility to the attack relies on the state of security in the rest of the Internet. Attackers can apply different types of attacks and also can have variety of objectives. Some of them try to reroute messages and some of them try to damage the whole network and degrade its performance or overload the system with lots of unwanted packets, whereas others disrupt communication over the network and leave servers inaccessible to legitimate users by performing Denial of Service attacks (DoS). There are three basic kinds of DoS attacks: 1. sending lots of packets and consuming limited resources (network, CPU, memory). 2. Changing or damaging configuration information. 3. Changing or damaging the components of network.

In this section some general attacks are discussed:

2.1.1. ARP poisoning

ARP poisoning is a technique used to attack a wireless network or a wired network. As shown in Figure 1, in order to intercept network traffic between host A and host B, the attacker sends a malicious ARP reply (no request before) to host A and combines his MAC address with host B's IP address and deceives host A. Host A therefore thinks that the attacker's computer is host B. It does the same with host B and deceives host B to think that the attacker's computer is host A. Finally, the attacker can sniff data frames and forward any network traffic it receives from host A to host B (by applying an operating system feature which is called IP forwarding) [1].

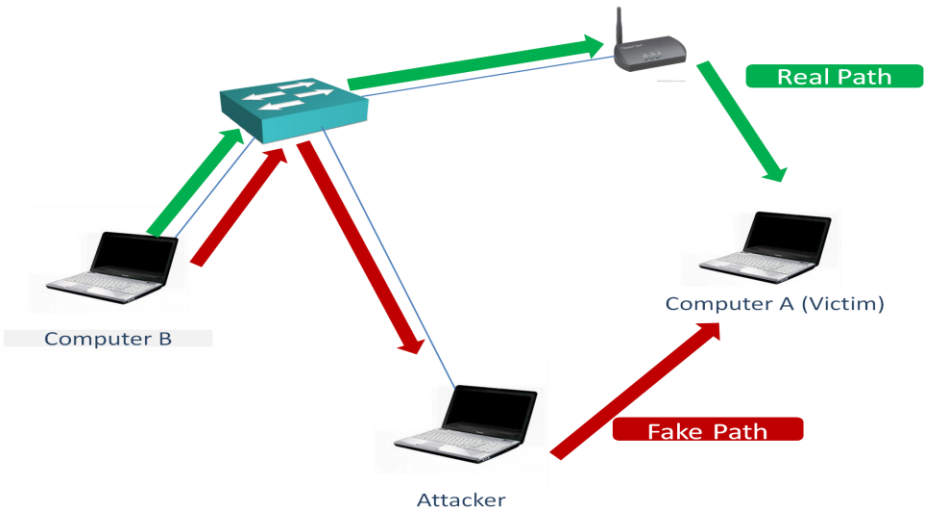

Figure 1: Implementation of ARP poisoning

2.1.2. MAC Spoofing

In this type of attack, by applying Mac Makeup software (MMS), the attacker can alter the MAC address of a wireless adapter which has been assigned by the manufacturer to the MAC address he wants to impersonate. The attacker can observe the traffic by capturing wireless packets with any packet capturing software and learn the MAC address of the victim (Figure 2).

The attacker assigns the IP address of the victim computer whose MAC address has been spoofed to his computer. Then he/she performs DOS attack against the victim to disconnect the victim's computer from the network and tries to connect to the access point with the spoofed MAC address of the victim [1].

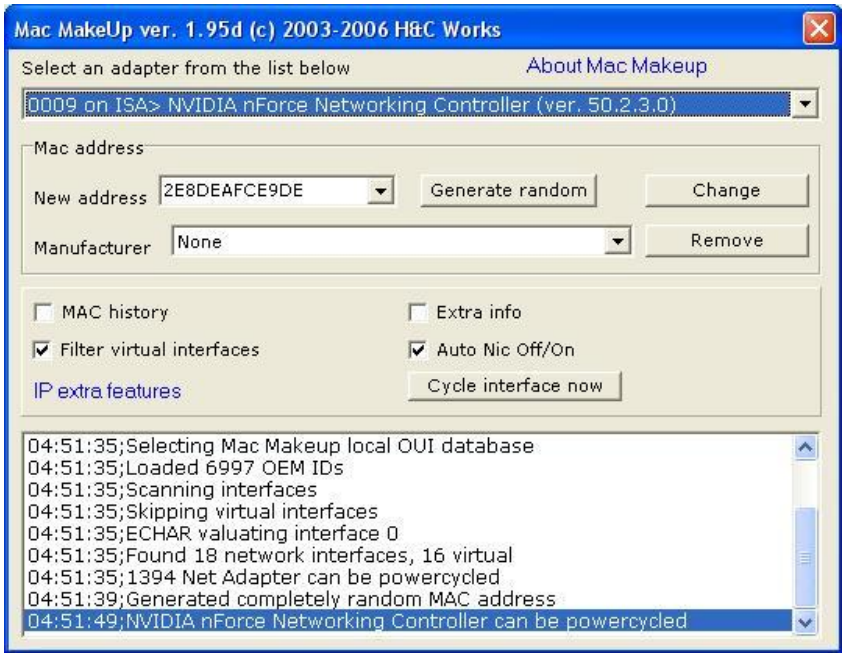

Figure 2: Mac Makeup Software (MMS)

2.1.3. Web Spoofing

In a web spoofing attack, the attacker creates a "shadow copy" of the entire web page and directs visitors to a web page that looks like the original one. The real web page, however is hosted in a different location, usually for the purpose of obtaining personal and sensitive information such as credit card numbers and passwords (figure 3) [1].

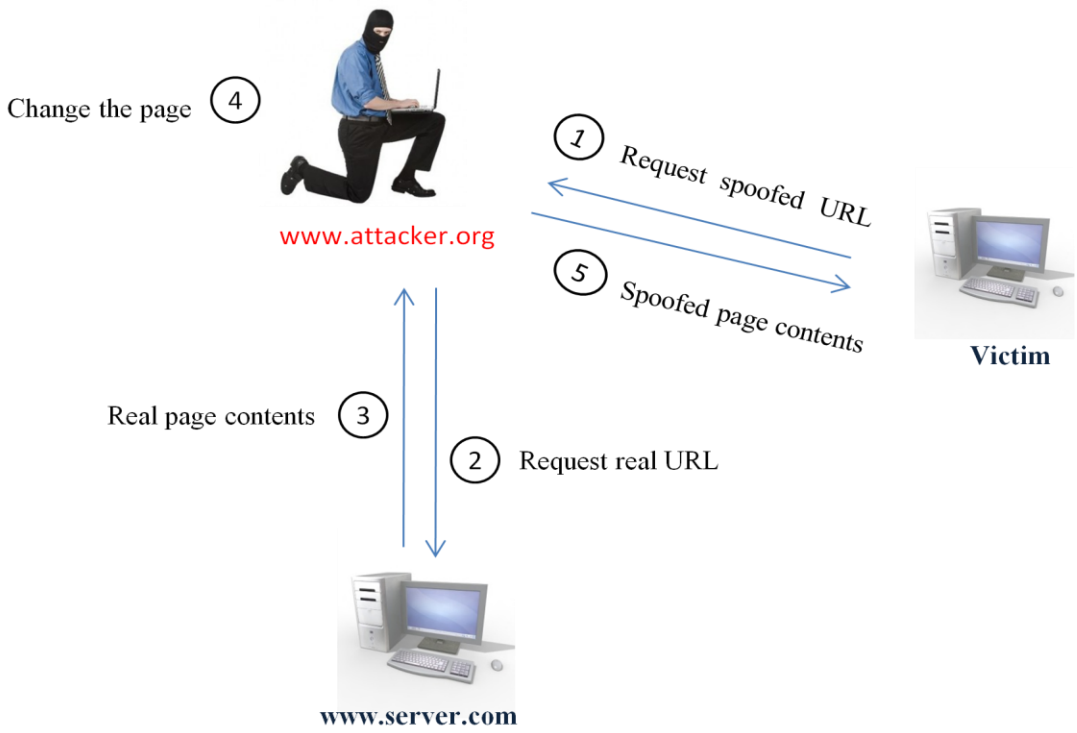

Figure 3: Web spoofing

2.1.4. DNS Spoofing

In the DNS spoofing attack, like web spoofing, the attacker directs the victim to a fake server (by altering the hostname-to-IP address mapping in DNS server reply) to gain sensitive information. So whenever the users request a host name, the attacker directs them to his server (Figure4) [2].

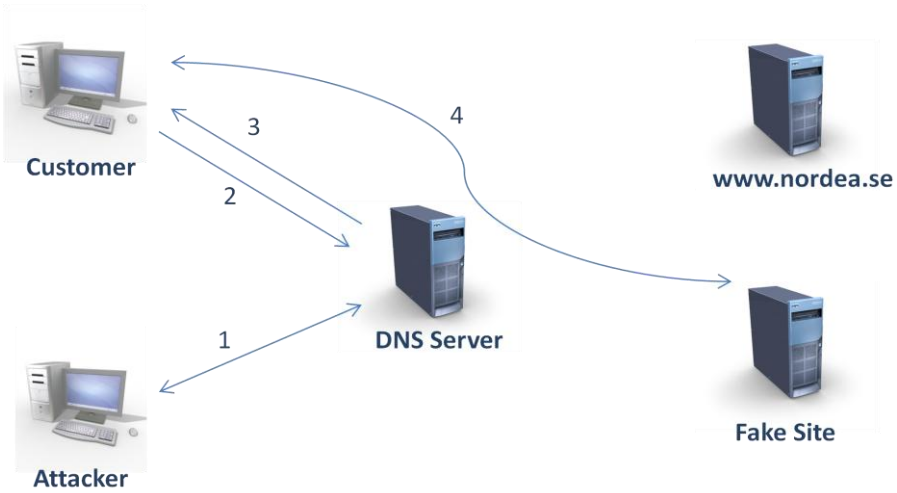

Figure 4: DNS spoofing

2.1.5. IP Spoofing

In IP address spoofing, the attacker abuses the trust relationship between two hosts. One possible attack is to use the fact that the victim's firewall may only let packets which have specific trusted source IP address to enter. So the attacker can generate packets with the IP address of a trusted host in order to impersonate the trusted host [3].

2.1.6. ICMP Flooding

ICMP flooding attack is a typical DoS attack which can overload the buffer of the victim computer with unwanted ICMP packets (Figure5) [1].

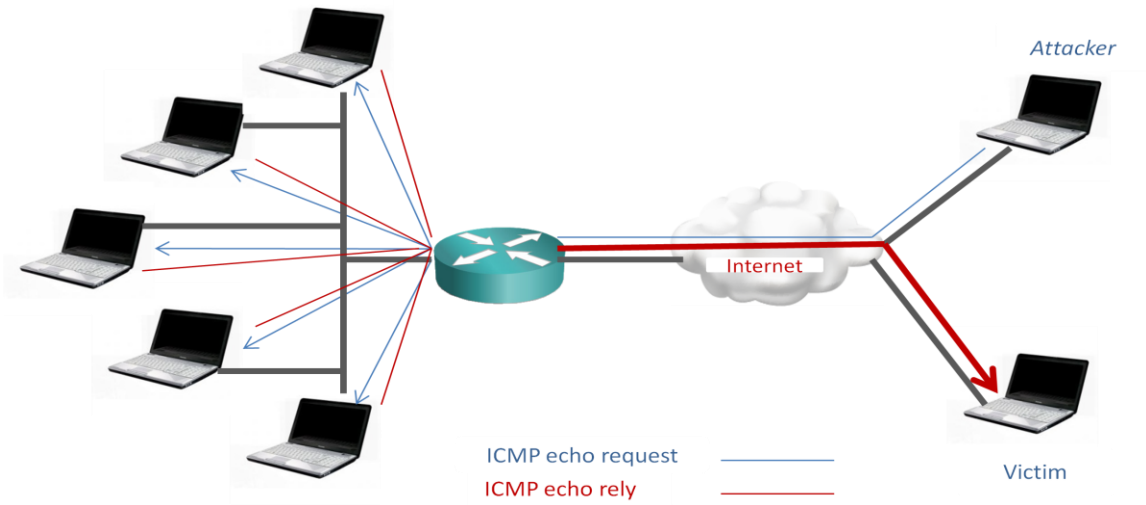

Figure 5: ICMP (Internet Control Protocol) flooding attack

2.1.7. SYN flooding attack

In the SYN flooding attack, the attacker creates large number of connections causing the connection queues to overload. The result is that other legitimate TCP users cannot initiate new connections [5].

2.1.8. UDP flooding attack

In this attack which is known as the "Pepsi attack", the attacker sends a UDP packet to a random port on the victim. When the victim receives the UDP packet, it will determine which application is waiting on the destination port. If there is no application owning the port, it may generate a destination unreachable ICMP packet to the fake source address. Therefore, if the attacker sends a large number of UDP packets to the victim, it may occupy network and CPU bandwidth [1]. However, if there is an application running, data may interfere with its normal data transfer since no sequence numbers are present in UDP.

2.1.9. Ping of Death

In this kind of attack, the attacker overflows the buffer by sending a ping (ICMP echo request) packet that is larger than 65,535 bytes (Figure6). Since a ping larger than 65,535 bytes is too large to fit in one packet for transmitting, IP allows a packet to be fragmented, essentially splitting the packet into smaller parts that are finally reassembled. When the packet is reassembled in the destination, the size of the packet results in buffer overflows and accordingly the system may crash or behave strange [1].

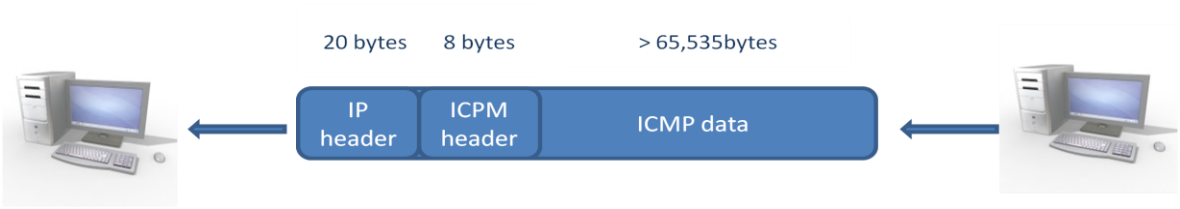

Figure 6: Ping of death attack (original packet)

2.1.10. Smurf attack

In the Smurf attack, which is a network-level attack, the attacker sends a large number of ICMP echo messages to IP broadcast addresses with a spoofed source IP address of a victim. If the router then sends the ICMP echo traffic to the IP broadcast address, all hosts on the network will receive the echo request, reply to it and send the echo reply to the victim and cause a huge traffic (Figure7) [1].

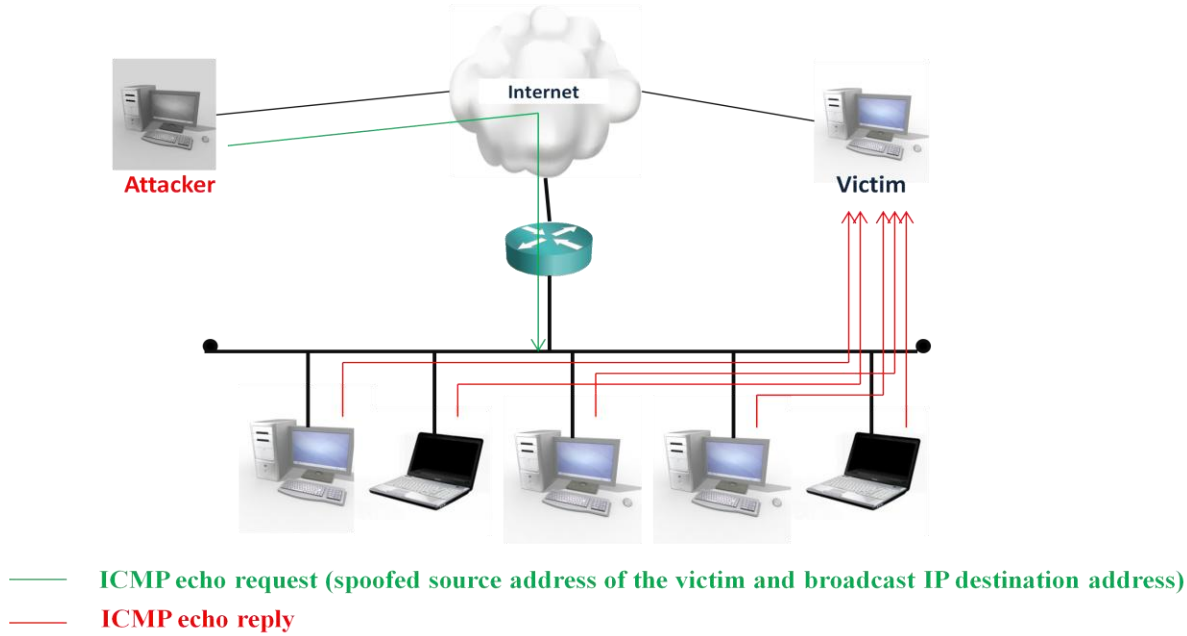

Figure 7: Smurf attack

2.1.11. Email flooding attack

In the email flooding attack, the attacker can drown a mail server with junk mails and cause the mail server to crash.

2.1.12. Distributed Denial of Service attack (DDOS)

The Distributed denial of service attack is a serious security threat to Internet communications. In this type of attacks, the attacker sends a large stream of packets through zombies to a victim and by consuming some key resources it prevents the victim from providing services to legitimate users (Figure8) or renders it unavailable to the victim's legitimate clients. Another approach is for the attacker to send a few malformed packets that confuse a protocol or an application on the victim machine. Yet another possible way to deny services is to sabotage machines in a victim network and consume some key resources so that legitimate clients from the same network cannot gain some inside or outside services.

The DDoS problem is very hard and complex to solve because the attacker can take control over thousands of machines and engage them to generate lots of packets simultaneously by using many automated tools. These tools are easy to use and can damage the target strongly [4].

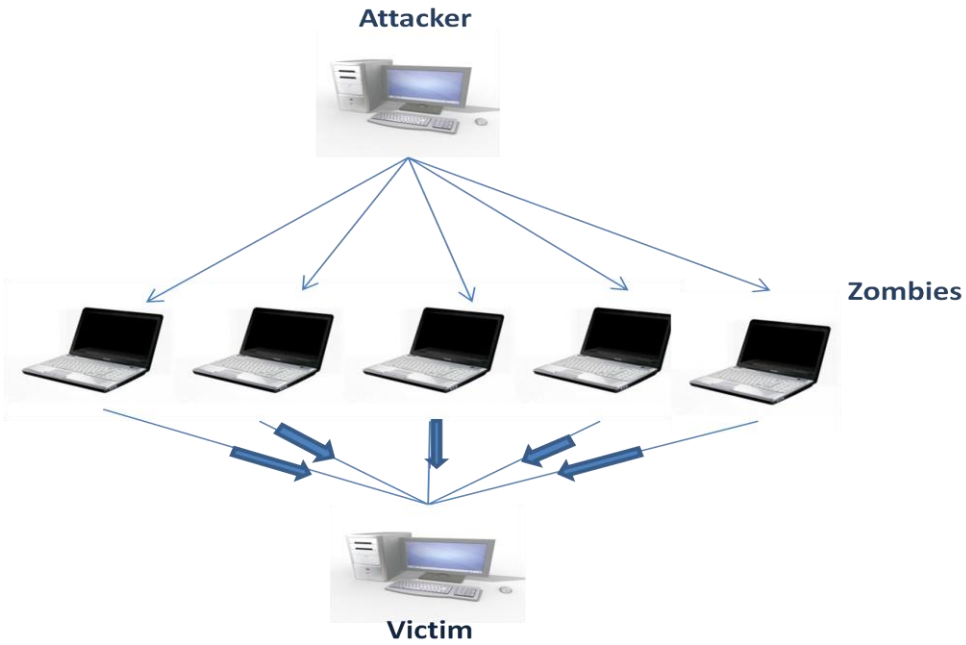

Figure 8: Implementation of DDoS Attack

2.2. Countermeasures

2.2.1. Protection against Spoofing

Since ARP packets in wireless networks are broadcasted without any authentication, performing ARP poisoning attacks and ARP spoofing attacks is not complicated. There are some countermeasures to reduce these kinds of attacks. A simple defense technique that only works for simple ARP spoofing attacks is the use of static IP-MAC mappings. Although, this only prevents simple attacks and it is not practical for large networks as the mapping has to be set for each machine.

Checking for the existence of MAC address cloning may also give a clue to the presence of ARP spoofing (although there are valid uses of MAC address cloning). Reverse ARP (RARP) is a protocol which is used to query the IP addresses related to one MAC address. If more than one IP address is found, MAC cloning is present. It is also possible to use Intrusion Detection Systems (IDS) to detect ARP poisoning attacks. Arpwatch is a tool that can monitor a network for any changes in MAC address to IP address association.

In order to be protected against IP spoofing, the solution is to apply ingress filtering and have all internal routers to disable source routing.

Web spoofing can be prevented by educating users to be conscious about the address window in a web browser that shows the web address they are directed to [1]. In addition, DNS spoofing can be prevented by securing the DNS servers and by adding anti-spoofing measures to the filter-list to check site ratings for URLs by their name and IP address. DNS lookups are supported to filter-list information for improved IP address lookups.

2.2.2. Protection against DDoS attacks

In comparison with other attacks, DDoS attacks are more fatal and therefore more precautionary schemes are needed such as using firewalls and routers due to ingress (inbound) and egress (outbound) filtering, applying antivirus software with up-to-date signatures and also installing some updated security patches. Additionally, by capturing packets, looking at the network traffic and comparing it with the normal traffic pattern, abnormal traffic from a specific source can be blocked. Generally, the following countermeasures can be taken as precautionary techniques against DDoS attacks:

- Filtering the packets with broadcast address as a destination address which are coming into the networks.
- Turning off directed broadcast address on all internal routers.
- Blocking any packet with the source addresses which contain address space 10.0.0.0, 172.16.24.0, 192.168.0.0 and loop back address 172.0.0.0 to enter.

- Setting rules in the firewalls to block any packet that apply a port or protocol which is not for Internet communication in the local area network.
- Preventing packets with a source address belonging to the inside to enter the network.
- Applying DoS detection tools like Air Magnet and Air Defense.
- Scanning the computer systems and network to ensure that they contain no publicly known vulnerabilities.

If these precautionary techniques fail and DoS attacks are detected, non-critical services should be disabled or degraded and services should be shutdown until the attack has been subsided [1][4].

2.2.3. Protection against Eavesdropping Data

A combination of strong authentication and encryption (such as 802.1x RADIUS authentication and WPA or WPA2 encryption with TKIP) can be used to prevent attackers from accessing sensitive and confidential information by eavesdropping access points (figure 9) [1].

Figure 9: Eavesdropping

3. Security issues in Smartphones

Smartphones are very similar to PCs and laptops; therefore they encounter almost the same security problems and even worse with respect to memory and space limitations. Security in smartphones is usually neglected since the manufacturers focus on development of new features and fast releases of new services more than security issues. Since smartphones as opposed to ordinary mobile phones use different technologies and provide extra services, they are more exposed to different attacks.

Although the different types of smartphones use different operating systems such as Symbian OS, Microsoft Window Mobile, Palm OS and embedded Linux (Android) where design, functionality and network stack architecture vary, they all have the same following features[9] [10]:

- They all support different cellular standards such as GSM/CDMA and UMTS to access cellular networks.
- They can access the Internet through different network interfaces such as Bluetooth, WLAN (IEEE 802.11), infrared and GPRS, and have a TCP/IP protocol stack for connection to the Internet.
- They can be synchronized with desktop PCs.
- They are able to multi-task and run multiple applications simultaneously.
- They have open APIs (Application Programming Interface) to develop the applications.

In the next section different ways that smartphones can be damaged and disabled are described.

3.1. Attacks against the network stack in smartphones

Smartphones are vulnerable through their network stacks. Since most operators apply Network Address Translation (NAT) for connection through 3G, GSM and GPRS, attackers are not able to scan and detect the smartphones and their services they may offer to the Internet. So, NAT can be a protection against lots of attacks. WLAN access, though, is different and the IP addresses being used on the WLAN may be detected by any user in the Internet. Therefore many different link-level attacks can be launched through wireless access points.

Vulnerabilities in the network stacks in smartphones depend on what operating system they have and on the implementation. Lots of tests have been done by researchers to assess the robustness and stability of the network stack in smartphones with different operating systems.

In the following paragraphs, some valuable test results of stability and robustness of the network stacks in smartphones with two different operating systems is described.

3.1.1. Security problems of the network stack in smartphones based on Windows mobile 5.0 platforms

Some tests such as network scanning, vulnerability scanning and penetration testing have been done by researchers to assess the security level of the network stack in smartphones which were based on the Window Mobile 5.0 platform. In network scanning, by applying the Nmap tool as a port scanner, all hosts on the network with their active ports and all services running on them were identified. In vulnerability scanning, all hosts, open ports and also some information about possible problems such as vulnerability in application level protocols or problems in applications themselves were determined. In addition, the vulnerability scanning showed out-of-date versions of software and also lack of relevant patches. Finally, in penetration testing some actual attacks were implemented by known attack tools against the network stack to analyze the robustness of the network stack [6].

In the following, the results of these tests have been described and it is possible to observe how vulnerable the smartphones based on mobile 5.0 platforms handle various attacks [7]:

- The result from network scanning shows that by capturing the packets and analyzing the TCP and IP header, the network stack's architecture of smartphones is very similar to the operating systems of other Microsoft windows desktop systems. So, the same vulnerabilities in windows systems exist in these types of smartphones.

- The result which has been extracted from the vulnerability scanning proves that, the Etherleak problem which is a common vulnerability in many operating systems exists in these smartphones. Therefore attackers on the same subnet can send an ICMP echo message and get information stored in the memory of the target's operating system due to a bug in the Ethernet driver. Unfortunately, although the desktop operating systems have patches for this problem, no patches have been received for Windows Mobile 5.0 yet.

- It was observed that these types of smartphones are vulnerable to denial of service attacks (DoS attacks). For example by using the ArpSpoof tool the attacker can spoof the ARP entry of the router or gateway (as a victim) and send a gratuitous ARPs to the smartphone which opens up for MITM attacks. Another scenario for performing a DoS attack is to intercept the traffic between the smartphone (target) and router (AP) by using fake ARP reply packets. This can be done without seeing any warning messages.

- Another security problem found in these smartphones is that they are vulnerable to the well-known IP Options attack (IGMPv3 exploit). In this type of attack, the attacker can hang the smartphone by sending specially crafted IGMP packets. So when the

smartphone receives theses packets it hangs completely, becomes unusable and it requires being reset to go back to the normal state.

- Since these types of smartphones have dual stack architecture, they are vulnerable to Neighbor discovery spoofing. In this type of attack, the attacker can perform a spoofing attack via the neighbor discovery protocol in IPV6. For example, by spoofing neighbor advertisement a malicious node can make the Duplicated Address Detection process fail for a host which is seeking to assign itself a network address with auto configuration. Consequently, the host will stop to use that address and it may never be able to find a valid IPv6 address. Sending spoofed advertisements can also overwrite the neighbor's caches on nodes. Therefore, some packets may be sent to the wrong destination, which results in service DoS.

It should be mentioned that the smartphones which have been tested had no firewall, antivirus or intrusion detection system installed. Maybe, by installing such protection tools on the smartphone some of the mentioned vulnerabilities can be solved. Despite some well-known attacks such as Ping of Death, IP/TCP Fuzzing, Bonk, Naptha, Teardrop, Land attack, Boink, Blat and Newtear/Opentear that these devices could handle successfully, these types of smartphones are not suitable to work in complicated and unfriendly networks environments.

3.1.2. Security problems of the network stack in Symbian based smartphones

In order to analyze the robustness and stability of the Symbian based smartphones, the same test methodology has been used. When implementing these tests, two different Symbian based smartphones from Nokia and Sony Ericsson, some well-known attack methods and also tools such as Wireshark and packet sniffing software were used. Although these devices are come from different Vendors, they use the same operating systems and they are vulnerable against the same attacks.

In the following, some test results have been mentioned to show the stability and robustness of the Symbian based smartphones [8]:

- By performing network scanning and applying Nmap "host discovery techniques", it is possible to find the IP address, MAC address and all open/closed/filtered ports of the smartphone. In addition, by using a fingerprinting technique it is possible for attacker to check which operating system is running on the device and get more information about the network stack architecture and its services in preparation to launch an efficient attack.

- The test results show that these devices are vulnerable to the SYN DOS attack. When the Sony Ericsson device was flooded with SYN packets, it stopped to work and it couldn't communicate with the access point on the WLAN and it needed a restart whereas the Nokia device acted smarter and just became very slow.

- The results from the penetration tests show that these devices are vulnerable to ARP spoofing attacks. This attack was done with the arpspoof tool, with one Linux host as an attacker and one router/gateway as a victim whose ARP entry was being spoofed and two smartphones. This attack was performed in two different ways. In the first scenario, an address conflict was created by using the target's own IP address and a MAC address which did not belong to the device. As a result both devices determined that there was a collision in IP addresses and asked for a new address using DHCP and this behavior was repeated every other second and the network connection was impaired consequently. In the second scenario, the attack was performed with the target's own IP and Mac address in order to confuse it. Hence, the Sony Ericsson device hanged after a short while but the Nokia device behaved normally and no changes observed during this attack.

- Yet another security problem found in these smartphones was that the traffic between the AP/router and the target can be hijacked by using fake ARP requests, and no warning message will be shown in the smartphones.

It should be mentioned that the smartphones which have been tested had no firewall, antivirus or intrusion detection system installed. Maybe, by installing such protection tools on the smartphone some of the mentioned vulnerabilities can be solved. Despite some well-known attacks such as Neighbor discovery spoofing, Ping of Death, IP/TCP Fuzzing, Bonk, Naptha, Teardrop, Land attack, Boink, Blat and Newtear/Opentear that these devices could handle successfully, these types of smartphones are not suitable to work in complicated and unfriendly networks environments [8].

3.2. Infections from the Internet

The evolution of smartphone viruses is at a very fast space, maybe because of the experience virus writers have obtained from the computer and Internet world. Since Smartphones like PCs are capable to be Internet endpoints by using web browsers, email and other applications, they can be infected by various viruses, worms and Trojan horses in the same way as PCs and other systems [10].

Without proper protection, web browsers like other software are vulnerable to different attacks. There are many browser-based attacks originating from "bad" websites. Due to poor security in web applications and vulnerabilities in software supporting web sites, attackers are able to compromise many trusted web sites to send malicious payloads to visitors. Attackers can also add scripts that don't alter the website's appearance in order to redirect the visitors to another web site which may cause malicious programs to be downloaded into smartphones and obtain personal information. This type of attack is called a phishing attack which is also typically carried out by e-mail or instant messaging.

In addition, smartphones can be infected by downloading any electronic material such as attachments and phone applications from the internet. Many malicious applications can be downloaded to the smartphones to steal phone numbers, address information and notes stored on the devices such as passwords or bank account details. These applications can be hidden within something seemingly harmless like a game. Consequently, smartphone users can be lured into downloading files such as *Doomboot* and *Skulls*, disguised as games, and end up getting infected by virus. For example, recently a Symbian based Trojan horse has been found in famous game software in smartphones.

3.3. Infection through compromised PCs

Smartphone users usually need to establish a trust relationship between their smartphones and their PCs due to synchronization of calendar, emails, music and other data through synchronization software such as ActiveSync or iTunes. Accordingly, many viruses could potentially penetrate the smartphone in the event of synchronization. Although, in order to do this the virus must first compromise the PC before it can be transferred to the smartphone [10].

3.4. Peer smartphone attacks

Smartphones are wireless mobile devices and they can move between locations easily. Because of the mobility feature, they can connect to other smartphones through Bluetooth or Ultra Wideband in various locations (Figure10). Therefore attackers can abuse this ability and infect other peer smartphones through one compromised smartphone. Cabir, The first smartphone worm, which was released in 2004, applied this technique for infection.

In addition, Smartphones can be infected by receiving malformed SMS from other malicious smartphones' users [10].

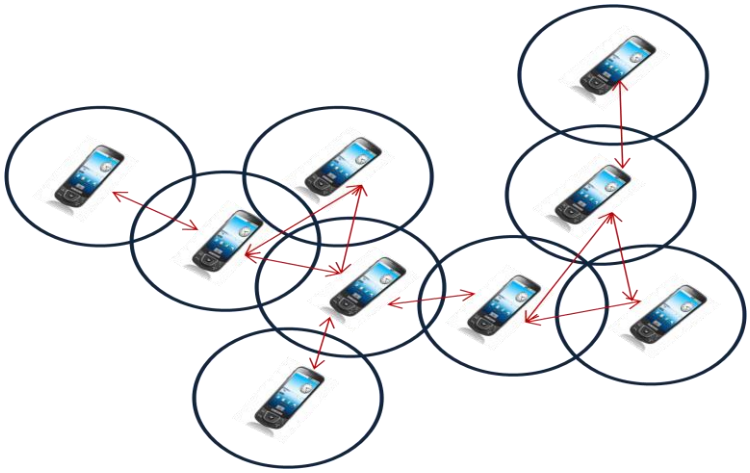

Figure 10: Peer smartphone attack

4. Potential Bluetooth vulnerabilities in smartphones

Bluetooth technology has been introduced to smartphones in order to create a personal area network and also exchange data more conveniently among them. Bluetooth security in smartphones is optional and discoverable mode has been considered as a manufacturing default mode. It should be mentioned that Bluetooth viruses are innovative in that its spreading doesn't rely on the existence of any network infrastructure. Instead, it uses the short range wireless connectivity and the mobility of the mobile users to infect nearby Bluetooth users directly. Security vulnerabilities in Bluetooth-enabled smartphones have lead to serious and severe breaches. With respect to this issue, some potential Bluetooth weakness and implementation flaws in smartphones are presented in this chapter:

4.1. Paring

Bluetooth devices such as smartphones are vulnerable to active and passive attacks during the paring procedure that take place once between two devices. Thus the probability of attacks may increase if this procedure is done in public places. In this section, the attack against the combination key, which also easily applies to unit key, is explained:

The Unit key and combination key are two types of link keys applied for authentication and encryption between Bluetooth devices. The paring procedure between two devices A and B needs the establishment of an initialization key (K_{INIT}) which is calculated with the E22 algorithm with three inputs: Bluetooth device address (BD_ADDR), random number (IN_RAND) and a secret passkey or PIN (PKEY). K_{AB} is a combination key which is not sent specifically through the air. Actually it is made by a local generated random value (LK_RAND) and it is transmitted by $K_{INIT} \oplus$ LK_RAND (Figure11). Both devices are able to derive the respective LK_RAND because they have common understanding of an initialization key. SRES is an authentication output and E1 is used in authentication phase using verifier AU_RAND, K_{AB} and claimant BD_ADDR.

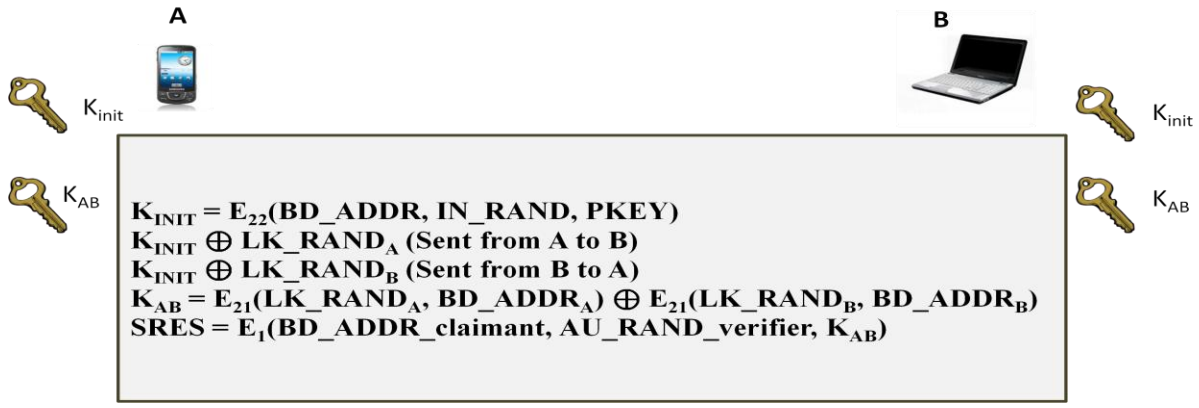

Figure 11: Paring procedure algorithm

When device A and B perform the paring procedure, the attacker can see the following information in clear text over the air (figure12).

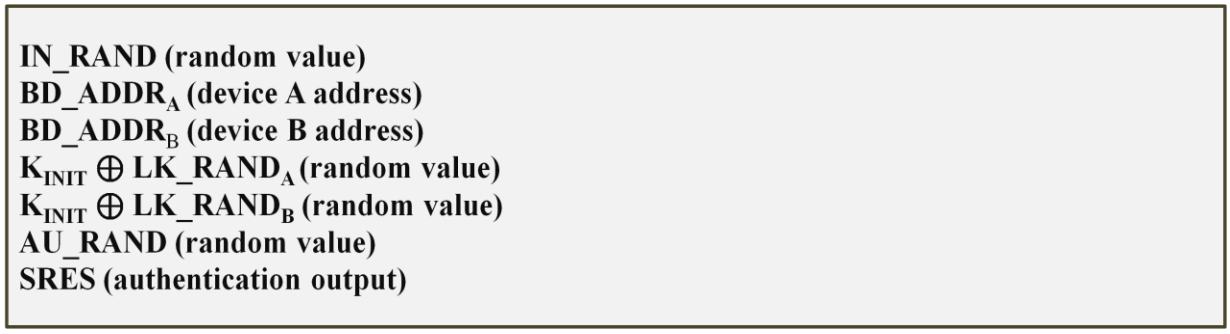

Figure 12: Information transmitted in clear text

After such an attack, the passkey is the only unknown parameter in the computation of current link key (combination key). Then the attacker tries a range of passkey applying the result to calculate the corresponding SRES, and later verifies with the observed SRES value offline. In this attack scenario, first the attacker secretly listens and collects all the above transmitted information between two paring devices. Then the attacker executes an offline brute force attack on a range of passkeys in order to find the right passkey (the only unclear parameter). The attacker can verify the correctness of the passkey by matching the corresponding SRES with the observed SRES value. Therefore during the paring procedure, any smartphone which uses short and easily guessable passkeys for connecting to other devices is exposed to eavesdropping and man-in-the-middle attacks [11] [18].

4.2. Key disclosure

Since secure storage and access control of the link key database has not been specified in the Bluetooth specification, the danger of improper key storage which leads to key disclosure and key database modification may increase. In most smartphones the key database is kept in memory and an attacker may access the memory by applying special equipment and proper knowledge. However, in smartphones acquisition of link keys is easier due to an external Bluetooth Compact Flash or SD input/output adapter.

If the link keys are kept in plain text in the memory, an attacker can impersonate the real Bluetooth adapter with a malicious adapter to regain the stored link keys. This is done by using command HCI link key request with BD-ADDR as a parameter. By applying the link key and the device address, the attacker can pretend to be the actual device and abuse some services offered by smartphones [11].

4.3. Key database modification

By changing or inserting link keys/address pairs in the key database, an attacker acquires unlimited access to all Bluetooth services on the victimized smartphone without having to perform a paring procedure. So instead of impersonating an existing device, the attacker can connect to a victimized smartphone which is using an altered entry in the key database. Due to lack of integrity check of the database and lack of methods for detection of altered key database in the Bluetooth specification, an attacker can spoil the key database by changing all the link keys/address pairs [11].

4.4. Inquiry attack

The Bluetooth device address (BD_ADDR) is a unique identification for a Bluetooth enabled device. Attackers can deploy numerous Bluetooth devices in a specific area to find the exact location of the targeted users. In the case where the victim device is in the discoverable mode, attackers can execute an inquiry scan in order to find the device and maintain a log of all the device addresses that are discovered. This data can be correlated with time to manifest users' movement and their relation with other users who gather at the same area [11].

4.5. BlueSnarf attack

There are some security oversights in the Bluetooth specification which affect the overall device security and have lead to faulty implementations that can be exploited using tools such as BlueSnarf. This vulnerability lets an attacker to connect to a Bluetooth enabled device without execution of the normal paring procedure. Then the attacker can access stored information such as calendar details, phonebook, business cards, International Mobile Equipment Identity (IMEI) and real time clock settings without warning the owner. This attack can be performed even if the device is not in the discoverable mode [12].

4.6. Backdoor attack

Some security vulnerabilities in Bluetooth let the smartphones leave some information on a device although the former pairing information has been deleted from the paired device list. Since the pairing entry is not visible to the user, full access to the device is given without the owner's knowledge according to the former trust relationship. In this type of attack, the attacker can pair the devices secretly. Not only the attacker can manipulate smartphone's data but also he/she can get access to modem, WAP and GPRS services and the victim would not be aware of the unauthorized access unless he/she observes the small icon showing an established Bluetooth connection [11].

4.7. BlueBug

Another type of Bluetooth attack which is caused by lack of awareness is Bluebugging. BlueBug is based on ASCII Terminal commands (AT) which is very common for configuration and control of telecommunications devices like modems. When the smartphone is attacked, this security flaw lets many things happen without notifying or alerting the user such as:

- Starting phone calls
- Reading SMS from the phone
- Sending SMS to any number
- Writing phonebook entries
- Reading phonebook entries
- Setting call forwards
- Connecting to the Internet
- Compelling the phone to apply a specified services
- Updating calendar
- Configuring phone settings
- And many more things

In addition, the vulnerable smartphone can be abused as a bug to eavesdrop on conversations which happen around the phone by making smartphone to call the attacker [13].

4.8. Bluejacking

The Bluejacking attack is done by sending flirt and unsolicited messages in a Spam-like manner to Bluetooth enables devices, mostly in the form of vCards. In order to perform Bluejacking attack, an attacker can create a phonebook contact with an attractive message in the name filed and propagate it in a crowded area via the OBEX protocol. Although this attack doesn't change or remove any saved data in smartphone, it bothers the user with unwanted messages. This vulnerability can be abused as a marketing tool by vendors to advertise their objects. Generally, a Bluejacker sends only a text message, but with new modern phones it is possible to send sounds and image as well [14].

4.9. Blue Smack attack

The Blue Smack attack is a Bluetooth version of the Ping of Death attack. In this type of attack, attackers try to overwhelm the insecure device by sending large ping packets which could cause it to crash [15].

4.10. DoS attacks

Bluetooth-enabled smartphones are vulnerable to DoS attacks. For example, attackers can perform a DoS attack against the smartphones' battery. In this case, continuous query or responding to constant requests from the receiving side can degrade the battery of the smartphone (Figure13).

Figure 13: Effect of DoS attack on smartphone

Another feasible scenario for this type of attack would be to saturate the smartphone with invalid Bluetooth packets thereby blocking communication channels and the victim cannot use the other Bluetooth services for a period of time. The physical communication link of the Bluetooth uses two logical channels, Synchronous Connection Oriented (SCO) and Asynchronous Connection Oriented (ACL). In addition, Bluetooth devices guarantee a maximum number of active connections simultaneously with 2Mbps bandwidth. In order to block the bandwidth, an attacker can pretend to be a trusted smartphone which is paired with the victimized device and make requests with no acknowledgment. When the acknowledgement is not received, the smartphone will resend asynchronous data over the ACL link. Therefore by using several smartphones to connect to the device and requesting large number of asynchronous data, the DoS attack can be implemented [16].

4.11. Uncontrolled propagation of Bluetooth signals

Since attackers may use Bluetooth devices with high-gain 2.4GHz directional antennas (HGA) and amplifiers to enhance the weak Bluetooth signal, they are able to eavesdrop from a distance more than the common range. So, it is possible for attackers to read the transmitted data from a very long distance without being detected.

Moreover, attackers will have enough time to implement attacks from the more secure distance. For example, an attacker can send a low-level jamming signal to interrupt the connection and

reconnect the victim's smartphone with an external keyboard. After calculating the passkey it is possible to register every keystroke by listening secretly to the paring procedure [11].

4.12. Blueprinting

Every Bluetooth enabled device has specific attribute like unique device address (BD-ADDR). Blueprinting is the Bluetooth version of fingerprinting which is a technique to get information regarding the smartphone's attributes such as model type, device manufacturer and firmware version. By applying this technique, an attacker can reveal unsecure smartphones [17].

4.13. Relay attack

A Relay attack is rather similar to Man-in-the-middle attack, although the attacker doesn't have to know the link key or passkey. This attack is a form of active eavesdropping in which the attacker makes independent connections with the victims (for example, attacker C communicates with A impersonating as B and communicates with B impersonating as A) and relays messages between them without changing the contents making them believe that they are talking directly to each other over a private connection. However, in fact the entire conversation is controlled by the attacker. The attacker can cause DoS attack by delaying or stopping the relaying procedure [11].

5. Smartphone attacks against the telecom networks

When evaluating security, we should not only focus on attacks against the smartphones but also it should be considered that it may be used as a conduit to connect to different networks. Since Smartphones are interoperable devices, they can operate between the Internet and the Telecom networks (Figure14). In other words, smartphones are endpoints in both networks and can connect the telecom network and Internet together. These devices are possible bridges for bringing Internet security problems to the telecom networks. They can cause serious damages such as privacy violation, DDoS attacks against call center and identity theft.

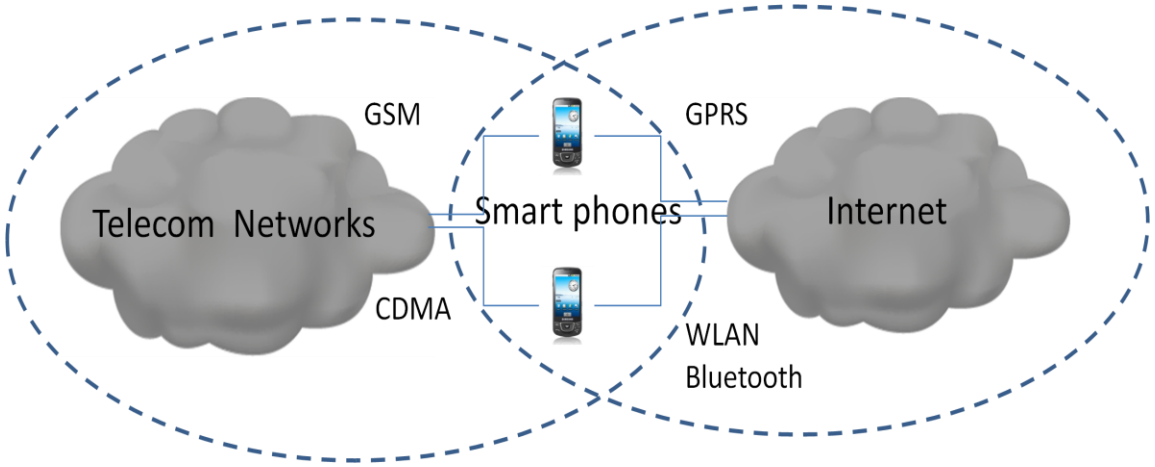

Figure 14: Smartphones are endpoints of both the telecom networks and Internet

In this section before describing different attacks against the telecom network, a brief description of the GSM cellular network as an example of a telecom network is given.

5.1. GSM background

As seen in Figure 15, GSM comprises of three sub systems [19]:

- The Mobile Equipment (ME): has a Subscriber Identity Module (SIM) to store identities such as IMSI (International Mobile Subscriber Identity).

- The Base Station Sub-system (BSS): consists of BTS (Base Transceiver Station) and BSC (Base Station Controller). The BTS is used for handling radio interface between MEs and BTS. The BSC is used for managing radio resources and handovers.

- The Network Switching Sub-system (NSS): applies MSC (Mobile Switching Center) for routing phone calls and connecting GSM to PSTN or other public networks.

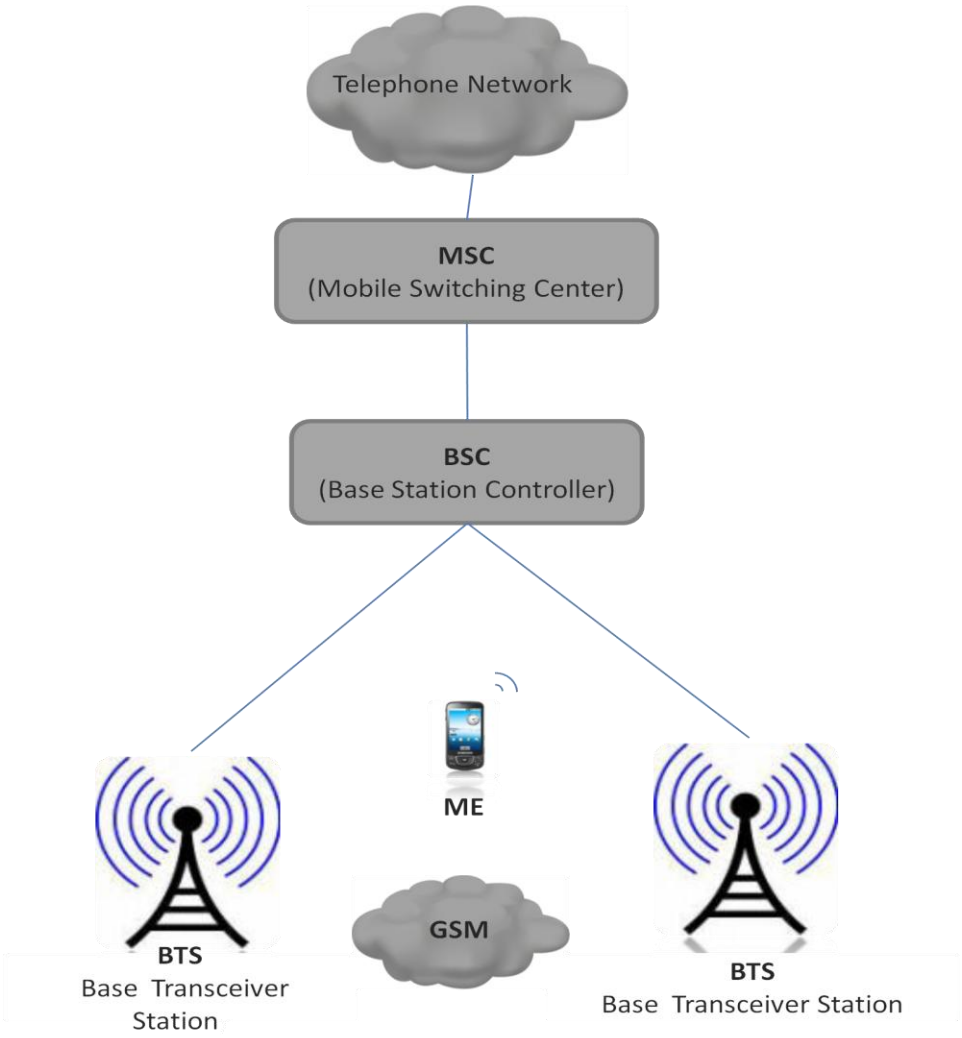

Figure 15: The GSM network

GSM offers various services besides of the voice communication such as Short Message Service (SMS), Multimedia Message Service and General Packet Radio Service (GPRS) for Internet access.

In general, in any cellular system the radio spectrum is a scarce resource. For space-sharing or time-sharing of the radio resources, GSM applies a combination of Time and Frequency Division Multiple Access (TDMA/FDMA). FDMA separates the maximum 25 MHz bandwidth into 124 carrier frequencies of 200 KHz bandwidth each. One or more carrier frequencies are designated to a base station. Then each of the carrier frequencies is split into 8 time slots with the TDMA

scheme. If a base station has *n* carrier frequencies, then the maximum amount of voice users which it can support is at most *8n* (*C=8n*).

Telecom networks run according to two assumptions:

- User identities with their SIM cards or telephone numbers are firmly coupled. Thus SIM cards or telephone numbers are applied for accounting purposes.

- Their traffic is extremely predictable. Therefore according to this traffic prediction model, telecom carriers can plan their network capacity [19].

5.2. Possible Smartphone attacks

There are different possible smartphone attacks against the telecom network such as:

- Bandwidth exhaustion attack against base stations
- DDoS against call centers and switches
- Remote wiretapping
- Phone blocking
- SMS spamming
- Identity theft and spoofing
- Physical attacks

In the following, some of these attacks are described:

5.2.1. Bandwidth exhaustion attack against Base Stations

The radio channel of a GSM base station with *n* carrier frequencies is a limited resource and can be easily overflowed by *8n* smartphone zombies in the same cell starting calls and consuming all the base station's time slots. As soon as the call setups complete, the smartphone zombies hang up and try to restart new calls and so on. In the case that a callee is also compromised and configured not to answer the phone call, the time slot at both sides of the caller and the callee can be occupied for about one minute in each call. Although the caller doesn't have to pay for this incomplete call, the radio resource has been consumed and wasted.

This kind of attack has a direct impact on the availability of the cellular network. Call blocking rate in telecom networks is a metric to determine the availability of the network. The call blocking rate should be less than 0.01%. The probability of the call blocking is estimated with the Erlang B formula:

$$B(s,a) \equiv p_s = \frac{a^s / s!}{\sum_{j=0}^{s} \frac{a^j}{j!}}.$$

s: The number of radio channels
a: The planned call volume to support
B: The call blocking probability

Typically the planned call volume is an average of 15-16 concurrent [10] users (a=15.63) and since the call blocking rate should be less than 0.01%, this base station requires 4 carrier frequencies and a sum of 32 voice channels (4* 8 time slots), therefore S is equal to 32 (s=32).

This formula presumes ordinary telephone calls, meaning that they are idle most of the time and the traffic volume from many phones is extremely predictable. However, these presumptions can be broken easily by compromised smartphones. For example, 8 compromised smartphones taking 8 out of 32 radio channels increase the probability of the call blocking rate to 1.2% (Figure 16). The call blocking rate may rise to 16.4% and 53.6% if 16 and 24 channels are occupied respectively and eventually the system will be out of service if all 32 radio channels are occupied. Therefore several compromised smartphones can saturate a small bandwidth capacity and obviously endanger the availability of the base station [10].

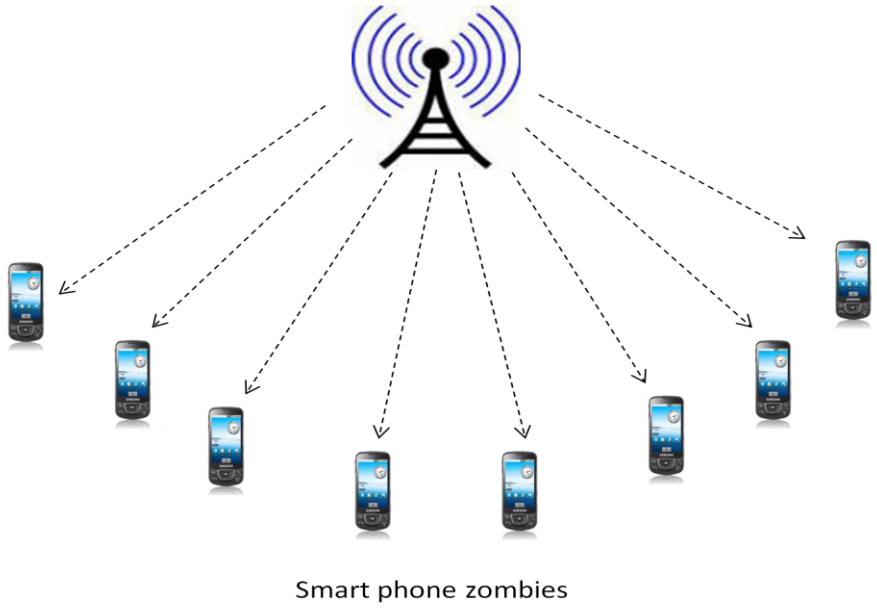

Figure 16: Bandwidth exhaustion attack against Base Stations

5.2.2. DDoS attacks against Call Centers

This type of attack is similar to the bandwidth exhaustion attack but unlike the previous attack where the aim was to exhaust radio resources, the aim of this attack is to bring call centers to a halt which is similar to DDoS attacks to web servers. A call center attack was not reasonable to implement in the past when traditional telephones were used because it was necessary to access many phones physically to dial call center numbers manually. In addition, it was very easy to trace back and find the attacker. Today, it is possible to compromise smartphone zombies making their owners victims while the attackers hide behind the victims. Consequently tracing back to the real attackers becomes very hard (Figure17).

Similar to call centers attacks a DDoS attacks can be done against cellular switches and PSTN which are designed for a limited Busy Hour Call Attempts (BHCA)[1]. By making the BHCA value out of the limited range, these cellular switches may break down. For instance, just after the terrorists' attack on September 11, 2001 in New York, it was very hard to call the residents because the phone switches was under a heavy load.

Smartphones DDoS attacks may not only disrupt some services and cause heavy financial losses, they can also endanger national security by attacking critical numbers such as 911 [10].

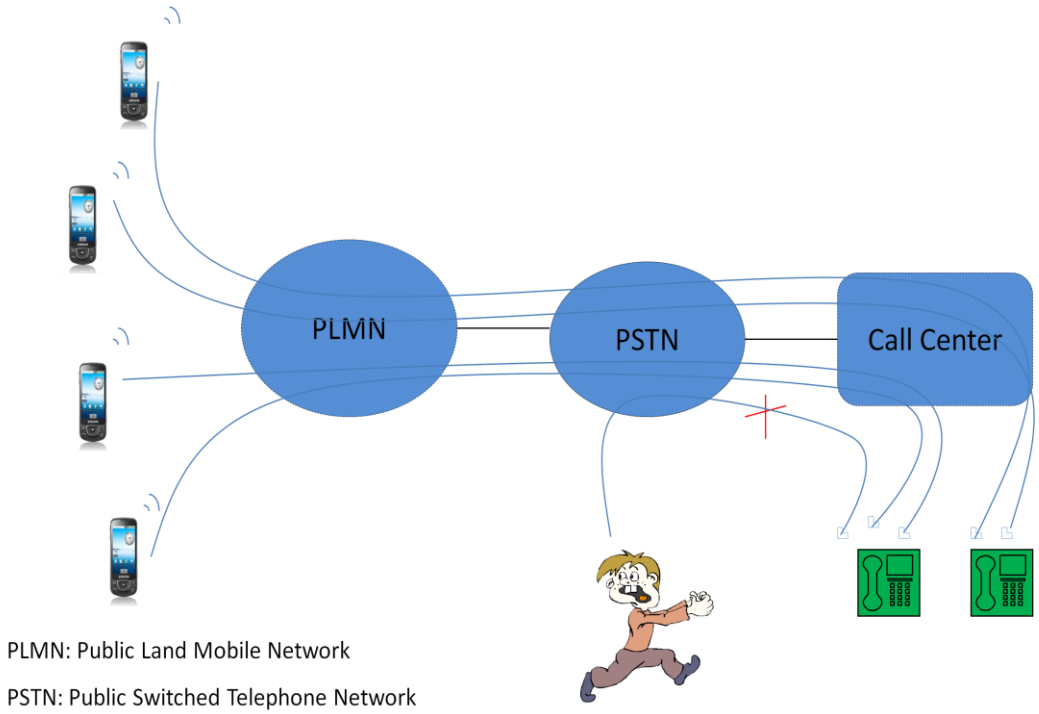

Figure 17: DDoS to call center

[1] BHCA is the number of telephone calls attempted at the busiest hour of the day (peak hour)

5.2.3. Spamming Attacks

In this type of attack, the attacker abuse smartphones and uses them as zombies to send lots of marketing messages or junk massages through SMS. In this scenario, the owner of the compromised smartphone is not aware of sending free spam [10].

5.2.4. Spoofing attacks and identity theft

It is hard to spoof the Telephone numbers or IMSIs stored on SIM cards which is the fundamental rule of authentication and accounting mechanisms in Telecom networks. Nowadays performing a spoofing attack or identity theft with smartphones is easy. When a smartphone is compromised, the attacker is in possession of the identity of its owner for any activity in his/her name.

Moreover it should be mentioned that with the possession of an identity and using application such as Voice-Over-IP, an attacker can pretend to be the smartphone's owner through a smartphone zombie for both incoming and outgoing phone calls [10].

5.2.5. Remote Wiretapping

In this type of attack, an attacker can record the conversion of a victim passively through a compromised smartphone on which a spyphone software such as FlexiSPY is installed (Figure 18). This software which is considered as a Trojan, is able to steal or read call logs, e-mail documents, SMS messages and GPS data from smartphones. Then, the captured data will be uploaded to an online server, where it can be observed by the attacker. It also causes the compromised smartphone to be used as a listening device. When a call is received from a predefined number, the phone will answer it automatically, which allows the caller to eavesdrop on active phone calls and private discussions. Therefore, it can result in blackmailing and espionage activity to extract more information. Physical access to the target phone is required for the Trojan to be installed. Depending on the operating system the installation takes only 3 to 15 minutes.

There are some signs to identify whether a cell phone is infected by Trojan or not:

- **Low charge:** Depending on the type of cell spyware, a battery life-span might be a lot shorter than the usual quantity of hours.
- **Unexpected invoices**
- **Strange flashes:** Suspicious lights up with no reason.
- **Weird sounds:** It is common in some spy software such as BlackBerry which has a live call interception feature.

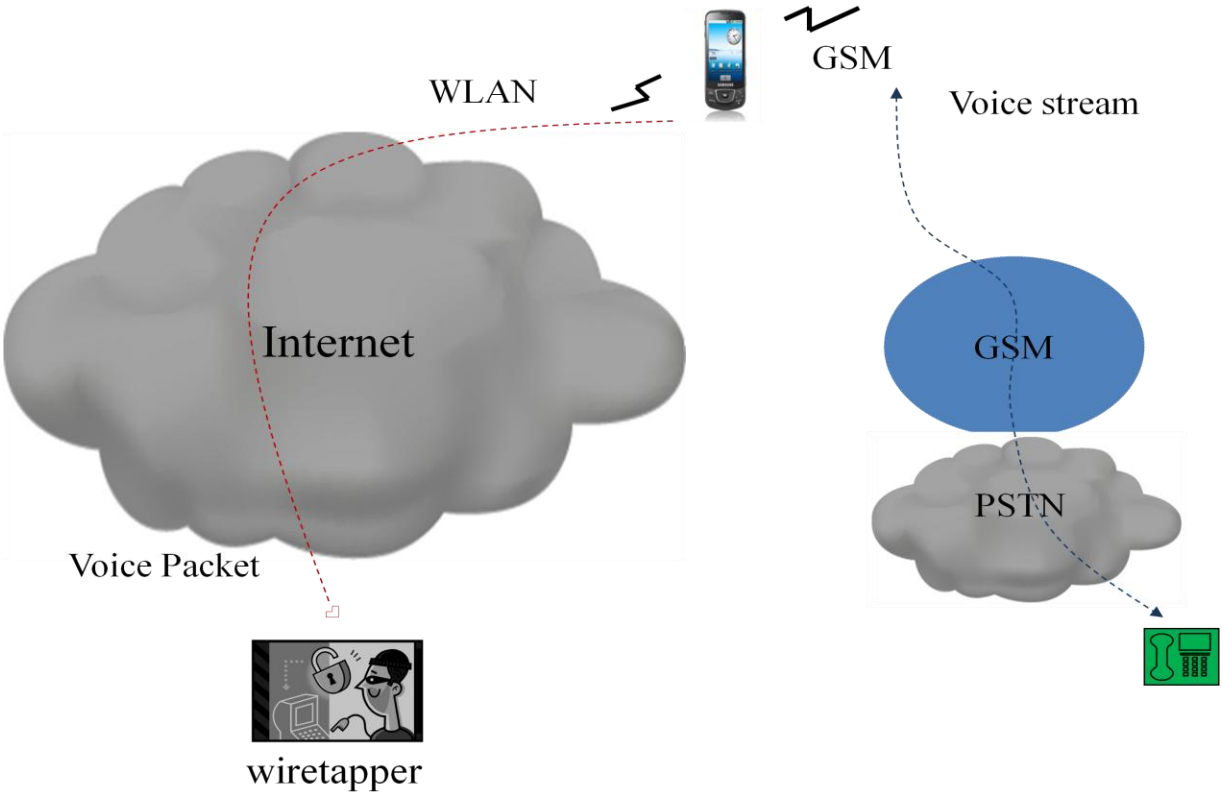

Figure 18: Remote wiretapping [22]

6. Defense techniques

In this section first, *SmartSiren*, a virus detection and alert system for smartphones is presented as a security solution that can effectively combat those viruses that spread through cellular messaging systems or Bluetooth. Then, some defense techniques against the smartphone attacks from four different viewpoints are described: What coordination may be needed between Telecom networks and the Internet; how it is possible to harden smartphones to be more secure; Internet side protection; and finally Telecom side protection. However these defense techniques can't protect against smartphones attacks 100%, they can be useful outlines for more challenging and better solutions.

6.1. SmartSiren: Virus detection and alert system for smartphones

As earlier described, smartphones are vulnerable to viruses due to their versatile communication capabilities. They are also difficult to harness because of their intermittent network connectivity and resource limitations which restrict the effectiveness of complex and on-device anti-virus solutions. Therefore, viruses can easily spread out and cripple both smartphones and the cellular and telephony infrastructures.

SmartSiren is a collaborative virus detection and alert system for smartphones. It can collect communication activity information from smartphones to detect both single-device and system-wide abnormal behaviors. The target of SmartSiren is to stop the potential virus outbreak by decreasing the number of smartphones that will be infected by a new released virus. The basic idea of the SmartSiren is quite simple: each smartphone runs a light-weight agent and keeps track of the communication activities (such as the usage of Bluetooth interface and cellular SMS service) on the device and periodically reports a summary of these activities to a centralized proxy. A centralized proxy is used to assist the virus detection and identify each smartphone as either infected or non-infected in order to alert the infected smartphone users about the suspicious activities. It also alerts those smartphone users that may immediately be vulnerable to infection from infected devices [23].

The proxy-based architecture has two advantages. First, since smartphones have restricted resources in terms of storage, battery power and computation, the use of a powerful proxy can offload most of the processing burden from the smartphones. Secondly, it can make the cooperation among the smartphones easier in order to have accurate virus detection and quick alerts. As it is illustrated in Figure 19, the architecture of SmartSiren consists of a large set of smartphones that want to be protected from virus outbreaks and a centralized proxy which interacts with smartphones through either IP-based Internet or cellular networks [23].

The most noticeable feature of SmartSiren is the protection of user privacy. In practice, most users don't like to disclose the activities on their phones to the proxy. SmartSiren can address this requirement by an anonymous and ticketed report submission scheme. This scheme not only

prevents the proxy from knowing the activities of any user, but also it doesn't let a virus or an attacker to abuse the privacy mechanism and inject fake reports in order to mislead the virus detection results [23].

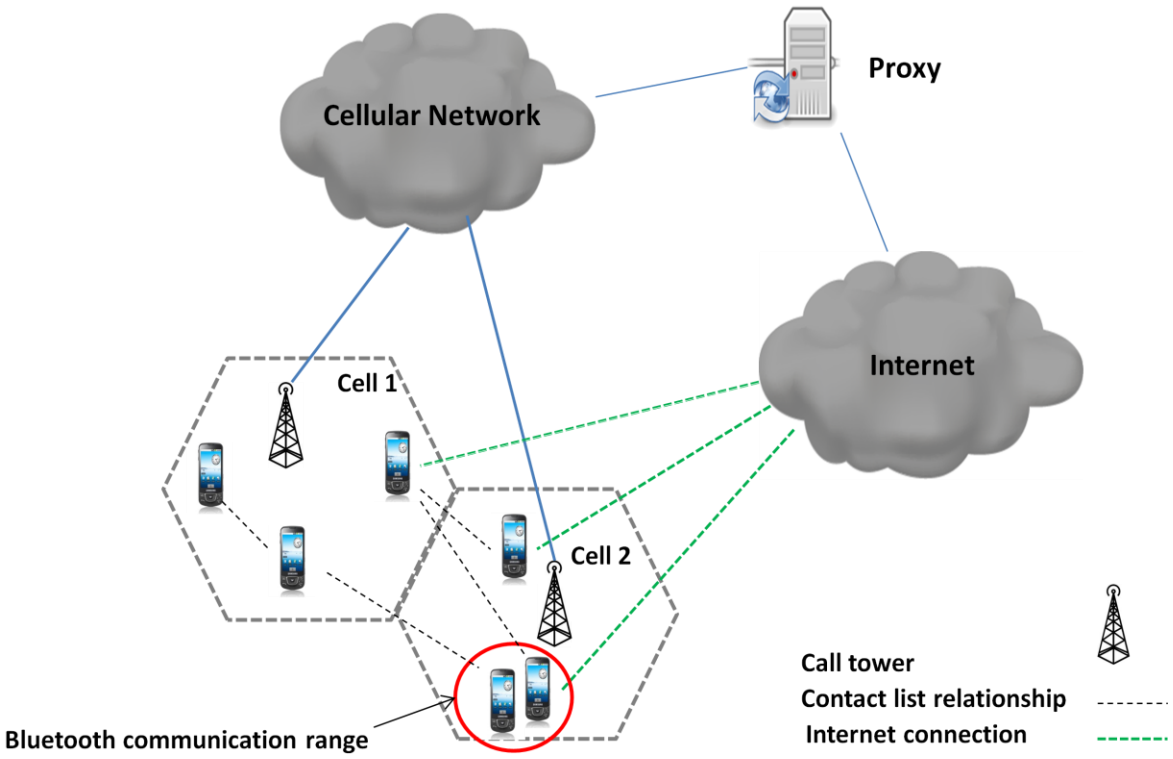

Figure 19: The architecture of SmartSiren [23]

6.2. Coordination between the Telecom Networks and Internet

Cooperation between the Telecom network and the Internet would be desired. In this part some opportunities and obstacles in cooperation between the Telecom networks and Internet for protecting against smartphones attacks are discussed.

Since attack information and well-known vulnerabilities can be interchanged between the telecom network and the Internet, the effect of smartphone attacks may be decreased by not enabling vulnerable services as much as possible. For example, getting information regarding the target of an attack from the Internet side (which call center will be a target of the attack) can help the call center to prepare against the attack through call filtering and rate limiting. In the same way, a telecom carrier can, by giving the black list of smartphone zombies, help the Internet community to refuse those zombies from connecting to the Internet.

In other words, when smartphone attacks are detected from the Internet, the Internet can inform the telecom operators to prepare in advance. In the same way when telecom operators detect smartphone attacks they can inform Internet users to place zombies on a black list [10].

6.3. Hardening the Smartphones

Smartphone hardening is one of the recommended solutions to make smartphones less vulnerable. There are some strategies for hardening smartphones [10]:

- **Operating system hardening (OS hardening):** some security issues can be enforced by smartphone operating systems. For example they always show the callee's phone number and also brighten LCD display when dialing. This can be achieved by only using security modified APIs to applications. There are also further policies for hardening operating systems such as using security patches and bug patches to software and limiting user privileges and disabling unnecessary processor.

- **Hardware hardening:** Smartphone already has an embedded smart-card (the SIM card) which has evolved to incorporate the use of the SIM Toolkit (STK)[1]. STK allows the mobile operator to provide services by loading them into the SIM card without modification of the GSM handset. One intriguing method is merging the STK card and TCG's Trusted Platform Module (TPM) for smartphone hardware hardening without additional security chips [10].

- **Feature reduction:** one simple protection technique is to reduce inactive features as much as possible. Although smartphones are always on, most of their features are not necessary to be active. For instance, Bluetooth and WiFi should be turned off when not in use.

6.4. Internet side defense

Some protection techniques that have been proposed for the Internet can be also applied to smartphones. For instance, more intensive software patching and vulnerability-driven network traffic shielding will definitely be useful protection for smartphones against well-known vulnerabilities. It would be desired for smartphone Internet service providers to guarantee that devices which access them are shielded or patched. It means that unshielded devices should not be granted access to the Internet.

Nowadays most smartphones connect to the Internet through telecom data networks such as CDMA or GPRS. In this case, base stations can first check whether smartphones have been patched or shielded correctly and if not they will be denied access [10].

[1] An Application Programming Interface (API) for loading applications to the SIM securely.

6.5. Telecom side defense

Despite some Internet-side protection techniques, there will be some subverted smartphones. Telecom networks must propose abnormal behavior detection and reaction methods in order to maintain normal operation. Luckily telecom traffic is not the same as the Internet traffic. Since telecom traffic can only be SMS or voice traffic, it is extremely predictable and it is easy to recognize misbehaviors. In order to detect the smartphone attacks described here, analyzing the following information from telecom networks can be helpful for telecom carriers:

- **Anomalous blocking rate of a base station or a switch:** Commonly, the call blocking rate must be under a threshold (< 0.01%). So a sharp increase in the blocking rate can be a conspicuous sign of an ongoing attack. In the same way, an anomalous drop rate of the data packet at the CDMA or GPRS Internet access networks can be a good indicator.

- **Call center load information:** if a call center experiences a sudden flash crowd and user behaviors are anomalous (see next bullet) then the call center is susceptible to attack.

- **End user's misbehavior:** Abnormal behavior such as connected calls with no voice traffic; lengthy data packet transmission from a single user or to a single user and sending the same message to many different users (spamming).

Most of the solutions proposed here can be achieved from network management devices for telecom networks. In order to recognize user misbehavior, the content of the message should be analyzed. For example, for junk SMS messages, email spam filtering can be used.

When the telecom side faces misbehaviors, telecom networks can apply different techniques which are available in their current infrastructures such as call filtering or putting the zombie smartphones IDs into a black list. Therefore it seems easy to protect the telecom networks against many attacks [10].

7. Conclusion and future work

Different general attacks and a full set of effective defense mechanisms have been explained comprehensively within this work. Furthermore, various vulnerabilities and attacks as well as a number of countermeasures in the smartphones domain have been discussed.

As mentioned before, smartphones use various network technologies such as 3G, Bluetooth, infrared and WLAN (IEEE 802.11) and they offer several extra services compared to traditional mobile phones. Therefore Smartphone users need to be aware of the potential risk associated with these services and they should always practice some basic safety procedures when using these devices in order to mitigate the risks. Such procedures include:

- Applying authentication and encryption whenever possible.
- Switching off Bluetooth functionality whenever not in use.
- Never pair with unknown devices.
- Scanning the computer system to ensure that there is no infection before synchronizing the smartphone with that.
- Applying ingress filtering.
- Educating users to be conscious about the address window in a web browser that shows the web address they are addressed to.
- Applying a mixture of Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS).
- Increasing the connection SYN ACK queue.
- Applying vendor software patches and also diminishing the time-out waiting for three way handshakes can be useful.
- Using firewalls and Setting rules in them to block any packet that apply a port or protocol which is not for Internet communication in the local area network.
- Filtering the packets with broadcast address as a destination address which are coming into the networks.
- Preventing packets from entering networks which source addresses belonging to inside the network.
- Removing sensitive information from public networks and limiting the connection time.
- Monitoring the network and preventing from access to foreign stations to come into contact the network repeatedly.
- Applying DoS detection tools.
- Scanning the device and network in order to find vulnerabilities.
- Hardening the smartphones via security patches and tools.
- Limiting user privileges and disabling unnecessary process.
- Decreasing the attack surface as far as possible.
- Using SmartSiren, a collaborative virus detection and alert system for smartphones.

I believe that performing the above procedures which takes into account all security issues known today would be the best way to overcome the mentioned security vulnerabilities in smartphones. Although, these solutions will not cover all security issues of smartphones, they will be beneficial for manufacturers and consumers. An advantage of these solutions is their compatibility with current technologies since they are basically implemented on the top of existing infrastructure. Therefore, no fundamental alterations will be required.

Furthermore, it should be mentioned that smartphone users should always use Bluetooth or other services with caution until smartphone manufacturers present more secure smartphones and Bluetooth SIG enforces more detailed defense solutions.

Since Smartphones are interoperable devices and can be applied as a conduit to connect to different networks, I have also investigated some security threats that Internet compromised smartphones have brought to the telecom networks. Moreover, a number of security protection mechanisms and countermeasures have been introduced in order to make these threats ineffective. By providing Internet side defense, telecom side defense and cooperation between these networks, attackers won't be able to threat the telecom networks. Therefore, wiretapping, spamming attacks, spoofing attacks, DoS and DDoS attacks will be mitigated and as a result call centers and base stations can be protected.

Finally, once again I would like to add more weight to the need for security countermeasures in smartphones and telecom networks. The use of insecure smartphones may have terrible consequences which will be to the detriment of users and manufacturers as well. Moreover, imminent danger of potential smartphone attacks against telecom networks may cause irreparable damages which can range from privacy violation and identity theft to emergency center outage resulting in national crises. Hence, due to recent security improvements in smartphones and connecting them to the telecom networks, suitable security mechanisms must be developed in parallel to decrease the risk of malicious and unauthorized behavior in smartphones and the telecom networks domain.

8. Reference

[1] Lawan A. Mohammed; Biju Issac; "Detailed DoS Attacks in Wireless Networks and Countermeasures", Int. j. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 1, Swinburne University of Technology (Sarawak), 2006, Malaysia.

[2] Ian Green;"DNS Spoofing by The Man in the Middle", the SANS Institute Reading Room site, 2005, Viewed March 2010, < http://www.sans.org/reading_room/whitepapers/dns/dns-spoofing-man-middle_1567>

[3]Victor Velasco;"Introduction to IP Spoofing", the SANS Institute Reading Room site, 2000, Viewed March 2010, < http://www.sans.org/reading_room/whitepapers/threats/introduction-ip-spoofing_959 >

[4] M. Jelena; Peter R; "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms', *ACM SIGCOMM*, *Computer Communication Review*, Vol. 34, No. 2.pp. 39 – 53, 2004.

[5] Huegen. C., A (2000), 'Network-Based Denial of Service attacks (CISCO systems)', viewed March 2010, < http://www.pentics.net/denial-of-service/presentations/msppt/19980513_dos.ppt>

[6] Wack, John; Tracy, Miles; Souppaya, Mrurgiah; "Guideline on Network Security Testing", NIST Special Publication 800-42, October 2003.

[7] Habib, Sheikh Mahbub; Jacob, Cyril; Olovsson, Tomas: "A Practical Analysis of the Robustness and Stability of the Network Stack in Smartphones". *IEEE International Conference on Computer and Information Technology, ICCIT 2008*, Department of Computer Science & Engineering, Chalmers University of Technology, Gothenburg, Sweden.

[8] Habib, Sheikh Mahbub; Cyril, Jacob; Olovsson, Tomas: "An Analysis of the Robustness and Stability of the Network Stack in Symbian-based Smartphones". *Journal of Networks*, Vol 4 (No. 10, 2009) pp. 968-97, Department of Computer Science & Engineering, Chalmers University of Technology, Gothenburg, Sweden.

[9] Collin Richard Mulliner, "Security of Smartphones", Master's Thesis submitted in University of California, Santa Barbara, June, 2006.

[10] Guo, Chuanxiong; J.Wang, Helen; Zhu, Wenwu; "Smart-Phone Attacks and Defenses", *ACM SIGCOMM HotNets*, Association for Computing Machinery, Inc., November 2004.

[11] Lih Wern Wong; "Potential Bluetooth Vulnerabilities in Smartphones", AISM, 2005, the School of Computer and Information Science (SCIS) & Edith Cowan University, Perth, Australia.

[12] BlueSnarf (2004). Viewed July 2010, http://trifinite.org/trifinite_stuff_bluesnarf.html

[13] BlueBug (2004). Viewed July 2010, < http://trifinite.org/trifinite_stuff_bluebug.html>

[14] What is Bluejacking, (2003), viewd July 2010, http://www.bluejackq.com/what-is-bluejacking.shtml

[15] BlueSmack (2004). Viewed July 2010, <http://trifinite.org/trifinite_stuff_bluesmack.html>

[16] Carlos A. Soto, 20 Jul 2005, "A menu of Bluetooth attack", viewed July 2010, <http://gcn.com/articles/2005/07/20/a-menu-of-bluetooth-attacks.aspx>

[17] Blueprinting (2004), Viewed July 2010, <http://trifinite.org/trifinite_stuff_blueprinting.html>

[18] Andreas Becker, "Bluetooth Security & Hacks", Seminar ITS, Ruhr-Universität Bochum, SS 2007, <http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/slides_bluetooth_security_and_hacks.pdf>

[19] Moe Rahnema, "Overview of the GSM System and Protocol Architecture". *IEEE Communications Magazine*, April 1993.

[20] Ian Angus, "An Introduction to Erlang B and Erlang C", *Telemanagement*, July-August 2001.

[21] Smartphone vulnerabilities: securing your data; (2010); viewed July 2010, <http://www.info4security.com/story.asp?storycode=4125251>

[22] Chuanxiong Guo; Helen J. Wang; Wenwu Zhu, "Smart-phone Attacks and Defenses", viwed July 2010, < http://www.engr.uconn.edu/~bing/cse330/slides/smartphone.ppt>

[23] Jerry Cheng, Starsky H.Y.Wong, Hao Yang, Songwu Lu. "SmartSiren: Virus Detection and Alert for Smartphones", Dept. of Computer Science, UCLA, 2007. Viwed Augest 2010, <www.usenix.org/events/mobisys07/full_papers/p258.pdf>