On Cellular Botnets: Impact of Malicious Devices on a Cellular Network Core

Loreto Felipe Sánchez-Infante

Seminar “Security in Telecommunications”

WinterSemester 2009/2010

Technische Universität Berlin (TU Berlin), Deutschland.

INDEX

ABSTRACT

Cellular networks are evolving very fast to catch up with all the new technologies. The problem is, is security running at the same speed? Wireless infrastructures are becoming a succulent target for hackers as they improve their characteristics similarly to PCs, to the point that a malicious attack can degrade service to area-code sized regions by 93%.

Nowadays mobile phones are such an important tool in our daily life that not being able to make a call or to send a SMS can provoke serious disappointments in users, which mobile phone companies cannot allow.

This paper makes an overview of Patrick Traynor´s work [1], explaining the balance between progress and safety in this ambit. It is explained the behavior of a normal mobile network and how malicious manipulate it to provoke serious outages for example with security in Internet mobile connections, whereas banking online, mailing or any other private activity.

Although defenses are not quite investigated yet, the avoidance of these attacks and the counter measures that may help to partially mitigate the threads are starting to be as important as developing new applications.

1. INTRODUCTION

Mobile phones are making hard efforts to progress in the new world technologies, but what should be an advantage, has become the reason for hackers to take them as a new target. The development of new services (Internet Connection, Bluetooth, etc.) turns themselves into easier penetrable barriers. At first, mobile phones were very safe because we had all our information in a SIM card to which only users could have access. Nowadays, an entire failure of the system would suppose millionaire losses for the mobile companies.

While attacks on these networks are becoming more diverse, academic research in this area has only focused on two general thrusts. The first one is the lack of authentication for signaling traffic in the wired network would allow an adversary with physical access to cause significant outages [2] and the second one concerns how attacks targeting the wireless portion of the network result in either the saturation of a wireless link [3] or the conversion of a mobile phone into spam generators or nodes used to attack Internet-based resources.

However, previous studies have not investigated whether compromised mobile phones can generate sufficient amounts of traffic to impair the network core itself, but attempted to measure the damage caused by such traffic. As on the Internet, Deny of Service attacks (DoS) are the most common ones, as explained in the following chapters.

From some investigations [1] we conclude that relative small botnets can cause a significant reduction of the networks total throughput in area-code sized regions if the attack is carefully planned. We will see that selecting a concrete request or knowing how to avoid typical mobile network obstacles (hierarchical architecture, bottlenecks, …) can provoke a widespread outage with the minimal effort for malicious.

Despite its similarity, it is important to remark the different between these attacks being performed on a cellular network the or on the Internet. An attack to the core of the wireless infrastructure would make the device immediately unreachable and of course that would suppose the loss of all the mobiles connected to it. In the second case, if the DNS (Domain Name Server [12]) or the BGP (Border Gateway Protocol [13]) are attacked, we can always find another way to make our message reach the destination.

In the following chapters it is going to be explained the attack characterization and qualification, how to reduce adversary´s workload and how to provide intelligent control mechanisms which coordinate the compromised hosts avoiding bottlenecks and other impediments which may be found.

2. RELATED WORK

Denial of service attacks have been studied in a wide variety of systems. Some of the most frequent targets of malicious traffic, including Domain Name Server roots, are software vendors, news services, search engines and online casinos. The problem is that such attacks are not only theoretical, but they have even impacted in the physical world, and caused significant outages in areas such as banking, emergency and even postal services.

Although there are lots of companies investing on the research to mitigate these attacks on the Internet, the tendency is not so common for cellular networks according to its prematurity. Previous investigations focused on the malicious overload of cellular networks entirely on the wireless domain.

Some of the results showed that:

- A small volume of text messages targeted at a geographic area could be used to deny legitimate voice and SMS service [14].
- Similar results were possible by overloading paging services on shared uplink channels [15].
- Other problems related to resource allocation algorithms on the air interface [16]. Unprotected devices which include Bluetooth, Internet connection or Multimedia Messaging Subsystem (MMS) [39]

Some of these results took the researchers to new conclusions about these attacks on cellular networks: The problem of this targeting was the architecture of the network itself. In some provoked attacks it was proved that it was the design of the cellular network that caused the tension by the meeting of best effort IP networks and the circuit-switched air interface of cellular networks.

However, these devices have a total lack of even the most basic operating system security mechanisms, feeling totally vulnerable to any attack. This is the reason why their ability to on the network functionality must be investigated

3. OVERVIEW OF CELLULAR SYSTEMS

In this section, we provide an overview of important background information, including the architecture of cellular networks, the hardware of mobile phones and a discussion of how devices are likely to become infected.

3.1 Network Architecture and Components

As we can see on Figure 1 [4], cellular networks are divided into 3 big blocks: mobile devices (mobile phones, smartphones, PDAs Laptops...), connection infrastructure (Base Station Controller, Home Location Register, Mobile Switching Center...) and the different services it can provide (Internet or Public Switched Telephone Network).

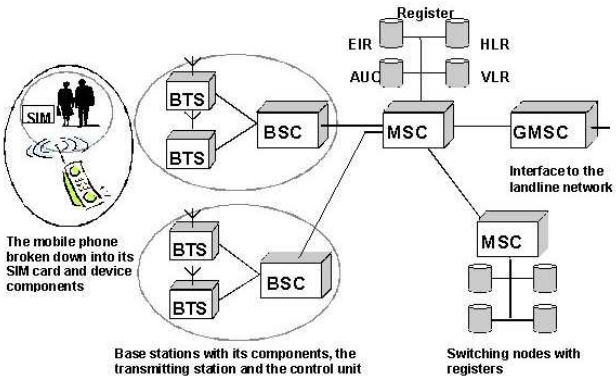

Figure 1: Cellular Network architecture.

The whole network as shown in Figure 1 is ruled by the *Home Location Register (HLR).* This central database is the heart of each cellular network and contains the details of each mobile phone subscriber that is authorized to use the GSM core network. Users are assigned to specific HLRs based on their phone numbers if they attempt to call a user, requesting for the targeted user's current location. It is also responsible for authentication and call-forwarding, billing and, of course, providing service in a network with mobile endpoints. The *Mobile Switching Centers (MSCs)* are also very important. MSC acts as telephony switches and deliver circuit-switched traffic in a GSM network. "Handoffs" between Base Stations and billing operations also performed here. They can function as gateways to both wired and neighboring cellular systems. The *Visiting Location Register (VLR)* assists the MSCs to identify and store information about currently associated subscribers. However, information requests for other subscribers still require interaction with the HLR. Last but not least is the *Base Station Subsystem (BSS).* Mobile phones and other cellular-enabled devices connect wirelessly to it so they can get logic for operations such as wireless resource management, encryption and frequency hopping.

3.2 Mobile Phone Architecture

Mobile phones operate using two processors. The *Application Processor* supports functionality including traditional operating system duties (e.g., memory management) and user services such as the camera and music players. It communicates with the *Baseband Processor* passing an Attention, or AT Command [5], when a process needs the network. This processor takes care of Bluetooth connections, serial links and even other applications with the necessary privileges, so malware infecting such devices can therefore easily initiate interaction with the network core.

3.3 Infecting Phones

Mobile devices have rapidly transformed from limited embedded systems to highly capable computing platforms. While such devices have long enjoyed significant diversity in hardware and operating systems, the rising popularity of smart phones and the ability to sell applications to users is leading to the establishment of standardized mobile software platforms and operating systems, such as Microsoft's Windows Mobile, Google's Android and Apple's Mobile OS X. Although all of them provide the latest technological services, many of them are unlikely to include security mechanisms including memory protection and separation of privilege, what makes these systems an increasing target for malware.

Recent researches showed that as mobile phones included more applications, the risk of being maliciously manipulated raised too. Given that 10% of cellular users downloaded games to their mobile devices once per month and the wide availability of free ringtones, downloadable content and executables make mobile devices susceptible to malware propagated not only through the cellular network itself but also through Bluetooth and Wi-Fi [6] because of the multiple communications interfaces it permits.

4. ATTACK OVERVIEW

The principal aim of hackers attempts to prevent legitimate users of a cellular network from sending or receiving calls or text messages. This is why their target will then be the HLR, so most of the functionality (delivery of all phone calls and text messages, authentication service, billing…) of these networks relies on the availability and proper functioning of it. As on the Internet, the most frequent attack is DoS which stands for "Denial of Service attacks". The procedure implies the overwhelming of the HLR with a large volume of traffic making the center of the networking unable to give service to legitimate users which rely on it as their requests will be dropped. In fact, there are several differences depending on the platform on which they are being developed; Mobile devices can not transmit entirely arbitrary requests to the HLR; rather, only specific types of messages can be exchanged and such requests must be made in a manner such that unnecessary traffic or side effects are not generated. This behavior may

prevent the attacks with auto-dialers from achieving widespread outages in cellular networks possible if the HLR were instead reached.

To understand such attacks we should first characterize the normal performance of an HLR (Chapter 5) and then see the effects of DoS on its functioning (Chapter 6). As we quantify these experiments, we should always compare the relative impact of a variety of interactions with the HLR with the size of a cellular botnet. It is also important to study bottlenecks and discuss ways in which they can be avoided (Chapter 8).

5. CHARACTERIZING HLR PERFORMANCE

In this section it is characterized the HLR performance to explain how its significant susceptibility to infection represents a realistic threat if the malicious approaches its failure.

To characterize the HLR performance means to measure the impact caused by the invocation of the range of services it can provide. We use Telecom One (TM1) benchmarking suite [7] to help us with the quantification, evaluating the different hardware and software configurations prior to deploying equipment. With the testing results, we can identify the most expensive classes of service requests, thereby reducing the effort needed for an adversary to effectively render an HLR unavailable. For the HLR database we should distinct between MySQL and SolidDB.

5.1. Normal HLR Behavior

Providers consider two factors when deploying an HLR. The first one is the number of subscribers serviced by the database is influenced by practical concerns including population density, equipment capability and available resources. In reality, each HLR is able to serve a range from a few hundred thousand to five million subscribers. We should remember these numbers when we quantify the outages of the attack. The second one is the rate and type of service requests from mobile devices to HLR in well established patterns based on functions of device mobility and call rates.

To simulate read and write operations in the network we are going to use TM1´s “Default Mix” [8] which is composed only of a small set of generic back-end operations, 80% read and 20% write meta-commands, enough to support all possible requests in an HLR. It is consistent with reality because read operations are more often than write ones.

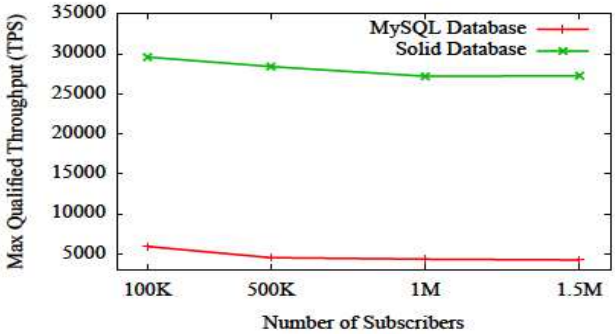

Figure 2: Throughput for an HLR with varying number of subscribers using TM1´s Default Mix.

Figure 2 shows the impact of the number of subscribers on the Maximum Qualified Throughput for both the HLRs running MySQL and SolidDB database. The difference between the two curves relies on the MySQL´s property of storing in memory just the caching data and indexes so system throughput quickly becomes a result of disk throughput. This makes SolidDB much more robust when handling elevated traffic from large populations of users and, of course, in case of a massive attack. The degradation of performance in this case is lower because the database itself is stored in main memory and it employs a more advanced concurrency control technique. These results are consistent with previously published studies given equivalent hardware configurations [9].

5.2. Characterizing Meta-Commands

An adversary should first observe and then attack. As previously shown, read and write operations on databases have different costs, which, used cleverly, could improve severely the efficiency of an attack.

The meta-commands used for this experiment are:

- Delete/Insert Call Forwarding
- Update subscriber data
- Update Location
- Get access data
- Get new destination
- Get subscriber data

Accordingly, we characterize the performance of an HLR for each of them, as it is illustrated on Figure 3:

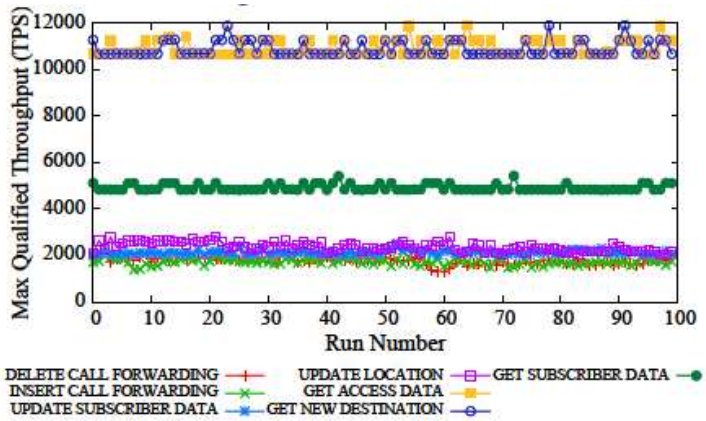

Figure 3: Throughput for each meta-command with 500K subscribers on HLR running SolidDB

We can appreciate from the Maximum Qualified Throughput (MQTh) that, as expected, read-only transactions perform significantly better than those performing writes.

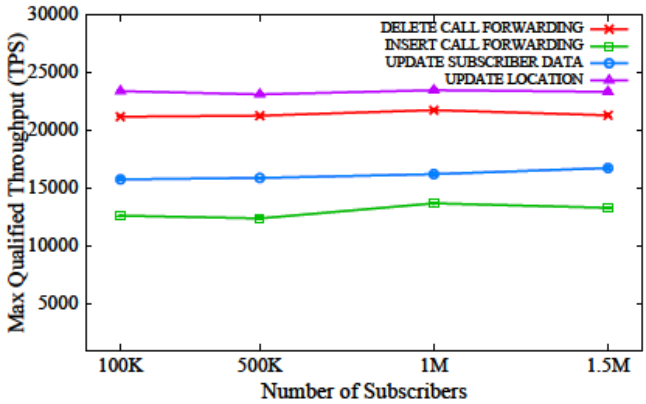

Figure 4: Comparison of candidate transaction types based on the resulting Throughput in SolidDB database

Figures 4 is the evidence of the impact of varying the number of users for each meta-command. It provides a relatively stable ranking of the relative expense required to service these requests.

Through this analysis, an adversary could know which subsets of service requests should select to improve the efficiency of his attack.

6. PROFILING NETWORK BEHAVIOR

The experiments in the last chapter demonstrated that write requests are significantly more expensive than reads, which from an attack perspective means that an important selection of the classes of messages would improve the effectiveness of the failure.

In this chapter we are going to characterize and measure the network behavior for four of the six meta-command previously appointed

6.1 Update Location

Update location is the meta-command in charge of alerting the HLR periodically whether the device changes location keeping always the track of the user over the networks. For example when a device moves between two stations connects to a different Serving GPRS Support Node (SGSN) and Mobile Switching Centre (MSCs) or when a device turns on and off. This is considered one of the “expensive operations” before mentioned.

To minimize the impact on the network some caching mechanisms have been designed. The HLR amortizes the cost of device authentication by pushing most of the load to SGSNs so that the messages do not reach the HLR, avoiding the overwhelm.

To understand better the procedure, we should have a look to Figure 6.

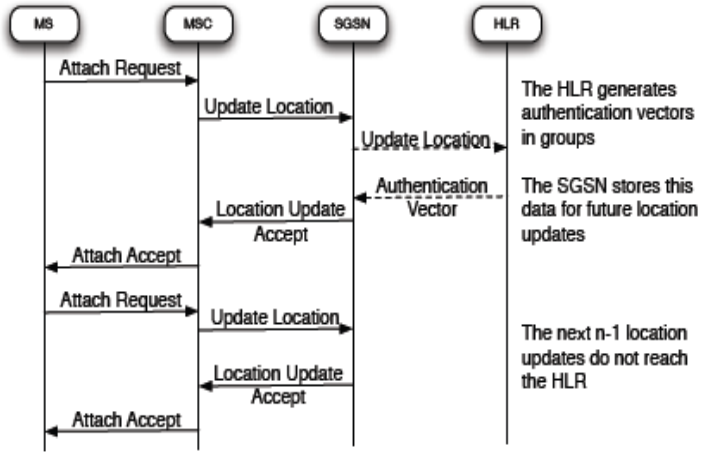

Figure 5: Update Location message flow.

We can observe that there is only one “Update Location request” reaching the HLR. After his, it generates a n-vector which is stored in the SGSN in order to serve the next n-1 updates automatically. In case of infection, only one out of n updates would reach the HLR causing an outage. So if the hacker wanted to manipulate the network, he would have to create large amounts of traffic to raise the probability and succeed.

6.3 Update Subscriber Data

Update Subscriber Data concerns the update of user profiles, as activation/deactivation parameters of the database. This command includes services such as Call Waiting, Call Barring and Modify PDP Context, from which we is only studied Call Waiting.

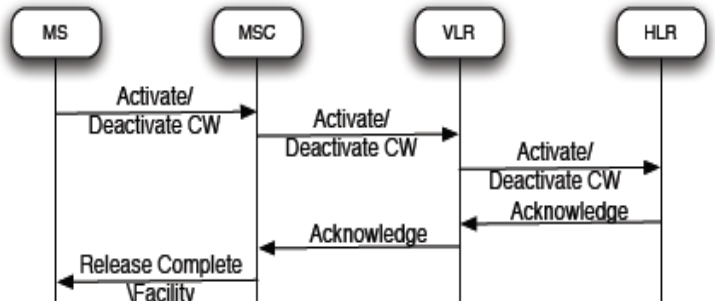

Figure 6: Update Subscriber Data message flow.

As shown in Figure 6, in this case all Call Waiting enable requests are directed to the HLR. This way, the HLR acknowledges the receipt of this request to both the client and the client's VLR, using this information to confirm whether Call Waiting is currently activated or not. The same operations occur when Call Waiting Disable requests are sent.

The response times for Call Waiting Enable and Disable are consistent although some erratically spikes indicating contention for shared wireless resources (Random Access Channel, RACH) may appear. The minimizing of this contention will be explained in the Chapter 8, with "Bottlenecks".

The results of the experiments [1] related to this meta-command represented a significant improvement over Update Location (Section 6.1.).

6.4 Insert/Delete Call Forwarding

Insert/Delete Call Forwarding allows a user to redirect incoming phone calls to other devices. It is used, for example, when the user does not want to carry your mobile phone.

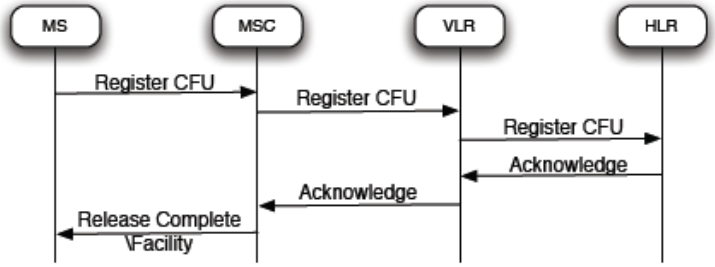

Figure 11: Insert/Delete Call Forwarding message flow

As we can see on Figure 7, the activation and deactivation of this service requires a single exchange with the HLR. It is important to remember that the information needed for the procedure is only stored in the HLR, so the interaction is directly with it.

From the result of injecting this type of requests on a cellular network [1], it is important to remark that, although both operations, insert and delete of Call Forwarding, perform very similarly, but the low response time associated to the second one turns out to be the best candidate. But, because you cannot delete if you have not insert and due to its expensive process, Insert Call Forwarding is the most attractive command for an adversary to use.

7. ATTACK CHARACTERIZATION

In this section, we are going to quantify the impact of the previously explained attacks on normal traffic, considering “Insert Call Forwarding” as the most expensive meta-command. The objective is to realistically estimate the number of infected devices an adversary would require to cause widespread outages.

For this characterization it is used a multi-threaded malicious TM1´s client which is able to coordinate the transmission of specific volumes of traffic. This permits the determination of the impact of different sized attacks and service requests without waiting for acknowledgements, which makes the attack more aggressive.

It is important to note that increasing the number of legitimate requests during an attack will often improve the successful probability of legitimate clients. This phenomenon can clearly be seen on Figure 12. While the HLR runs SolidDB database it is certainly capable of maintaining service during small attacks, but the performance of these systems can also be extensively degraded.

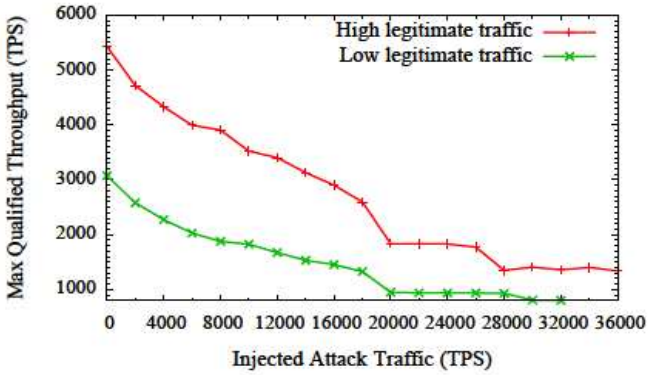

Figure 12: Effect of an attack on an HLR running SolidDB supporting one million users

Figure 12 illustrates the impact of attacking constantly with 4000 “Insert Call Forwarding” TPS (Transmissions Per Second) when in the network there is high and low levels of legitimate traffic. These results show that with low intensity traffic stream the throughput reduces from 3075 to 803 TPS and with high stream from 5424 to 1340 TPS. Both cases reduce the throughput of legitimate traffic more than a %.As expected As mentioned experiments: as we increase the number of legitimate requests during the attack, we also improve the success rate of legitimate clients, because it increases the probability that legitimate traffic will arrive between malicious requests.

From these attacks, it now becomes possible to calculate the number of devices an adversary requires to successfully launch an attack against an HLR [1]. The number for a SolidDB database rates approximately 141,000 infected mobile phones, low and high traffic respectively. Which, comparing to the normal amount of devices an HLR can serve, only 14,1% rates of infection.

The results for an HLR running MySQL the number of infected devices should rate from 11,750 to 23,000, only a 1.2-2.4% of the total amount of traffic. This database shows a throughput degradation by 93% according to its weak robustness. This database would be suitable in case of attacking a network.

The main problem starts when the corruption spreads to other platforms, such as Bluetooth, because it cannot be bounded. But, as discussed in chapter 8, it is still possible for bottlenecks in the wireless portion of the network to prevent such attack from being successful.

8. AVOIDING WIRELESS ATTACKS: BOTTLENECKS

We then examine issues of command and control and consider both the reuse of traditional schemes and the operation of unique cellular techniques.

As the title implores, in this section is commented the number of wireless bottlenecks needed to try to impede an attack from being carried out. It is essential to understand these choke points geographically know where the compromised nodes concentrated are.

8.1. Wireless Bottlenecks

In congestion issues, this is one of the main parts. The wireless portion of the network consists of two channels: Random Access Channel (RACH) and the Standalone Dedicated Control Channels (SDCCH). The saturation of these channels dues to their limited capacity. They are used when a mobile phone attempts to initiate service with the network. Access requests would be sent between the device and the base station in order to arrange signaling over shared-access RACH. SDCCH is used for signaling with the HLR.

To explore the avoidance of obstruction in mobile communications, it is important to explore the performance characteristics of these two channels.

8.1.1. Random Access Channel

Random Access Channel *(*RACH) is a resource shared between all devices in the area, so access must be regulated in order to evade congestion in high traffic situations. The procedure corresponds to GSM multiplexation of traffic on a single frequency beyond Time Division Multiple Access (TDMA). Devices attempting to initiate signaling with the network need only gain access to a single RACH timeslot, as all further communications will take place on dedicated channels.

To understand how congestion affects this common supply, first we should explain how “slotted ALOHA protocol” [10] governs it. The maximum throughput S can be calculated:

$$S=G*\exp(-G)$$

Where G is the number of transmission attempts per time slot. We should take into consideration the case when G=1 which maximizes S at 37%. G can also be known as offered load or ρ:

$$\rho=\lambda/\mu$$

where λ is the arrival rate and μ the service rate.1/μ is the channel hold time.

According to some calculations [1], if the compromised hosts are well distributed across the network, RACH congestion is unlikely to act as the main bottleneck. However, if there is large amount of devices within close proximity the competition for resources would gain importance, but this is part of the communication issues described for SDCCH in the following section.

8.1.2. Standalone Dedicated Control Channel limitations

SDCCH stand for Standalone Dedicated Control Channels. These are the primary means of communication between the mobile devices and the network core, HLR. The services here performed are critical in the operation of these networks. Some examples are handoff, receiving a text message, setting up a call or authenticating with the network.

In this case, the attack would focus on not overwhelming completely the HLR by elevating signaling load if it wants to successfully cause larger-scale outages.

If we combine RACH and SDCCH limitations, we can fairly accurate that the bottleneck of the network can be here developed. From some calculations [1] we can estimate that although both RACH and SDCCH can act as bottlenecks in our network, SDCCH can be much more limiting. If compromised nodes are evenly distributed throughout the network, such contention is unlikely to play a significant role in reducing the amount of attack traffic that reaches the HLR. .

Geographic location can be significant when preparing an attack. When two infections spread across high concentrated areas without significant dispersion of compromised devices, they tend to cancel themselves out accidentally whether than damaging the service. This may be one of the possible defenses for this kind of attacks.

8.2. Command and Control of Botnets

Cellular networks are still a challenge for malicious especially on this “command and control” ambit. The botmaster must develop new ways to coordinate compromised hosts to carry out the attack avoiding bottlenecks. In this section we are going to resume the most common approaches used to manage cellular botnets, very useful from the malicious point of view.

- *Internet Coordination:* It is important to remember, that with the new technologies, mobile phones are starting to gain more connectivity, for example, to the Internet. What should be an advantage is becoming a handicap as far as adversaries could reapply easily many of the command and control techniques used in these domains to assail cellular networks. A simple example would be a 3G mobile device with an IRC connection to which someone could attempt to avoid monitoring and blocking of the peer-to-peer communication. Other example could be reducing control overheads combined with time triggered attacks. However, cellular networks have a special architecture which is not designed to handle large amounts of traffic. In this case, users serviced by the same platform may not receive answer to their requests or may have high delays [11]. This can sometimes be used to prevent from attacks.

- *Local Wireless Coordination:* Nowadays, new devices not only have Internet access but also Bluetooth and 802.11 wireless Radio, which permit direct communication between multiple compromised phones and so avoid common approaches such as bottlenecks. However, this communications are significantly limited by range so an increase of the density of infected devices would reduce the local resources and the attack would unlikely be effective. The bad stuff comes when the adversary manages to get control of compromised phones (associated with traditional wireless access points, 802.11) and uses this connection to reach the core of the network and provoke its failure. Because both of these means of communication are separate from cellular networks, a botmaster would need to consider coverage issues before relying on either method.
- *Indirect Local Coordination:* As previously mentioned, if lots of individual cells are attacked may cause significant contention of resources and diminish the effectiveness of the infection. Even without directly communicating with the other nearby infected devices, it is possible to coordinate and improve the throughput of attack traffic. There is a back off algorithm in GSM which consists on multiplicative increasing and decreasing to change the channel conditions randomly and it is able to reduce congestion in areas with high density of infection. The contra is that reducing RACH contention using exponential back off causes inefficiencies in the use of the network too.

9. ATTACK MITIGATION

These systems are vastly expanded on programmability and have increased their connectivity to external data networks, what has become a free barrier for malicious to act. Many cellular networks use database replication to defense themselves from widespread outages if the HLR fails. If this happens, the traffic is rerouted to another HLR with a backup copy of the attacked database. To carry out this defense, it is supposed that the other HLR can support the

additional load and, in that case, the failure of one HLR can provoke the overload of others, spreading the attack to other networks.

Filtering is another method used against this attack if they are aggressively tuned without much worry of the impact of false positives. Another useful technique is the “Call Gapping”, which can potentially be adapted for signaling overload attacks. Basic filtering and shedding are two examples of possible network defenses a service provider can implement.

The challenge for mobile devices companies is to develop software intelligent enough to ease dynamic attacks according to the difficulty for the provider to distinct between benign and malicious messages, unlike as in the Internet. The only way to solve this problem would be filtering, and sometimes it may be too late to avoid the attack. A lot of work and research is still to be done in this area before adversaries develop new attacks against our actual networks.

10. CONCLUSION

Are we save enough to use our cell phones? The fact is that cellular have evolved from high limited SIM Card devices to mini portable computers with Internet, radio, external systems etc access. Ironically, security has not catched up with it yet. And this is not only a problem for big networks, but, as demonstrated [1], quite small botnets composed entirely of mobile phones can be significant threats to the successful functioning of the network. Mitigating these attacks on mobile networks is becoming an important issue of research, as lots of users can be unlikely aware of them if they end on widespread outages.

This paper tries to overview the conditions which make these networks so nacked to DoS attacks from the malicious perspective and how to mitigate them. Understanding the running of the proper network permits the enemy with little efforts a successful damage, but, as we commented during the paper, some of these attacks can be overcome using the combination of multiple network interface features, such as bottlenecks or filtering. The architecture of the network should also be studied deeply because it is unlikely to be attacked in this way.

Although command and control is potentially more challenging in this environment, we should see this work from a warning perspective. Researchers should focus on the HLR, core of the network as the main target, to develop new defenses according to the increasing interest that these systems are starting to awake on hackers. Mobile companies should investigate and invest more in sophisticating protections as the effects already caused on the Internet platform have been devasting. It is also important to limit the widespread of the so called attacks to avoid them from controlling other platforms, such as Bluetooth or WiFi access.

10.REFERENCES

[1] Patrick Traynor: *"On Cellular Botnets: Impact of Malicious Devices on a Cellular Network Core"* http://www.patrickmcdaniel.org/pubs/ccs09b.pdf

[2] C.-C. Lo and Y.-J. Chen. *Secure communication mechanisms for GSM networks*. IEEE Transactions on Consumer Electronics, 45(4), 1999.

[3] P. Traynor, P. McDaniel, and T. La Porta. On Attack Causality on Internet-Connected Cellular Networks. In Proceedings of the USENIX Security Symposium, 2007

[4] GSM Cellular Network https://www.bsi.bund.de/ContentBSI/EN/publications/GSMCellularNetwork/index_e_htm.html

[5] Smart Computing Encyclopedia. Smart Computing Encyclopedia - Hayes. http://www.smartcomputing.com/editorial/dictionary/detail.asp?guid=&searchtype=&DicID=17562&RefType= Encyclopedia, 2008.

[6] F-Secure Corporation. F-Secure Computer Virus Descriptions: Cabir. http://www.f-secure.com/v-descs/cabir.shtml, December 2004.

[7] Solid Information Technology. Telecom One (TM1) Benchmark Test Suite Guide Version 3.0-1, November 2006

[8] N. Gupta. Enabling High Performance HLR Solutions. http://www.sun.com/products-n-solutions/hw/networking/atca/HLR-on-ATCA-v2-Final.pdf, 2006.

[9] Solid Information Technology. The TM1 Benchmark Results. http://www.soliddb.com/TM1Results, 2008.

[10] Slotted ALOHA protocol http://www.laynetworks.com/slotted%20aloha.htm

[11] P. Traynor, P. McDaniel, and T. La Porta. On Attack Causality on Internet-Connected Cellular Networks. In Proceedings of the USENIX Security Symposium, 2007.

[12] R. Farrow. DNS Root Servers: Protecting the Internet. Network Magazine, 2003.

[13] V. J. Bono. 7007 Explanation and Apology. http://www.irbs.net/internet/nanog/9704/0440.html, 1997.

[14] P. Traynor, W. Enck, P. McDaniel, and T. F. La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. Journal of Computer Security (JCS), 2008.

[15] J. Serror, H. Zang, and J. C. Bolot. Impact of paging channel overloads or attacks on a cellular network.In Proceedings of the ACM Workshop onWireless Security (WiSe), 2006.

[16] R. Racic, D. Ma, H. Chen, and X. Liu. Exploiting Opportunistic Scheduling in Cellular Data Networks.In Proceedings of the Networking and Distributed Systems Security Symposium, 2008.