Cellular warfare

Karlis Podins

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Karlis.podins@ccdcoe.org

Published in the Proceedings of the 8th European Conference on Information Warfare and Security,
ECIW 2009, 6-7 July, Lisbon, Portugal.

Abstract

In this paper we explore the possibilities of cyber warfare activities connected to cell phone networks. We analyze known attacks that originate in and/or target cellular phone networks as weapons of cyber warfare.

The historic high reliability of cellular networks has caused a significant reliance on them as the sole means of communication in many developed countries, making it a part of national critical infrastructures. The growing popularity of smartphones opens up cellular network both to the advantages and disadvantages currently associated with the internet.

The possibility that an attacker could deny cellular voice/SMS services to legitimate users is already widely discussed. Such attacks could begin by using internet services to send SMS messages or using a botnet consisting of smart cellular phones. Such attacks could be aimed at a core infrastructure to shut down or cripple a cellular network; even very small botnets could be used to launch attacks that disrupt or limit cellular services in targeted geographical areas.

We evaluate the possible usage of such techniques both by nation-states and by non-state-actors that could be used as effective digital cover for their actions. The advantage of such attacks is that virtually no hardware is needed to launch them and all activities can be developed, tested and controlled remotely from a safe location. This makes them a good choice for parties seeking asymmetric advantages. Another technique we discuss is the use of cellular botnets to launch a denial of service attack against emergency call services or other phone lines in critical infrastructure.

We note that the excellent record of cellular networks does not prove that cellular networks are reliable; we believe that there has simply been a lack of real-world attacks so far. An overview of current and possible countermeasures is provided to show the level of complexity of such a task. We estimate that the importance of this threat will increase together with the rise in both the popularity and the complexity of smartphones.

Keywords: Keywords: cellular networks, denial of service, cyber warfare, botnets

1. Introduction

According to the official European Union (EU) statistics body Eurostat (Eurostat, 2007), the number of cellular telephone subscriptions has increased almost fourteen-fold between 1996 and 2005 in the 27 EU countries, from 7 subscriptions per 100 inhabitants in 1996 to 96 in 2005. In 2005, thirteen member states had more than 100 cellular phone subscriptions per 100 inhabitants. Highest penetration was found in Luxembourg (158), Lithuania (127), Italy (122), the Czech Republic (115) and Portugal (111) and Romania (62), Poland (76), France (77) and Bulgaria (80) the lowest. The number of fixed telephone lines per 100 inhabitants in the EU27 shows much less dynamics, increasing from 43 lines per 100 inhabitants in 1996 to 48 in 2005. The pattern in the member states varies: the number of fixed telephone lines has fallen in twelve member states, while it increased in fourteen and remained stable in one. The member states with the highest number of fixed telephone lines per 100 inhabitants in 2005 were Germany (67), Denmark (61), France and Sweden (both 58), and the lowest were Romania (20), Slovakia(22), Lithuania (23), the Czech Republic and Poland (both 31) . In the EU25 in 2006, 18% of households had cellular phone access, but no fixed telephone access. The proportion varied largely among the member states: it was less than 10% in Sweden (0%), Malta (3%), the Netherlands (4%) and Luxembourg (8%), and 40% or more in Lithuania (48%), Finland (47%), the Czech Republic (42%) and Latvia (40%). By comparison, US Census Bureau data (US Census Bureau, 2008) shows that in the year 2005, there were 58.74 land lines and 71.50 cellular phone subscriptions per 100 inhabitants.

Although the US is less dependent on cellular networks (the US lags behind EU countries in number of cell phone subscriptions but has more fixed telephone lines at the same time), penetration rates for both EU and USA indicate that cellular networks are an important means of communication. Data shows that by the year 2006, in some countries almost half of the households relied exclusively on cellular networks for telecommunication services, underlining that cellular networks are likely now a part of national critical infrastructures.

The paper is structured as follows: brief introduction to cellular network technologies is given in section two, followed by overview of known DoS attacks on cellular networks in section three. Section four is on smartphones and smartphone-malware. In section five we explore ways how compromised smartphones can be used in cyberwarfare. Section six explores possible defense measures.

2. Cellular network technologies

There are two primary cellular phone systems – GSM/3G and CDMA. According to (Global mobile Suppliers association, 2009), GSM/3G system is the dominant cellular network technology, with market share of 88.5%, followed by CDMA at 10.39%. Other technologies accounted for just over 1%.

2.1. GSM/3G

Cell is the area of coverage around a base station in a wireless network. There are five different cell sizes in a GSM network: **Error! Bookmark not defined.**, micro, pico, femto and umbrella, differing in coverage area. Cell radius varies depending on antenna height, antenna gain and propagation conditions from a couple of hundred meters to 35 kilometers or even more.(wikipedia - gsm, n.d.)

An excellent introduction to GSM is given by Traynor et al. (Patrick Traynor, 2006). Each cell is typically partitioned into multiple (usually three) sectors. Wireless communication is traditionally divided into two classes of logical channels: Control Channels (CCHs) and Traffic Channels (TCH). TCHs carry voice traffic after call setup has finished successfully. CCHs transport information about the network and assist in call setup/SMS delivery. There are several types CCHs. In order to alert a targeted cellular device that a call or text message is available, a message is broadcasted on the Paging Channel (PCH). Upon hearing its identifier on the PCH, available devices inform the network of their readiness to accept incoming communications Random Access Channel (RACH) uplink. A cellular device is then assigned a Standalone Dedicated Control Channel (SDCCH) by the Access Grant Channel (AGCH). If a text message is available, the base station authenticates the cellular device, enables encryption, and then delivers the contents of the message over the assigned SDCCH. If instead a call is incoming for the cellular device, the SDCCH is used to authenticate the cellular device and negotiate a TCH for voice communications.

The capacity of GSM network is described by Guo et al. (Chuanxiong Guo, 2004). Most 2G GSM networks operate in the 900 MHz or 1800 MHz bands. For GSM900, a 25MHz wide band is split into 124 carrier frequencies, each spaced by 200kHz. For GSM1800, a 75MHz-wide band is split into 372 carrier frequencies. Each carrier frequency is divided into 8 time slots (channels), with a Time Division Multiple Access scheme. The theoretical maximum number of channels in a given geographic location is 124·8=992 for GSM900 and 372·8=2976 for GSM1800. Since each user in a voice communication is given a separate channel, the maximum number of channels is also the maximum number of parallel voice communications.

If multiple phone network operators service a given area, each gets a portion of the carrier frequencies. The operator divides these allocated frequency bands between cells so that overlapping cells do not use common carrier frequencies to avoid interference with each other.(Nilesh Agrawal, 2004)

In real systems, the total number of SDCCHs available in a sector is typically equal to twice the number of carriers, and the number of carriers can be up to six in densely populated metropolitan areas. There is however only one paging channel. In such a scenario, a base station with three sectors and six carriers per sector, the total number of TCHs is 108.(William Enck, 2005)

2.2. CDMA

Overview of CDMA is given by Serror et al. (Jeremy Serror, 2006). Apart from implementation specifics, Code Division Multiple Access (CDMA) technology, and particularly the popular CDMA2000, is quite similar to GSM. The air interface in turn is divided into traffic channels and control channels. Traffic channels carry voice and data traffic. Control channels are used for signaling, delivery of short messages, etc. An important control channel is the paging channel. The paging channel carries signaling and SMS traffic from a base station to a group of cellular devices. Key role of the paging channel is to carry messages used to locate a cellular device. Each base station operates up to 64 channels simultaneously, one of them being a dedicated paging channel. The access channel is used by the cellular devices to send messages to the base station. When a cellular-terminated call is made, the cellular device is paged by a General Page Message (GPM), which is sent in a time slot monitored by the called device. One GPM is sent per time slot, and 8 or 9 phones can be paged, depending on the implementation. Cellular device receive the GPM and send replies on the access channel. The base station receives reply from cellular device and sends two messages on the paging channel: an acknowledgement message (ACK) and a channel assignment message (CAM), assigning a traffic channel to the cellular device. The cellular device acknowledges the base station and uses the assigned traffic channel for further communication. If the paging request is for an SMS termination, the CAM is replaced by a data burst message (DBM) containing the SMS. Because a network usually does not know the location of a cellular device down to the precision of a cell, a GPM is usually broadcasted to a set of cells. Overhead traffic is also delivered over the paging channel, and occupies about 25% of its capacity.

3. Attacks on cellular networks

Denial of service (DoS) attacks on cellular networks have already been demonstrated. Attacks on GSM networks have been discussed theoretically in (William Enck, 2005; Chuanxiong Guo, 2004; Patrick

Traynor, 2006) and experiments with attacks in real CDMA networks are described in (Jeremy Serror, 2006).

3.1. Attacks on GSM networks

The vulnerability in GSM cellular networks that allows for targeted text message attacks to occur is the result of bandwidth allocation on the air interface between control and traffic channels. Under normal operating conditions, the small ratio of bandwidth allocated to control versus traffic data is sufficient to deliver all message. However, because text messages use the same control channels for delivery as voice calls for set up (SDCCHs), contention for resources occurs when SMS traffic is elevated. Given a sufficient number of SMS messages, control channels will be fully utilized and arriving voice calls will be blocked for lack of available resources.(Patrick Traynor, 2006)

A DoS attack targeting a whole network requires more resources and is easier to detect by a network operator, so adversaries would like to target an attack to a particular geographic location. Enck et al. in (William Enck, 2005) addresses the issue of creating hit-lists of phone numbers with a high probability of being located in the target area. A very convenient tool is the North American Numbering Plan, where traditionally all phones with a given prefix are registered in a single geographic area and administrated by a single service provider. Due to number porting and the portability of cellular devices, there is no guarantee that a given number is in the targeted network and in the targeted area. There are some web services that provide information about which network a given phone number belongs to. To narrow down the hit-list to real phone numbers only, web search engines and some scripting tools can be used.

When a hit-list is created, a DoS attack can be started, sending SMS messages to listed phone numbers. Enck et al. propose using websites for SMS insertion, but as discussed later, a botnet of smartphones could be used as well.

As each cellular device can hold only a limited amount of SMSes, such DoS attack cannot be sustained for prolonged periods of time. Patrick et al. (Patrick Traynor, 2006) states that under realistic network conditions, adversaries can achieve blocking rates of more than 70%. Only experiments with real networks could show how well the real world fits into this model, because the blocking rate for voice calls depends on the queuing strategy deployed at the base station. Guo et al. (Chuanxiong Guo, 2004) describes an DoS attack where voice calls are used. Compromised smartphones can make phone calls to the numbers in a hit-list, consuming all TCHs and blocking voice communication to and from the targeted base station. The base station supports only a small number of parallel voice communications, so a relatively small cellular botnet is needed to DoS a base station. SMS service also could be affected, if the number of initiating voice calls saturates paging and control channels.

3.2. Attacks on CDMA networks

In the experimental attack described by Serror et al. (Jeremy Serror, 2006), UDP packets from the internet to data users in a cellular network are injected. A single UDP packet generates several signaling messages on the paging channel, as described before. In this attack the paging channel is targeted as a bottleneck, so UDP packets can be of minimum length. The signaling for voice and SMS communication is similar, so calls and SMSs can also be used in an attack instead of UDP traffic from internet. Each paging request consumes about 0.75% of the paging channel's capacity. Experiments in a production network showed that to consume 10% of the channel capacity, about 13 paging requests per second were required. An attempt to DoS a base station in a production network is not possible, so Serror et al. report network statistics records during real storming events, where drop rates of crucial paging channel messages are 99%. That ties in well with the theoretical model, suggesting that throughput collapses to zero when the paging load exceeds a critical value.

4. Smartphones and cellular malware

According to Nielsen Mobile (Nielsen mobile, n.d.), more than 26 million cellular subscribers use a smartphone device and smartphones represent 16% of recent cellular device acquisitions in the US. 10% of Americans have a smartphone. The picture is similar in Europe. Smartphones accounted for 18.5% of the European subscriber base in 2Q of 2008, according to Industry Strategic Outlook(market research, 2008). If we look at the specification of a typical smartphone, a 500MHz processor and 128MB of RAM are common. These values are similar to specification of a desktop PC ten years ago. Richly featured multi-tasking operating systems are used to run variety of applications, but these also expose vulnerabilities that can be exploited by an attacker.

Bearing in mind the similarity in processing power between smartphones and older desktop PCs, the amounts of smartphone malware is lower than could be expected. Cellular botnets are mentioned as a major threat in 2009 (Georgia Tech Information Security Center, 2008). As with PCs, cellular botnet owners could rent out their botnets. Information and software that helps building your own botnet is freely available online, similar content will be available for cellular botnets too, thus lowering the amount of intellectual resources needed by an adversary to control a cellular botnet.

A botnet of cellular devices would be ideal for carrying out the attacks described above. If a DoS attack is carried out by sending SMSs from websites, network operators could disable this functionality, which would completely disarm the adversary. When attack SMSs are sent by compromised smartphones, network operators hava no easy way to filter attack messages from legitimate traffic. This poses a challenge that is equivalent to filtering DDoS attack packets from regular traffic on the internet. The same is true for calls made by compromised smartphones. In the event of SMS attack on a GSM network, even with a sound queuing strategy at the targeted base station, legitimate incoming SMS traffic would be blocked. If an SMS attack is combined with a call-based attack, only outbound SMS communication would be possible, and only if the base station has an appropriate queuing strategy.

A cellular botnet can be used against a CDMA network as well, since establishing voice calls and sending SMSs consumes the resources of paging channel. If the load of the paging channel exceeds a critical value, throughput collapses to zero and both voice and SMS communication are blocked in both directions (Jeremy Serror, 2006).

5. Possible uses of cellular botnets in cyber warfare

The recent cyber attacks on Estonia, Georgia and Kyrgyzstan seem to be aimed at nation-states, rather than specific companies or institutions. It seems that the aim of such attacks is to cause maximum disruption of everyday life. If so, the ability to operate a cellular botnet would be highly regarded by the adversaries. Denying the service of cellular networks to a technologically advanced country would fit well with previous attacks trying to disrupt banking and internet (Rhoads, 2009) services. An attack on a capital city or a nation’s financial centers would also be very disruptive and require a smaller botnet than a nationwide attack.

Instead of trying to disrupt a cellular network, Guo et. al. (Chuanxiong Guo, 2004) propose an attack where a botnet is used for dialing emergency call centers like 911 or 112. With some effort, a hit-list of phone numbers to important entities such as hospitals, police stations, military and government institutions can be made. Such an attack can also be launched against all landlines in a target area. Prefixed numbering schemes make hit-list creation easy. If a botnet is large enough, landlines will be called incessantly, blocking all legitimate incoming calls. Wheather it would be possible to make an outbound call under such attack is unclear, as it depends on how well telecom switches could handle such load.

Such attacks can be used as part of a pure cyber conflict, because no physical presence in the targeted area is needed. They could also be used to support conventional military operations or even a terrorist attacks such as took place in Mumbai (Singeputa, 2008). Denying communications in a targeted area even for a couple of minutes could give significant advantage to attackers, and a call-attack against emergency call centers and police offices would hamper response actions.

Call-based attacks could also be carried out by a botnet of PCs with VoIP functionality allowing to dial regular (landlines/cellular) numbers. Once it is known that attacks come from a VoIP network, disconnecting the VoIP provider from regular telecommunications networks would quickly restore attacked services.

Such attacks can also be used for cybercriminal activities, for example extorting companies who rely heavily on phone use.

6. Defense

Guo et. al. (Chuanxiong Guo, 2004) propose telecommunications side protection, where cellular network operators have misbehavior detection possibilities. When abnormal behaviors are observed at the telecom side, network operators can perform rate limiting, call filtering or the blacklisting of zombie-phones. Apart from the technical challenges and their associated costs, such approach is unlikely to restore cellular service immediately after an attack is discovered. In the event of call center blocking the number of involved parties is bigger, making any mitigation efforts even more complicated.

An obvious telecommunication side defense is as following: when an attack against a base station is carried out, incoming voice/SMS traffic should exceed outgoing traffic. The targeted base station should detect the overload on incoming traffic and share channel resources more fairly than first-come-first-serve. Separating incoming and outgoing traffic would allow voice and SMS communications initiated from the attacked base station to reach emergency call centers.

An effective defensive measure would be that before sending SMS or making a voice call, some proof of human interaction would be provided. As a logical proof, some kind of CAPTCHA mechanism could be deployed, where the puzzle is sent from base station to the cellular device and the communication is not established until solution is provided. Obviously it cannot be used when dialing emergency call centers, because the caller could be unable to solve the required puzzle.

A physical proof would be even better and easier to implement. Usually cell phone user is pushing a designated hardware button to send SMS or voice call. Even the best malware in the world cannot push a button on the keyboard. If a formally verified hacker-proof hardware is included in each smartphone, network operator can distinguish between software and human initiated communications. A software-initiated communication doesn’t inherently mean it is part of an DoS attack, but when overload is detected, human-initiated communication could be given higher priority. Such method could possibly eliminate cellular DoS attacks. Given the short average lifetime of a smart phone, most smartphones would be secured in a couple of years. The biggest drawback to such an approach concerns how to enforce smartphone manufacturers to carry it out.

7. Conclusion

Described attacks pose real threat to so far excellent reliability of cellular networks. Satellite imagery was only available to technologically advanced nations 10 years ago, nowadays it is just a mouse click away. The same is likely to happen with smart phone based attacks. Cellular networks designed in 1980s and early 1990s (wikipedia - gsm, n.d.; wikipedia - IS-95, n.d.) are not ready for such attacks, as shown by both theoretical and experimental research. The only question open is how long will it take for criminal groups to find a business opportunity profitable enough to develop commercial smartphone-malware, converting theoretical attacks to publicly available powerful weapons.

8. Bibliography

Guo, C. et al., (2004). “Smart-Phone Attacks and Defenses.” In *HotNets III,* San Diego, CA, USA.

eurostat news release (2007) Eurostat [Online]. Available at: http://epp.eurostat.ec.europa.eu/pls/portal/docs/PAGE/PGP_PRD_CAT_PREREL/PGE_CAT_PREREL_YEAR_2007/PGE_CAT_PREREL_YEAR_2007_MONTH_11/3-27112007-EN-AP.PDF [accessed 5 January 2009]

Emerging CyberThreats Report for 2009. (2008) Georgia Tech Information Security Center. [Online]. Available at: http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf [accessed 6 January 2009]

GSA - The Global mobile Suppliers association.(2009) Global mobile Suppliers association. [Online]. Available at: http://www.gsacom.com/gsm_3g/market_update.php4 [accessed 26 January 2009]

Serror, J et al., (2006). “Impact of Paging Channel Overloads or Attacks on a Cellular Network.” In *Proceedings of the 5th ACM workshop on Wireless security,* Los Angeles, CA, USA.

Industry Strategic Outlook #14.2008: European Wireless Outlook: A detailed review of operator strategies and metrics in Europe. (2008) Market Research. [Online]. Available at: http://www.marketresearch.com/product/display.asp?productid=2026740&g=1 [accessed 25 January 2009]

Smartphone statistics. Nielsen mobile. [Online]. Available at: http://www.nielsenmobile.com/html/press%20releases/SmartphoneStatistics.html [accessed 23 January 2009]

Agrawal, N. et.al.,(2004) “Capacity Analysis of the GSM Short Message Service.” In *National Conference on Communications,* Bangalore.

Traynor, P., et.al., (2006). “Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks.” In *Proceedings of the 12th annual international conference on Mobile computing and networking*, Los Angeles, CA, USA.

Rhoads, C., (2009). *Kyrgyzstan knocked offline - WSJ.com*. [Online]. Available at: http://online.wsj.com/article/SB123310906904622741.html [accessed 30 January 2009]

Singeputa, S., 2008. *At Least 100 Dead in India Terror Attacks*. [Online]. Available at: http://www.nytimes.com/2008/11/27/world/asia/27mumbai.html [accessed 23 January 2009]

US Census Bureau. (2008). US Census Bureau. [Online]. Available at: http://www.census.gov/compendia/statab/2008/tables/08s1354.pdf [accessed 22 January 2009]

wikipedia - gsm. *wikipedia - gsm*. [Online]. Available at: http://en.wikipedia.org/wiki/Gsm [accessed 28 January 2009] wikipedia - IS-95, n.d. *wikipedia - IS-95*. [Online]. Available at: http://en.wikipedia.org/wiki/IS-95 [accessed 30 January 2009]

Enck, W. et. al., (2005). “Exploiting Open Functionality in SMS-Capable Cellular Networks.” In *Proceedings of the 12th ACM conference on Computer and communications security,* Alexandria, VA, USA.