A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications

David Perez - david@taddong.com
Jose Pico - jose@taddong.com

Black Hat DC 2011 (Jan. 18-19)

ABSTRACT

In this article we present a practical attack against GPRS, EDGE, UMTS and HSPA (2G/3G) mobile data communications. We demonstrate that an attacker with a budget of less than $10,000 can set up a rogue BTS, make the victim devices connect to such BTS, and gain full control over the victim's data communications. Three vulnerabilities make the attack possible: first, the absence of mutual authentication in GPRS and EDGE (2G), which makes GPRS and EDGE devices completely vulnerable to this attack; second, the standard's requirement that mobile terminals must support the GEA0 encryption algorithm (i.e. no encryption); and finally, the mechanism implemented on most UMTS and HSPA (3G) devices that makes them fall back to GPRS and EDGE when UMTS or HSPA are not available, which makes it possible to extend the attack to these 3G devices.

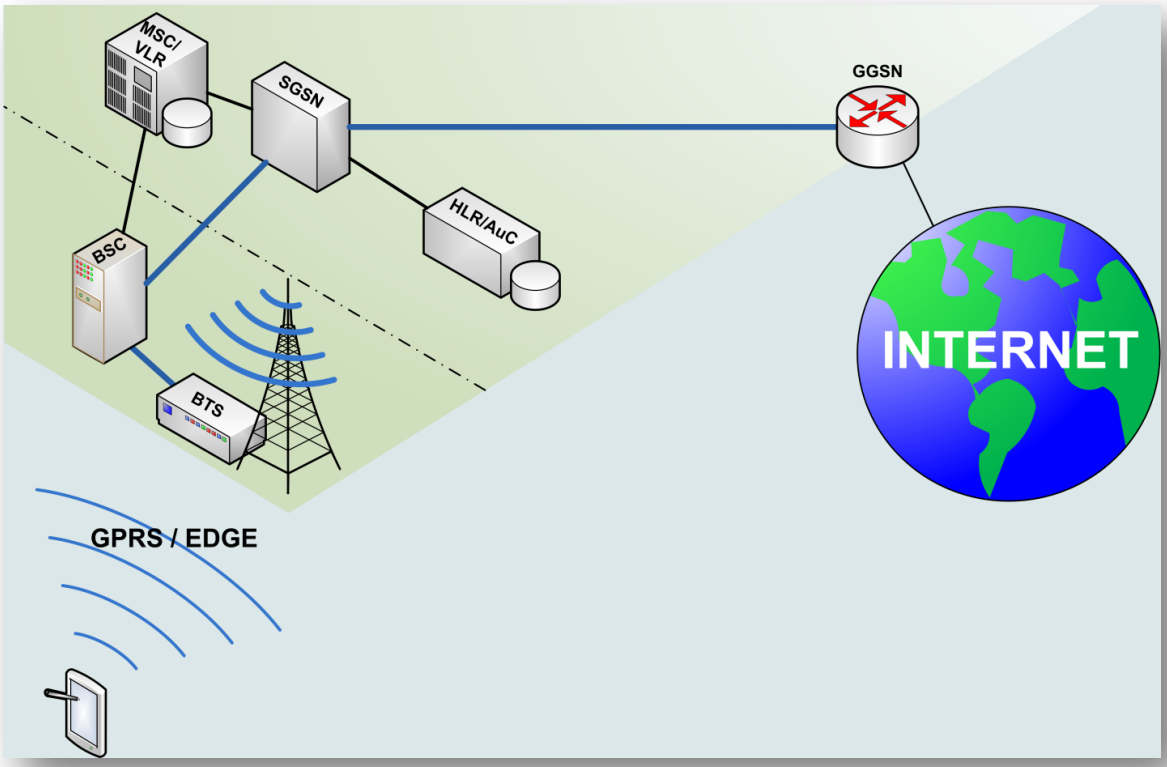
INTRODUCTION

GSM has already been proven to be very insecure. The cryptographic algorithms involved in GSM have been broken. Furthermore, the absence of network authentication makes it possible for an attacker to take full control of the voice calls and SMS messages of victim mobile devices by setting up a rogue BTS and forcing the devices to connect to it. Note that the attack with a rogue BTS does not rely on any weakness in the cryptographic algorithms used in GSM, so it has always been possible, even before the cryptographic algorithms were broken. In recent times this attack has gained a lot of attention because nowadays a rogue BTS can be set up for under $4,000.

GPRS and EDGE, the data communication protocols added to GSM after its initial deployment, have all along been suspected of being just as insecure as GSM itself. In this article, we prove these suspicions to be right on the mark. We show that an attacker, with a budget of less than $10,000, can set up a rogue GPRS/EDGE capable BTS, make the victim devices connect to such BTS, and gain full control over the victim's data communications, be it GPRS (2G), EDGE (2.5G), or, in some cases, which will be detailed later, even UMTS (3G) or HSPA (3.5G).

THE GPRS/EDGE/UMTS/HSPA ARQUITECTURE

The following diagram depicts the architecture of a normal GPRS/EDGE connection:



The mobile station (MS), which might be a smartphone, a laptop with a 2G/3G modem, an iPad with 3G support, or any other 2G/3G enabled device, establishes a wireless connection with the nearest BTS (Base Transceiver Station) of a Public Land Mobile Network (PLMN) to which the user is a subscriber. After authentication of the mobile user has taken place, an IP data connection is established (tunneled) between the MS and the GGSN (Gateway GPRS Support Node), going through the BTS, the BSC (Base Station Controller) and the SGSN (Serving GPRS Support Node). The MS gets assigned an IP address by the GGSN during the establishment of the tunnel. The MS sends all IP packets through the tunnel so that they are received by the GGSN. The GGSN decapsulates the IP packets coming from the MS and routes them to the Internet. Conversely, the GGSN receives from the Internet all packets going to the MS, encapsulates them, and sends them to the MS through the previously established tunnel.

In the air interface, encryption may or may not be used, at the choice of the BTS. The MS will indicate to the BTS which encryption algorithms it supports, and the BTS will indicate to the MS which of those protocols it will have to use during the rest of the connection. The algorithms to choose among are GEA0 (no encryption), GEA1, GEA2 and GEA3. We will not spend more time describing the differences between these algorithms, because the attack works regardless of which encryption algorithm the real

PLMN uses. Simply note that a BTS might select GEA0, which means using no encryption at all, and all MS are required, by the standards, to support this (no-) encryption algorithm. This fact will be exploited later during the attack.

THE VULNERABILITIES

Vulnerability 1: Lack of mutual authentication in GPRS/EDGE (2G, 2.5G)

GPRS and EDGE use plain old GSM authentication, which is unidirectional, as opposed to mutual. The MS has to prove to the PLMN that the SIM card inserted on it belongs to the subscriber it claims to be, identified by its International Mobile Subscriber Identity (IMSI), but not the other way around: the BTS to which the MS connects, does not need to prove to the MS that it belongs to a real PLMN, known by the SIM card.

This fact allows an attacker to set up a rogue BTS that broadcasts information pretending to belong to any PLMN of the attacker's choice, and the victim MS will connect to it as if they were connecting to the real PLMN.

The use of a rogue BTS against victim MS to intercept GSM voice calls and SMS messages has been shown several times recently[1], but, as far as we know, not yet for GPRS/EDGE data connections.

Vulnerability 2: Support for no encryption (GEA0)

The standards require all GPRS/EDGE devices to support the encryption algorithm GEA0, which actually means no encryption at all.

This fact allows an attacker using a rogue BTS to convince the victim MS to send and receive all information unencrypted.

Vulnerability 3: Fall back to GPRS/EDGE of UMTS/HSPA (3G, 3.5G) devices whenever UMTS/HSPA service is not available

UMTS and HSPA (both HSDPA and HSUPA) use UMTS authentication, which is mutual. Thus, an attack using a rogue base station should be infeasible against UMTS/HSPA devices, unless the cryptography used in the authentication process were broken. This holds true for devices that would only accept to connect to a UMTS/HSPA network and refuse to connect to anything else, like a GSM/GPRS/EDGE network. But the reality is that most UMTS/HSPA devices are also GSM/GPRS/EDGE capable, and are configured to try and connect to a GSM/GPRS/EDGE network whenever a suitable UMTS/HSPA network is not available.

This fact allows an attacker to force these devices to behave as simple GSM/GPRS/EDGE devices, by simply using a jammer against the UMTS/HSPA frequencies, thus extending the previous two vulnerabilities to them.

Again, this third vulnerability applies to, and only to, any UMTS/HSPA devices that are also GSM/GPRS/EDGE capables, and that are configured to try and connect to a GSM/GPRS/EDGE network whenever a suitable UMTS/HSPA network is not available.

THE THREAT

Vulnerabilities are not a problem as long as there are no threats against them. But in the case of mobile communications, the threat is very real.

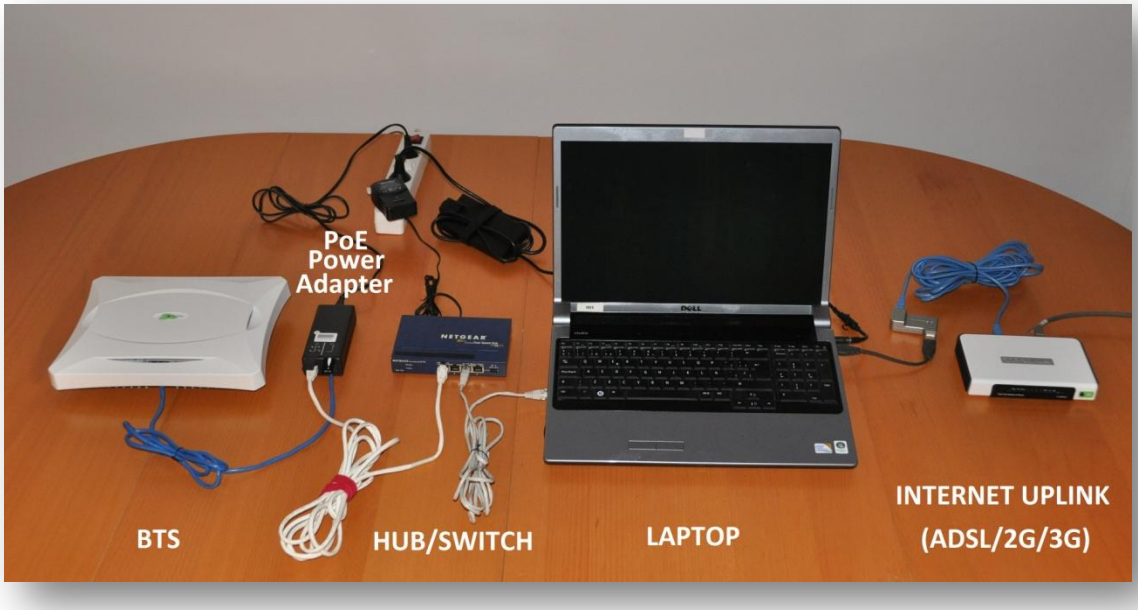
How many people, organizations, or, in general, entities, might be interested in eavesdropping and/or manipulating the mobile data communications of other entities, like competitors, nation enemies, etc? Obviously, we do not have accurate statistics on which to base our answer to this question, but common sense tells us that the most probable answer is "many", and that is probably an understatement.

And how many of those potential attacking entities could dedicate a budget of $10,000 to this purpose? Again, no statistics are available to us, but common sense tells us that the answer is, once more, "many".

THE TOOLS

All the tools that an attacker would need to perform the attack that will be described in the following section, are available to anyone via the Internet. Some of the tools are software programs that are freely downloadable, while other tools are hardware equipment that can be bought via the Internet.

In particular, an attacker could use the following tools:



ip.access nanoBTS - Model 165CU - EGSM900

This is a GSM+GPRS+EDGE capable BTS, manufactured by ip.acccess (www.ipaccess.com).. It features an IP over Ethernet Abis interface, which means that its connection to the BSC is made through an Ethernet cable, which is very convenient (other BTS use DS-1, ES-1, or E1 TDM circuits) [2].

More information can be found at: http://www.ipaccess.com/products/EDGE.htm.

PC (preferably a laptop/netbook, to carry it around easily) with an uplink to the Internet

We have used a Dell studio 1737 laptop (www.dell.com), sometimes with an additional external Gigabit USB 2.0 Ethernet adapter connected to an ADSL router, and sometimes with a 2G/3G USB modem instead, but any PC with an Ethernet interface and some other way of connecting to the Internet, would be good. The uplink to the Internet may be a WiFi connection, a USB port with a USB 2G/3G modem, an additional Ethernet port connected to a DSL or cable router, or any other.

OpenBSC

Quoting the description from the home page of the OpenBSC project (http://openbsc.osmocom.org/trac/) [4] :

"[OpenBSC] is a project aiming to create a Free Software, GPL-licensed Abis (plus BSC/MSC/HLR) implementation for experimentation and research purpose. What this means: OpenBSC is a GSM network in a box software, implementing the minimal necessary parts to build a small, self-contained GSM network."

The OpenBSC software is freely available for download at the afore mentioned home page of the OpenBSC project.

Note: We would like to thank the developers of OpenBSC, namely Harald Welte, Dieter Spaar, Andreas Evesberg and Holger Freyther, for sharing their awesome work with the community.

Note: Please note that the purpose of OpenBSC is not to serve as an attack tool, but to allow for experimentation and research of GSM communications in general.

OsmoSGSN

OsmoSGSN is a software application included in the OpenBSC project. Quoting the description from the web page dedicated to OsmoSGSN in the OpenBSC website (http://openbsc.osmocom.org/trac/wiki/osmo-sgsn) [5]:

"OsmoSGSN (also spelled osmo-sgsn when referring to the program name) is a Free Software implementation of the GPRS Serving GPRS Support Node (SGSN). As such it implements the GPRS Mobility Management (GMM) and SM (Session Management). The SGSN connects via the Gb-Interface to the BSS (e.g. the ip.access nanoBTS), and it connects via the GTP protocol to a Gateway GPRS Support Node (GGSN) like OpenGGSN?"

OpenGGSN

Quoting the description from the home page of the OpenGGSN project (http://sourceforge.net/projects/ggsn/) [6]:

"OpenGGSN is a Gateway GPRS Support Node (GGSN). It is used by mobile operators as the interface between the Internet and the rest of the mobile network infrastructure."

The OpenGGSN software application is available for download at the afore mentioned home page of the OpenGGSN project.

Mobile phone jammer

Quoting the definition in the Wikipedia (http://en.wikipedia.org/wiki/Mobile_phone_jammer) [7]:

"A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones."

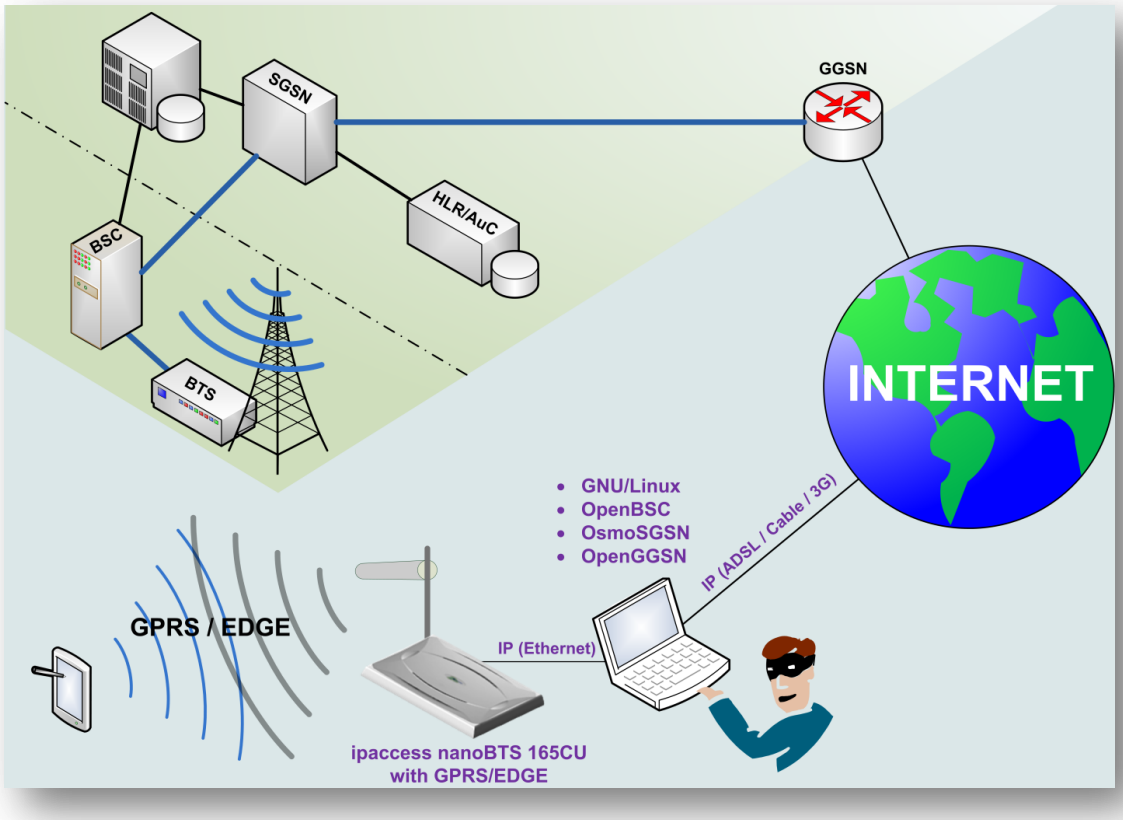
In particular, the attacker would need a mobile phone jammer capable of jamming the frequency bands assigned to UMTS/HSPA in a particular location (different countries assign different bands), while leaving the GSM/GPRS/EDGE bands undisturbed.

Mobile phone jammers of this kind abound in the Internet for sale. As an example, we provide the following reference: Techwisetech PCB-1050 (http://www.techwisetech.com/products/PCB1050.htm) [8], which sells for about $200. Please note that even owning a cell phone jammer is illegal in some countries.

THE ATTACK

An attacker wanting to intercept the mobile data communications of a victim user may perform the following steps to achieve her objective.

The following diagram illustrates the attack:



Step 1

The attacker positions herself close enough to the target so that the power radiated by her own BTS can reach the target.

Note: The range of the attack can be increased by using a high gain directional antenna and/or an amplifier.

Step 2

The attacker listens in the radio spectrum, in the frequency band in which she intends to emit, looking for a suitable frequency to use. Her choice would preferably be one that is declared as a "neighbor" frequency by the beacons of the surrounding cells of the real PLMN, and that is not being actually used by the real PLMN, or, if it is being used, it is received with very low power at that location. The PLMN in this scenario is the PLMN to which the victim user is a subscriber.

Note: The PLMN of the target will have to be known by the attacker in advance, or she can just try the attack with all the different PLMNs present in the area in turn, and eventually she will hit the right one.

Step 3

The attacker configures her BTS to emit in the frequency chosen in the previous step, and it also configures it to impersonate the real PLMN, by setting its MCC (Mobile Country Code) and MNC (Mobile Network Code) codes to those of the real PLMN. She also sets up her BTS to accept the connection of the target user, identified by his IMSI (International Mobile Subscriber Identity) code, which uniquely identifies the SIM card of the user, or his IMEI (International Mobile Equipment Identity), which uniquely identifies the MS (Mobile Station).

Note: Again, the attacker needs to know in advance the IMSI and/or IMEI of the victim, or she may simply monitor and record connection attempts from any IMSI/IME in the area, and either intercept all of them, or reject them and repeat the experiment in different locations at times when the target is known to be in the area. After a few repetitions of the test, only the IMSI/IMEI of the target would show up at all locations.

Step 4

The attacker makes sure that her laptop has a working uplink to the Internet, using any means available to her, for example a 2G/3G connection to a real PLMN, an ADSL connection or a cable connection, and she makes sure to configure OsmoSGSN, OpenGGSN, and her routing tables correctly, so that the traffic from the victim will be forwarded to the Internet (or redirected to wherever she wants) and the replies from the Internet get back to the victim.

Note: If the attacker would only want to establish an IP connection to the attacker and would not intend to actually forward his traffic to the Internet, she might skip this step.

Step 5

The attacker powers up her BTS, providing coverage to the victim. If everything goes well, the victim MS will then abandon its connection to the real PLMN and it will connect to the BTS of the attacker. There are a few other minor details involved in this decision taken by the MS to switch from one BTS to another, but it mainly depends on the power level: the MS will basically try to connect to the most powerful BTS it sees.

When the victim MS gets attached to the rogue BTS, the BTS will instruct the MS to use GEA0 as the encryption algorithm, which means no encryption at all.

Note: Providing more power than the real BTS to the victim MS is possible even if the BTS of the attacker only emits a fraction of that of the real one, as long as it is closer to the victim MS.

Step 6

Once the victim MS is attached to the BTS of the attacker, she has full control over the data connections of the victim. She can read, modify, redirect of modify any IP packet sent or received by the victim MS through the GPRS/EDGE connection.

Note: What exactly the attacker might want to do with the victim's data will depend on who the victim is, what the motivation for the attack is, etc. The possibilities are just endless.

EXTENSION OF THE ATTACK TO 3G

If the target victim is using a 3G connection instead of a 2G connection, the attacker can still perform the attack against him, provided the MS of the victim is configured to fall back to 2G whenever 3G is not available. That being the case, all the attacker has to do is add the following initial step to the attack:

Step 0

Switch on a jammer configured so that it creates interference in the UMTS frequency bands used at that location. The victim MS will loose its 3G connectivity and fall back to a 2G connection.

The rest of the steps are just the same.

THE IMPACT

The impact can be summarized like this: the attacker gets full man-in-the-middle access to the IP connection of the victim MS to the Internet. She can, then, for example:

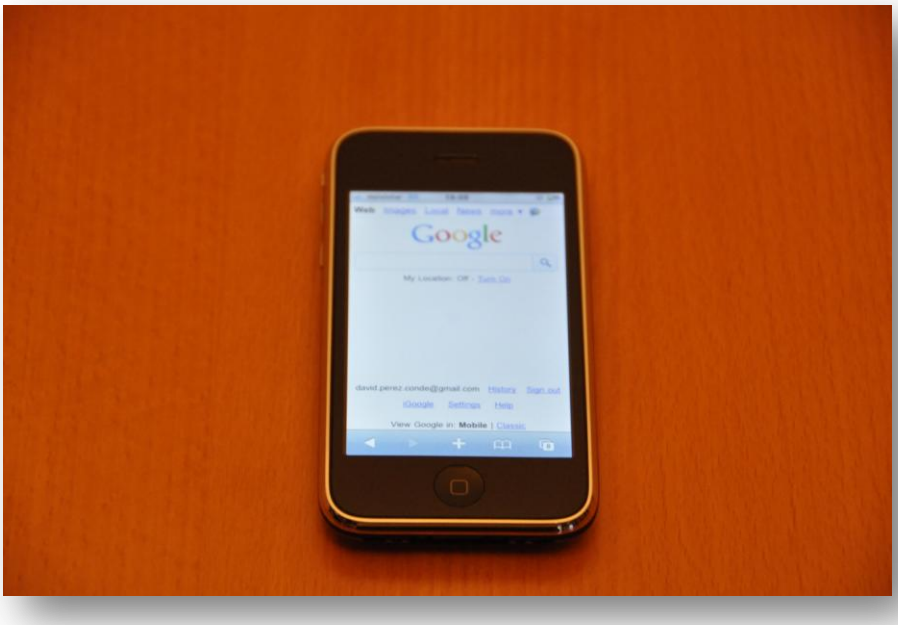
- sniff the traffic and get cleartext credentials (e.g. HTTP, FTP, TELNET),
- redirect outgoing connections to phishing sites, rogue SMB servers, rogue web servers serving malicious contents or any other malicious endpoints,
- alter traffic to insert malicious content in HTTP replies, or
- directly attack the victims IP stack doing port scanning and exploiting any vulnerable services the victim MS may be running.

Again, these are just a few examples of ways the attacker can leverage the privileged man-in-the-middle position she would gain from performing the rogue base station attack.

SAMPLE ATTACK SCENARIOS

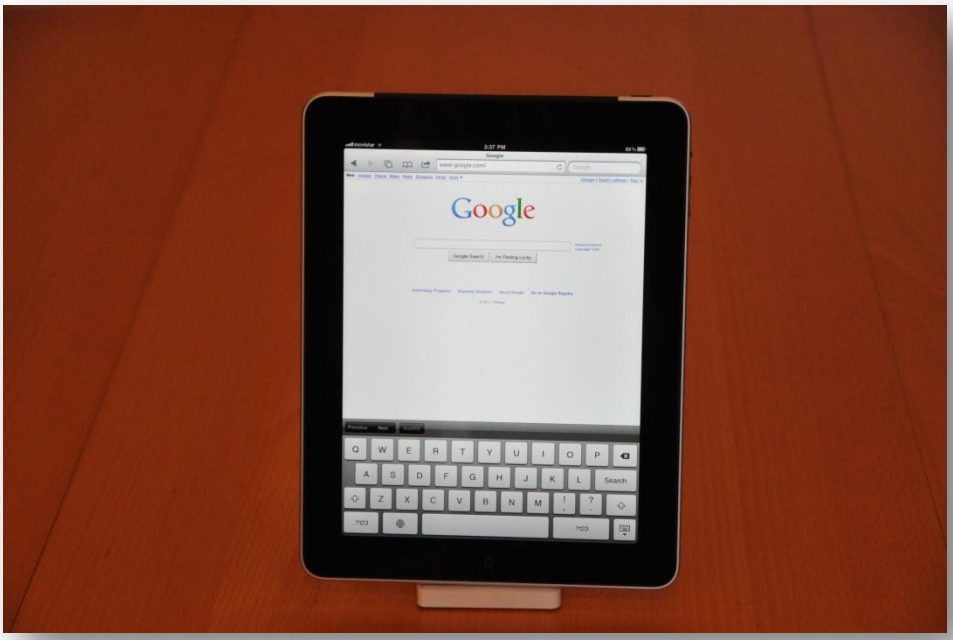
The attack would be effective against virtually any mobile device that the victim user might be using. The following scenarios describe some examples of devices that we have tested the attack against.

Attack scenario 1: Sniffing traffic from an smartphone (iPhone)



A user of the iPhone performs a search in Google using the iPhone web browser Safari. The attacker gets to see all the traffic, including the terms the user searched for and the results from the search.

Attack scenario 2: Redirecting traffic of an iPad to a rogue web server



A user of an iPad tries to navigate to her bank web site by typing the correct HTTPS:// URL in the web browser. The attacker redirects the connection to a rogue web server. The user receives a warning stating that the presented certificate cannot be trusted, but she accepts the connection anyway. The rogue web server presents a phising page, the user types in her user and password, which are then obtained by the attacker.

Attack scenario 3: Exploiting a vulnerable service of a laptop

A user of a laptop is connected to the Internet using a USB 3G modem. Its firewall configuration allows access to some services. The attacker port scans the laptop, identifies all accessible services, finds one with a known vulnerability, executes an exploit against it, and gains full access to the victim laptop.

Attack scenario 4: Compromising a 3G Router to attack all devices behind it

A branch office is connected to the Internet using a 3G router. The network of the branch office includes some servers, printers and client computers. The attacker makes the 3G router to connect to its rogue base station. Instantly, all comunications to and from the branch office go through the atacker's system, and are totally under her control. She can then perform any of the above attacks against the traffic of any of the devices behind the router, not just one.

Other attack scenarios

The types of GSM enabled devices in use today goes far beyond these 4 examples: from point-of-sale (POS) devices, to SCADA monitoring devices, including some GPRS/EDGE based surveillance systems. The list is just endless and growing.

COUNTERMEASURES

Unfortunately, GSM/GPRS/EDGE is insecure by design: it cannot be fixed without major modifications to the protocols, the network equipment and the mobile devices. We do not believe this will happen.

Instead, we, as users, can only take the following measures to try and protect our mobile data connections from attacks like the one described in this presentation:

- Use higher level protocols that provide endpoint authentication and encryption, like SSL or IPsec. These protocols should protect your data in transit even if the underlying communication channel is insecure.
- Use only UMTS/HSPA: configure your MS to connect to, and only to, UMTS/HSPA networks. If your MS does not accept to fall back to 2G, your data connections will not be vulnerable to this or any other known attack against 2G (GSM/GPRS/EDGE). Unfortunately, this would mean you would be out of coverage whenever you can't get a 3G connection.
- Be afraid, be very afraid... of GPRS/EDGE data connections!

REFERENCES

- [1] PRACTICAL CELLPHONE SPYING. Chris Paget. DefCon 2010. http://www.defcon.org/html/defcon-18/dc-18-speakers.html
- [2] Base Station Subsystem. http://en.wikipedia.org/wiki/Base_station_subsystem
- [3] ip.access nanoBTS. http://www.ipaccess.com/products/EDGE.htm
- [4] OpenBSC. http://openbsc.osmocom.org/trac/
- [5] OsmoSGSN. http://openbsc.osmocom.org/trac/wiki/osmo-sgsn
- [6] OpenGGSN. http://sourceforge.net/projects/ggsn/
- [7] Mobile phone jammer - Definition. http://en.wikipedia.org/wiki/Mobile_phone_jammer
- [8] Mobile phone jammer- Techwisetech PCB-1050. http://www.techwisetech.com/products/PCB1050.htm

AUTHORS

David Perez Founder & Senior Security Analist with Taddong (www.taddong.com)

Jose Pico Founder & Senior Security Analist with Taddong (www.taddong.com)