Mobile operators vs. Hackers: new security measures for new bypassing techniques

Introduction

After all the loud news around the insecurity of the mobile networks and some harsh real cases that were revealed, mobile operators started taking more sophisticated security measures. Apart from the SMS Home Routing solutions, a newly grown market of the signaling firewalls is being slowly adopted into the operator's infrastructure.

This is the right way to withstand the basic attacks. We have been continuously investigating signaling networks security for years. The results of last year's security assessments and security monitoring projects show that the situation became a little better. However, the same vulnerabilities are being exploited in a sneaky complicated way that is enough to bypass the "straight-forward" security mechanisms.

In this talk, I am going to show some statistics on how the network vulnerability state evolved during last 3 years. Moreover, I cannot go away without showing some new techniques caught during security monitoring and developed during penetration testing. These techniques allow bypassing security measures in some networks and include SMS Home Routing bypass, location tracking with position refinement and the SS7 firewall bypass.

Advanced SS7 attack description

SMS Home Routing bypass

A malefactor can easily bypass most security systems if they have configuration mistakes that are not evident at first sight.

Some operators believe that if they have implemented SMS Home Routing solution and configured core equipment to block Category 1 messages, it would be impossible for an intruder to obtain IMSI and perform more dangerous attacks from the SS7 network. SMS Home Routing is a hardware and software solution that supports proxy functions of confidential subscriber identifiers and equipment addresses when receiving texts from external connections. Category 1 contains all the SS7 messages, which should normally only be received from within the same network and not on interconnect links from other networks, unless there is an explicit agreement to do so.

IMSI is considered confidential data because it is used to address subscribers in a majority of operations. An attacker can conduct more sophisticated attacks exploiting a retrieved IMSI. Sometimes, the IMSI is the attacker's final target. For example, banks use IMSIs to authenticate SIM cards. They can buy information about IMSIs either from operators or from third-party service providers that disclose IMSI values via SS7 vulnerabilities.

However, we should remember about the STP node that receives external signaling traffic. The STP contains many routing rules for signaling traffic, for example, routing a SendRoutingInfoForSM message to an SMS Router. Apart from that, the STP should process addresses of different numbering plans. For example, an UpdateLocation message should be routed to the appropriate HLR based on the address in the E.214 numbering plan.

Telecom standards have several numbering plans for signaling messages routing. The most frequently used of them have codes: E.164, E.212, E.214.

The E.164 is an ITU-T recommendation, which defines the international public telecommunication numbering plan used in the PSTN and some other data networks. It also defines the format of telephone numbers. E.164 numbers can have a maximum of 15 digits. All the global title addresses and mobile numbers that we use for calling are in this format.

The format of the E.164 address is as the following:

CC (country code) + NDC (network destination code) + SN (Subscriber Number)

For example, CC of France is 33, NDC of an French operator is 854. SN can be any unique number, here I used some random digits 1231237.

So the number is 33 854 1231237.

IMSI stands for International Mobile Subscriber Identity. It conforms to the ITU E.212 numbering standard and is a unique identification associated with all GSM, UMTS, and LTE network users. It is stored on the SIM card and is sent to the network for a mobile equipment identification. The IMSI identifier helps the network to identify the subscriber and provide all the required services. The E.212 number can have a maximum of 15 digits.

The format of the E.212 address is as the following:

MCC (mobile country code) + MNC (mobile network code) + MSIN (mobile station identification number)

For example, MCC of France is 208, MNC of an French operator is 80. MSIN can be any unique number, here I also used random digits 4564567894.

Therefore, the IMSI is 208 80 4564567894.

The E.214 is a numbering plan used for delivering mobility management related messages in GSM and UMTS networks. The E.214 number is derived from the IMSI. The E.214 number is composed of two parts. The first part is the combination of CC and NDC of a destination network. The second part of the number is the MSIN of the IMSI, which identifies an individual subscriber.

For example, for the IMSI 208804564567894, the corresponding E.214 number is formed by replacing MCC (208) with CC (33) and MNC (80) with NDC (854), and keeping MSIN as it is. The IMSI 208 80 4564567894 translated to the E.214 numbering plan becomes 33 854 4564567894.

The SS7 network uses the new prefix 33 854 to enable the signaling message to reach the destination network. The destination network uses the MSIN 4564567894 to enable the signaling message to reach the appropriate HLR.

The E.214 numbering plan is usually used at subscriber authentication and registration under a new MSC. Commonly, the new MSC does not usually have information about the new subscriber. Since the IMSI identifier is located on the SIM card, the mobile phone sends the IMSI to the network via radio interface. Then the network transforms the IMSI of the E.212 numbering plan to the E.214 numbering plan and uses the new compiled number for routing SS7 messages of authentication and registration, such as SendAuthenticationInfo and UpdateLocation, to the destination network.

If the routing rule in the STP disregards an operation code for messages processed under the E.214, a malefactor could benefit from this misconfiguration and send the SendRoutingInfoForSM message addressing it in the E.214 (See Figure 1). Although digits of the E.214 must correlate with the IMSI, they can be bruteforced easily: any IMSI stored in the same HLR is enough.

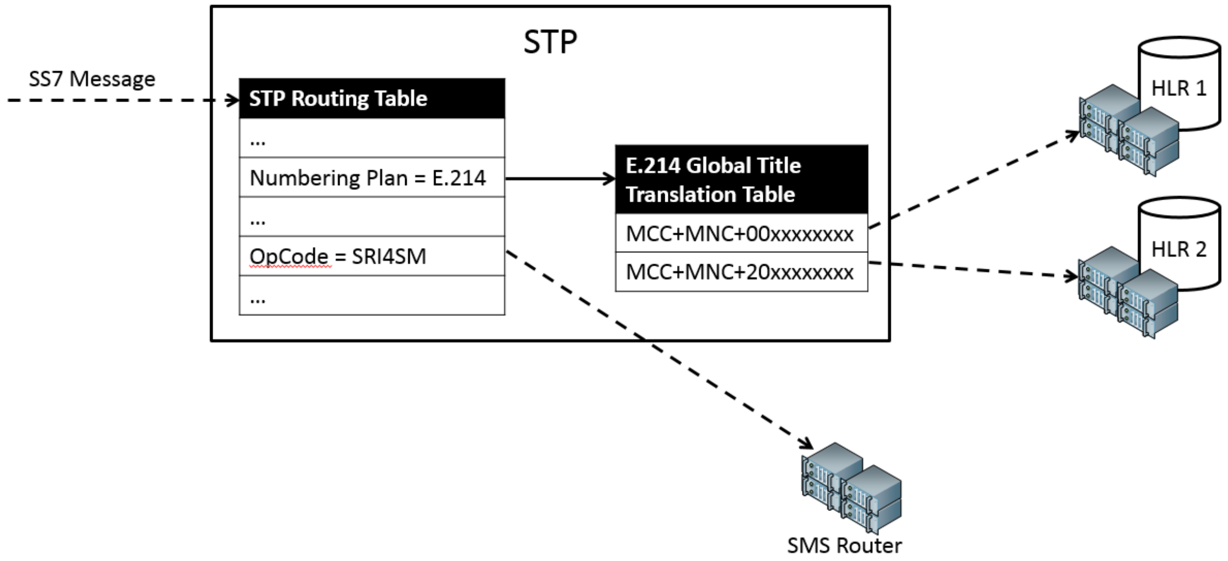


Figure 1. STP routing table misconfiguration

As we can see, the SMS Home Routing solution may be useless if there are errors in the border STP configuration.

Location tracking with positioning refinement

One of the most popular attacks on SS7 networks is location tracking. A request for subscriber location is sent via SS7 networks, the response includes the base station ID. Each base station has specific geographic coordinates and covers a particular area. Because of urban density, the coverage area in a city ranges from tens to hundreds of meters.

An attacker can make use of these mobile network peculiarities to generate location requests, as well as to locate the base station by its ID using a variety of publicly available Internet resources. Accuracy of the location discovery depends on the base station coverage area. Actually, the malefactor determines the position of the base station that serves the subscriber at the moment. However, our investigations show that intruders have learned to determine the subscriber location with better accuracy.

A mobile device usually receives signals from several base stations. If the malefactor determines coordinates of two or three base stations nearest to the subscriber, the subscriber location can be narrowed down.

Normally, a mobile device chooses a base station with the best radio conditions during a transaction. Therefore, the mobile device should interchange signals with the network. The malefactor can use a so-called silent SMS to initiate a hidden transaction with the target subscriber. However, the information about these messages is available in the subscriber's account. A more effective way to hide a transaction is to use silent USSD notifications. Although such transactions are not registered by the billing system, they initiate signal exchange between the mobile device and network. The malefactor can improve location accuracy manipulating base station identifications and silent USSD notifications (See Figure 2).

First, the intruder requests the identifier of the current base station (See Step 1 in Figure 2). Then the intruder sends a silent USSD notification in order to force the subscriber's equipment to carry out a transaction via radio interface (See Step 2 in Figure 2). If the malefactor gets lucky, the network may choose a new base station for this transaction, and the VLR database updates the subscriber location. After that, the intruder requests the subscriber location once again and receives the identifier of the new base station (See Step 3 in Figure 2). Thus, the intruder can narrow down the area where the subscriber is located at the moment.

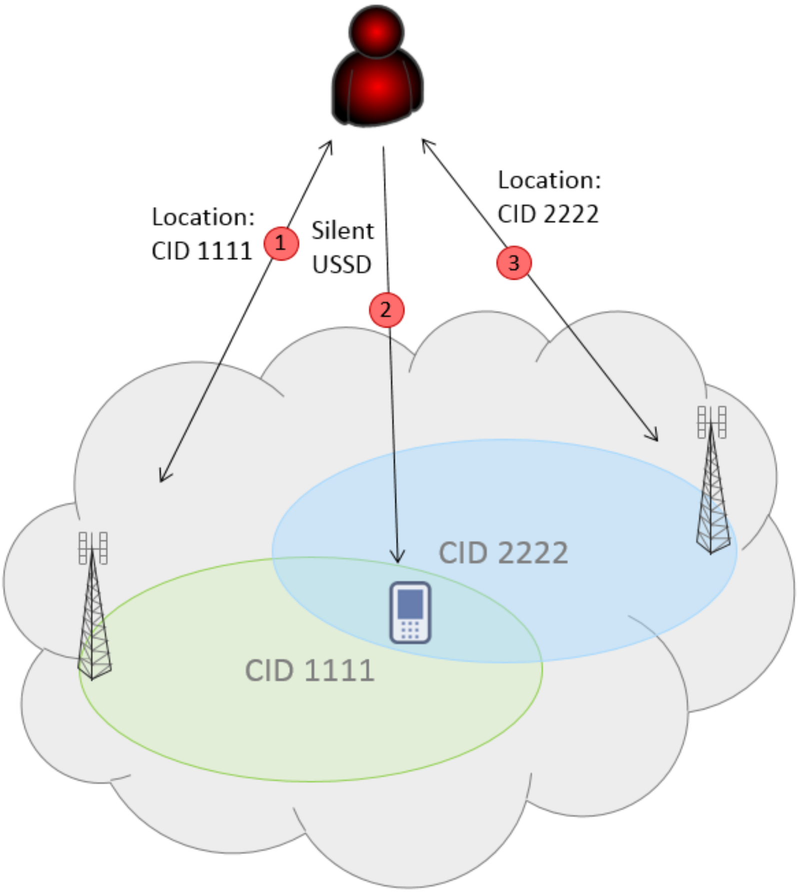


Figure 2. Positioning refinement

Short message interception and SS7 firewall bypass

SMS interception is one of the most dangerous attacks on SS7 networks. Many services still use SMS as a trusted channel. For example, banks use SMS for OTP delivery, social networks—for password recovery, messengers—for access to the application.

In order to intercept an incoming SM, the intruder must register a subscriber in a "fake" network using the necessary equipment. The attack simulates a subscriber being in roaming in a visited network. The HLR gets a record of the subscriber's new location where terminating calls and SMS messages are routed. In case of an originating call, the first attempt fails, as the network registers the subscriber back in its home network. The attacker sees it and can repeat the attack to make the next call attempt fail.

Moreover, if the attackers control the network element, which is indicated as a new MSC, they can intercept terminating SMS messages and redirect terminating voice calls.

As soon as the registration is finished, all incoming SMs are routed to the network element indicated as MSC and VLR in the UpdateLocation signaling message. The attacked subscriber may return to the home network as soon as one of following events is triggered:

- Outgoing call
- Outgoing SM
- Moving to the area covered by another mobile switch
- Mobile phone restart

From the attacker's point of view, keeping the subscriber registered in the "fake" network is unreliable because it is impossible to predict all actions of the subscriber.

The malefactor can register the subscriber in the "fake" network spoofing the MSC address only, keeping the real VLR address (See Step 1 in Figure 3). The attack simulates a subscriber registered in another network so that the current MSC/VLR is used for voice calls and originating SMS messages (See Step 2 in Figure 3), and a fake MSC is used to receive terminating SMS messages (See Step 3 in Figure 3).

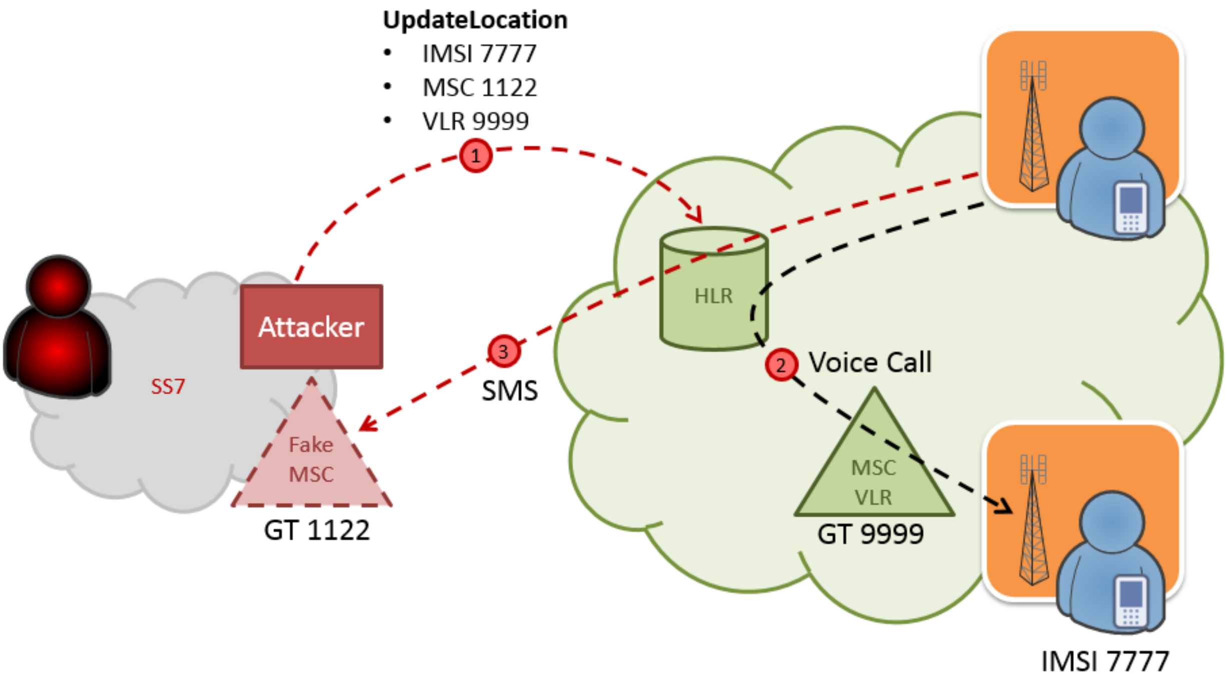


Figure 3. SM interception attack

The attackers can use this to attack services of other companies (for example, bank accounts) that use SMS as a channel to inform clients of any changes. If the intruder controls the network element, which is indicated as a new MSC, they can intercept terminating SMS messages sent by services like mobile banking, password recovery for Internet services, getting access codes for messengers, etc.

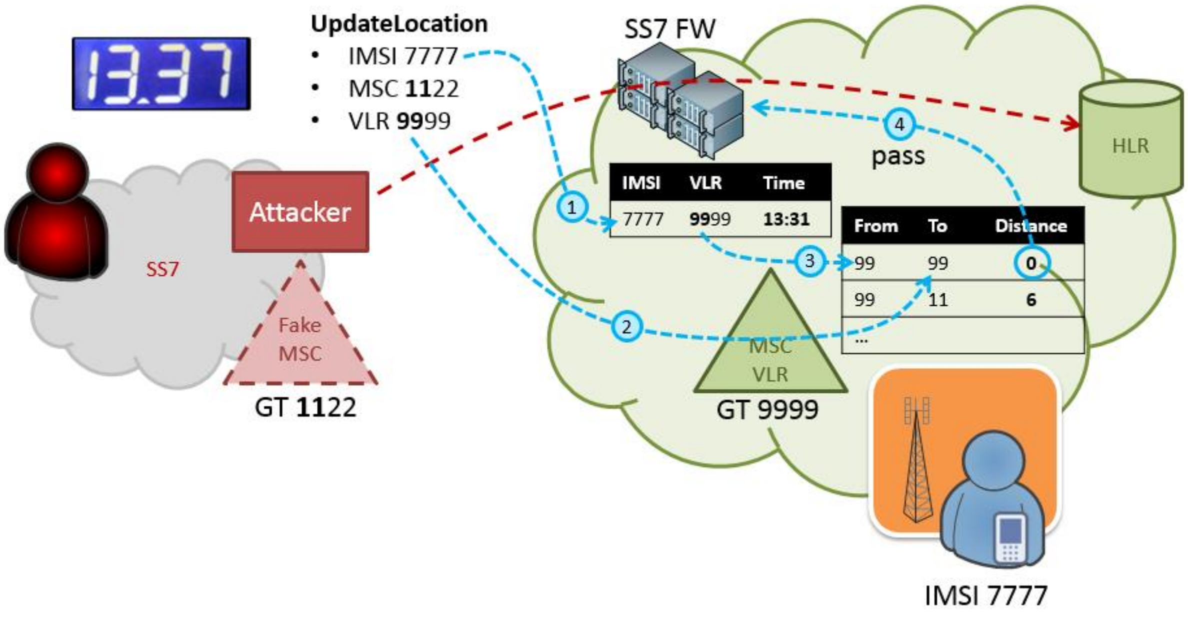
These manipulations do not prevent the attacked subscriber from making originating calls and sending SMs, but incoming SMs go to the spoofed MSC address.

Moreover, this vulnerability is well known, and all SS7 firewall vendors try blocking registration in "fake" networks. Usually, the blocking mechanism in an SS7 firewall relies on its own database that contains current subscribers' locations. Apart from that, an SS7 firewall should have a relative distance table reflecting approximate time to reach any country. For example, the relative distance between the France and Italy is zero because these countries have a common border; the relative distance between the France and Ireland is 2, which is the approximate duration of a direct flight, and so on.

When an UpdateLocation message is received by the network, the SS7 firewall extracts the following information from it: the subscriber's identifier IMSI (See Step 1 in Figure 4) and the address of a new VLR (See Step 2 in Figure 4). After that, the SS7 firewall looks for the latest subscriber's location and registration time in the database (See Step 3 in Figure 4). If the time shift is shorter than the value of the relative distance for the new VLR's country, the UpdateLocation message is regarded as hostile and should be blocked. Otherwise, the UpdateLocation message should be permitted (See Step 4 in Figure 4).

In order to bypass such a protective mechanism, the malefactor can register the subscriber in the "fake" network spoofing the MSC address only, keeping the real VLR address.

Thus, registration with spoofed MSC and real VLR addresses is more reliable for an intruder and helps bypassing some SS7 firewalls.



IMSI	VLR	Time
7777	9999	13:31

From	To	Distance
99	99	0
99	11	6
…		

Figure 4. SS7 firewall bypass

As we can see now, an SS7 firewall is not a reliable protection tool, despite of the fact that the attack signature is quite simple.

Security management process

In order to reduce risks, operators should employ a global approach to SS7 protection. They should conduct regular security audits of the signaling network and develop appropriate measures to mitigate risk based on vulnerabilities as they evolve.

First, the operator needs to know if its network is vulnerable to signaling attacks. After the relevant assessment, the operator obtains information about weak chains and has a clear view of what and how should be changed to improve security.

Then the operator has to monitor external SS7 connections in order to detect malicious and suspicious signaling traffic. As soon as the operator sees unauthorized activity originating from the SS7 network, it has to decide which measures should be taken to prevent it.

The following measures can be taken:

- Sending a note to the operator that generates unauthorized activity. This is the easiest and quickest way to stop bad signaling traffic.
- Blocking the hostile GT. But first, the operator must make sure that the blocking does not affect the operator's services.

Configure the core equipment to ensure security.

Our research demonstrated that telecom companies employ various measures of protection but they are not enough to counteract all possible ways for attackers to penetrate the network. Even large operators are not protected against conversation tapping, message monitoring, and fraudulent activity such as call redirection and stealing. Additionally, hackers can pinpoint a subscriber's location at any given moment.

Clearly, all operators need to employ additional security measures to better address threats.