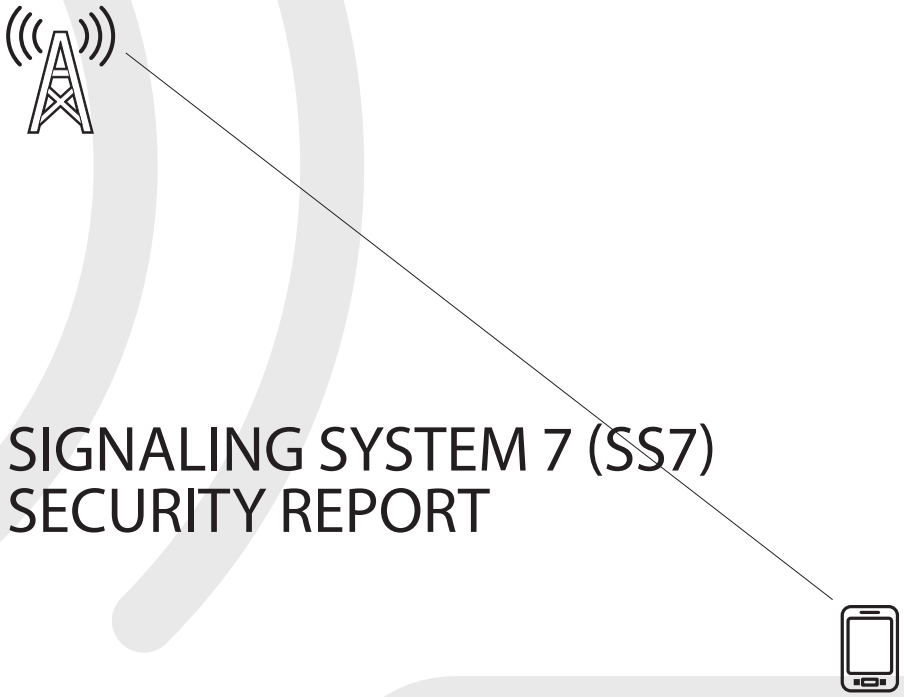
POSITIVE TECHNOLOGIES



SIGNALING SYSTEM 7 (SS7) SECURITY REPORT

POSITIVE TECHNOLOGIES

CONTENTS

1. INTRODUCTION

Nowadays mobile networks are the most dynamic part of critical communication infrastructures and the key instrument used to perform daily activities ranging from voice and text messaging to providing signaling for emergency services and critical infrastructure.

Regardless of what security assurances mobile network operators provide, there is plenty of hard evidence that in fact shows how vulnerable these systems are. Lately, it seems like a common occurrence when private telephone conversations or pictures of government officials, celebrities and business leaders appear on the Internet, even though these individuals usually take extra precautions when it comes to their personal privacy and safety.

In many instances, a common misconception is that security breaches like these are very complicated and expensive to execute and can only be accomplished by high-ranking security intelligence agencies, organized crime or the most sophisticated hackers. This perception is understandable, since most people are trained to view a mobile communication network as a system made up of only the most cutting edge technologies. However, in reality a telecommunications network is a complex system built on subsystems that each have different technological levels, with the security of the whole network usually defined by the security level of the weakest link.

In particular, the process of placing voice calls in modern mobile networks is still based on SS7 technology which dates back to the 1970s. At that time, safety protocols involved physical security of hosts and communication channels, making it impossible to obtain access to an SS7 network through a remote unauthorized host. In the early 21st century, a set of signaling transport protocols called SIGTRAN were developed. SIGTRAN is an extension to SS7 that allows the use of IP networks to transfer messages [1]. However, even with these new specifications, security vulnerabilities within SS7 protocols remained. As a result, an intruder is able to send, intercept and alter SS7 messages by executing various attacks against mobile networks and their subscribers.

The findings in this report were gathered by the experts at Positive Technologies during 2013 and 2014, based on a series of in-depth tests conducted at several large mobile operator sites. These finding were then validated against known vulnerabilities and features of an SS7 network.

An intruder doesn't need sophisticated equipment. Positive Technologies used a popular Linux based computer and a publicly available SDK for generating SS7 packets.

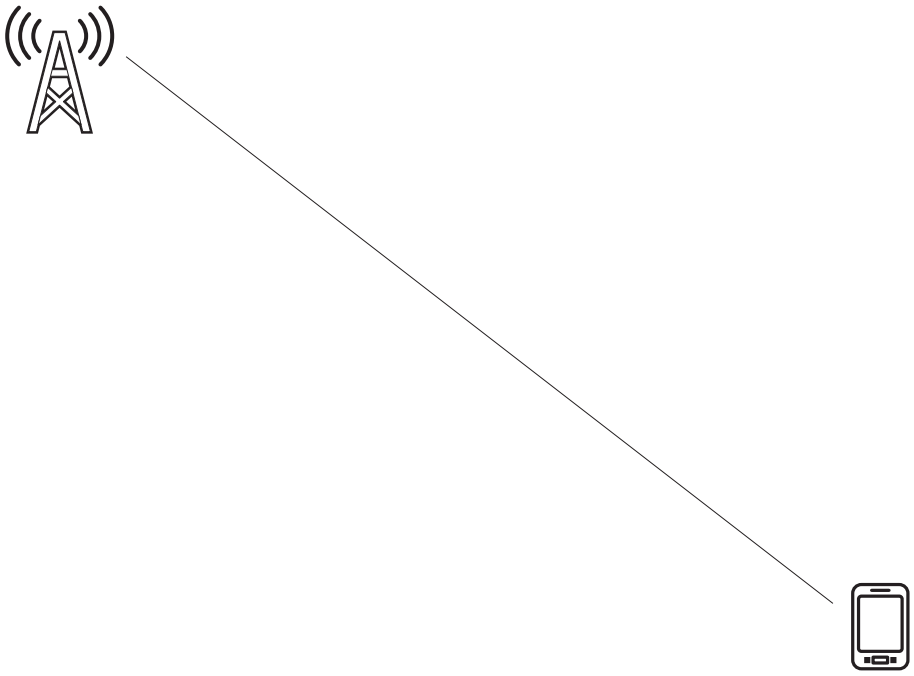
2. KEY FINDINGS

Vulnerabilities in SS7 based mobile networks allow an intruder with basic skills to perform dangerous attacks that may lead to direct subscriber financial loss, confidential data leakage or disruption of communication services. During network security testing, Positive Technologies experts managed to perform such attacks as discovering a subscriber's location, disrupting a subscriber's service, SMS interception, Unstructured Supplementary Service Data (USSD) forgery requests (and transfer of funds as a result of this attack), voice call redirection, conversation tapping and disrupting the availability of a mobile switch.

The testing revealed that even the top 10 telecommunications companies are vulnerable to these attacks. Moreover, there are reported cases of such attacks internationally, including discovering a subscriber's location and eavesdropping on conversations.

Common characteristics of these attacks:

+ An intruder doesn't need sophisticated equipment. Positive Technologies used a popular Linux based computer and a publicly available SDK for generating SS7 packets.
+ After performing an initial attack using SS7 commands, the intruder is able to execute additional attacks using the same methods. For instance, if an intruder manages to determine a subscriber's location, only one further step is required to intercept SMS messages, commit fraud, etc.
+ Attacks are based on legitimate SS7 messages. Therefore, you cannot simply filter messages as it may have a negative impact on the overall quality of service.



A phone network node was once a "black box", but now nodes are built on popular hardware and software platforms (Linux, Solaris, and VxWorks).

3. RESEARCH METHODOLOGY

Prerequisites for an attack

Most SS7 network attacks are based on the main principle of cellular telecommunication networks: subscriber mobility. First, for the a to reach a subscriber, data about the subscriber's location must be stored and updated in the system. Second, subscriber mobility requires that services be available any place within a home area and while roaming on partner networks.

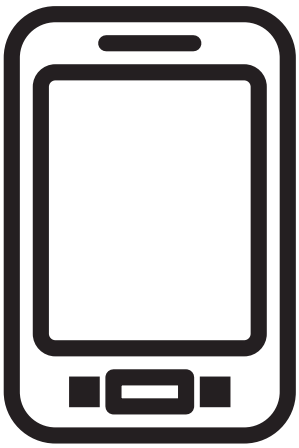
The exchange of subscriber information between mobile carriers is done using SS7 messages, are commonly used by most operators. An attacker can be anywhere. Messages can be sent from any country to any network. At the same time certain message types must be passed to ensure roaming or long-distance communication.

Moreover, telephone communication systems are more and more integrated with IT systems. A phone network node was once a "black box", but now nodes are built on popular hardware and software platforms (Linux, Solaris, and VxWorks).

An attacker's profile

An attacker can be a person or a group of people sufficiently qualified to build a node to emulate that of a mobile operator. To access an SS7 network, attackers can acquire an existing provider's connection on the black (underground) market and obtain authorization to operate as a mobile carrier in countries with lax communications' laws. In addition, any hacker who happens to work as a technical specialist at a telecommunications operator, would be able to connect their hacking equipment to the company's SS7 network. In order to perform certain attacks, legitimate functions of the existing communication network equipment must be used. There is also an opportunity to penetrate a provider's network through a cracked edge device (GGSN or a femtocell).

Besides having different ways of accessing an SS7 network, attackers likely also have different motives for doing so including performing fraudulent activities, obtaining a subscriber's confidential data or disrupting service for certain subscribers or the whole network.



4. RESEARCH SUMMARY

Each of the following scenarios carries a medium level of difficulty to execute the attack. While the likelihood that a bad actor could repeat each of the following attacks is high.

4.1. IMSI disclosure

Goal: Analyze a service provider's network to obtain subscriber information.

Description: In mobile networks, subscribers are identified by the international mobile subscriber identity (IMSI), which is considered confidential information.

This attack is based on requesting the Mobile Switching Center (MSC) Visitor Location Register (VLR) address, and the IMSI. The request is part of the SMS delivery protocol, which allows the source network to receive information about the subscriber's location for further routing of the message. The initial data includes the target subscriber number.

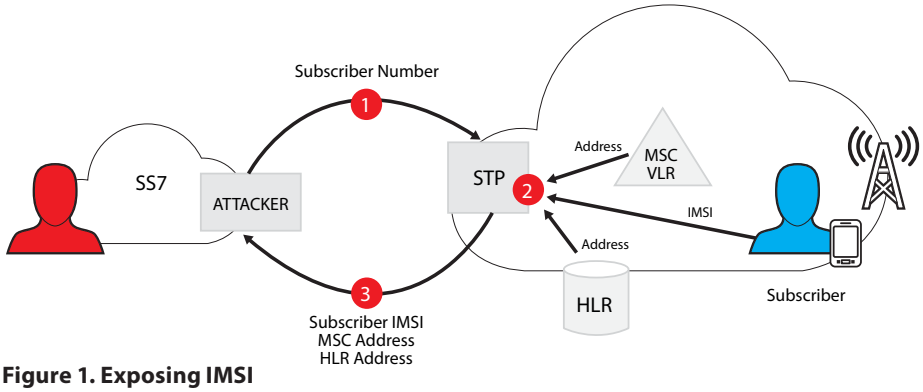


Figure 1. Exposing IMSI

Result: In case of successful exploitation, an attacker obtains the following data:

+ Subscriber's IMSI
+ Servicing MSC/VLR address
+ Home Location Register (HLR) address where the subscriber's account data is located

The MSC/VLR address will determine the subscriber's location down to the regional level. Moreover, the intruder can use the obtained data in more complex attacks (as described below).

4.2. Discovering a subscriber's location

Goal: Determine the subscriber's location

Description: This attack is based on an unauthorized request of the subscriber's location. Received data is commonly used for real-time tariffing of the subscriber's incoming calls. The initial data is the IMSI and current MSC/VLR address, which can be obtained by conducting a successful Attack 1 (section 4.1).

In cities and urban areas, the accuracy of a subscriber's location can be determined within a few hundred meters.

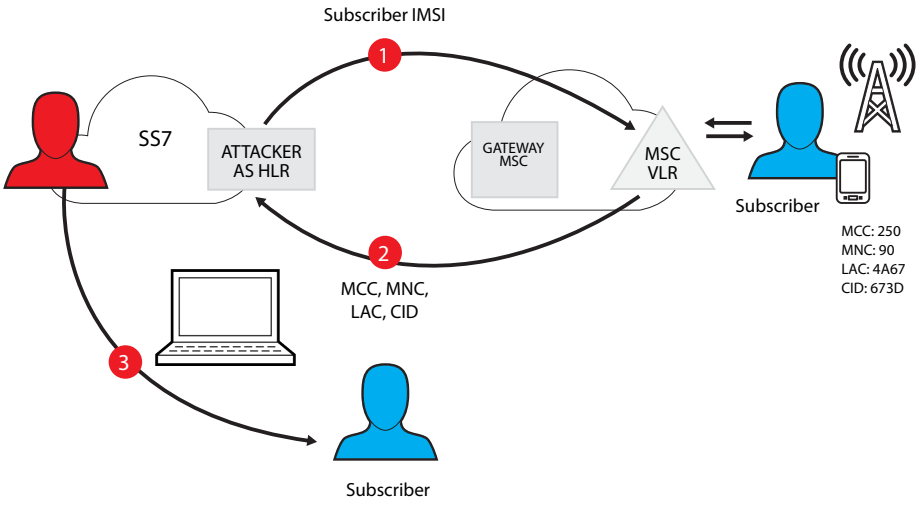


Figure 2. Determining a subscriber's location

Result: The intruder obtains the CGI, which consists of:

+ Mobile Country Code (MCC)
+ MNCMobile Network Code (MNC)
+ Location Area Code (LAC)
+ Cell Identity (CID)

There are a number of services available on the Web that allow determining a base station's location using these identifiers. In cities and urban areas, the accuracy of a subscriber's location can be determined within a few hundred meters.

4.3 Disrupting subscriber service

Goal: Block a subscriber from receiving incoming calls and text messages

Description: This attack requires registering a subscriber within a fake MSC/VLR coverage zone. A similar process happens when a subscriber is registered for roaming in a partner network. Again, the initial data used is the IMSI and current MSC/VLR address.

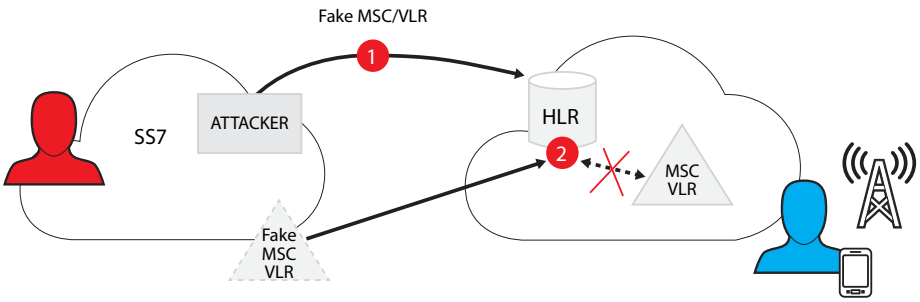


Figure 3. Blocking subscriber service

Result: Although the phone indicates connectivity to the network, the subscriber cannot receive calls or text messages. Subscriber services remain blocked until he/she travels to another MSC/VLR area, reboots the phone or makes an outgoing call.

After registering the subscriber with the fake MSC/VLR, SMS messages intended for the subscriber are instead sent to the attacker's host.

4.4. Intercepting incoming SMS messages

Goal: Intercept a subscriber's incoming SMS messages.

Description: This attack is an extension of Attack 4.3 and does not require additional actions by the attacker.

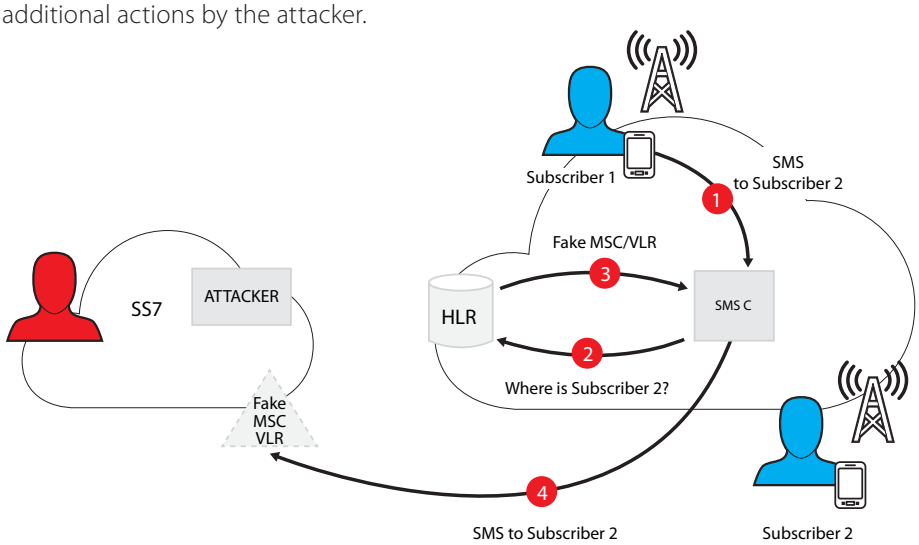


Figure 4. Intercept incoming SMS messages

Result: After registering the subscriber with the fake MSC/VLR, SMS messages intended for the subscriber are instead sent to the attacker's host.

The attacker is able to:

+ send a confirmation that the message was received (it will look to the sender as if the message was delivered)
+ re-register the subscriber to the previous switch so that he/she also gets the message.
+ send a confirmation to the sender, re-register the subscriber to the previous switch and send him/her an altered message

The attack can be used to:

+ steal one-time mobile banking passwords delivered as SMS messages
+ Intercept or recover passwords used for various internet services (email, social networks, etc.)

4.5. USSD request manipulation.

Goal: Send USSD requests directly to HLR

Description: This attack is a good example of using a legitimate message with a USSD request sent from VLR to HLR. The initial data is the target subscriber number, the HLR address and the USSD string. The subscriber number is usually known from the beginning. The HLR address can be obtained as outlined in 4.1 and USSD requests are described on the service provider's site.

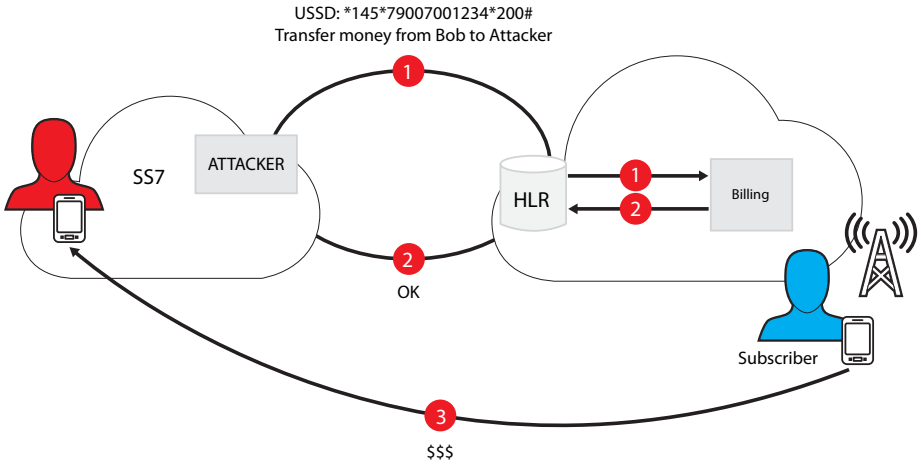


Figure 5. USSD request manipulation

Result: The most dangerous scenario related to this attack would be sending a request to transfer funds between a subscriber's accounts. Such an action might go unnoticed for quite some time, even if the service provider sends an SMS notification about the transaction. Further, to block any such notification, an attack could combine this attack with the one described in section 4.4.

4.6. Subscriber Profile Manipulation in VLR

Goal: Spoof the network with fake subscriber profile data

Description: When a subscriber registers on a switch, his/her profile is copied from the HLR database to the VLR database. The profile contains information about active and inactive subscriber services, call forwarding parameters, the on-line billing platform address, etc. An attacker can send a fake subscriber profile to the VLR.

The initial data includes the target subscriber number, the subscriber IMSI, the VLR address and the subscriber profile details. The subscriber number is usually known from the beginning. IMSI and the VLR address can be obtained as in section 4.1 and the subscriber profile details can be found as in section 4.3.

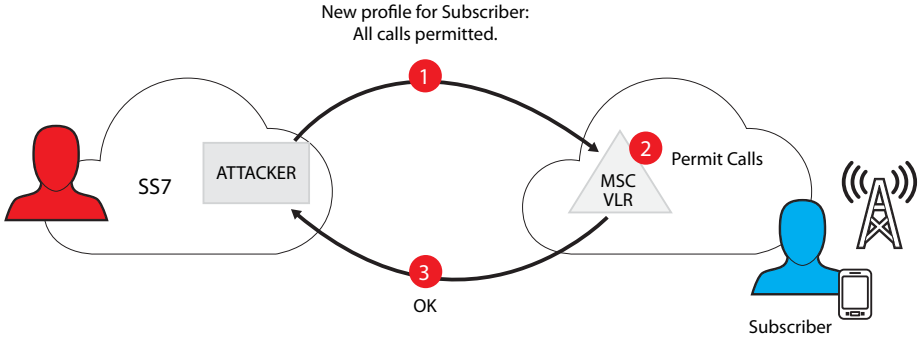


Figure 6. Subscriber profile manipulation

Result: A fake profile will fool the MSC/VLR into providing services to the subscriber based on altered and fraudulent parameters. For example, the subscriber will be able to make voice calls that bypass the billing system.

Variations: In addition, this attack scenario can be used to intercept the target subscriber's communications.

A fake profile will fool the MSC/ VLR into providing services to the subscriber based on altered and fraudulent parameters.

4.7. Intercepting outgoing calls

Goal. Redirecting outgoing subscriber voice calls and data messages to an attacker's device.

Description. This attack is an extension of Subscriber Profile Manipulation in VLR attack, described in section 4.6 above. An attacker substitutes a billing platform address with their equipment address, in the subscriber's profile. When the subscriber makes a call, the billing request along with the number of the destination subscriber are sent to the attacker's equipment. The attacker can then redirect the call and create a three-way (destination subscriber, calling subscriber and an attacker) conference call.

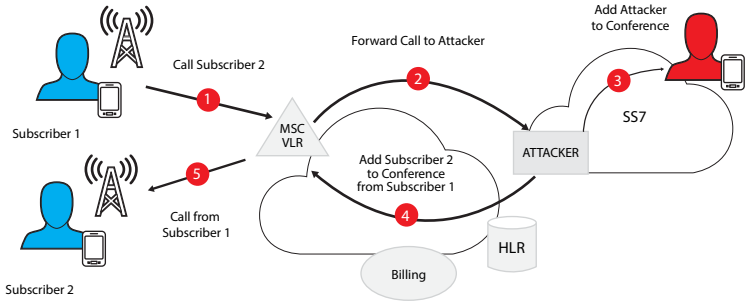


Figure 7. Interceptiing outgoing calls

Result. An attacker is able to intercept and then illegally join a voice call between two authorized subscribers.

4.8. Redirecting incoming calls

Goal: Change voice call routing and redirect incoming calls

Description: This attack is for incoming calls and is an extension of the attack described in section 4.3. When a call is terminated, the gateway MSC (GMSC) sends a request to the HLR to identify the MSC/VLR that currently serves the subscriber. This data is necessary to route the call to the appropriate switch.

After successfully performing the attack in section 4.3, the HLR will redirect the received request to a fake MSC/VLR, which in turn will send the Mobile Station Roaming Number (MSRN) to redirect the call. The HLR transfers this number to the GMSC, which redirects the call to the provided MSRN.

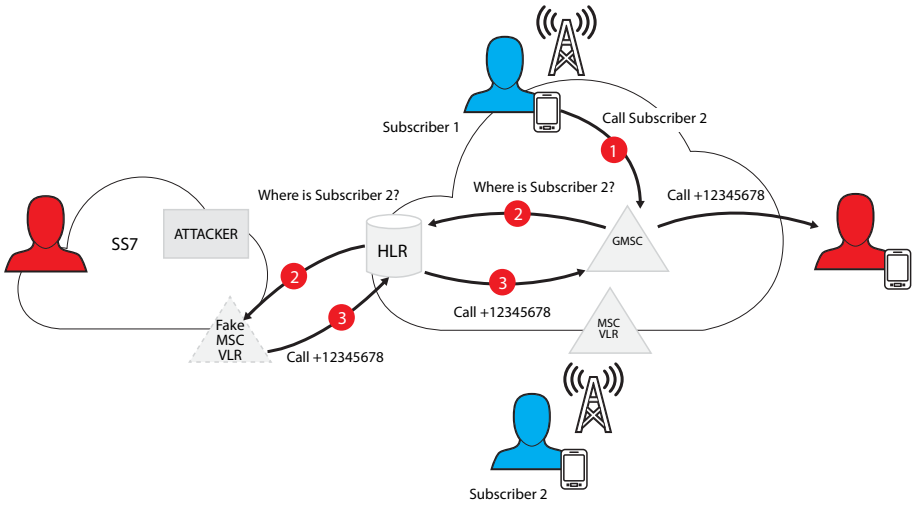


Figure 8. Redirecting incoming calls

Result: An attacker is able to redirect calls. In this particular case he/she redirects an incoming call to an arbitrary number.

Variations: This attack can be much more costly if calls are redirected to an expensive international number. An opportunistic attacker could use such a scheme to sell call traffic.

As a result of such an attack, all subscribers located in the coverage area of the affected switch will lose their calling service.

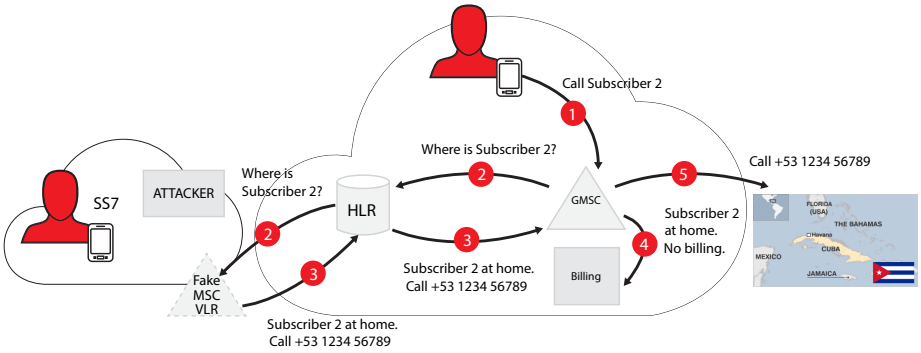


Figure 8. Redirecting incoming calls to an expensive number

4.9. MSC denial of service for incoming calls

Goal: Denial of service for incoming MSC calls

Description: This attack is based on the procedure of assigning a roaming number (MSRN) when receiving a voice call. When a call is received, the current subscriber's MSC/VLR is identified, after which a voice channel is established to this switch using a temporary roaming number. Normally, a roaming number lives for a split second. However, the default values of timers responsible for holding a roaming number, which are specified on the equipment, are 30—45 seconds. If an attacker sends numerous roaming number requests, to a switch using default parameters, then the pool of available numbers will be used up quickly. As a result, the switch will not be able to process incoming mobile calls.

The initial data includes: the IMSI of any subscriber and the switch address, which can be obtained as in section 4.1.

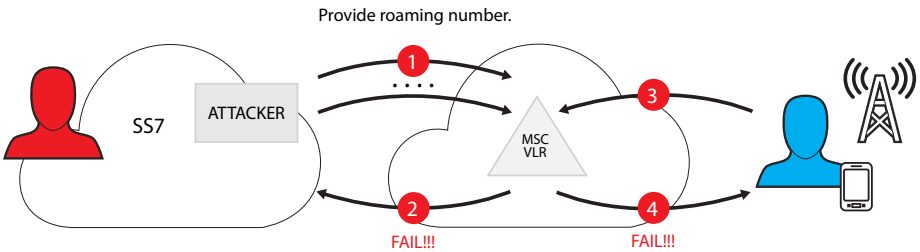


Figure 9. MSC denial of service

Result: As a result of such an attack, all subscribers located in the coverage area of the affected switch will lose their calling service.

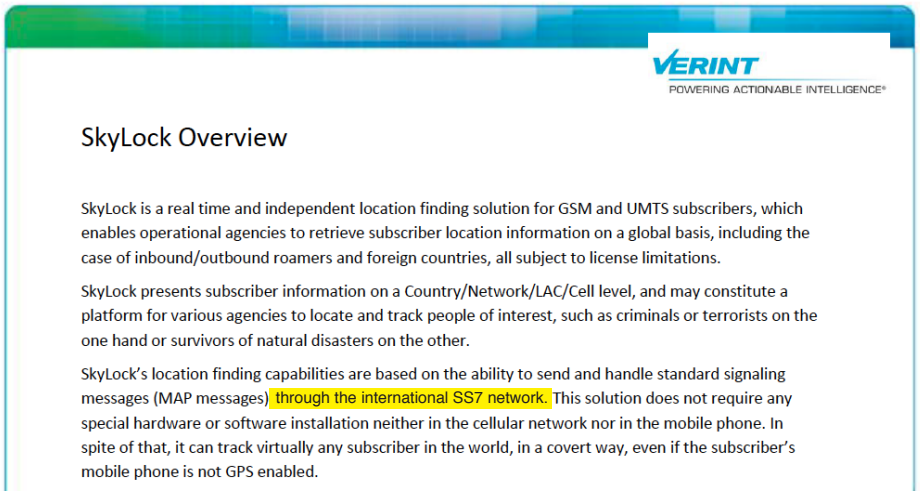
5. SS7 VULNERABILITIES ARE NOT NEW

One of the first public presentations about SS7 vulnerabilities was given in 2008 at the Chaos Computer Club Conference, in Germany. German researcher Tobias Engel showed how the location of a mobile phone could be determined [6]. However, the risks associated with SS7 vulnerabilities have long been understood. Well before Engel's demonstration, telecom engineers had warned that various attacks using SS7 were possible [2, 3, and 4]. Some governments also knew of the potential threats. For example, the book "How to Cheat at VoIP Security" by Thomas Porter and Michael Gough (2007) contains the following excerpt from an official US report about possible GSM threats:

"The risk of attack has been recognized in the USA at the highest level with the President's office indicating concern on SS7. It is understood that T1, an American group, is seriously considering the issue." [5].

For obvious reasons, providers didn't want the public to know about these associated risks. However, the issue received publicity in 2013 when former CIA specialist Edward Snowden disclosed the fact that the National Security Agency (NSA) had been exploiting SS7 vulnerabilities to spy on people [10].

Soon after, a host of private companies began offering a range of commercially available services (like the ones described) to the general public. By example, USA based Verint Systems provides a service called SkyLock for determining the location of a mobile subscriber anywhere in the world:



VERINT
POWERING ACTIONABLE INTELLIGENCE®

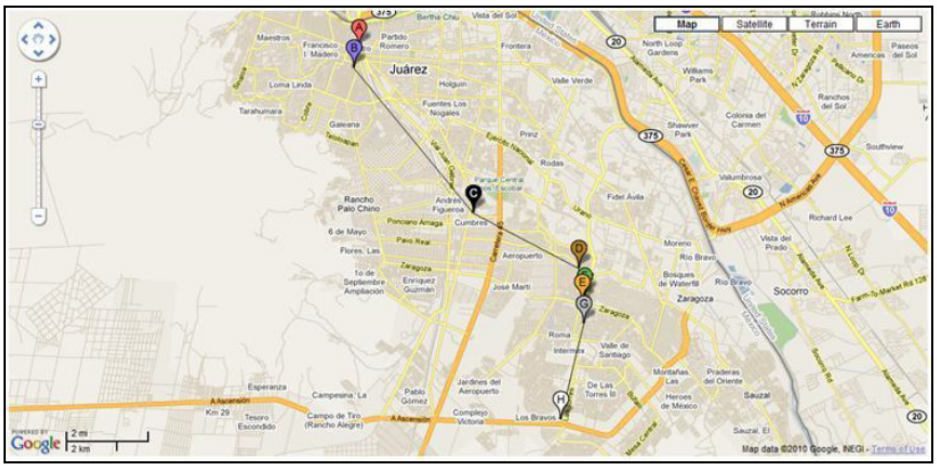
SkyLock Overview

SkyLock is a real time and independent location finding solution for GSM and UMTS subscribers, which enables operational agencies to retrieve subscriber location information on a global basis, including the case of inbound/outbound roamers and foreign countries, all subject to license limitations.

SkyLock presents subscriber information on a Country/Network/LAC/Cell level, and may constitute a platform for various agencies to locate and track people of interest, such as criminals or terrorists on the one hand or survivors of natural disasters on the other.

SkyLock's location finding capabilities are based on the ability to send and handle standard signaling messages (MAP messages) through the international SS7 network. This solution does not require any special hardware or software installation neither in the cellular network nor in the mobile phone. In spite of that, it can track virtually any subscriber in the world, in a covert way, even if the subscriber's mobile phone is not GPS enabled.

Route - Presents the route of a target, up to the last 8 queries, plotted in chronological order. This module enables tracking a target's movements over time.



Route module screen

6. CONCLUSIONS

Stealing money, determining subscriber location, tapping calls and disrupting communication services are all threats made possible by exploiting SS7 vulnerabilities.

With connections made possible by the Internet, mobile communication has become a preferred attack point for hackers looking to penetrate critical infrastructures and the enterprise.

If mobile providers do not implement protection systems against SS7-based attacks, there is little doubt that the public, private organizations or even entire nations will be among the victims of such attacks in the near future.

The combination of these products and services has already proven to be a reliable protection measure against SS7 attacks in several large telecommunications companies around the world.

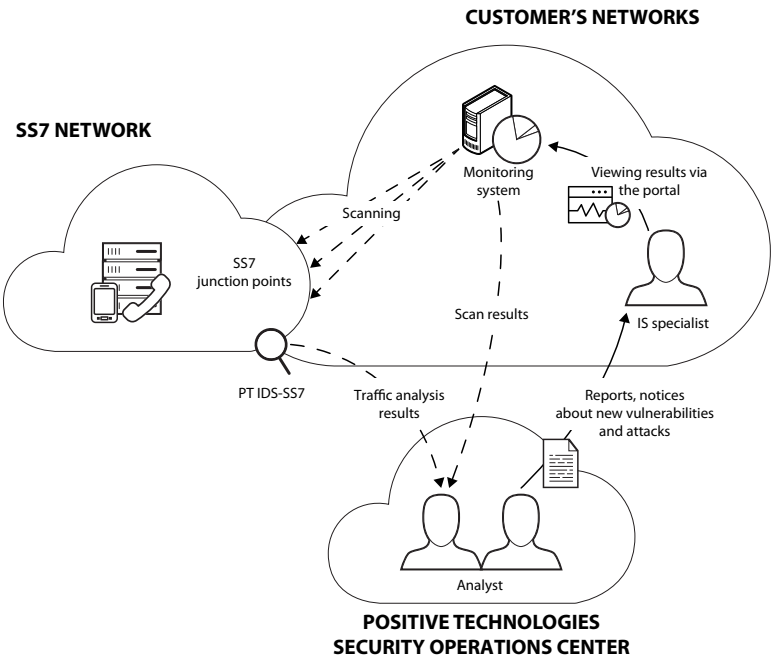
The experts at Positive Technologies offer the following recommendations for protecting SS7 networks:

+ Analyze provider hosts in the SS7 network
+ Control message filtering
+ Monitor SS7 traffic
+ Examine the potential for attacks and fraud
+ Find equipment configuration errors and vulnerabilities in protocols

In addition, Positive Technologies provides these solutions to help automate your protection:

+ **PT SS7 Scanner:** Installed on the provider's network, PT SS7 Scanner automatically controls and tracks the state of the hosts in the SS7 network. Moreover, PT SS7 Scanner detects associated vulnerabilities quickly, reducing risks related to both known and unknown threats.
+ **PT IDS-SS7:** PT IDS-SS7 assures traffic monitoring in the SS7 network's junction points, which enables the detection of attacks and fraud attempts in real time.

MaxPatrol Vulnerability and Compliance Management: MaxPatrol's combination of vulnerability detection and analysis, penetration testing, network and database scanning, system and application testing, configuration and inventory assessments and detailed compliance checks delivers the most comprehensive vulnerability and compliance management solution available.



conclusion continued

In addition to the products highlighted above, Positive Technologies offers several services for performing risk analysis, allowing you to decide whether or not to make changes in system configuration, accept risks or extend monitoring for potential attacks.

The combination of these products and services has already proven to be a reliable protection measure against SS7 attacks in several large telecommunications companies around the world.

7. REFERENCES

1. Signaling Transport (sigtran). — The Internet Society, 1999-2007.
http://datatracker.ietf.org/wg/sigtran/documents/

2. A Study of Location-Based Services. — Lennart Ostman, CellPoint Systems, 2001.
http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf

3. SMS SS7 Fraud 3.1 — GSM Association, 2003-2005.
http://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf

4. Can Active Tracking of Inroamer Location Optimise a Live GSM Network? — Katerina Dufková, Jirí Danihelka, Michal Ficek, Ivan Gregor, Jan Kouba, CTU-Ericsson-Vodafone R&D, 2007.
http://www.rdc.cz/en/publications/publications/dufkova07ss7tracker.pdf

5. How to Cheat at VoIP Security. — Thomas Porter, Michael Gough, 2007.
http://www.amazon.com/How-Cheat-at-VoIP-Security/dp/1597491691

6. Locating Mobile Phones Using Signalling System #7. — Tobias Engel, 2008.
http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf

7. Getting in the SS7 Kingdom. — Philippe Langlois, P1 Security Inc, 2010.
http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf

8. Dmitry Kurbatov. Five Nightmares for a Telecom. — Positive Hack Days, 2013.
http://www.slideshare.net/phdays/d-kurbatov-5-nightmaresfortelco

9. How to Determine a Subscriber's Location — Sergey Puzankov, Positive Technologies, 2013.
http://habrahabr.ru/company/pt/blog/191384/

10. New documents show how the NSA infers relationships based on mobile location data. — Washington Post, 2013.
http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/

11. For sale: Systems that can secretly track where cellphone users go around the globe. — Washington Post, 2014.
http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

12. MTS Subscribers under Close Surveillance Independent News Bureau, 2014.
http://www.mobile-review.com/articles/2014/image/crimea-roam/doc.pdf

13. Ukrainian Cell Phone Tapping: How It Is Done and How to Protect Yourself — Sergey Puzankov and Dmitry Kurbatov, Positive Technologies, 2014.
http://habrahabr.ru/company/pt/blog/226977/

8. ABBREVIATIONS

CGI (Cell Global Identity) is a standard identifier for a GSM network used to identify a certain cell of the Location Area.
CID (Cell ID) is an identifier of a base station.
GMSC (Gateway MSC) is an edge switch.
HLR (Home Location Register) is a register that contains data about mobile phone subscribers.
IMEI (International Mobile Equipment Identity) is an international unique mobile equipment ID.
IMSI (International Mobile Subscriber Identity) is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.
LAC stands for Local Area Code.
MAP (Mobile Application Part) is an SS7 application subsystem for mobile communication.
MCC stands for Mobile Country Code.
MNC stands for Mobile Network Code.
MSC is a Mobile Switching Center, a specialized automatic telephone system.
MSISDN (Mobile Subscriber Integrated Services Digital Number) is a number uniquely identifying a subscription in a mobile network.
MSRN stands for Mobile Station Roaming Number .
SMS (Short Message Service) is a text messaging service component of phone, Web, or mobile communication systems.
SS7 (Signaling System 7) is a common channel signaling system used for international and local phone networks all over the world.
USSD (Unstructured Supplementary Service Data) is a protocol used by GSM cellular telephones to communicate with the service provider's computers.
VLR (Visitor Location Register) is a database that contains information about subscribers roaming within the territory.

SS7REPORT_WP_A4.ENG.0036.01.DEC.28.2014