SC Telecom
Era of Private Communication

SS7 VULNERABILITY

AS A THREAT TO MOBILE NETWORKS SECURITY

Version 3.0 (2023)

Table of Contents

1 Caution: Any Subscriber is Subject to Hacking

Cellular service in the modern world is an essential means of two-way data exchange. Transfer of information through its channels is carried out in various areas of human activity and often requires compliance with an increased confidentiality.

Nevertheless, a significant number of leaks from state, municipal, commercial and non-profit organizations prove complete vulnerability of the system. Telecommunications networks are still not particularly perfect and have a number of security breaches, among which is an outdated SS7 technology.

SS7 also referred to as the Signaling System #7 or CCS-7 was introduced about 40 years ago (in 1970s) and in those years has been a breakthrough in terms of security.

For the first time ever, service commands for subscriber connection and data packet delivery were transferred via a signal sole use channel physically separated from the speaking channel, which excluded connection of unauthorized persons to it. But this situation changed with an advent of SIGTRAN specification[5] that allowed the use of IP networks to transfer messages. After that, access to unprotected protocols became possible from the outside, and the signaling network ceased to be isolated.

In 2014, having thoroughly studied and analyzed the current situation in practice, SC TELECOM specialists tried to show how easy it is to hack into a cellular network with the help of pretty unsophisticated software and came to a disappointing conclusion: SS7 has no protection from external fraudsters.

The problem requires publicity and urgent action, as numerous telecom operators keep on using this signaling system internationally, while some cases of real attacks have already been reported.

What are the consequences of such vulnerability, how these attacks can be performed and what are the ways to fight against such emerging threats? Find the answers in this paper.

2 SS7: Nervous System of a Phone Network

The first public talk about SS7 vulnerability was given in the end of 2008 after the Chaos Computer Club hackers' conference, where the German expert Tobias Engel explained about the scheme of spying on mobile network subscribers and showed how knowing only their phone number lets criminals detect and track any inhabitant of the planet[3].

However, workers of telecommunication companies, as well as some governments knew about various techniques of fraud through SS7 much earlier[6]. Thus, the U.S. Presidential Administration in the early 2000s in its report about potential GSM threats expressed serious concern about the attacks based on SS7[2], whereas mass media publication of the state level telephone negotiations in Ukraine and wiretapping cases of MTS-Ukraine subscribers triggered a wave of great scandals in the country[1].

In those days, mobile operators and regulatory authorities were not in a hurry to admit the problem. Nevertheless, after a decade has passed, it was brought up again. This was facilitated by the former CIA employee Edward Snowden, who disclosed a number of sensational revelations of U.S. special services. It was then that the signal network became identified as one of the techniques used to spy on people[4].

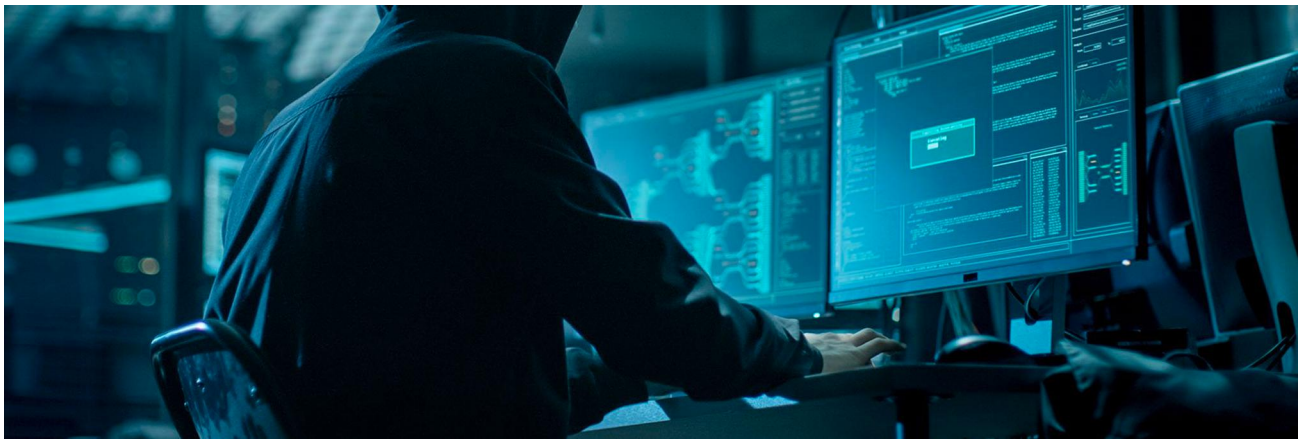
Edward Snowden

is an American computer professional,
former Central Intelligence Agency (CIA) employee,
and former contractor for the United States government

Soon, many organizations seeking to make money on this security breach began to emerge. For instance, an American company VERINT that has developed the SkyLock program not only can determine the mobile subscriber location but also track the target's movements. Its services are offered quite officially and at the global level, which means that this organization cooperates with special services of various countries.

2 SS7: Nervous System of a Phone Network

Today, a growing number of people wish to take advantage of SS7 vulnerability. According to the number of hackers' offers posted on the Internet, as well as announcements of clients looking for such performers demand on attacks via SS7 is increasing, such services become widely available and prices for them are significantly declining. So the fact of network insecurity no longer surprises anyone.



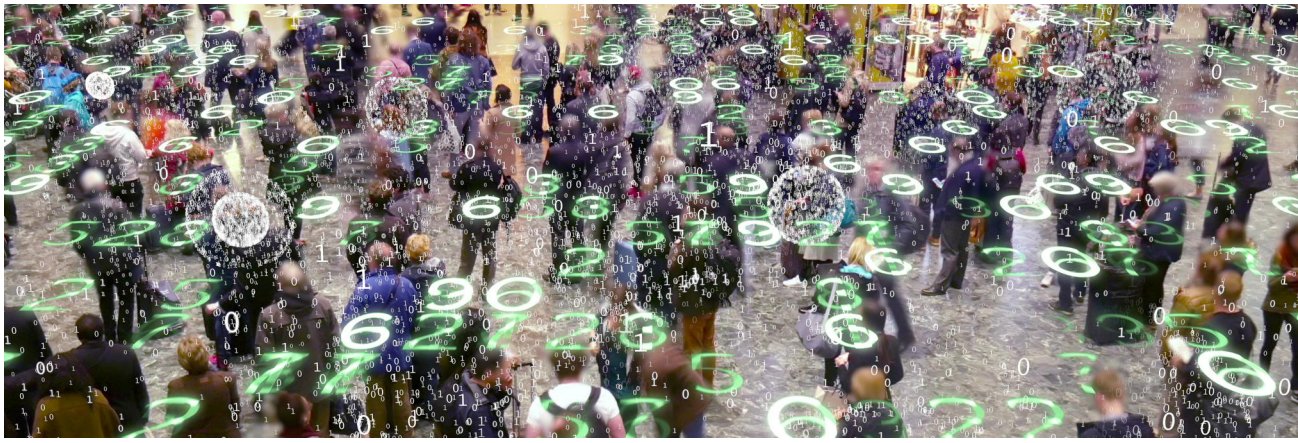
But how serious is the problem?

3 Attacks on Signaling Protocols: How and Why

In order to investigate the SS7 vulnerability, SC TELECOM made an attempt to implement probable attacks. The results showed that small companies in the field of cellular communication are poorly protected from outside intruders. However, even the largest top operators do not provide an adequate level of security for their subscribers. This means that everybody can be put at risk.

To become a victim, one should simply be a mobile subscriber: be as accessible as possible in home network and roaming, as well as regularly store and update location data.

Hackers' interaction with the victim is carried out using standardized messages from anywhere in the world. They are able to monitor telephone conversations, intercept text messages, withdraw money from subscribers' accounts, track their location, block their actions, spoof their profiles, redirect voice calls and even conduct DoS attacks.



As a result of such actions the following problems occur: leakage of personal data, transfer of confidential information to third parties and loss of funds. Manipulations with mobile communication can also cause misinformation and therefore provoke mass unrest, as well as adversely affect the enterprises management systems and negatively reflect on vital resources in society. Not only subscribers of mobile network and organizations, but also the whole country can become the target.

3 Attacks on Signaling Protocols: How and Why

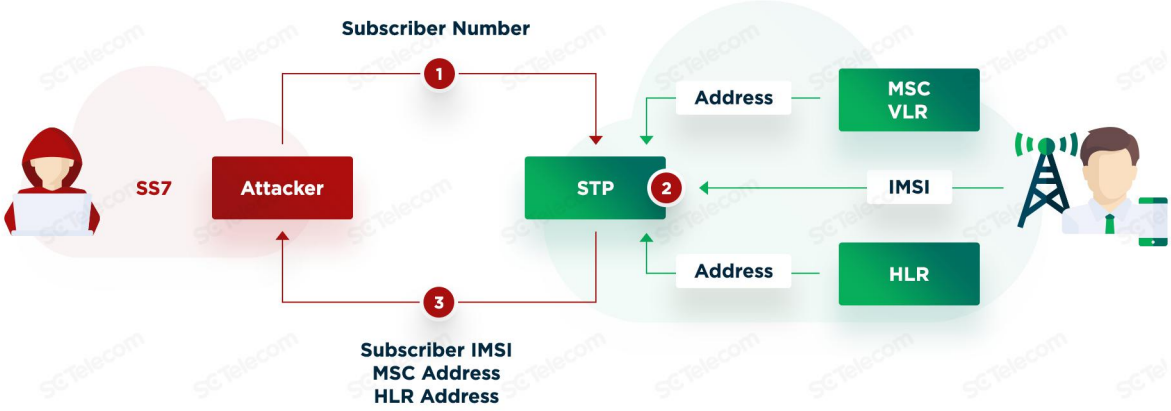
We shall notice that even a novice hacker can perform these attacks. To do this, he/she should buy a mobile operator license on the black market, or gain access to the network by hacking the edge device, or, at best, work as a technical specialist in a cellular communication company.

Telephony is more and more based on the widely used software, so a Linux-based computer and a publicly available SDK for SS7 packets generation are the only things an attacker needs. Due to the fact that the system does not check the source of packet (it is impossible to filter packets, since it is impossible to reliably establish their legitimacy), the attacker's commands are processed in the same way as legitimate ones, which allows to fully "wedge" into the process.

What is more, transition from one attack to another is interrelated. So, having performed one attack with the help of existing commands, fraudster can without any effort proceed to the next one (reproducibility of all attacks is high and complexity of their implementation is medium).

3.1. Data Acquisition

To commit an attack, hacker needs to obtain an international mobile subscriber identity (or "IMSI"). This can be done by delivering text message from external "network" emulated on the computer. In response to request, home network reports the MSC/VLR address, which helps find out whether the subscriber is at home or in roaming; and if in roaming, which network he/she is using (in order to send SMS there). At the same time transmission of IMSI occurs that is also necessary for message routing.



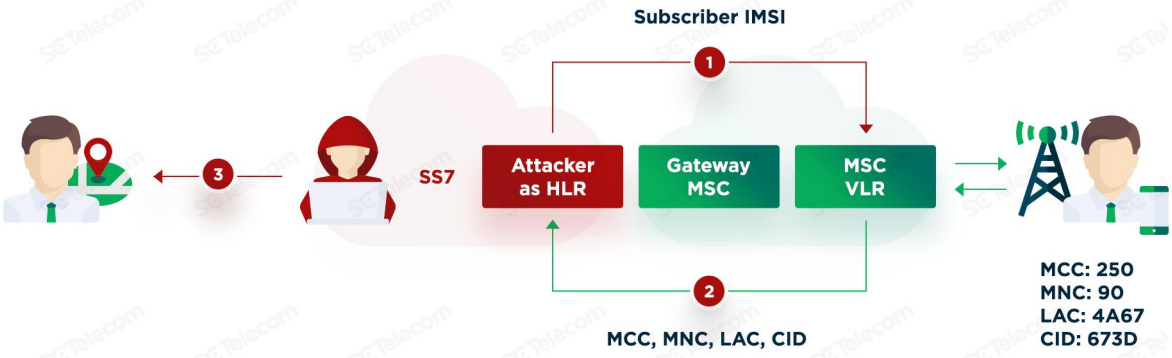
3 Attacks on Signaling Protocols: How and Why

As a result, an attacker obtains the subscriber's IMSI to control parameters of his/her "profile", HLR address where these parameters are stored, as well as the MSC/VLR address (information about what region (country) this subscriber is currently in).

3.2. Location Identification

To find out the exact location of subscriber who has a specific IMSI, an attacker can request information about which base station he/she is using and in response receive a unique CGI cell identifier that consists of four parameters:

- MCC (Mobile Country Code);
- MNC (Mobile Network Code);
- LAC (Location Area Code);
- CID (Cell Identity).

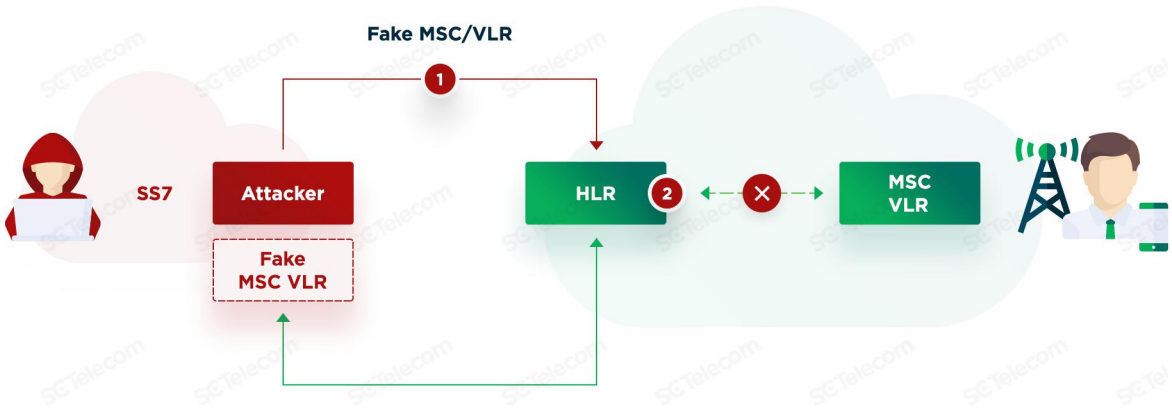


Using these parameters, the open database can to the nearest hundred meters show where the victim is currently located.

3.3. Services Lockout

To block subscriber from receiving incoming calls and text messages, fraudster can inform HLR that subscriber has registered in the roaming network and transfer there his/her IMSI jointly with a new MSC/VLR address.

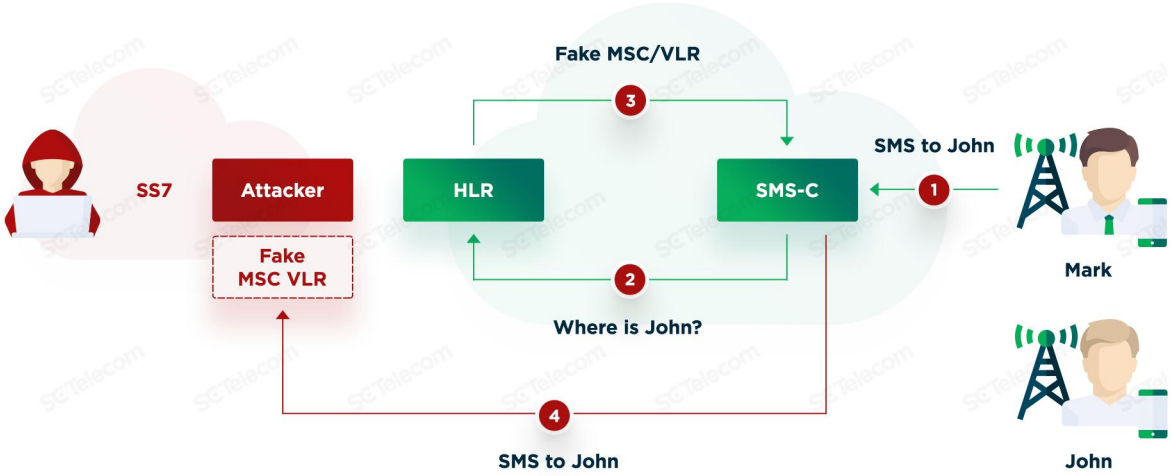
3 Attacks on Signaling Protocols: How and Why



Then home network will be redirecting requests to nowhere. At the same time, subscriber will still be in the network coverage area, but receipt of incoming calls and messages will pause until victim moves into the coverage area of another MSC/VLR, reloads his/her phone or makes an outgoing call.

3.4. SMS Interception

Interception of text messages is carried out after blocking subscriber's services. No additional actions are required for this attack.



Since SMS requests from MSC/VLR delivery of confirmation, attacker has several options:

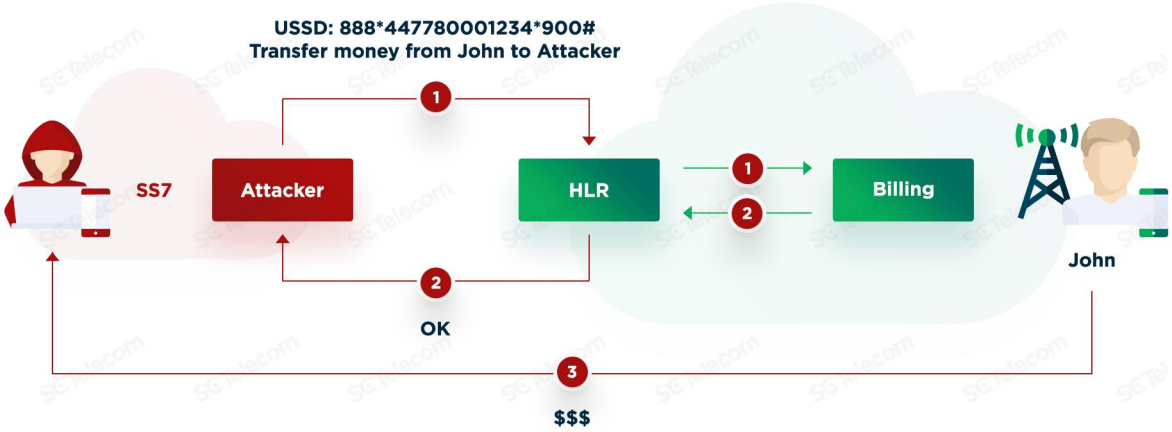
- to send to the sender confirmation on the message delivery,
- send confirmation to the sender and a modified message to subscriber, or
- do not send confirmation to the sender, intercept the message to his/her address and request to resend this message to subscriber.

3 Attacks on Signaling Protocols: How and Why

If desired, an attacker can specify his/her MSC/VLR address and start receiving the victim's traffic: read all message history or request one-time SMS passwords for authorization on various online services.

3.5. Sending USSD Requests in Subscriber's Name

USSD commands allow organizing a conversational interaction of subscriber and telecom operator in the mode of sending short messages.

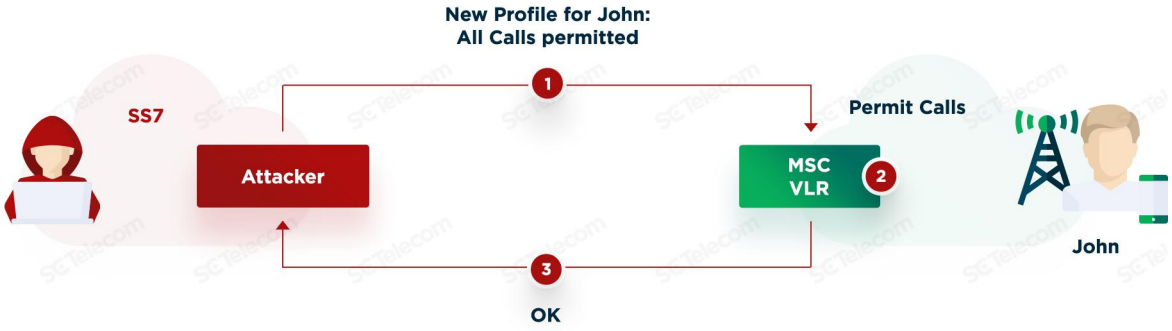


If an attacker knows MSISDN and HLR address, he/she can simulate a specific request in the form of numbers combination, asterisks and grids from VLR to HLR and as a result get access to balance management, connection of various services and tariff options. For example, by sending a request to transfer funds from one account to another, an intruder can deprive subscriber of funds on his/her phone. Intruder's activities will remain completely unnoticed provided that he/she intercepts text messages (in case if SMS authorization is need to confirm operation).

3.6. Profile Spoofing

The subscriber's profile contains information about connected services, forwarding options, address of online billing platform, etc.

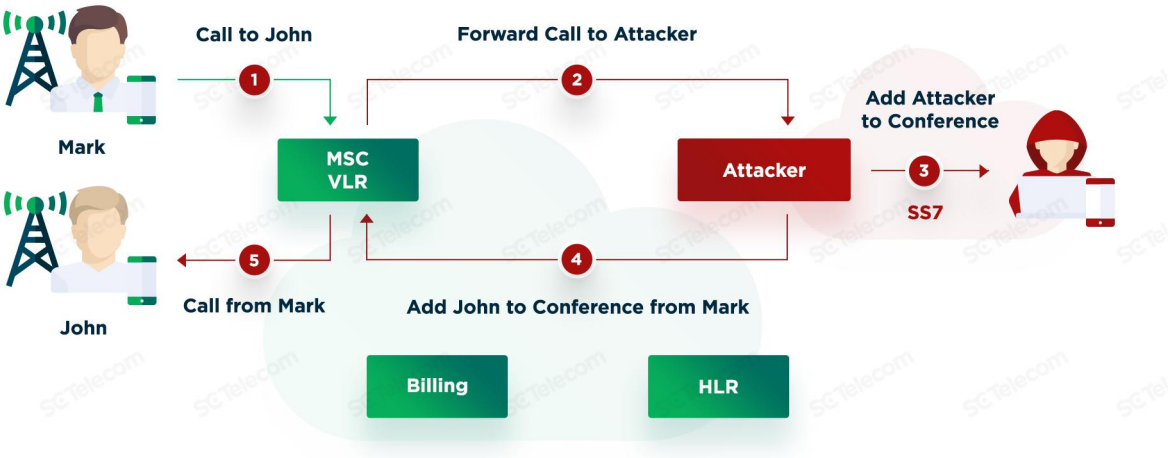
3 Attacks on Signaling Protocols: How and Why



When sending a fake subscriber profile to MSC/VLR, an attacker can force it to serve subscriber according to parameters he/she sets, e.g. make voice calls bypassing the billing system.

3.7. Wiretapping

Using profile spoofing, hacker can change address of the balance platform and specify an address of equipment that is under his/her control. Then call forwarding will go to the number of attacker, who will illegally interfere into conversation.

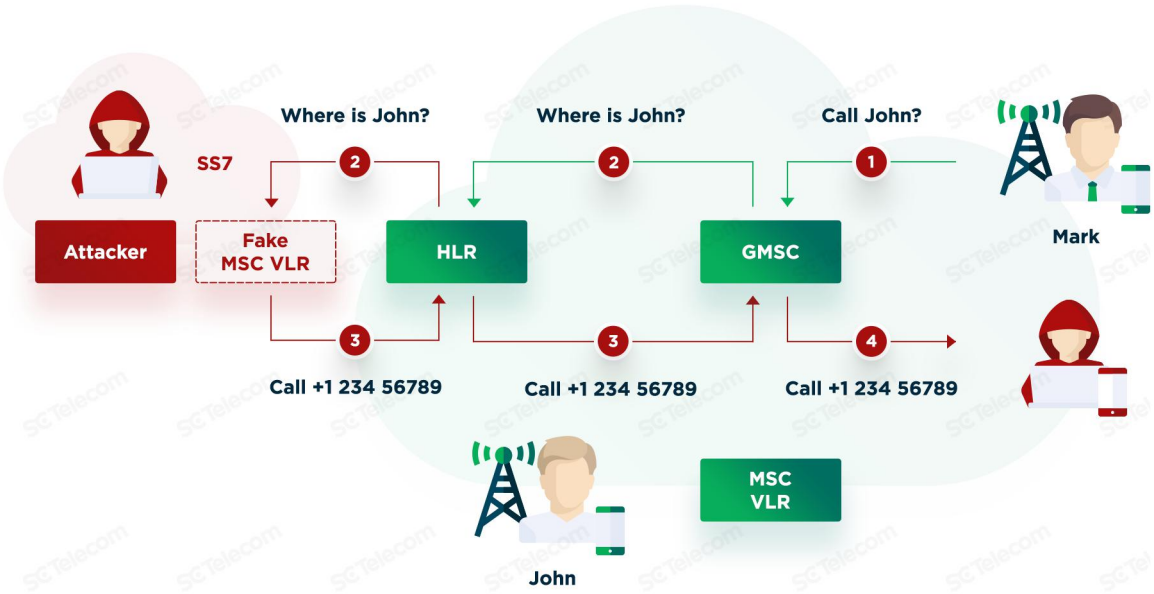


Such manipulation is carried out in a few seconds, and interlocutors do not have time to suspect that there is someone third between them.

3 Attacks on Signaling Protocols: How and Why

3.8. Redirection of Incoming Calls

Attacker has the power to influence the voice call routing mechanism by redirecting the incoming call to an arbitrary number. With an established fraud scheme, this number, for example, can serve as an expensive international route, the traffic of which is put up for sale. In this way a huge connection fee will be charged from the unsuspecting caller.

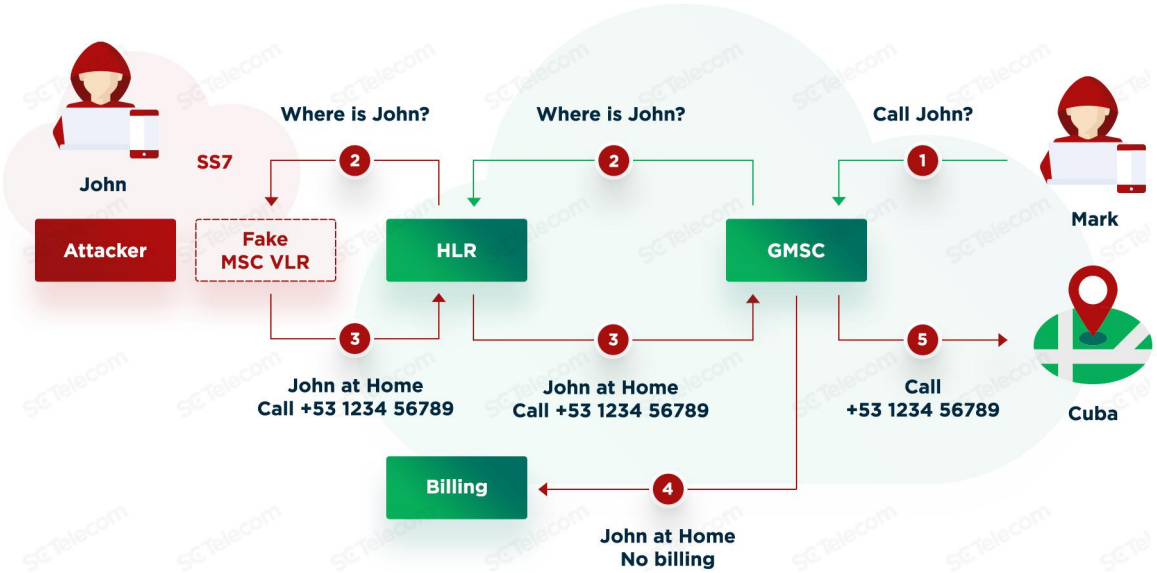


With this scheme, intruder first identifies the MSC/VLR that currently serves subscriber. Blocking his/her receipt of incoming calls and text messages, HLR forwards request to a new MSC/VLR, which in turn sends a phone number to redirect the call. Then this number is transferred by HLR to the GMSC, which redirects the call to the provided MSRN.

3.9. DoS Attacks on Switch

Finally, with the help of SS7 attacker can launch a serious attack on the switch that will make it impossible for subscribers in their service area to receive incoming calls.

3 Attacks on Signaling Protocols: How and Why



When registering in VLR, a temporary roaming number is usually allocated. If subscribers massively send requests for allocation of such numbers, their pool will quickly end, and no one will be able to reach “real” subscribers due to the switch overload.

From the foregoing, it becomes obvious that cellular operators are subject to various vulnerabilities, which can be easily exploited by an external intruder.

So, how to protect against such attacks?

4 Security Tools against Attacks are Real

Competent measures to prevent and resolve the existing problem should have an integrated approach. The analysis on possibility of attacks implementation should be hold, risk assessments should be made, errors in equipment configuration should be found, node inventory and traffic monitoring should be performed, as well as message filtering should be checked.

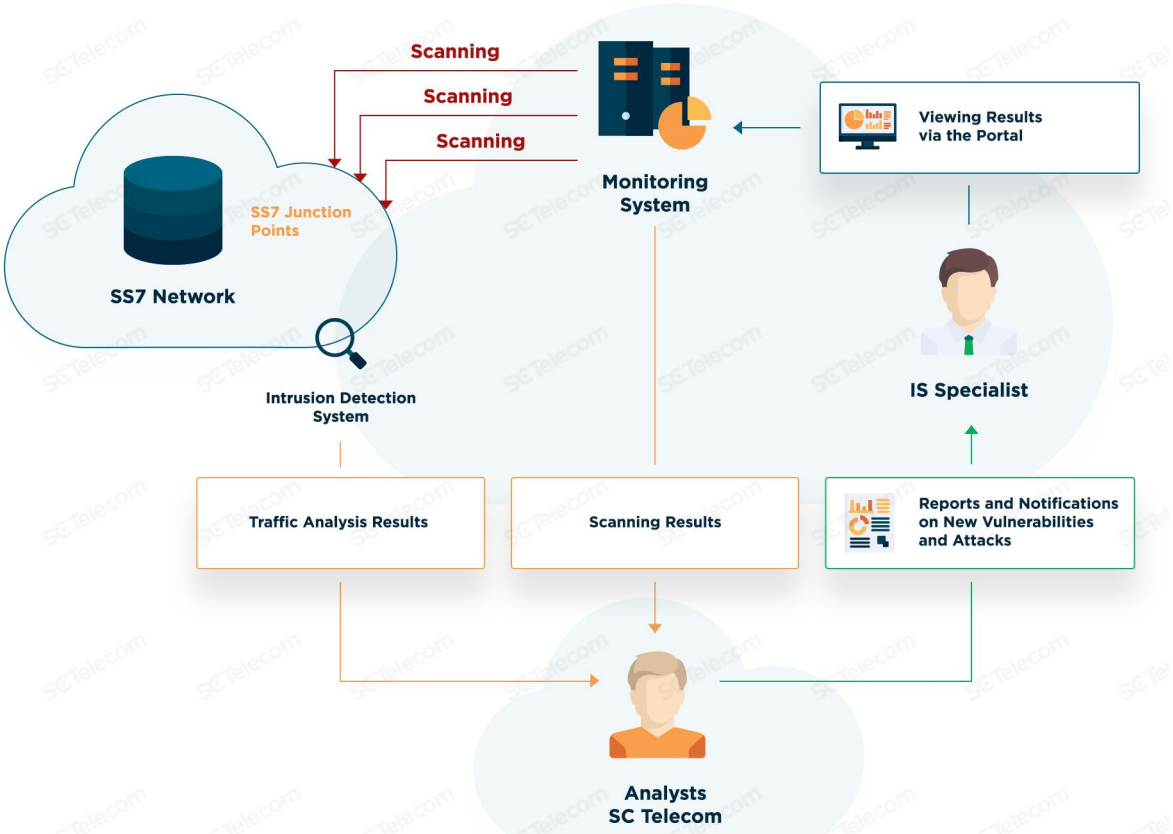
In particular, we use the following security methods for our members:

- **anonymous subscriber connection;**
- **MSISDN and IMSI hiding;**
- **installation of unique firmware on SIM cards;**
- **random routing of voice traffic;**
- **possibility to replace outgoing numbers and change voice;**
- **ban of geodata transfer;**
- **lack of billing;**
- **calls within the group;**
- **virtual incoming numbers;**
- **secure Internet.**

Our software constantly scans for vulnerabilities and compares them with a regularly updated database. By monitoring traffic at the SS7 junctions, we identify attacks and technological fraud, thereby monitor network security and look for errors related to equipment configuration.

With the use of methods and systems mentioned above, we are able to reliably protect conversations of members.

4 Security Tools against Attacks are Real



Our team has proved itself to good advantage both in Russia and abroad. We successfully combat vulnerabilities, promptly eliminate existing threats and provide reliable communications in GSM and VoIP networks.

References

[1] MTS Subscribers under Close Surveillance. – Independent News Bureau, 2014.

https://www.mobile-review.com/articles/2014/image/crimea-roam/doc.pdf

[2] How to Cheat at VoIP Security. – Thomas Porter, Michael Gough, 2007.

https://www.amazon.com/How-cheat-at-voip-security/dp/1597491691

[3] Locating Mobile Phones using Signalling System #7. - Tobias Engel, 2008.

http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf

[4] New documents show how the NSA infers relationships based on mobile location data. – Washington Post, 2013.

https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?noredirect=on&utm_term=.64c625aa1093

[5] Signaling Transport (sigtran). – The Internet Society, 1999-2007.

https://datatracker.ietf.org/wg/sigtran/documents/

[6] SMS SS7 Fraud 3.1 – GSM Association, 2003-2005.

https://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf

Terms and Definitions

CGI (Cell Global Identity) is a global identifier for mobile phones cells

CID (Cell ID) is an identifier for mobile phones cells

GMSC (Gateway MSC) is an edge switch

HLR (Home Location Register) is a database that contains data about mobile phone subscribers

IMSI (International Mobile Subscriber Identity) is an internationally standardized unique number to identify a mobile subscriber

LAC (Local Area Code) is a unique number of current location area

MCC (Mobile Country Code) is a code of the country where the base station is located

MNC (Mobile Network Code) is a code of mobile network

MSC (Mobile Switching Center) is a specialized automatic telephone exchange

MSISDN (Mobile Subscriber Integrated Services Digital Number) is a number uniquely identifying a subscription in a GSM or a UMTS mobile network

MSRN (Mobile Station Roaming Number) is a roaming number of mobile station

SS7 (Signaling System 7) is a Signaling System #7 or CCS-7 (Common Channel Signaling System 7)

VLR (Visitor Location Register) is a database that contains information about subscriber's roaming within the territory

SC Telecom

Era of Private Communication