**SS7 PROTOCOL HACK REVEALED – HOW HACKER CAN ACCESS YOUR CALLS AND TEXTS**

* October 4, 2016
* Posted by: CyberFrat
* Category: [Blogs](https://cyberfrat.com/category/blogs/)

[1 Comment](https://cyberfrat.com/ss7-protocol-hack/#comments)



The Signaling System No 7 (SS7), also known as Common Channel Signaling System 7 (CCSS7) or Common Channel Interoffice Signaling 7 (CCIS7), is a set of protocols developed in 1975 that allows the connections of one mobile phone network to another. The information passed from a network to another are needed for routing calls and text messages between several networks.  
The SS7 performs out-of-band signaling in support of the call establishment, billing, routing, and information exchange functions of the public switched telephone network (PSTN).  
When users access a PSTN, he constantly exchanges signaling with network elements, for example, signaling information are exchanged between a mobile user and the telephone network.  
Information includes dialing digits, providing dial tone, sending a call-waiting tone, accessing a voice mailbox, etc.  
The term Out-of-band signaling is used to specify that signaling that does not take place over the same path as the conversation. The digital channel used for the exchange of a signaling information is called signaling link, when a call is placed, the dialed digits, trunk selected, and other information is sent between switches using their signaling links, rather than the trunks used to carry the conversation.  
Out-of-band signaling has the following advantages:  
• It allows for the transport of more data at higher.  
• It allows for signaling at any time in the entire duration of the conversation, not only at the beginning of the call.  
• It enables signaling to network elements to which there is no direct trunk connection.

The SS7 is also used to implement the network roaming when users need to use different network providers.  
A hacker accessing the SS7 system can snoop target users, locate them, and transparently forward calls.  
The access to the SS7 system is possible by using any number of networks.  
In response to the disclosure of security issues related to the SS7 protocol, telco bodies, and operators, including the GSMA, have introduced monitoring services to prevent intrusions or abuse.  
Recently a group of hackers demonstrated how spy on mobile users simply using their phone numbers; they have chosen as a target complacent US Congressman.  
The group is led by the popular German security expert Karsten Nohl; the researchers demonstrated they were able to eavesdrop and geographic track the politician just knowing his phone number.  
There is nothing new in the revelation because the telco community was aware of the technique adopted by security experts, the same team illustrated in the past the technique that exploits security flaws in the Signalling System No. 7, also known as an SS7 protocol.  
An attacker can exploit security issued in the SS7 protocol to spy on private phone calls, record them and monitor target’s movements.  
Exactly one year ago, Channel Nine’s 60 Minutes reported the existence of a security hole in modern telecommunication systems that could be exploited by cybercriminals to listen in on phone conversations and read text messages.  
Karsten Nohl and his team investigated the presence of security flaws in the SS7 system back in 2014.  
In that occasion, Nohl and his colleagues were able to intercept data and geo-track every mobile user by exploiting a flaw in the SS7 signaling system.

https://youtube.com/watch?v=GeCkO0fWWqc

In December 2014, a group of German researchers at the Chaos Communication Hacker Congress revealed the existence of serious security issues in the protocol used by a large number of carriers of mobile telephony. Despite the huge investment in security made by telco companies, the adoption of flawed protocols exposes customers to serious privacy and security risks.  
“It’s like you secure the front door of the house, but the back door is wide open,” said Tobias Engel, one of the German researchers.

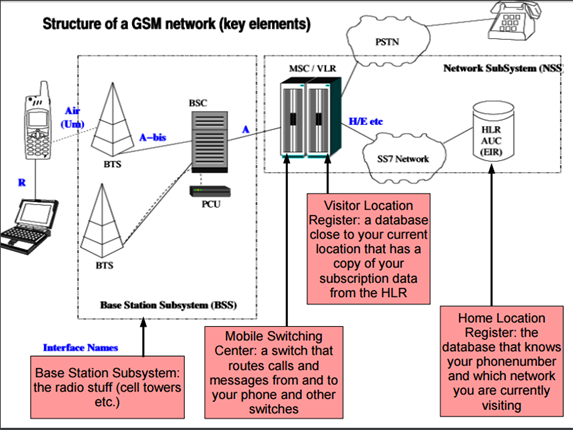


Figure 1 – Tobias Engel Slides presented at CCC Berlin

What does the network know about your location?  
Tobias explained that the network knows the location of the cell tower that could be used to have a pretty good approximation of a user’s location. Despite the access to the information managed by operators is restricted to the technical operation of the network, voice calls, and short messages can be initiated to your phone number from almost anywhere in the global SS7 network.

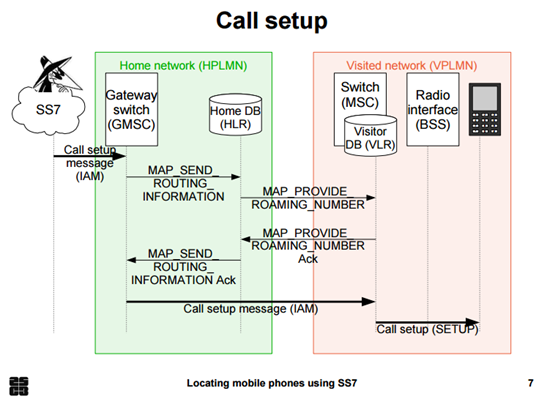


Figure 2 – Tobias Engel Slides presented at CCC Berlin

Below the presentation made by the expert Tobias Engel:

https://youtube.com/watch?v=lQ0I5tl0YLY

Attacks relying on these security issues already happened in the past, one of the major incidents was registered by the NKRZI (which is the National Commission for the State Regulation of Communications and Informatization in Ukraine) and involved Russian addresses back in April 2014.  
The expert noticed that many Ukrainian mobile phone holders have been targeted by SS7 packets sent from Russia to track them and steal information from the mobile devices.  
According to the security firm AdaptiveMobile who analyzed the case, a number of Ukrainian mobile subscribers “were affected by suspicious/custom SS7 packets from telecom network elements with Russian addresses over a three day period in April 2014. The packets were revealing the subscribers location and potentially the contents of their phone calls to be obtained.”  
A series of SS7 packets were sent to the MTS Ukraine’s SS7 network that caused the modification of the control information stored in network switches for several MTS Ukraine mobile users. The effect was that one of the affected MTS used tried to call someone else, their call would be forwarded to a physical land line number in St. Petersburg, Russia allowing the interception of the communication.  
“In the document, the investigation stated that the custom SS7 packets themselves came from links allocated to MTS Russia, the parent company of MTS Ukraine. The Ukrainian regulator then assigned responsibility for the nodes that generated the SS7 based on the origination addresses in the SS7 packets received. According to the report, some of the SS7 source addresses that originated the attack were assigned to MTS Russia, while others were assigned to Rostov Cellular Communications.” stated the AdaptiveMobile.  
The incident was not isolated, other cases were observed in different countries, let’s consider for example that the same protocol is being used by major Australian providers, this means that Aussies data could be exposed to hackers. Names, addresses, bank account details and medical data stolen due to a security vulnerability that could give hackers the access to their mobile devices.  
Another case was reported by the Guardian that revealed security tests conducted by an operator in Luxembourg took Norway’s largest network operator Norway offline for over three hours due to an “unexpected external SS7 event.”  
A preliminary report issued by Telenor states the problem was caused by the reception of “unusual signaling” from another international operator into their networks. Software from Ericsson misinterpreted this very rare signaling messages stopping parts of mobile traffic up.  
Ericsson identified how the misperception of signaling occurred and applied the necessary correction to fix the issue.  
The reality is that old and insecure protocols could harm our privacy dramatically enlarging our surface of attack.