SS7 flaw allows hackers to spy on every conversation

August 18, 2015 By Pierluigi Paganini

http://securityaffairs.co/wordpress/39409/cyber-crime/ss7-flaw-surveillance.html

My Page

By Exploiting a flaw in the SS7 protocol hackers can access every conversation and text message mobile users send from everywhere in the world.

Hackers can spy on every mobile phone user wherever it is.

Channel Nine's 60 Minutes has revealed the existence of a security hole in modern telecommunication systems that could be exploited by cyber criminals to listen in on phone conversations and read text messages.

The program explained that German hackers, who are based in Berlin, were able to intercept data and geo-track every mobile user by exploiting a flaw in the SS7 signalling system.

SS7 is a set of protocols used in telecommunications ever since the late 1970s, enabling smooth transportation of data without any breaches.

The security issue in the SS7 signalling system could be exploited by criminals, terrorists and intelligence agencies to spy on

communications. The SS7 protocol allows cell phone carriers to collect location data related to the user's device from cell phone towers and share it with other carriers, this means that exploiting the SS7 a carrier is able to discover the position of its customer everywhere he is.

"The flaws, to be reported at a hacker conference in Hamburg this month, are the latest evidence of widespread insecurity on SS7, the global network that allows the world's cellular carriers to route calls, texts and other services to each other. Experts say it's increasingly clear that SS7, first designed in the 1980s, is riddled with serious vulnerabilities that undermine the privacy of the world's billions of cellular customers.

The flaws discovered by the German researchers are actually functions built into SS7 for other purposes – such as keeping calls connected as users speed down highways, switching from cell tower to cell tower – that hackers can repurpose for surveillance because of the lax security on the network." reports The Washington Post.

In the hacking community is known the existence of several techniques that hackers and snoopers can make use of, in order to eavesdrop and intercept phone calls or written text messages. In December 2014, German researchers have placed the matter to the public for consideration at the Chaos Communication Hacker Congress, since there can be a great many problems emerging.

Carriers of mobile telephony spend large amounts of money towards expanding their network and securing the conditions of communication with 3G and high-end encryption. To quote Tobias Engel, one of the German researchers mentioned above,

"It's like you secure the front door of the house, but the back door is wide open".

One of the major incidents registered by NKRZI (which is the National Commission for the State Regulation of Communications and Informatization in Ukraine) involved Russian addresses back in April 2014.

The expert noticed that many Ukrainian holders of mobile phones have been affected by notorious SS7 packets that possibly derived from Russia. As a result, the mobile phone holders were intercepted of their address details and everything that was stored inside each phone. MTS Ukraine obviously participated in the interception, in relation to MTS Russia.

As a direct consequence of security breaches related to SS7 protocols of telecommunication, the eminent threat is none other than the surveillance taking place between different countries.

The system 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.

“Everything about our lives is contained in the palm of our hand,'” reporter Ross Coulthart said. ‘Your sensitive, private data is opened for anyone to see. You could be bugged, tracked and hacked from anywhere in the world. It’s long been the dirty little secret of international espionage. What it means is that your smartphone is an open book.”

In the TV show, Mr Coulthart was speaking from Germany with the Independent senator Nick Xenophon who was located at the Parliament House in Canberra at the time of phone call.

With the support of the German hacker Luca Melette, Mr Coulthart demonstrated how to track its interlocutor by exploiting the security issue into the SS7.

"What if I could tell you *senator, that it's possible to listen* in to *any mobile phone from anywhere in the world – would you believe me?'" Mr Coulthart* asked to *Mr Xenophon while* Melette *was* listening *the conversation.*

"I find it very hard to believe." replied the incredulous Mr Xenophon.

Mr Coulhart then asked the senator for consent to record the phone call.

"But if you reckon they can pull it off, I give my consent but I find this incredibly hard to believe." responded Mr Xenophon.

The reporter also anticipated to Mr Xenophon hat the hackers could intercept his text messages, but once again he skeptical immediately sent the following text message:

"Hi Ross, I don't believe you!! Nick."

The senator was shocked by the live demo provided by the reporter and the hacker.

"This is actually quite shocking because this affects every Australia," Mr *Xenophon said. "It means anyone with a mobile phone can be hacked, can be bugged – it's just chilling. This is the end of anyone's privacy as we know it." 'This is not about spies or terrorists and pollies – this is about every Australian that is vulnerable because their phones can be hacked."*

The attack scenario is worrying and open the door to massive surveillance activities, months ago the American Civil Liberties Union (ACLU) has also warned people against possible abuse of such vulnerabilities by Intelligence agencies and Law enforcement.

"Don't use the telephone service provided by the phone company for voice. The voice channel they offer is not secure," principle technologist Christopher Soghoian told Gizmodo. *"If you want to make phone calls to loved ones or colleagues and you want them to be secure, use third-party tools. You can use FaceTime, which is built into any iPhone, or Signal, which you can download from the app store. These allow you to have secure communication on an insecure channel."*

Unfortunately, the vulnerabilities into SS7 protocol will continue to be present, even as cellular carriers upgrade to advanced 3G technology to avoid eavesdropping.

http://securityaffairs.co/wordpress/39409/cyber-crime/ss7-flaw-surveillance.html

New security flaws in the SS7 protocol allow hackers to spy on phone users

December 19, 2014 By Pierluigi Paganini

http://securityaffairs.co/wordpress/31262/hacking/flaws-ss7-protocol-spy-on-phone.html

My Page

German researchers have announced the discovery of news security flaws in SS7 protocol that could be exploited by an attacker to spy on private phone calls.

A team of German researchers has discovered security flaws that be exploited by a threat actor to spy on private phone calls and intercept text

messages on a large scale, even when the mobile cellphone are using the most advanced encryption now available.

The flaws will be reported at the next hacker conference in Hamburg, and once again the attackers will exploit insecurity in the SS7 protocol, also known as Signaling System Number 7, that is the protocol suite used by several telecommunications operators to communicate with one another with directing calls, texts and Internet data.

The researchers also explained that the flaws in the SS7 protocol could be also exploited by criminal crews to defraud users and cellular carriers.

"The flaws, to be reported at a hacker conference in Hamburg this month, are the latest evidence of widespread insecurity on SS7, the global network that allows the world's cellular carriers to route calls, texts and other services to each other. Experts say it's increasingly clear that SS7, first designed in the 1980s, is riddled with serious vulnerabilities that undermine the privacy of the world's billions of cellular customers.

The flaws discovered by the German researchers are actually functions built into SS7 for other purposes – such as keeping calls connected as users speed down highways, switching from cell tower to cell tower – that hackers can repurpose for

surveillance because of the lax security on the network." reports The Washington Post.

The SS7 protocol allows cell phone carriers to collect location data related to the user's device from cell phone towers and share it with other carriers, this means that exploiting the SS7 a carrier is able to discover the position of its customer everywhere he is.

In a previous post, I explained that surveillance vendors using the SS7 protocol are able to geo-localize users with great precision.

"The tracking technology takes advantage of the lax security of SS7, a global network that cellular carriers use to communicate with one another when directing calls, texts and Internet data." reports the Washington Post.

As explained by the researchers, the problem resides in the intrinsic security of the Protocol that is considered outdated due to the presence of several serious security vulnerabilities which can lead to the violation of the privacy for billions of mobile users worldwide.

In time I'm writing, the researchers haven't provided other information on the security vulnerabilities discovered in the SS7 protocol, but the experts believe that hackers can exploit them to track an individual or redirect user calls to the attackers.

The attack scenario is worrying and open the door to massive surveillance activities, The American Civil Liberties Union (ACLU) has also warned people against possible abuse of such vulnerabilities by Intelligence agencies and Law enforcement.

"Don't use the telephone service provided by the phone company for voice. The voice channel they offer is not secure," principle technologist Christopher Soghoian told Gizmodo. *"If you want to make phone calls to loved ones or colleagues and you want them to be secure, use third-party tools. You can use FaceTime, which is built into any iPhone, or Signal, which you can download from the app store. These allow you to have secure communication on an insecure channel."*

Unfortunately, the vulnerabilities into SS7 protocol will continue to be present, even as cellular carriers upgrade to advanced 3G technology to avoid eavesdropping.

"But even as individual carriers harden their systems, they still must communicate with each other over SS7, leaving them open to any of thousands of companies worldwide with access to the network. That means that a single carrier in Congo or Kazakhstan, for example, could be used to hack into cellular networks in the United States, Europe or anywhere else." states the Washington Post

"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.

The team of researchers did not find evidence that the flaws discovered have been "marketed" to governments on a widespread basis, anyway it is impossible to understand is intelligence agencies are already exploiting them for their operations.

"Many of the big intelligence agencies probably have teams that do nothing but SS7 research and exploitation. They've likely sat on these things and quietly exploited them," Soghoian said.

Stay Tuned for further information …

http://securityaffairs.co/wordpress/31262/hacking/flaws-ss7-protocol-spy-on-phone.html