29.09.2015

XURA

Digital Communications

Exploring SS7 signaling fraud that threatens mobile network security and subscriber privacy

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Mobile communications is a prime target for hackers who desire to penetrate critical infrastructures and businesses

Growing concern over escalating misuse

Signaling System 7 (SS7) is a telecom network technology widely used by cellular companies to enable mobile subscribers to communicate with anyone, anywhere. SS7 provides the operator the ability to manage communications as well as bill subscribers for services provided. Capabilities provided include call setup and network registration, among other vital functions. Because each network component in the core network uses SS7 to interface with other network components any vulnerability related to SS7 protocol severely threatens the trust and privacy of subscribers. Although designed for use as a 'trusted network', the fact is that the network is not as secure as was earlier believed. Given that there are more users of the SS7 network worldwide than there are of the Internet, concern about SS7 security by operators and subscribers alike is widespread, serious, and to be treated with utmost importance.

As early as 2008, SS7 vulnerabilities were openly discussed in public at the Chaos Computer Club Conference in Germany. A German researcher demonstrated how the location of a mobile phone could be determined. Prior to that, we now know that Telecom engineers warned of possible risks. Even government officials of the highest level were aware of the threat and voiced concern. However, it was not until 2013 that the issue received widespread publicity when it became known that a government security agency had exploited SS7 vulnerabilities for spying purposes.

As recent incidents have revealed, unauthorised access to the network is not only possible, but much easier than once known. Unfortunately, this access is coupled with a lack of end-to-end authentication leaving networks vulnerable to fraud and misuse shaking consumer trust in the operator's ability to provide privacy and prevent fraud. Loopholes in the SS7 protocol have been used to steal money, listen in on conversations, monitor messages, determine a subscriber's location, manipulate network and subscriber data, and generally disrupt services.

As potential threats to the SS7 network are increasingly coming from many sources including national security agencies, fraudsters, and hackers with ill intent, it is clear that subscribers, regulators, and operators face increasing pressure to protect subscriber privacy.

Working within operator parameters

In the past, it was difficult to obtain SS7 access via an unauthorised remote host. 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 unauthorised host. Today, the process of placing voice calls in modern mobile networks is still based on that same SS7 technology which dates back to the 1970s. New signaling transport protocols known as SIGTRAN, however, are now deployed which allow SS7 to run over IP. The ultimate goal of SIGTRAN was to move from converged TDM / IP network to an all-IP network to take advantage of bandwidth, redundancy, reliability and access to IP-based functions and applications. Yet, moving onto IP has unfortunately provided a new points of vulnerability. In addition, the newly deployed 4G networks use the same concept of all-IP network and have adopted Diameter as the signaling protocol that runs over IP. The technological concept though, for providing end-user services within the evolved packet cores (EPCs) enables similar procedures as in SS7-based networks.

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Exposing subscriber and operator SS7 vulnerabilities

Signaling is the central nervous system of the mobile operator's network with mission-critical real-time data on subscriber identity, status, location, technology and servicing network elements. This enables the authentication of subscribers and their devices, performs call setups, authorises charging, enforces data policies, manages quality of service, and enacts roaming or interconnection agreements. Gaining access to this information and using it for commercial purposes in acceptable ways can be very valuable in the right hands. Or, it can be very risky if used by the wrong people in unacceptable ways.

Someone with the right technical skill and malicious intent can now exploit the mobile network and its subscribers. Attackers with the right expertise build nodes to emulate network elements while acting within a mobile network or on behalf of it. Simulated elements range from Base Transceiver Stations (BTSs) to Mobile Switching Centres (MSCs), Gateway GPRS Support Nodes (GGSNs), to Short Messaging Service Centres (SMSCs). While location data, for example, is used by the operator to perform certain functions which are legitimate and acceptable (think of mobile banking services), the IP as transport layer was not designed to detect acceptable versus unacceptable traffic. As example, there are number of entry points in a SS7 network exposed at various levels:

- Peer relationship between operators;
- STP connectivity;
- SIGTRAN protocols;
- VAS systems, e.g. SMSC, IN;
- Signaling Gateways, MGW;
- SS7 Service providers (GRX, IPX);
- GTT translation;
- ISDN terminals;
- GSM phones;
- LIG (Legal Interception Gateways);
- 3G Femtocell;
- SIP encapsulation.

Therefore, SS7 exploits that take various forms including:

- Obtaining the mobile subscriber's confidential identity (IMSI)
- Determining subscriber's location
- Blocking a subscriber from receiving incoming calls and text messages
- Intercepting a subscriber's incoming SMS messages. This includes the ability to send a confirmation message and alter the subscriber's message
- Sending a request to transfer funds between a subscriber's accounts
- Manipulating the subscriber's profile to bypass billing
- Redirecting the incoming calls
- Denying the incoming calls

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

SS7 Exploitations

The SS7 exploitations listed below are hypothetical threats highlighted specifically for mobile network operators. This security issue is new to the industry and real world discovery of actual exploits are only being exposed as knowledge and understanding develop. While the impact of these threats being used would be devastating to the mobile network operator, it is important to note that this list is likely to grow as the sophistication of attackers improve.

Exploiting IMSI disclosure

IMSI (International Mobile Subscriber Identity) is a unique subscriber identification used by the mobile network operator and is generally considered to be secure confidential information. Armed with the IMSI and MSC/VLR address determining subscriber's regional location, the attacker can use this data for additional more complex exploitations.

Attacker's Goal: Successfully obtain the following data:

- The subscriber's IMSI
- The address of servicing MSC/VLR
- The address of the Home Location Register (HLR) where subscriber's account data resides

Approach: Using target subscriber number, request the Mobile Switching Center (MSC) Visitor Location Register (VLR) address, and the IMSI. This request is part of the routine SMS delivery protocol allowing the source network to receive subscriber's location information for routing of the message.

Exposing subscriber's location

In most urban areas, subscriber location can be determined down to a few hundred meters using specific data and any one of the services publically available on the internet that provide accurate base station locations using this specific data.

Attacker's Goal: Successfully obtains the CGI (Cell Global Identity) which is a GSMA standard used to identify a certain cell of the location area and consists of:

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

Approach: Using the IMSI and the current MSC/VLR address, this exploitation leverages data commonly used for real-time tariffing of subscriber's incoming calls to provide unauthorised access to the subscriber's location.

Disrupting subscriber services

The subscriber's handset will indicate network connectivity but, calls or text messages will not be received until they register in another MSC/VLR area, reboot the phone or reset the register by making an outgoing call.

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

Approach: Using the IMSI and current MSC/VLR address, the attacker registers the subscriber within a spoofed MSC/VLR coverage zone similar to the process that happens a roaming subscriber is registered in different network.

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Intercept incoming SMS

In addition to simply disrupting a subscriber's services, the attacker may also use the spoofed MSC/VLR to have incoming SMS messages intended for the subscriber routed to the attacker. Again, this will persist until the subscriber registers in another MSC/VLR area, reboots the phone or resets the register by making an outgoing call.

Attacker's Goal: Use data that may be contained in incoming SMS messages such as:

- One-time mobile banking passwords
- Two factor authentication interactions
- Password resets for various services (email, social networks, etc.)
- Critical personal information

Approach: Intercept the messaging stream and spoof the interaction to enable discovery of the intended information. Attacker may even provide delivery confirmations to the intercepted messages to avoid detection and then re-register the subscriber's MSC/VLR area to eliminate exposure.

USSD request manipulation.

In some markets, USSD (Unstructured Supplementary Service Data) commands on the handset is widely used by subscribers to communicate directly with automated services such as payments and billing offered by the mobile network provider or partner services including monetary transactions and banking.

Attacker's Goal: Use USSD commands to spoof transactions such as transferring funds between accounts or authorising purchases. If the attack is combined with interception of incoming SMS messages to eliminate confirmation messages, these transaction may be remain undetected for quite a while.

Approach: Using the subscriber number, HLR address and the USSD string, this is a legitimate USSD request sent from VLR to HLR that exploits the ability to send USSD requests directly to HLR.

Manipulate Subscriber Profile in VLR

The subscriber's profile is copied from the HLR database to the VLR database when they register on a switch. This profile includes information about active services, call forwarding parameters and billing platform data. Manipulating this data would allow the subscriber to use services such as making phone calls that either bypass the billing system or have an incorrectly applied tariff. Note: this same manipulation can also be used by an attacker to intercept subscriber's communications.

Attacker's Goal: Spoof the network with fake subscriber profile data to enable subversion of billing and charging tariffs

Approach: Using subscriber number, subscriber IMSI, VLR address and subscriber profile details all provided through other SS7 exploits, the attacker is able to manipulate a profile designed to fool the MSC/VLR into providing services to the subscriber based on the fraudulent spoofed parameters.

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Monitoring outgoing calls

There are legal methods in place to intercept and monitor outgoing calls from target subscribers that normally require court orders and having a secure technical framework in place. This process takes time and requires the discreet participation of several parties to stay within legal privacy laws. Attackers cannot be bothered.

Attacker's Goal: Intercept outgoing calls in an undetected manner and illegally monitor voice conversation between two parties.

Approach: This attack uses the same approach of manipulating the Subscriber Profile VLR attack but with the addition of substituting the billing platform address with a new equipment address. The result is that when the subscriber makes a call, the billing request along with the number of the destination subscriber are sent to the attacker's equipment where an undetected three way call is set up. The three way call is essentially a conference between the destination subscriber, the calling subscriber and the muted attacker.

Redirect incoming calls

Attacker's Goal: Spoof voice call routing information to redirect incoming calls to

- Mislead callers who assume they have reached intended party
- Redirect calls to competitors' number.
- Redirect calls to an expensive international number.
- Redirect calls to pay-per-use scheme and monetise traffic.

Approach: This attack extends the attack to disrupt subscriber services. Using the IMSI and current MSC/VLR address, the attacker registers the subscriber to a spoofed MSC/VLR, which sends the Mobile Station Roaming Number (MSRN) to redirect the call. The HLR then transfers this number to the GMSC which redirects the call to the provided MSRN.

Block all incoming calls at the MCS

Attacker's Goal: Block incoming calls for all subscribers located in the coverage area of targeted switch.

Approach: Using the IMSI of any subscriber and the switch address, this attack exploits the procedure of assigning a roaming number (MSRN) when receiving a voice call. When calls are received, the subscriber's MSC/VLR is identified and a voice channel is established using a temporary roaming number. Typically roaming numbers are only intended to exist for the call setup but, default timer values are often specified on equipment of 30 – 45 seconds. This is enough time to allow an attacker to flood the system with roaming number requests which quickly use up the pool of available numbers and render the switch unable to process incoming calls.

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Solving the SS7 security problem

The mobile ecosystem has begun work to define recommendations, build and implement solutions to detect and prevent potential attacks. Operators need a solution that is easy to deploy yet comprehensive, and ideally one that overlays the existing architecture. That means integration should be flexible eliminating the need and expense of redesigning the underlying signaling network architecture. The objective is not to merely block suspicious traffic but to use global threat intelligence and advanced analytics to secure the network against privacy and fraud attacks.

There are several layers of protection that can be suggested:

- **Filter and control incoming MAP/CAP request received.**
  SS7 MAP/CAP operation level control should prevent unauthorised usage of the network primitives revealing location and subscriber identity. This measure that often can be configured at the STP level is necessary but not exhaustive. The same interconnect elements originating legal MAP/CAP requests might still be used by the attacker as an entry point into the network. To efficiently address this aspect of fraud control, validation of requests should happen across all the layers of the SS7 stack.
- **Active validation of the originating entity**
  For any suspicious operation received from outside of the network originated on behalf of own subscriber, the actual location (VLR/MSC) of the subscriber should be validated. This is known as an anti-spoof technique which is often used for mobile originated SMS messages; however there is a whole range of MAP/CAP operations where this technique should be applied.
- **VLR/MSC update validation**
  The mobile nature of cellular communication assumes that subscribers are on the move. At the same time, it is physically impossible that the same subscriber will be appearing in the different parts of the world within a short time period. When a roaming subscriber identifies itself in one European country (for example Germany), it is physically impossible that the same subscriber can appear somewhere in Asia or Latin America in the next ten minutes. Such a situation should definitely raise an alarm at the operator security department.
- **Offline data analytics**
  Though some of the attack techniques have been identified and can be disclosed using one of the measures mentioned above, it should be recognised that attackers will be exploiting more and more ways to break subscriber privacy or harm the mobile network. Therefore any unusual activity should be detected in near real-time mode using modern, big data analytical tooling. As a result of such analysis, the source of the potential suspicious activity can be identified enabling enforced control on discovered network elements or subscribers.

Using the IMSI of any subscriber and the switch address, this attack exploits the procedure of assigning a roaming number (MSRN) when receiving a voice call. When calls are received, the subscriber's MSC/VLR is identified and a voice channel is established using a temporary roaming number. Typically roaming numbers are only intended to exist for the call setup but, default timer values are often specified on equipment of 30 – 45 seconds. This is enough time to allow an attacker to flood the system with roaming number requests which quickly use up the pool of available numbers and render the switch unable to process incoming calls.

Exploring SS7 fraud that threatens mobile network security and subscriber privacy

Summary

Given that mobile communications is a prime target for hackers who desire to penetrate critical infrastructures and businesses, we must find and implement protective measures quickly before subscribers, organisations, and even governments fall prey to misuse and are severely impacted. It is imperative that the ecosystem work together to build these critically needed solutions.

We are Xura

We offer our customers a pathway to next generation digital technology. Our thinking unlocks the possibilities of no boundaries communications.

For over 20 years, we have been working with Communications Service Providers (CSPs), operators and enterprises all over the world, helping them to meet the needs of tomorrow's multi-device, multi-services consumers.

We offer clever ways to financially realise opportunities from existing technology, while guiding customers to richer communications solutions by creating innovative products and services to disrupt digital.

We help 8 out of the top 10 global operators reach over 3 billion endpoints.

We are the enabler making the future of digital communications services happen.

Xura. We think beyond.

For more information
Please visit our website xura.com
or email contactxura@xura.com