The Fall of SS7 – How Can the Critical Security Controls Help?

GIAC (GCCC) Gold Certification

Author: Hassan Mourad, Hassan.morad@gmail.com
Advisor: Stephen Northcutt
Accepted:

Abstract

For decades, the security of one of the fundamental protocols in telecommunications networks, Signaling System No. 7 (SS7), has been solely based on the mutual trust between the interconnecting operators. Operators relied on their trust in other operators to play by the rules, and the SS7 network has been regarded as a closed trusted network. This notion of trust and security has recently changed after several security researchers announced major vulnerabilities in the SS7 protocol that threatens the user's privacy and can lead to user location tracking, fraud, denial of service, or even call interception. In this paper we will discuss each individual attack and examine the possibility of using the critical security controls to protect against such attacks and enhance the security of SS7 interconnections.

1. Introduction

In August 2014, the Washington Post Published an article titled "For sale: Systems that can secretly track where cellphone users go around the globe" (Timberg, 2014). The article described how surveillance equipment manufacturers where taking advantage of weaknesses in a telecommunication protocol named SS7 to track the whereabouts of its surveillance targets. The article also referenced a product brochure for one of those surveillance vendors describing how they use their access to SS7 networks to provide the exact location of their target. (Washington Post, 2014)

Later in 2014, during the Chaos Communications Congress in Berlin, several security researchers presented their findings on the insecurity of SS7. Tobias Engel, a German researcher presented how to abuse access to SS7 networks to attack mobile subscribers (Engel, 2014). Karsten Nohl, another German researcher, presented how to intercept and manipulate cellular conversation using such access (Nohl,2014), and finally Laurent Ghigonis and Alexandre De Oliveira from P1 Security presented their SS7 global security map(P1 Security, 2014).

For decades, the security of Signaling System No. 7 (SS7) has been solely based on the mutual trust between the interconnecting operators. Operators relied on their trust in other operators to play by the rules, and the SS7 network has been regarded as a closed trusted network. This is clearly no longer valid, and an urgent need rises to analyze the security gaps in such networks and implement the needed controls to close these gaps.

In this paper we will examine the attacks against SS7 and look into the critical security controls as one of the most effective control frameworks, in the hope of identifying relevant security controls that can be deployed to address SS7 insecurities as well as increase the core network security posture.

2. Core Network Architecture

The GSM Core network (CN) (or Network Switching Subsystem NSS) is the component of the GSM system that carries out call switching and mobility management for mobile phones. The CN consists of the following components

The Mobile-services Switching Center (MSC): constitutes the interface between the radio system and the fixed network. It performs all the needed functions to handle the circuit switched services to and from the mobile stations (3GPP, 2015, p26). The MSC usually consists of two systems: the MSC server, responsible for the signaling, and the media gateway (MGW) handling the user traffic.

The Home Subscriber Server (HSS) is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions (3GPP, 2015, p22). The HSS holds: user identification, numbering and addressing information, User security information, User location information, and user profile information. The HSS function is performed by two network components: The Home Location Register (HLR) and the Authentication Center (AuC)

The Home Location Register (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. Each user can only be associated to a single HLR.

The authentication center (AuC) is associated with a given HLR and stores an identity key for each subscriber registered with the associated HLR. The key is used to generate security data that are subsequently used for mutual authentication between the subscriber and the network, protect the integrity and the confidentiality of the communications (3GPP, 2015, p23).

The Visitor Location Register (VLR) is a database of the subscribers who have roamed into the jurisdiction of the MSC which it serves. When a Mobile Station (MS) enters a new location area it starts a registration procedure. An MSC in charge of that area notices this registration and transfers to a Visitor Location Register the identity of the location area where the mobile station (MS) is situated. If this MS is not yet registered in the VLR, the VLR and the HLR exchange information to allow the proper handling of CS calls involving the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC (3GPP, 2015, p25).

The Short Message Service Gateway (SMSC) acts as an interface between a Short Message Service Centre and the mobile network, to allow short messages to be delivered to mobile stations from the Service Centre (3GPP, 2015, p26).

The Signaling Transfer Point (STP) is responsible for the transfer of SS7 messages between other SS7 nodes, acting somewhat like a router in an IP network (Dryburgh, Hewet, 2005).

3. Signaling System No. 7

The Signaling System Number Seven (SS7) is a suite of protocols that were standardized in the 1980s in ITU-T Q.700 series. New protocols added in the 1990s and 2000s by ETSI and 3GPP to support mobile phones and the services they need (roaming, SMS, data...)

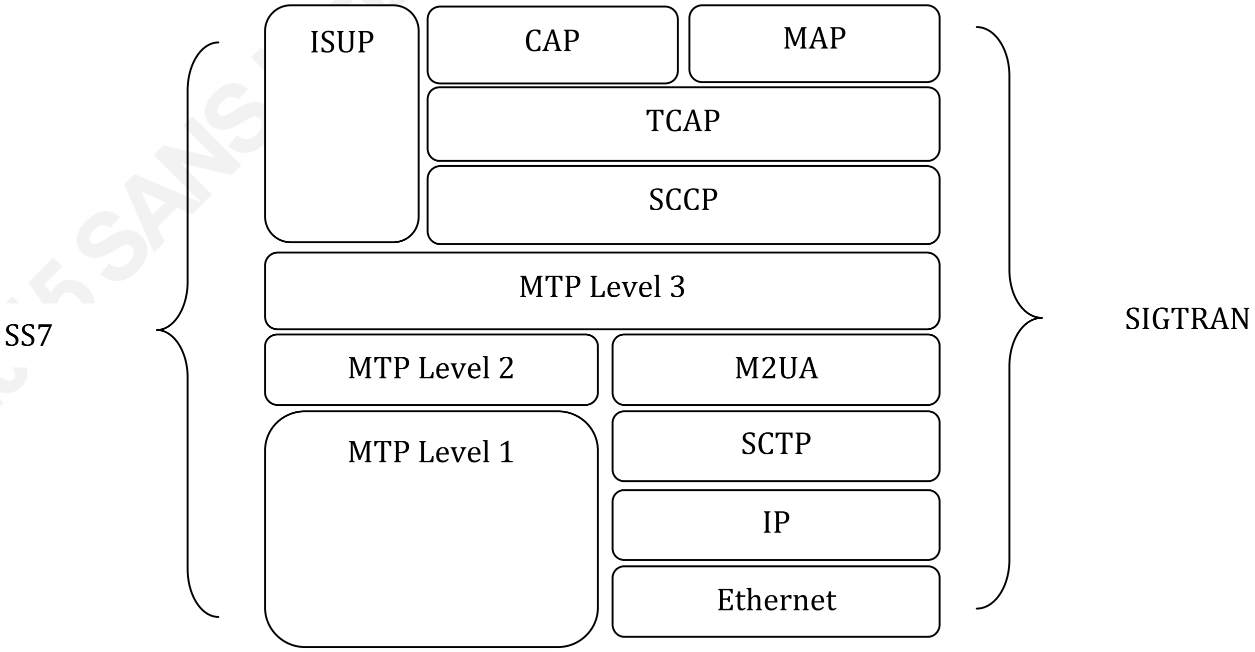


Figure 1. SS7 & SIGTRAN Protocol Suite

The Mobile Application Part (MAP) is an SS7 protocol that provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center and Serving GPRS Support Node (SGSN).

The MAP protocol is responsible for providing the following functionality: Mobility Management, Operation and Maintenance, Call Handling, Supplementary Services and Short Message Service (Dryburgh, Hewet, 2005)

The Customized Applications for Mobile network Enhanced Logic (CAMEL) was introduced to allow mobile operators to build custom services that were not possible through MAP. The CAMEL Application Part (CAP) along with the Mobile Application Part (MAP) is going to be the focus of this paper.

SS7 was traditionally served over Time Division Multiplexing (TDM) networks; however with the increasing use of IP networks, SIGTRAN (Derived from Signal Transfer) was introduced as part of the SS7 protocol family but uses an IP protocol called Stream Control Transmission Protocol (SCTP) as the transport layer for SS7 (IETF, 1999).

4. SS7 Attacks

As with many legacy protocols, SS7 was designed with little security in mind. Concepts such as authentication and authorization were hardly present or discussed. The SS7 security was solely based on trust. The core network elements were built accordingly with little if any defenses against abusing SS7 functionalities.

Being regarded as a closed network, very little security research has been done to assess the security of SS7. Security researchers had no access to SS7 networks, and service providers had little interest into looking at the topic.

But the SS7 network is no longer closed. Network providers are opening up their SS7 networks for third parties as part of their commercial offerings. Network elements such as Femtocells are leaving the closed boundaries of the operators and are based in untrusted locations; hackers may find their ways into the networks of mobile operators, and its needles to mention that some operators may be under the control of nation states with malicious intentions to abuse such unsecure networks.

Abusing SS7 insecurities can have a severe effect; the nature of the protocol allows access to information such as user location and call/SMS details. Financial services and authentication systems were built based on the trust of the services provided by such protocols. Denial of service attacks abusing those insecurities can be devastating to the telecommunication infrastructure of nations.

In the next sections, we will examine some of the attacks that were announced against SS7, in the hope of analyzing the missing controls and eventually propose some controls that can limit the effect of these attacks. These sections draw heavily on the work done by the security researchers Tobias Engel and Karsten Nohl in the areas of call and SMS interception, location tracking, fraud, and denial of service.

4.1. Call and SMS Interception

Intercepting communications has always been the ultimate target for any espionage operations. In the old days of wired phones, the attacker needed to physically tap into the wire to be able to listen to an ongoing call.

In the age of mobile communication, the call is transmitted over the radio between the calling parties and the mobile networks. Normally the traffic is encrypted over the air interface. The encryption is done using either A5/1 or A5/3 protocols. Recently the A5/1 suite has been broken and it is possible to decrypt the calls transferred over the air interface using cheap radio interceptors and rainbow tables (Nohl, Munant, 2010). As a result, the operators started to roll out the stronger ciphering protocol A5/3 to combat such attacks.

Yet the recently disclosed SS7 vulnerabilities opened multiple venues that facilitate the interception of calls and SMS transmitted over the mobile network. In the next sections we will discuss those techniques.

4.1.1. Call Interception - sendIdentification

The mobile switching center MSC normally holds the encryption keys used by each subscriber to be able to establish the call. When the subscriber is on the move, a handover process facilitates the smooth transition of the subscriber between the different radio cells while maintain the call progress.

In some cases the subscriber moves from one cell to another that is managed by a different VLR. In this case, the new VLR does not initially have the authentication information that would facilitate preserving the call, hence an inter MSC handover process is needed to transfer the keys to the new MSC.

This is done through a MAP message called sendIdentification. The new VLR sends a sendIdentification message to the old VLR, which in turn responds with the keys needed to maintain the ongoing call (Dryburgh, Hewet, 2005). Among these keys are the key used to encrypt the traffic over the air.

In the attack scenario the attacker captures the targets traffic over the air interface (requiring physical proximity from the target). With access to SS7, he can then use the sendIdentification message to retrieve the decryption keys for the target and use it to decrypt the traffic (Nohl, 2014, p7).

The sendIdentification is only needed within the internal network during handovers. It should have no legitimate usage from outside and hence should be filtered on the border.

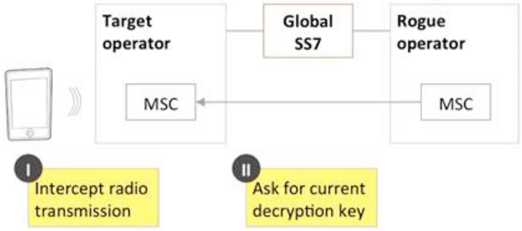


Figure 2. Using sendIdentification for call Interception (Nohl, 2014)

4.1.2. Interception – 3G IMSI Catcher

Second Generation (2G) networks did not offer the concept of mutual authentication, where the network authenticates itself to the subscriber. This made the subscriber vulnerable to an attack known as the 2G IMSI catcher (Strobel, 2007). In this attack, the attacker using a rogue radio cell could announce the same network as a legitimate network with higher power than the normal network. The target would then connect unknowingly to the rogue cell instead of the legitimate network. The attacker intercepts the call, and then forwards it to its destination.

In 3G networks, such attack was not possible, since the network has to authenticate back to the subscriber before a call is established. However with access to SS7, the attacker can send another MAP message called sendAuthenticationInfo to the HLR to get the info needed to successfully impersonate the legitimate network. (Nohl, 2014, p8)

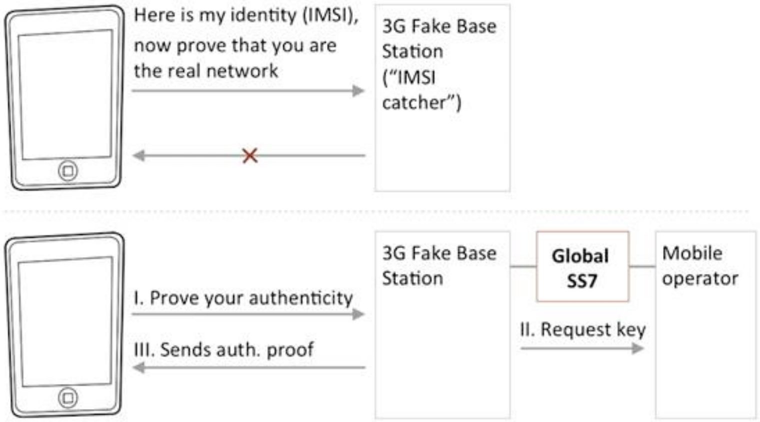

Here is my identity (IMSI), now prove that you are the real network
3G Fake Base Station ("IMSI catcher")
3G Fake Base Station
Global SS7
Mobile operator
I. Prove your authenticity
III. Sends auth. proof
II. Request key

Figure 3. 3G IMSI Catcher with sendAuthinticationInfo (Nohl, 2014)

Unfortunately sendAuthenticationInfo message is legitimately used in roaming scenarios and cannot be filtered out at the borders.

4.1.3. Intercepting Outgoing Calls – CAMEL gsmSCF

The GSM Service Control Function (gsmSCF) is a functional entity that contains the CAMEL service logic that decides for certain for a certain set of events if the desired action can continue modified, unmodified or aborted (Engel, 2014, p31). It can be for example used to modify outbound numbers to add the area code or international format.

An attacker with access to SS7 can use an insertSubscriberData message to change the subscriber's gsmSCF address to an address under their control (Engel, 2014, p34). The attacker is then able to re-write outbound dialed numbers to a number under his control. In this case the attacker will receive the outbound call, record the call before forwarding the traffic to the final destination (Engel, 2014, p35).

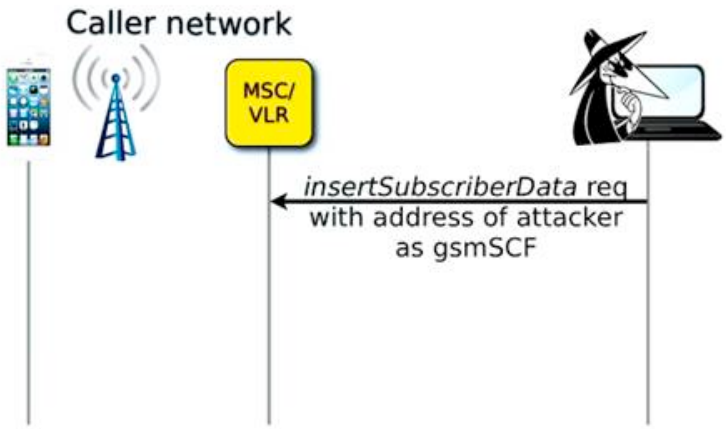


Figure 4. Manipulating the gsmSCF address for the target (Engel, 2014)

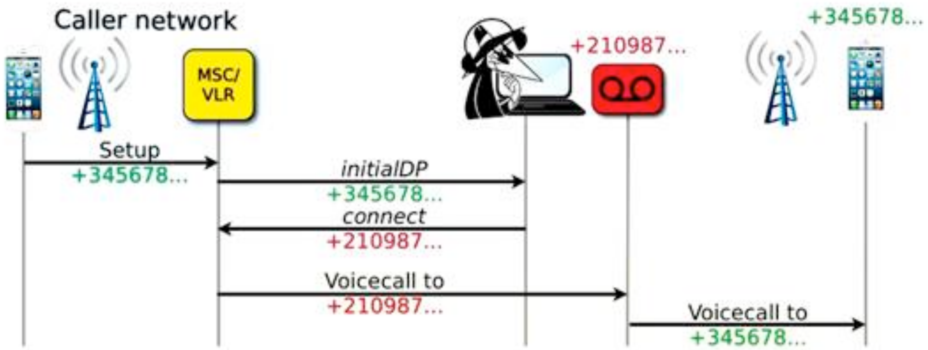


Figure 5. Rewriting outgoing number with an attacker controlled number (Engel, 2014)

The insertSubscriberData message should not be received from external networks for the operator's own subscribers, however it can be sent for subscribers of external networks roaming inside the operator's network. Filtering such messages on the border becomes trickier.

4.1.4. Interception – Incoming Traffic – Call forwarding

The registerSS message is used to register supplementary services to a subscriber. One of these services is the call forwarding service (Dryburgh, Hewet, 2005).

An attacker can use the registerSS message to enable call forwarding to a number under his control. Upon receiving the call, the attacker then uses eraseSS message to remove the call forwarding and then forward the call back to the subscriber. In this way the attacker is able to intercept and record the call.

4.1.5. Interception – SMS

The updateLocation message is used to update the subscriber's location in the network. It informs the network of which VLR/MSC the subscriber is currently connected to.

Using a fake updateLocation message the attacker claims that the victims MS is connected to their MSC. In this case, the subscriber SMSs will be forwarded to the attacker's SMS center to be delivered to the MS. (Engel, 2014, p42) In addition to intercepting personal SMSs of the target, this attack can be used against authentication systems that utilize SMS verification (SMS token, Facebook verification, etc.) and could lead to the compromise of the target's identity.

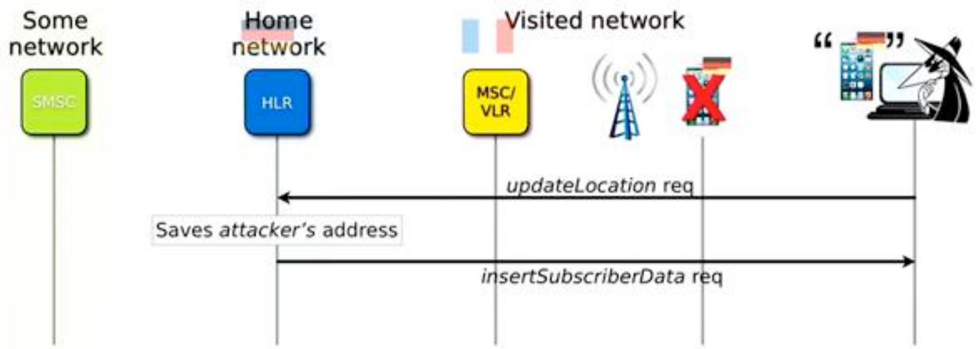


Figure 6. Update subscriber location with a fake location (Engel, 2014)

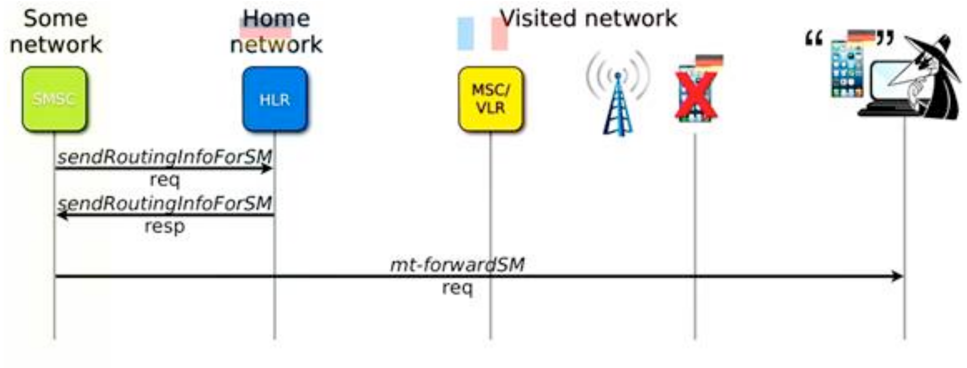


Figure 7. Attacker receives SMS intended to the user (Engel, 2014)

Unfortunately the updateLocation message has a legitimate use case when the subscriber is roaming outside the operator's network and cannot be filtered at network borders.

4.2. Location Tracking

Being able to track the location of your target is a valuable goal for espionage operations. Imagine the ability of a foreign country to track the exact location of their surveillance target without the need to physically monitor his movement.

In this section we will examine some SS7 vulnerabilities that could facilitate location tracking.

4.2.1. Location Tracking – anyTimeInterrogation (ATI)

When a MAP anyTimeInterrogation message is sent to the subscriber's HLR it triggers a provideSubscriberInfo (PSI) message that is then sent to the VLR/MSC to which the subscriber is connected. This returns the cell identifier (Cell-ID) of the subscriber among other information.

The attacker can use this message to acquire the cell-ID. The cell-ID can then be mapped to an actual location up to the street level using publically available mapping information (Engel, 2014, p13).

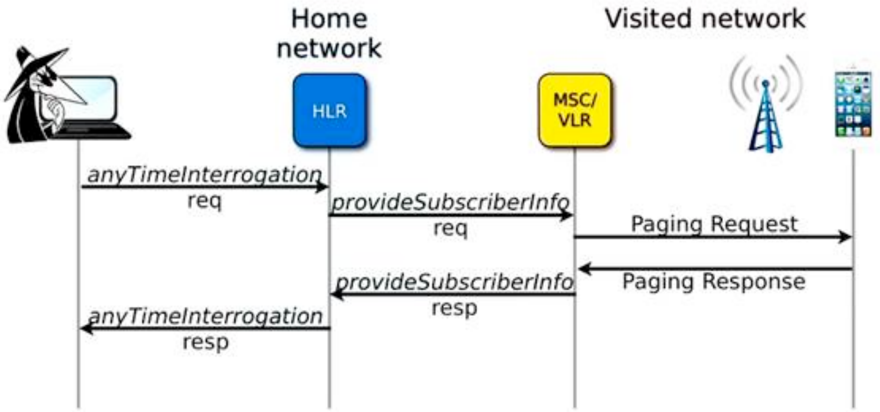


Figure 8. Abusing anyTimeInterrogation message to acquire target's location (Engel, 2014)

Fortunately the anyTimeInterrogation message has no legitimate case to be exposed to external networks and should be filtered on the network borders.

4.2.2. Location Tracking – provideSubscriberInfo (PSI)

In case the ATI message has been filtered, the attacker can still send the provideSubscriberInfo message directly to the MSC/VLR that the subscriber is on. The attacker will first need to find out the IMSI and address of the MSC using a message like sendRoutingInfoForSM that returns the Global Title (GT) address of the MSC (Engel, 2014, p17).

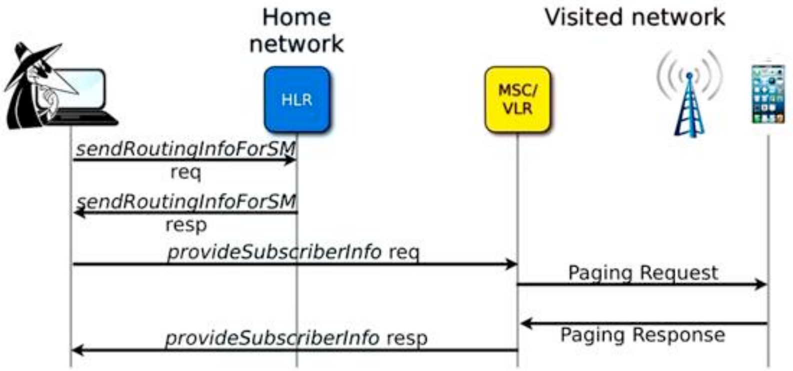


Figure 9. Acquiring cell ID using provideSubscriberInfo (Engel, 2014)

Under normal conditions, the PSI message should not be received from external networks for the operator's own subscribers; however it can still be received for the external operator's own subscriber's roaming in the local operator's network.

4.2.3. Location Tracking – provideSubscriberLocation

The provideSubscriberLocation (PSL) is legitimately used by the Gateway Mobile Location Center (GMLC) to provide the location of a subscriber. The MSC has no capability to authenticate a GMLC server but verifies its sender GT address (Engel, 2014, p24).

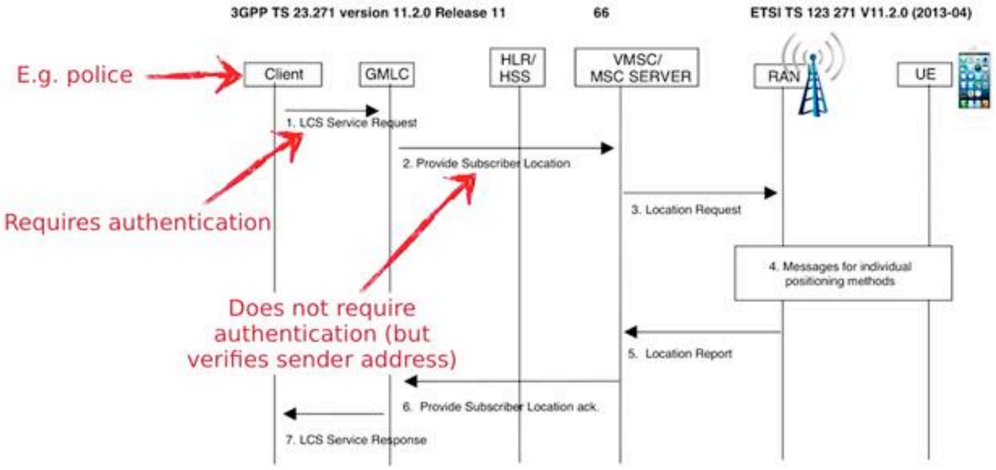

3GPP TS 23.271 version 11.2.0 Release 11
66
ETSI TS 123 271 V11.2.0 (2013-04)
E.g. police
Client
GMLC
HLR/ HSS
VMSC/ MSC SERVER
RAN
UE
1. LCS Service Request
2. Provide Subscriber Location
3. Location Request
Requires authentication
4. Messages for individual positioning methods
Does not require authentication (but verifies sender address)
5. Location Report
6. Provide Subscriber Location ack.
7. LCS Service Response

Figure 10 Location Services (Engel, 2014)

Unfortunately the attacker can still spoof the GMLC address and use it to send the PSL message.

4.3. Fraud

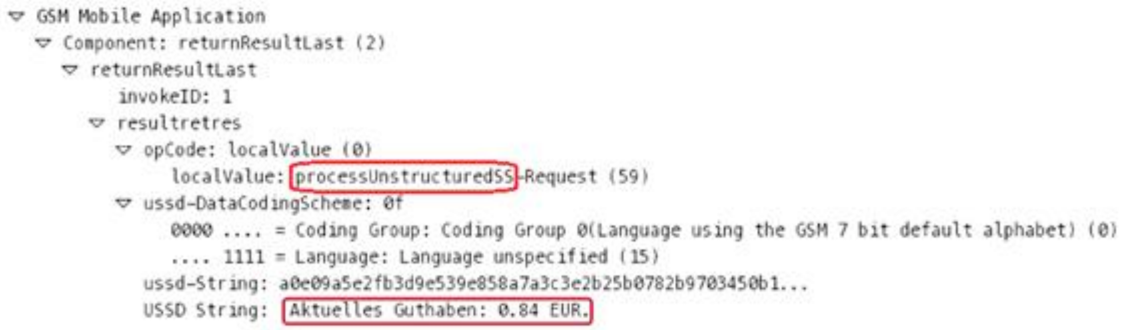
As mentioned previously, the SS7 networks are no longer exclusive to mobile operators, and access to SS7 is becoming more available to untrusted parties.

This opens multiple opportunities for initiating fraudulent transactions on behalf of the subscriber. In the next sections we will examine two possible fraud opportunities.

4.3.1. Fraud – USSD - processUnstructuredSS

USSD is a protocol traditionally used inside the operator's network to provide different services, such as dial enquiries, credit transfer, mobile payments, as well as several other services. The subscriber typically sends certain USSD codes (such as #100#) to fulfill certain transactions.

Using a processUnstructuredSS message, the attacker is able to send USSD codes on behalf of the customer, possibly authorizing a credit or money transfer transaction from his target (Engel, 2014, p44).



```
▽ GSM Mobile Application
  ▽ Component: returnResultLast (2)
    ▽ returnResultLast
        invokeID: 1
      ▽ resultretres
        ▽ opCode: localValue (0)
            localValue: processUnstructuredSS-Request (59)
        ▽ ussd-DataCodingScheme: 0f
            0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)
            .... 1111 = Language: Language unspecified (15)
          ussd-String: a0e09a5e2fb3d9e539e858a7a3c3e2b25b0782b9703450b1...
          USSD String: Aktuelles Guthaben: 0.84 EUR.
```

Figure 11 Abusing USSD for fraud (Engel, 2014)

Unfortunately in many cases the operator allows receiving this message from external networks, in case their roaming subscribers need to access these services while visiting another country which makes filtering such message at the border very hard.

4.3.2. Premium rate fraud – Call forwarding

As in the case of call interception, the registerSS message can be used to configure call forwarding for the subscriber to a premium rate number instead of the interception number.

4.4. Denial of Service

There are several ways an attacker can deny a service for certain subscribers. Using insertSubscriberData, or deleteSubscriberData, the attacker can remove critical services, or activate call barring for the target.

Using a cancelLocation message, the attacker can trick the network into removing the subscriber's connection to the network, and hence calls and SMSs cannot be delivered (Engel, 2014, p30).

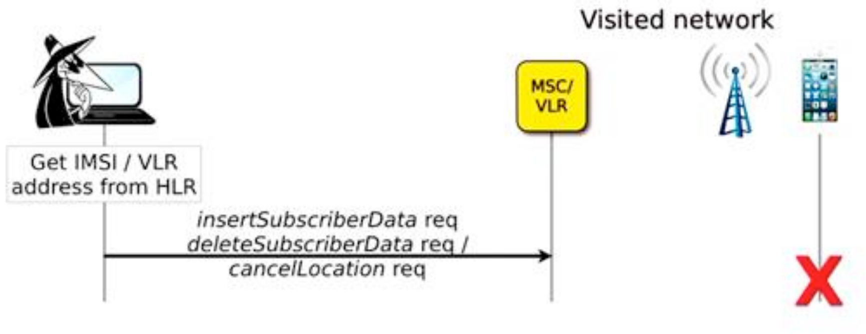


Figure 12 Denial of Service using SS7 (Engel, 2014)

One other point to consider; with very little research in SS7 security, one can hardly imagine that the different SS7 implementations are free from vulnerabilities that can lead to denial of service among other adverse effects.

5. Vulnerability Classification

In order to be able to address the attacks described in the previous section, we need to classify the different SS7 messages according to their business need, and need to exposure.

From the previously described attacks, we can classify those messages into three categories:

Category 1: Messages that has no legitimate use case for external exposures.

Category 2: Messages that has no legitimate need to be exposed externally for the operator's own subscribers, but can be received for other operator's roaming subscribers.

Category 3: Messages that has legitimate need for external exposure

The below table summarizes the different SS7 messages, the attack scenario they are used in, and their category.

Message	Attack	Category

sendIdentification (SI)	Interception	Category 1
sendAuthenticatioInfo	Interception	Category 3
insertSubscriberData + gsmSCF	Interception (Outgoing)	Category 2
registerSS – eraseSS	Interception (Incoming), Fraud	Category 3
updateLocation	Interception (SMS), Denial of Service	Category 3
processUnstructuredSS	Fraud	Category 3
insertSubscriberData	Denial of Service	Category 2
deletedSubscriberData	Denial of Service	Category 2
cancelLocation	Denial of Service	Category 3
anyTimeInterrogation	Tracking	Category 1
anyTImeModification	Tracking	Category 1
provideSubscriberInformation	Tracking	Category 2
provideSubscriberLocation	Tracking	Category 1
sendRoutingInformation (-SM, -LCS)	Facilitates multiple attacks	Category 3

Table 1 SS7 message classification

6. The Critical Security Controls (CSC)

“The Critical Controls for Effective Cyber Defense (the Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors”. (Council on cyber security, 2015)

In the context of this paper, we will examine the controls that are relevant to the prevention of the previously discussed attacks as well as those that can significantly enhance the security of SS7 interconnection and the core network.

6.1. Critical Security Control 13 – Boundary Defenses

In the core network and SS7 interconnections the notion of a boundary was limited to the use of STP which offered little if no capabilities that can be used to limit the attacks described in the previous section. CSC13 aims at "protecting internal systems by creating a hardened network perimeter" (Cole, Tarala, 2015, p. 1-67). In other words, establish a clear boundary to the network.

The need clearly rises for the introducing boundary defenses such as an SS7-aware firewalls and IDS/IPSs that has the capability of understanding SS7/MAP traffic and detect/block these attacks.

While the security industry is working on building such specialized defenses, we propose to reposition some of the traditional security defenses such as the IDS/IPS to detect and possibly block some of these attacks by utilizing custom filters.

For example, category one attacks can be detected by simply looking for the specific MAP messages used in these attacks. An example below is shown for a snort filter that is used to detect call interception using sendIdentification message.

alert ip $External_Operators any -> $STP any (msg:"Call Interception Attempt - sendIdentification"; content:"sendIdentification";

For category two attacks, detection can be based on custom filters looking for the presence of the MAP message as well as the operator's IMSI ranges. A snort filter to detect such attack would look like the following

alert ip $External_Operators any -> $STP any (msg:"Location tracking - provideSubscriberInformation"; content:"provideSubscriberInformation"; content: "6201XXXXXXXX";

The above method is based on the assumption that the signaling traffic is carried over IP (i.e. in the case of SIGTRAN), however such setup is still possible over TDM using specialized equipment that can convert TDM signaling messages to IP based ones.

Unfortunately category three requires correlating the MAP messages with further information on the current user state such as his last location. This cannot be achieved with custom signatures.

6.2. Critical Security Control 14 – Maintenance, Monitoring & Analysis of Audit Logs

CSC14 goal is "to log system events in order to later be able to analyze events on systems and have system awareness" (Cole, Tarala, 2015, p102). The audit trails are the eyes and ears of what is happening on your network. Auditing core network elements should be part of the organizations' log management process.

If possible, log the usage of specific MAP messages, either using native logging capabilities of the core network elements or through logs provided by quality of service nodes deployed to monitor network quality. These logs can then be analyzed for abnormalities such as those resulting from category one and two attacks, or even correlated to detect category three attacks.

An example of correlation would be receiving an updateLocation message from an external entity in a short period of time after receiving another message internally. This scenario is not normal in reality since it means that the user has travelled abroad in a very short period of time, indicating an attack against that user.

6.3. Critical Security Control 19 – Secure Network Engineering

With the new threats towards the core network, porting the concepts of secure network engineering into the core network becomes an absolute necessity. A flat core network exposes different network elements to risks that can be mitigated with proper segregation.

CSC19 aims to "implement a robust, secure network engineering process and network architecture" (Cole, Tarala, 2015, p103). Segmenting the network into different zones depending on the trust and exposure level enhances the security of the core. External entities should only gain network access to the STP, which should be separated from the other network elements such as the HLR or the MSC.

6.4. Critical Security Control 20 – Penetration Test and Red Team Exercises

Having established that SS7 interconnection is clearly a boundary between trusted and untrusted network, the need to assess the security posture and defenses of such boundary rises as a critical control.

CSC20 target's "identifying potential system vulnerabilities in business systems & improving the overall security of the system". In addition to identifying vulnerabilities, the red team exercise can also expose security monitoring flaws, response procedure gaps & personnel complacency. (Cole, Tarala, 2015, p1-127)

Regular external and/or internal penetration testing exercises should be conducted against the core network. Given the criticality of this part of the network, it is strongly advised to create a test bed that mimics production environment and conduct the tests against this environment.

6.5. Critical Security Control 4 – Continuous Vulnerability Assessment and Remediation

With access opened to external parties and more researchers working on SS7 security, more vulnerabilities are expected to be exposed in the near future. With an impact that can lead to the disruption of service for millions of subscribers, SS7 vulnerabilities can become the ultimate weapon in cyber warfare and the playground of nation states, if it is not already.

A clear need rises to build the needed tools and technologies to assess the SS7 vulnerabilities, and the need to establish a continuous process for assessing and remediating any discovered vulnerability.

CSC4 targets "protecting systems by remediating known vulnerabilities" (Cole, Tarala, 2015, p1-63). It is crucial that the organization's vulnerability management program is extended to include core networks elements. Critical patches should be evaluated in a test environment as soon as they become available, then deployed on production in a timely manner based on its risk rating.

6.6. Critical Security Control 18 – Incident Response and Management

Given the nature of SS7 networks and the fact that we only scratched the surface in researching its security and building proper defenses, it is inevitable that security incidents will occur. It becomes crucial to establish or enhance the incident management capabilities to be able to respond to incidents in the core network domain.

The goal of CSC18 is to minimize exposure to data loss risk by establishing an incident response team and enhancing the organization's ability to identify and respond to incidents in a timely controlled manner. (Cole, Tarala, 2015, p1-83)

It is important that the incident response ream includes expertise in the core network domain, as well as have the proper procedures to handle incidents in this domain. Periodic drills should be conducted to assess the response capabilities in different attack scenarios (e.g. Denial of service, Unauthorized Access, MAP message abuse, etc.)

6.7. Critical Security Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations & Servers

CSC3 targets "protecting systems by utilizing secure system configuration" (Cole, Tarala, 2015, p1-27). The core network elements are no exception to this requirement. Whether they utilize a general purpose OS or a proprietary one, the organization needs to establish & ensure the use of a standard secure configuration of the OS.

Normal hardening activities should be followed: Disable unused services, remove unused accounts, apply latest patches, and close open & unused ports to name a few. Similar hardening should be done to databases containing sensitive data.

The administration of the core network elements should be done over secure channels. Clear text protocols such as telnet and VNC should not be used to manage those critical nodes.

Unused MAP operations should be disabled on the relevant network element and only required messages should be allowed.

7. Conclusion

As a legacy protocol, SS7 was built with no security in mind. Newer signaling protocols such as SIP and DIAMETER might offer better security controls, yet they still have their own security issues.

Core network elements were also not built with the security controls to address the new threats. A clear need for specialized security solutions rises to prevent current and future attacks.

But change in telecom networks tends to be slower than in traditional IT networks because of the impact they might cause to millions of subscribers. It might take a long time before we see the introduction of new defense solutions into the operators' networks.

Until this happens it becomes an absolute necessity to look into our current arsenal of security solutions and controls to reduce the current exposure. The critical security controls, as a well-established control framework, presents itself as a possible answer to some of the presented threats that can significantly enhance the security of the core network.

References

Timberg, C. (2014, August 24). For sale: Systems that can secretly track where cellphone users go around the globe. Washington Post. Retrieved from 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

Washington Post (2013, Jan). Skylock Product Description 2013. Retrieved from: http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/

Engel, T. (2014, December). SS7: Locate, Track & Manipulate. [Video file] Retrieved from: https://www.youtube.com/watch?v=lQ0I5tl0YLY

Nohl K. (2014, December). Mobile Self Defense. [Video file] Retrieved from: https://www.youtube.com/watch?v=GeCkO0fWWqc

P1 Security (2014, December). SS7 Map. Retrieved from: http://ss7map.p1sec.com/

3rd Generation Partnership project (2015, June 21). Mobile-services Switching Center. In TS 23.002 Network Architecture, Release 13, p26. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Home Subscriber Server. In TS 23.002 Network Architecture, Release 13, p22. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Authentication Center. In TS 23.002 Network Architecture, Release 13, p23. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Visitor Location Register. In TS 23.002 Network Architecture, Release 13, p25. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

3rd Generation Partnership project (2015, June 21). The Short Message Service Gateway. In TS 23.002 Network Architecture, Release 13, p26. Retrieved from: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-d20.zip

Dryburgh L., Hewet J. (2005, June). SS7 Network Architecture. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 7) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=26

Dryburgh L., Hewet J. (2005, June). MAP Operations. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=115

IETF (1999, October). Framework Architecture for Signaling Transport. Retrieved from: https://www.ietf.org/rfc/rfc2719.txt

Nohl K., Munaut S. (2010, December). GSM Sniffing. [pdf document] Retrieved from: https://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

Dryburgh L., Hewet J. (2005, June). Mobility Management. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=116

Nohl K. (2014, December). Mobile Self Defense, p.7. [pdf document] Retrieved from: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

Strobel D. (2007, July). IMSI Catcher. [pdf document] Retrieved from: http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/slides_imsi_catcher.pdf

Nohl K. (2014, December). Mobile Self Defense, p.8. [pdf document] Retrieved from: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

Engel, T. (2014, December). CAMEL. In SS7: Locate, Track & Manipulate, p31. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Engel, T. (2014, December). Intercepting calls with CAMEL. In SS7: Locate, Track & Manipulate, p34. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Dryburgh L., Hewet J. (2005, June). Supplementary Services. In Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. (Chapter 13) Retrieved from: https://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=119

Engel, T. (2014, December). HLR: Stealing Subscriber. In SS7: Locate, Track & Manipulate, p42. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Engel, T. (2014, December). Cell level tracking with SS7/MAP. In SS7: Locate, Track & Manipulate, p13. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Engel, T. (2014, December). Location Services. In SS7: Locate, Track & Manipulate, p24. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Engel, T. (2014, December). HLR: Supplementary Services. In SS7: Locate, Track & Manipulate, p44. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Engel, T. (2014, December). Denial of Service. In SS7: Locate, Track & Manipulate, p.30. [pdf document] Retrieved from: http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

Council on Cyber Security (2015). The critical security controls. Retrieved from: http://www.counciloncybersecurity.org/critical-controls/

Cole E., Tarala J. (2015). Critical Security Control 13 – Boundary Defenses. In Implementing and auditing the critical security controls – In depth – Book4, p.1-67

Cole E., Tarala J. (2015). Critical Security Control 14 – Maintenance, Monitoring & Analysis of Audit Logs. In Implementing and auditing the critical security controls – In depth – Book4, p.1-102

Cole E., Tarala J. (2015). Critical Security Control 19 – Secure Network Engineering. In Implementing and auditing the critical security controls – In depth – Book5, p.1-103

Cole E., Tarala J. (2015). Critical Security Control 20 – Penetration Test and Red Team Exercises. In Implementing and auditing the critical security controls – In depth – Book5, p.1-127

Cole E., Tarala J. (2015). Critical Security Control 4 – Continuous Vulnerability Assessment and Remediation. In Implementing and auditing the critical security controls – In depth – Book2, p.1-63

Cole E., Tarala J. (2015). Critical Security Control 18 – Incident Response and Management. In Implementing and auditing the critical security controls – In depth – Book2, p.1-27

Cole E., Tarala J. (2015). Critical Security Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations & Servers. In Implementing and auditing the critical security controls – In depth – Book5, p.1-83

Appendix A

Glossary of Terms

- AuC: Authentication Center
- ATI: Any Time Interrogation
- CN: Core Network
- GMLC: Gateway Mobile Location Center
- gsmSCF: GSM Service Control Function
- GT: Global Title
- HSS: Home Subscriber Server
- HLR: Home Location Register
- MSC: mobile Switching Center
- PSI: Provide Subscriber Information
- PSL: Provide Subscriber Location
- SMS-GW: Short Message Service Gateway
- SRI-SM: Send Routing Information – Short Message
- VLR: Visitor Location Register