Cellusys®

SS7 Vulnerabilities

Contents

1. Introduction

The landscape of mobile communications is changing more rapidly than ever. These changes are having a significant impact on Mobile Network Operators (MNO) on a global scale. Operators are facing signaling challenges on multiple fronts – evolution for SS7 to LTE/EPC Diameter based networks, aging or End of Life equipment in the SS7 network, maintenance and support for 2 networks – SS7 and Diameter. Add to these changes another challenge of great concern -- according to the Washington Post, December 18, 2014:

> *"German researchers have discovered security flaws that could let hackers, spies and criminals listen to private phone calls and intercept text messages on a potentially massive scale – even when cellular networks are using the most advanced encryption now available.*
>
> *The flaws, - - - 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."*

These security threats include but are not limited to:

- The ability to determine a subscribers identification -- International Mobile Subscriber Identity (IMSI)
- The ability to hijack and monitor subscribers calls
- The ability to deny service to a subscriber

- The ability to intercept Subscribers Short Message Service (SMS) messages
- The ability to implement Denial of Service attacks at Mobile Switching Centers (MSC)
- The ability to manipulate Subscribers Unstructured Supplementary Service Data (USSD)

All of these attacks and threats are based on SS7 messages that are required for both intra and inter network calls. Moreover, these attacks can be launched with equipment costing as little as a few hundred dollars using commonly available information making access to the SS7 network is easier that ever.

SS7 security topics and other related challenges faced by Mobile Network Operators will be discussed in this paper.

2. Market Drivers and Business Challenges

The Global mobile Suppliers Association states in their study "Evolution to LTE Report, January 7, 2015 that there are currently 360 commercially launched LTE networks in 124 countries with 373 million subscribers. GSMA Intelligence reports that as of February 9, 2015 there are 3.67 Billion unique mobile subscribers worldwide. These subscriber numbers indicate that currently only 10% of the mobile subscribers worldwide are LTE -- the remaining 90% or 3.3 billion are served by 2G/3G Signaling System 7 based networks. These network and subscriber deployment research indicate that the SS7 network will be used for quite some time thus any issues need to addressed to ensure the integrity of the network.

2.1 History of SS7

The SS7/C7 protocol and its associated overlay, out of band signaling network was designed in the early 1980s with major deployment starting in the mid 1980s. During this time there were a limited number of network operators worldwide and the relationship between operators was one of trust. The networks were typically wireline and SS7/C7 access was through physical connectivity creating a walled garden approach to security. SS7 became the major inter office inter operator signaling methodology providing call setup and tear down, and enhanced services such as free call and Advanced Intelligent Services (AIN).

In the late 1980s new upper protocol levels were defined to support mobile telecommunications. These layers were Mobile Application Part (MAP) and CAMEL Application Part (CAP).

Due to the link and bandwidth limitations of SS7/C7, Signaling Transport (SigTran) was introduced in the mid 2000s. The SigTran Adaption layers used Stream Control Transmission Protocol (SCTP) in conjunction with Internet Protocol (IP) as the transport mechanisms.

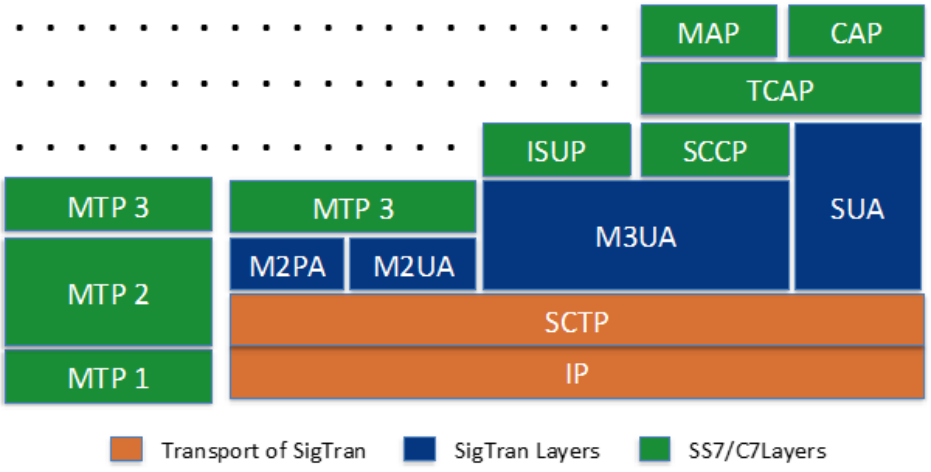
Message Transport Part1, 2, 3 (MTP1, MTP 2, MTP3) are the transport levels for SS7/C7.

ISDN User Part (ISUP) is used to setup and tear down calls in a circuit switched environment.

Signaling Connection Control Part (SCCP) contains the source and destination addresses for TCAP/MAP/CAP messages. SCCP also provides for Global Title Translations capabilities.

Mobile Application Part (MAP) provides special signaling for mobile communication including authentication, authorization, roaming, SMS and others.

CAMEL Application Part provides special signaling for mobile communications including prepaid and others.



SS7-C7-SigTran Protocol Stack

2.2 Evolution to Diameter

The telecommunications signaling network is undergoing major evolutionary changes in both design and protocols used to meet the requirements of next generation networks such as LTE. Session Initiation Protocol (SIP) is replacing the ISUP layer of SS7/C7. In the mobile environment SIP will be used in the

implementation of Voice over LTE (VoLTE) services. The Diameter Protocol defined by both the Internet Engineering Task Force (IETF) and the Third Generation Project Partnership (3GPP) is providing the functionality of TCAP, MAP and CAP layers of SS7.

3. SS7 Security Threats

3.1 Requirements for carrying out an attack

In the initial Walled Garden stage of the SS7 network the ability to gain access to the network was very limited or non-existent. Additionally, even if one were able to get access to the network the only way to build and send messages through the network was via SS7 test equipment. The test equipment costs from the tens of thousands of dollars to hundreds of thousands of dollars making it too expensive for attackers to purchase.

The addition and growth of Mobile Telecommunication to the SS7 environment coupled with third party providers including application services, hub providers, and the undermined the foundation of the "Walled Garden" and the walls of the came tumbling down.

The concept of open source software also had an unintended impact on the intruder's ability to attack the SS7 network. Today the ability to build and send messages in the SS7 network is essentially free and can be placed on everyday personal computers. Intruders can also source equipment to gain information from the air interface side of the mobile network from the hundreds of dollars to not much over a thousand dollars.

The ease of access and the inexpensive equipment opens the door to security breaches to the SS7 network, exposing subscribers and network operators to extensive fraud and financial losses.

3.2 Who is the Attacker?

In the early stages of the SS7 network design and implementation, knowledge of the network and protocol was limited to a small community including network operators, equipment vendors and maybe a few academicians. The

information regarding the network and protocol was limited and costly to obtain.

Today one can obtain specifications for the SS7 network and protocols very easily and by downloading the specification from the telecommunication standards bodies for free.

In essence an attacker can be someone:

- Who came from a network operator
- Who came from an equipment vendor
- Who came from a third party network
    - Hub provider
    - Application provider
- With the desire to learn the protocol and network

All of the information and knowledge required to perform intrusive fraud and network / subscriber attacks is available to anyone.

3.3 Types of Network / Subscriber Attacks

3.3.1 Subscriber Identity Disclosure

Since the "Subscriber Identity Disclosure"" uses a portion of the Short Message Service (SMS) capability a brief explanation of SMS call flow is in order.

When a subscriber enters an SMS Message it is transported over the air interface to the base station. The base station then sends the message to the serving MSC. The serving MSC imbeds the message in a MAP Mobile Originating Short Message Transfer message (MO-Forward-SM) and sends it to the Short Message Service Center associated with the MSC. A subsequent acknowledgement is sent from the SMSC to the MSC indicating the SMSC receipt.

Since the SMSC does not know the location of the terminating subscriber – the SMSC requests this information from the HLR containing the information pertinent to the terminating subscriber. This is accomplished using the MAP-Send-Routing-Info-For-SM query message (SRI-For-SM). The terminating subscribers' Mobile Station International Directory Number (MSISDN) is included in the SRI-For-SM to be used in the HLR query.

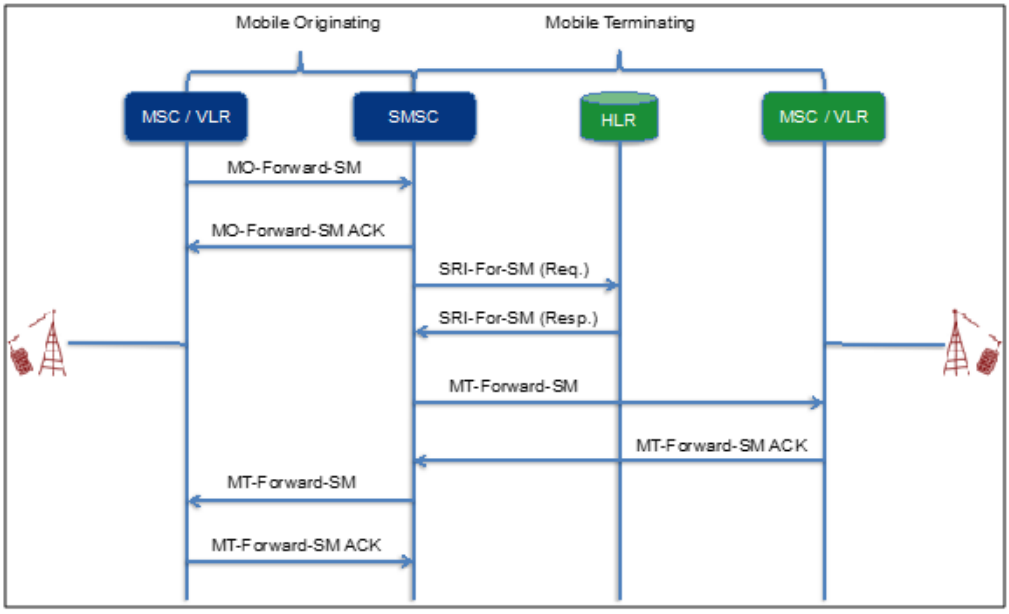
After the HLR lookup – it returns a SRI-For-SM response to the requesting SMSC. At the MAP level this message includes the:

- Point Code (address) of the current MSC/VLR serving the requested subscriber.
- International Subscriber Mobile Identity (IMSI) of the targeted Subscriber

The Message Transfer Part (MTP) or Signaling Connection Control Part (SCCP) of the message would contain the Point Code (address) of the HLR.

After the receipt of the SRI-For-SM response – the requesting SMSC would use a Mobile Terminating Short Message Transfer message (MT-Forward-SM) to send the SMS message to the MSC/VLR currently serving the terminating subscriber.

The previous explanation was not meant to be an exhaustive study of the SMS process but rather an overview and a lead in to the use of the SRI-For-SM sequence to fraudulently obtain network and subscriber information.



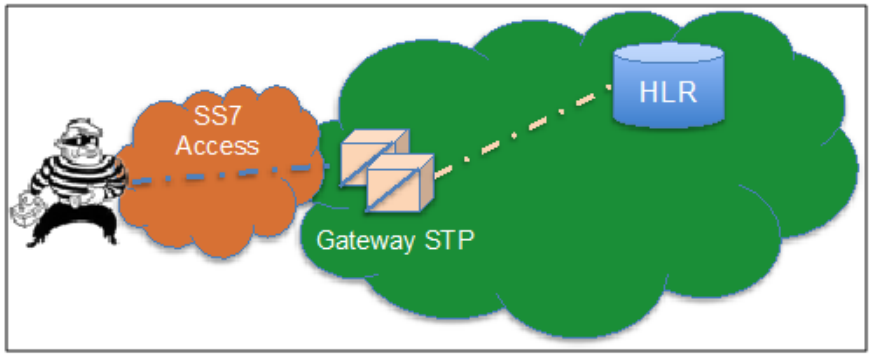
Short Message Service Call Flow

3.3.1.1 Purpose of Attack:

1. Obtain IMSI of a subscriber
2. Get address of MSC/VLR currently serving the target subscriber

3.3.1.2 Requirements For Attack:

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. MSISDN of target subscriber
4. SS7 Point Code of the Gateway STP of the targeted subscribers home network – fairly easy to obtain

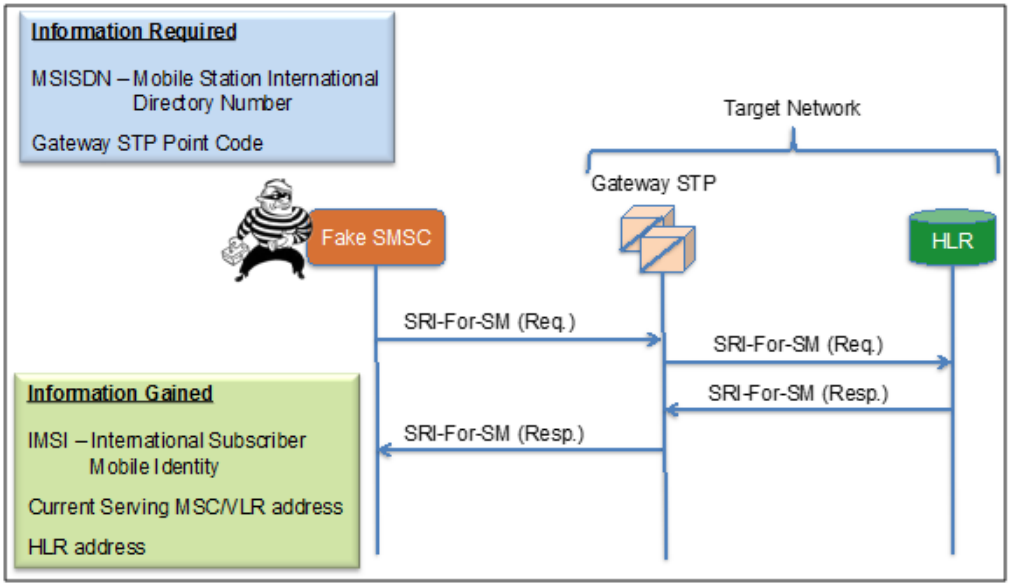


Threat Setup

3.3.1.3 Attack Call Flow:

In the scenario the intruder is posing as an SMSC wishing to deliver an SMS message to a subscriber. To deliver the SMS message the "Fake SMSC" requires the address of the MSC/VLR currently serving the target subscriber.

The "Fake SMSC" constructs an SRI-For-SM request message and includes the MSISDN of the target subscriber. It then addresses the message to the Gateway STP in the home network of the target subscriber. Since the intruder does not know the address of the HLR in question – they set Global Title Translations (GTT) and use the MSISDN as the SCCP called party address. The intruder's address will be placed in the SCCP calling party address field. The Gateway STP performs GTT to find the point code and subsystem of the HLR. The message is then routed to the HLR. The HLR queries its database using the MSISDN as the key. The query results are placed in an SRI-For-SM response and sent to the Gateway STP for routing back to the originator of the SRI-For-SM Query.



Subscriber Identity Disclosure Call Flow

3.3.1.4 Result of Attack:

The intruder currently has the following as a result of the attack:

1. MSISDN of Subscriber
2. IMSI of Subscriber
3. MSC/VLR currently serving Subscriber
4. SS7 Point Code Address of HLR in Subscribers home network

3.3.2 Discovery of Subscribers Location

Location services based on the SS7/MAP protocols and functions were developed for legitimate and lawful applications including:

- Enhanced services such as
  - Location based marketing
  - Fleet and Logistics
  - Financial Services
  - Healthcare
- Emergency Services location of mobile devices

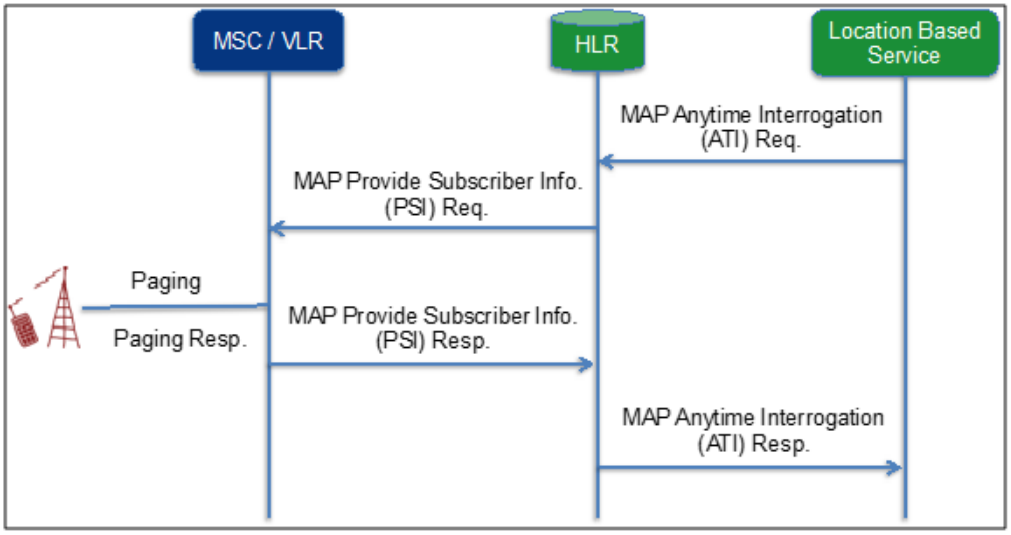
One example of SS7 Location Bases Services is shown in the graphic below. A brief explanation of the service follows.

> *The Location Based Service (LBS) application sends a MAP-Anytime-Interrogation (ATI) request to the HLR of the subscriber. The input to the HLR is the MSISDN of the subscriber. This triggers the HLR to send a MAP-Provide-Subscriber-Info (PSI) Request message to the serving MSC/VLR. The MSC/VLR intern triggers the paging procedure to get the most current location information. Once the MSC/VLR has received the updated location information in the paging response – it constructs a PSI Response and sends it to the HLR. The HLR takes the information received in the PSI and uses it to construct an ATI Response and send it to the requesting LBS application. The Cell Global Identity (CGI) information provided in the ATI Response includes:*
>
> - *Cell Id.*
> - *Mobile Country Code (MCC)*

- *Mobile Network Code (MNC)*
- *Location Area Code (LAC)*

This information can be used to find out longitude and latitude of the subscriber – there are applications available on the web that will translate this information into locations on a map. If the subscriber in question is located in an urban area the location accuracy can be within a few hundred feet due to the close proximity of cell sites.

Intruders were sending ATI messages to the HLR, for there are SS7 networks providing easy access to network and subscriber information, however, most operators have stopped responding to ATI messages received from foreign networks.



Location Service Call Flow using Anytime Interrogation & Provide Subscriber Info. Messages

Bases on the information received in the threat described in 3.3.1 Subscriber Identity Disclosure – the subscriber location information can be obtained without the use of the ATI message.

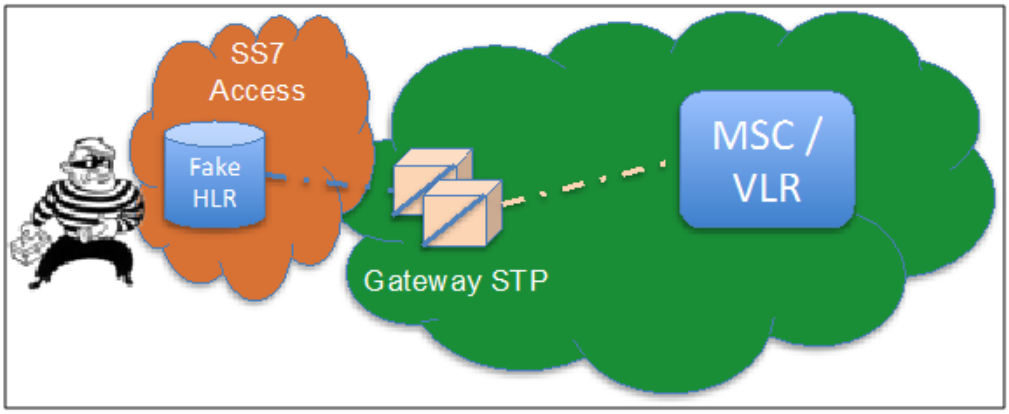
3.3.2.1 Purpose of Attack:

This attack is used to determine the location of the subscriber.

3.3.2.2 Requirements For Attack:

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. IMSI of target subscriber (Obtained in Threat 3.3.1)
4. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)

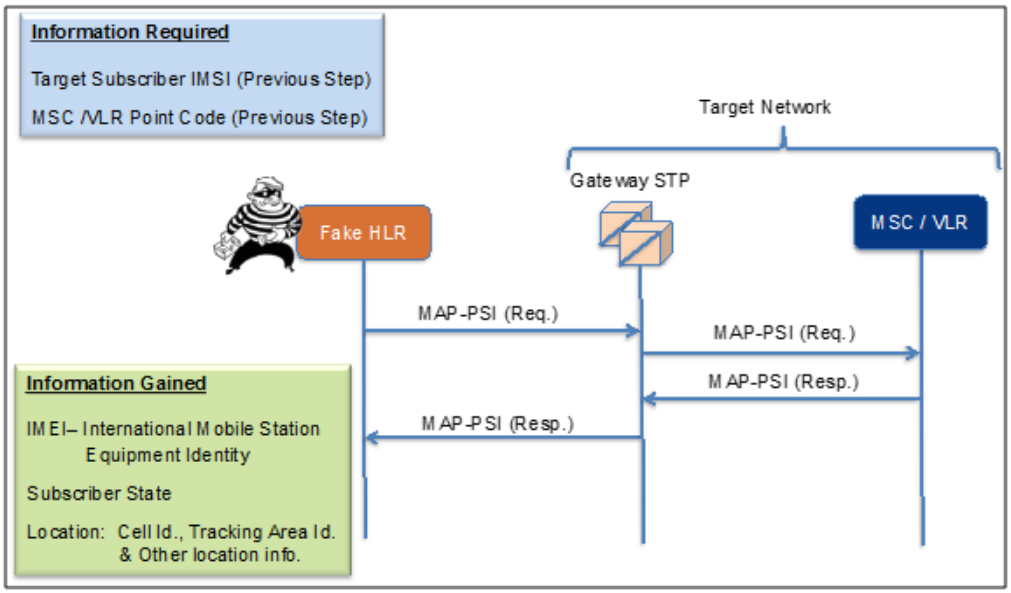
The premise for this attack is -- the intruder will pose as an HLR and send MAP-Provide-Subscriber-Info (PSI) Request message directly to the MCS/VLR serving the subscriber. This is possible due to the fact that in the previous threat the intruder received the address of the MSC/VLR, the IMSI of the subscriber



Threat Setup

3.3.2.3 Attack Call Flow:

In the scenario the intruder is posing as an HLR wanting to get the current location regarding a subscriber. The intruder would construct a MAP-PSI (Req.) message send it to the Gateway STP addressed for the Serving MSC/VLR (obtained in threat 3.3.1). The subscriber IMSI (obtained in threat 3.3.1) would be included in this message indicating the target subscriber. After the MSC/VLR updates the subscriber location information it would build and send a MAP-PSI (Resp.) message indicating the location information requested by the "Fake HLR".



Discovery of Subscribers Location Call Flow

3.3.2.4 Result of Attack:

As a result of the attack the intruder has the following information regarding the location of the target subscriber:

1. Cell Id.
2. Mobile Country Code (MCC)
3. Mobile Network Code (MNC)
4. Location Area Code (LAC)

3.3.3 Disruption of Subscribers Availability

In order to disrupt a subscriber's service, intercept subscriber's text messages or voice calls intruders can use portions of the normal update location procedures. This procedure is shown in the graphic "**GSM Update Location Call Flow".**

A subscriber moving to a new MSC serving area or turning on their mobile station in a new MSC serving area usually starts this procedure. The mobile station sends a Location update request to the new MSC.

The new MSC needs to authenticate the user therefore it sends Send Auth. Info to the HLR. The HLR responds with the authentication triplets.

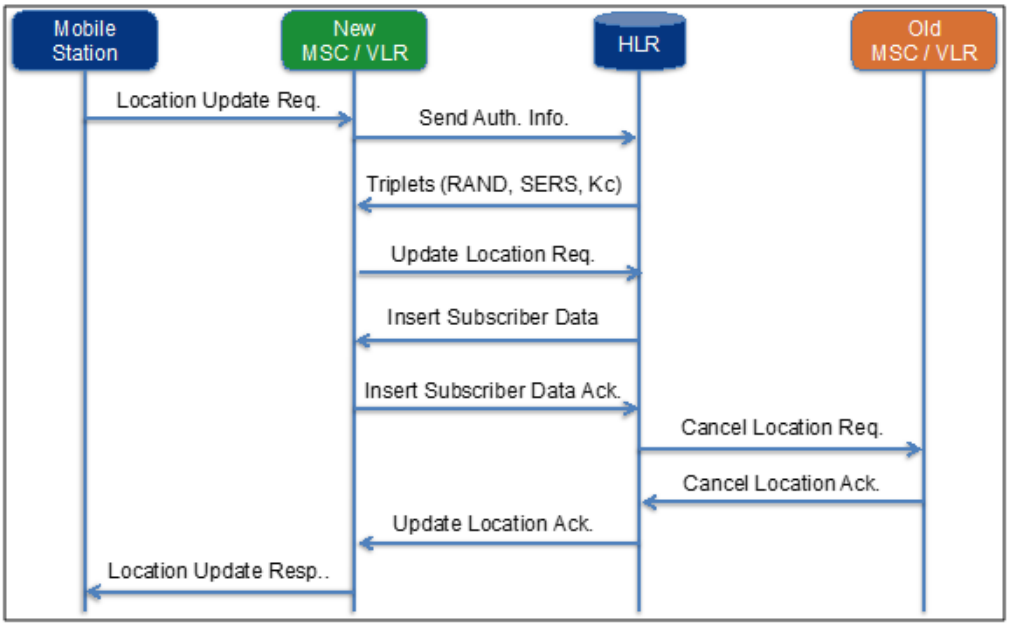
Upon proper authentication the MSC sends an Update Location Request to the HLR; indicating that the NEW MSC is the true location of the subscriber and that the HLR should use this location in future communications with the subscriber.

The HLR sends a copy of the subscriber information using the Insert Subscriber Data to the MSC – the MSC acknowledges its receipt with an Insert Subscriber Data Acknowledgement message.

The HLR then initiates a Cancel Location sequence with the previous serving MSC.

The HLR then sends an Update Location Acknowledgement to the new MSC. This is used to inform the new MSC that it is now considered the serving MSC for the subscriber and that the network portion of the Update Location is complete.

The New MSC sends a Location Update Response to the Mobile station completing the Update Location process.



GSM Update Location Call Flow

3.3.3.1 Purpose of Attack:

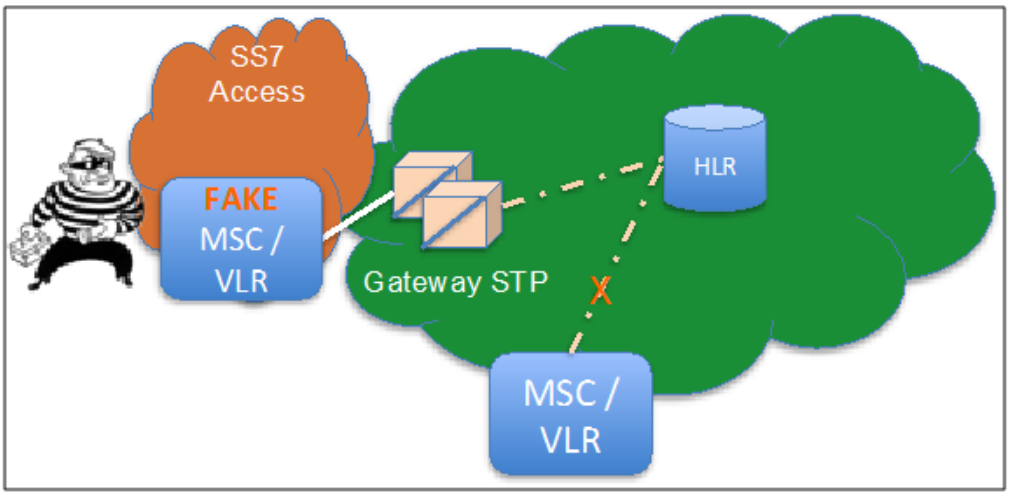
Interrupt the subscriber's service:

- Stop subscriber from receiving incoming calls
- Stop subscriber from receiving text messages

3.3.3.2 Requirements For Attack:

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. IMSI of target subscriber (Obtained in Threat 3.3.1)
4. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)
5. Address of subscribers HLR (Obtained in Threat 3.3.1)
6. Address of Fake MSC/VLR – attacker can make it up

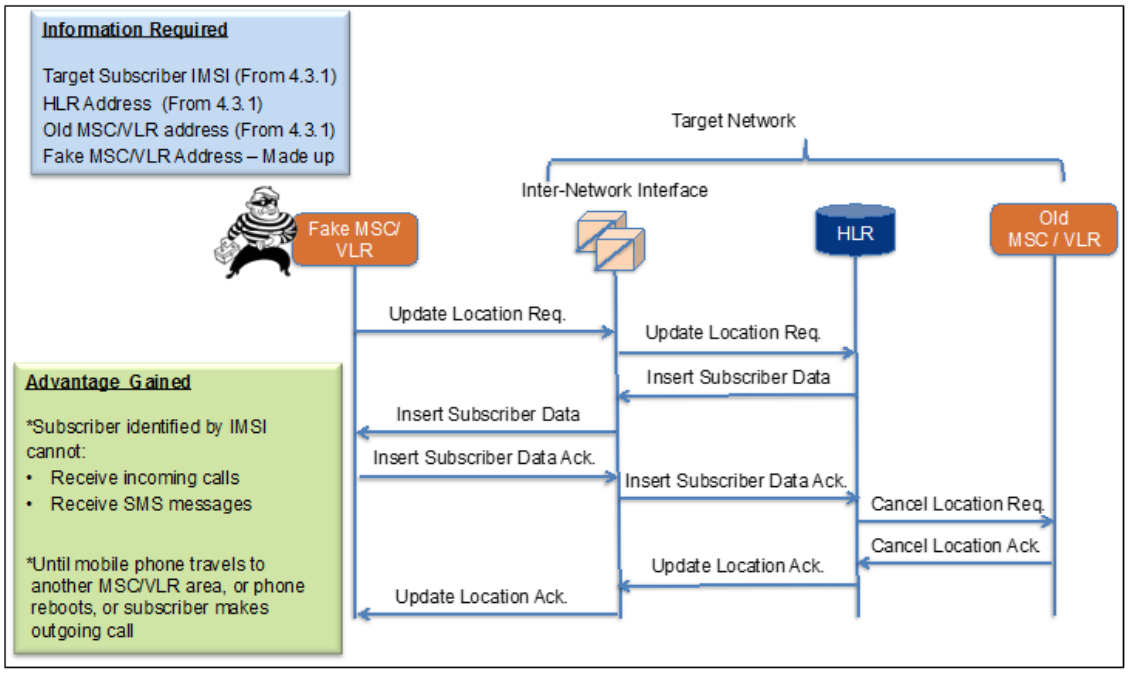
The premise for this attack is -- the intruder will pose as an MSC/VLR and send MAP-Update-Location- (UL) Request message directly to the subscribers HLR. Once the Update Location procedures are complete the Subscriber will not be able to receive incoming messages or calls until they move to another MSC/VLR or reboot the phone or place an outgoing call.



Threat Setup

3.3.3.3 Attack Call Flow:

This scenario uses the network portion of the Update Location Procedure. The intruder acting as a Fake New MSC sends an Update Location Request to the HLR. The HLR responds with the Subscribers information in an Insert Subscriber Data Message. This information will be stored in the VLR for future reference. The intruder then acknowledges the subscriber data receipt with a Insert Subscriber Data Acknowledge message. The HLR then initiates the cancel location sequence with previous serving MSC. Once this procedure is completed the HLR sends an Update Location Acknowledgement to the intruders Fake MSC. All subsequent incoming calls to the subscriber will be sent to the Fake MSC resulting in an interruption in incoming text messages and voice calls. This condition will continue until the subscriber reboots their phone, places an outgoing call or moves to a new MSC.



Disruption of Subscribers Availability Call Flow

3.3.3.4 Result of Attack:

Since the intruder was able to insert the Fake MSC/VRL in the call flow of messages toward the target subscriber – the subscriber will not receive any incoming calls or SMS messages until the subscriber reboots the mobile device, moves to a new MSC/VLR or places an outgoing call. The target subscriber will continue to have the indication on their mobile device that they are connected to the network.

3.3.4 Intercepting SMS Messages

This attack is the same as described in section 3.3.3. The difference in this attack is not to disrupt the subscriber's service, but the same scenario is used to intercept and use the data contained in the SMS messages.

3.3.4.1 Purpose of Attack:

Intercept subscribers SMS messages to:

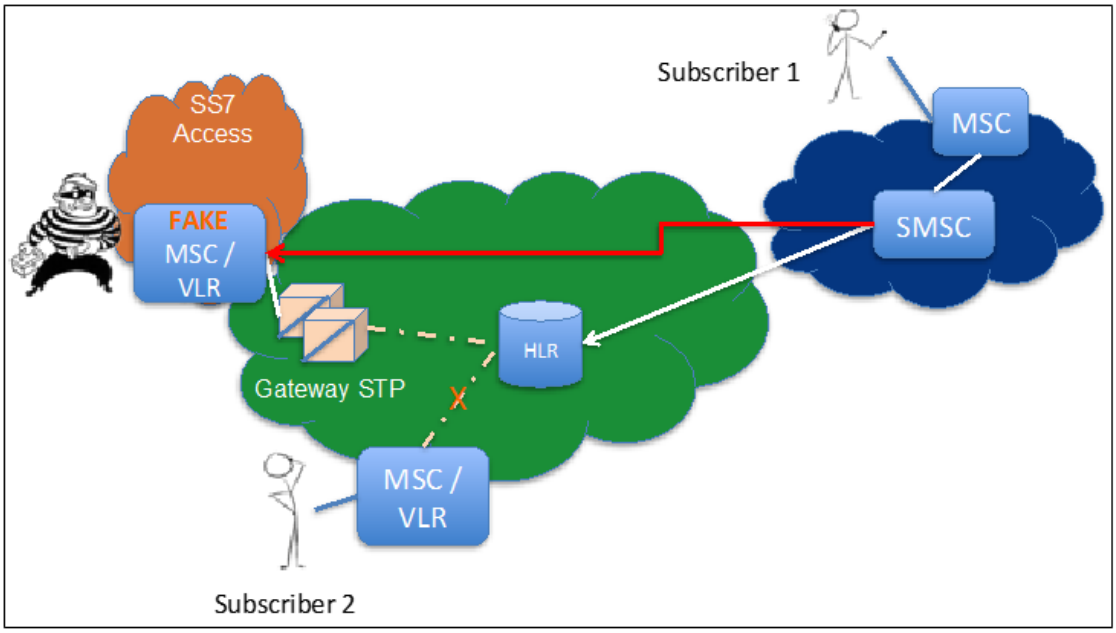
- Obtain Subscribers passwords.
- Be used in recovery and authorization of new passwords.

The intruder can use both of these to fraudulent financial gain.

3.3.4.2 *Requirements For Attack:*

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. IMSI of target subscriber (Obtained in Threat 3.3.1)
4. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)
5. Address of subscribers HLR (Obtained in Threat 3.3.1)
6. Address of Fake MSC/VLR – attacker can make it up

The premise for this attack is -- the intruder will pose as an MSC/VLR and send MAP-Update-Location- (UL) Request message directly to the subscribers HLR. Once the Update Location procedures are complete the intruder will capture the Subscribers SMS messages.



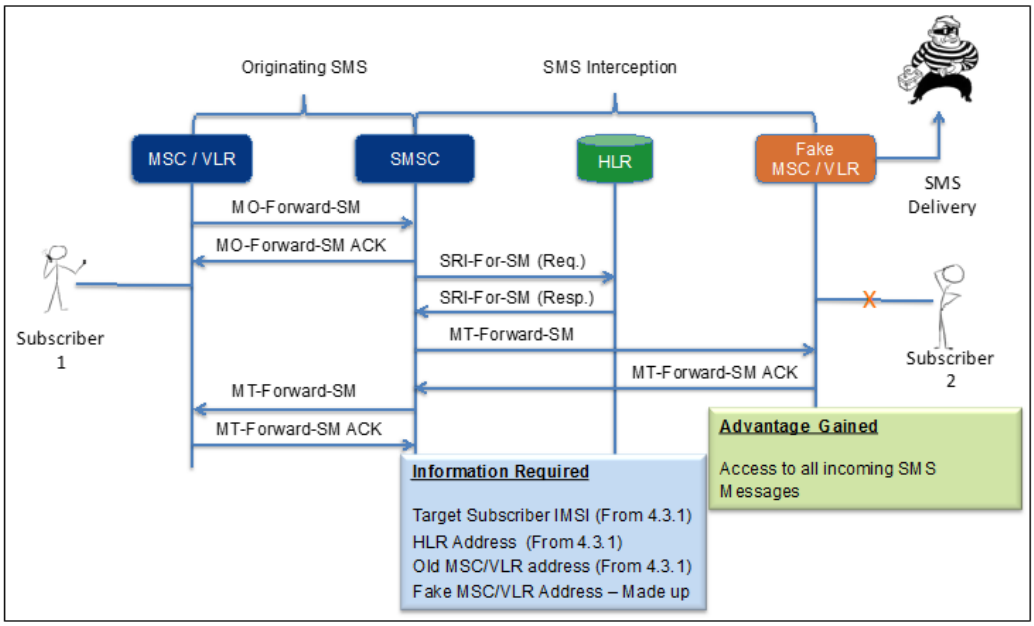
Threat Setup

3.3.4.3 *Attack Call Flow:*

This attack is an extension to the attack described in 3.3.3 where the intruder poses as a MSC/VLR. The fake MSC/VLR sends Update Location to the HLR to have its address in the database as the serving MSC/VLR. This part of the call flow was discussed in section 3.3.3.3.

Once the Update Location procedures are complete normal SMS delivery message flow occurs:

1. The Mobile Originating messages are sent from the originating subscribers MSC/VLR to its associated SMSC.
2. The SMSC then queries the HLR for the location of the terminating subscriber using the SRI-For-SM (Req.) message.
3. The HLR responds with SRI-For-SM (Resp.) message containing the current location of the terminating subscriber.
4. The SMSC uses the MT-Forward-SM to send the SMS message to the terminating MSC/VLR that in this case is the "Fake MSC/VLR" created by the intruder.
5. The "Fake MSC/VLR" responds with the appropriate MT-Forward-SM ACK. This final sequence provides the feedback to the originator that the message was received by the recipient, however, in this case the intruder – not the intended subscriber.



Interception of Subscribers SMS Messages Call Flow

3.3.4.4 Result of Attack:

Since the intruder was able to insert the Fake MSC/VRL in the call flow of messages toward the target subscriber, all incoming SMS

messages will be sent to the Fake MSC/VLR and can be used by the intruder.

Additional intruder steps can be added to this scenario to:

a. Reregister the terminating subscriber to the original MSC/VLR so the target subscriber gets SMS message as well.
b. Reregister the terminating subscriber to the original MSC/VLR – then the intruder sends the target subscriber an altered message.

3.3.5 Manipulation of USSD Request

According to 3GPP's definition – "The unstructured supplementary service data (USSD) mechanism allows the MS user and a PLMN operator defined application to communicate in a way which is transparent to the MS and to intermediate network entities." USSD is currently being used for mobile prepaid, online banking and other financially sensitive applications. Fraud linked to USSD can cause severe financial impacts to subscribers, network operators, financial institutions and many others.

3.3.5.1 Purpose of Attack:

Fraudulently transfer funds.

3.3.5.2 Requirements For Attack:

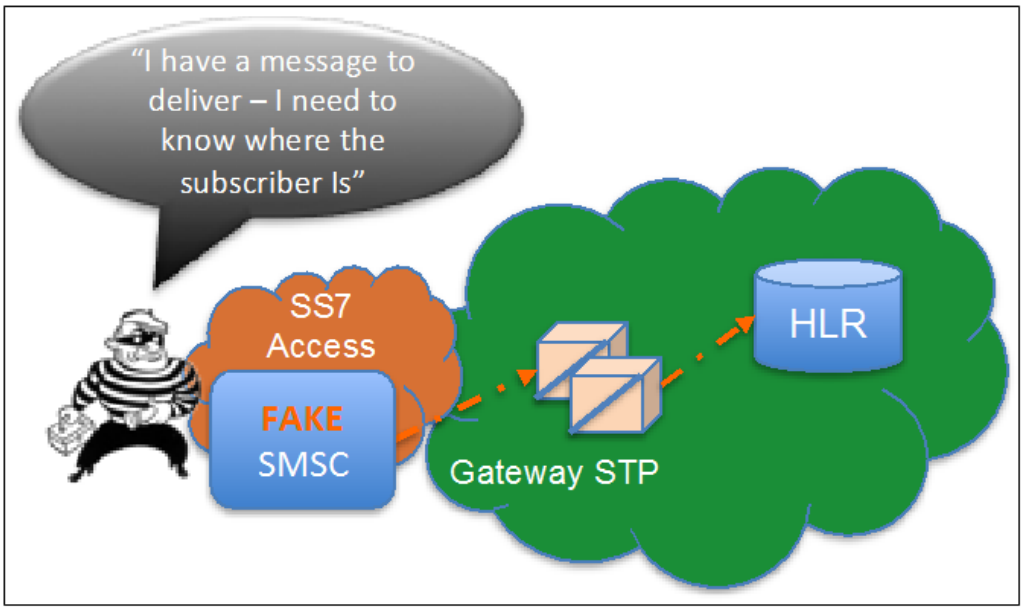
1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. MSISDN number of target subscriber

The premise for this attack is for the intruder to gain the information required (HLR address, Target Subscribers IMSI and Balance of Target Subscriber account) in order for the intruder to transfer target subscriber's funds to intruders account. This is a multi-stage attack.

Stage 1

Posing as a Fake SMSC the intruder gains valuable information including:

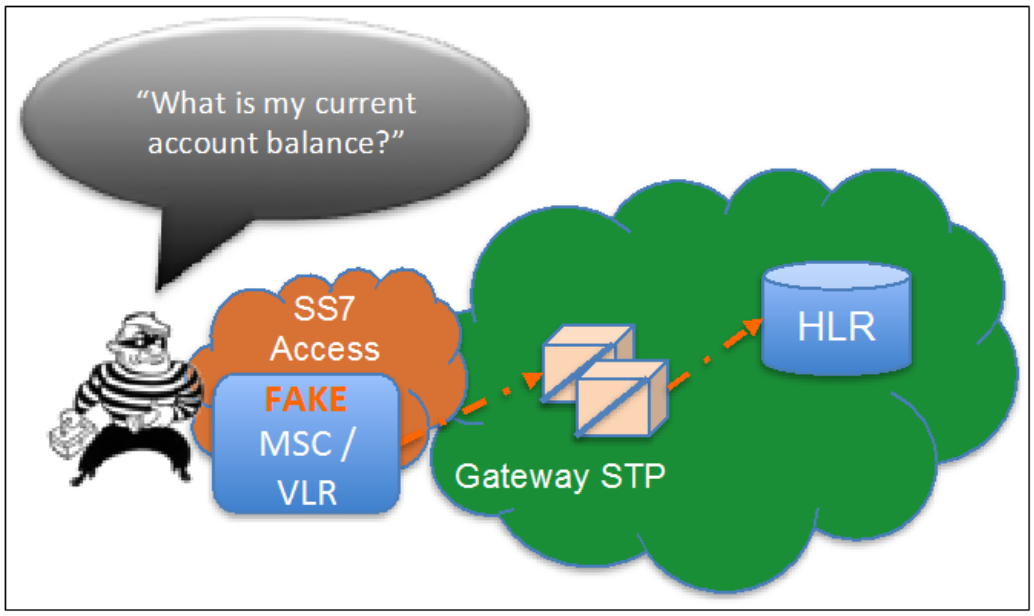
- The Global Title Address of the HLR
- The address of the MSC serving the Target Subscriber
- The IMSI of the Target Subscriber



Stage 1 – Threat Setup

Stage 2

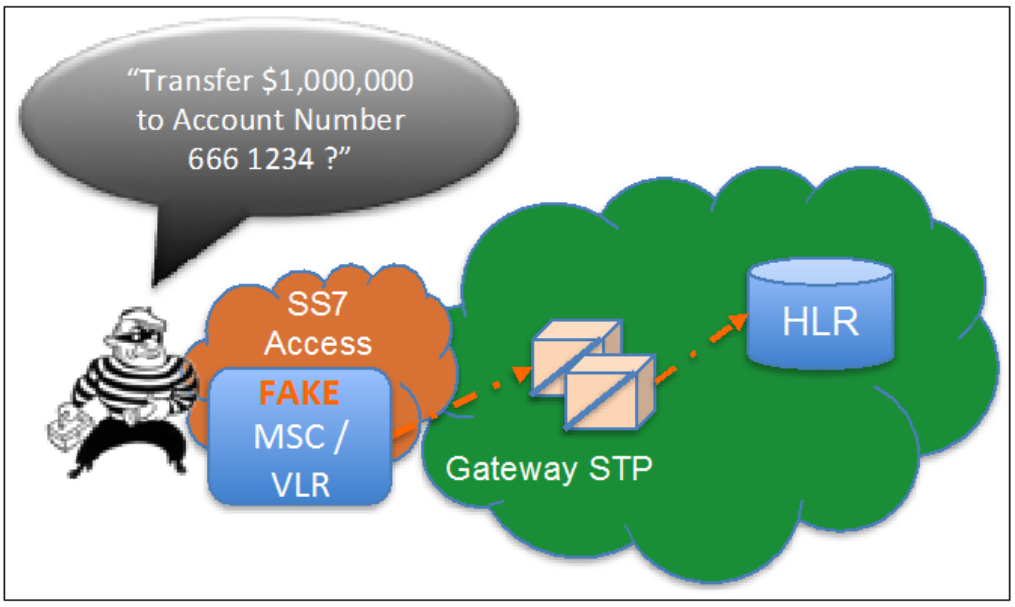
Posing as a Fake MSC/VLR acting on behalf of the subscriber, the intruder gains the target subscriber's account balance.



Stage 2 – Threat Setup

Stage 3

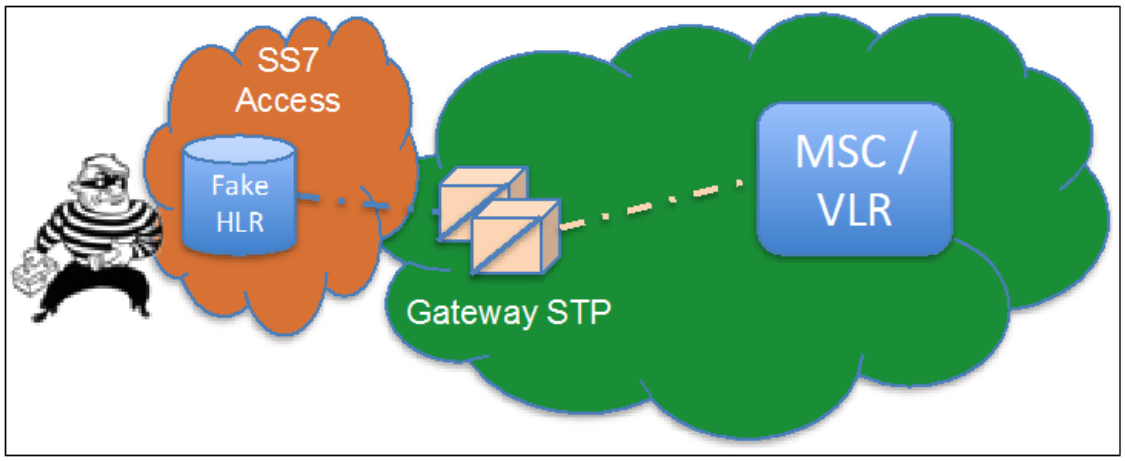
Posing as a Fake MSC/VLR on behalf of the target subscriber the intruder transfers funds from the target subscriber's account to his account.



Stage 3 – Threat Setup

Note: Normally the subscriber would receive an SMS indication the requested funds had been transferred. This indication could alert the

subscriber to the attack. However if the intruder coupled this attack with the one described in "Attack 3.3.4 Intercepting SMS Messages" the target subscriber would never receive the SMS message.



Threat Setup

3.3.5.3 Attack Call Flow:

In this scenario the intruder is posing as an SMSC wishing to obtain current location regarding a subscriber. The intruder would construct a Send Routing Information for SMS (SIR-For-SM) message and send it to the Gateway STP addressed for the HLR.

The HLR returns a SRI-For-SM Response that includes:

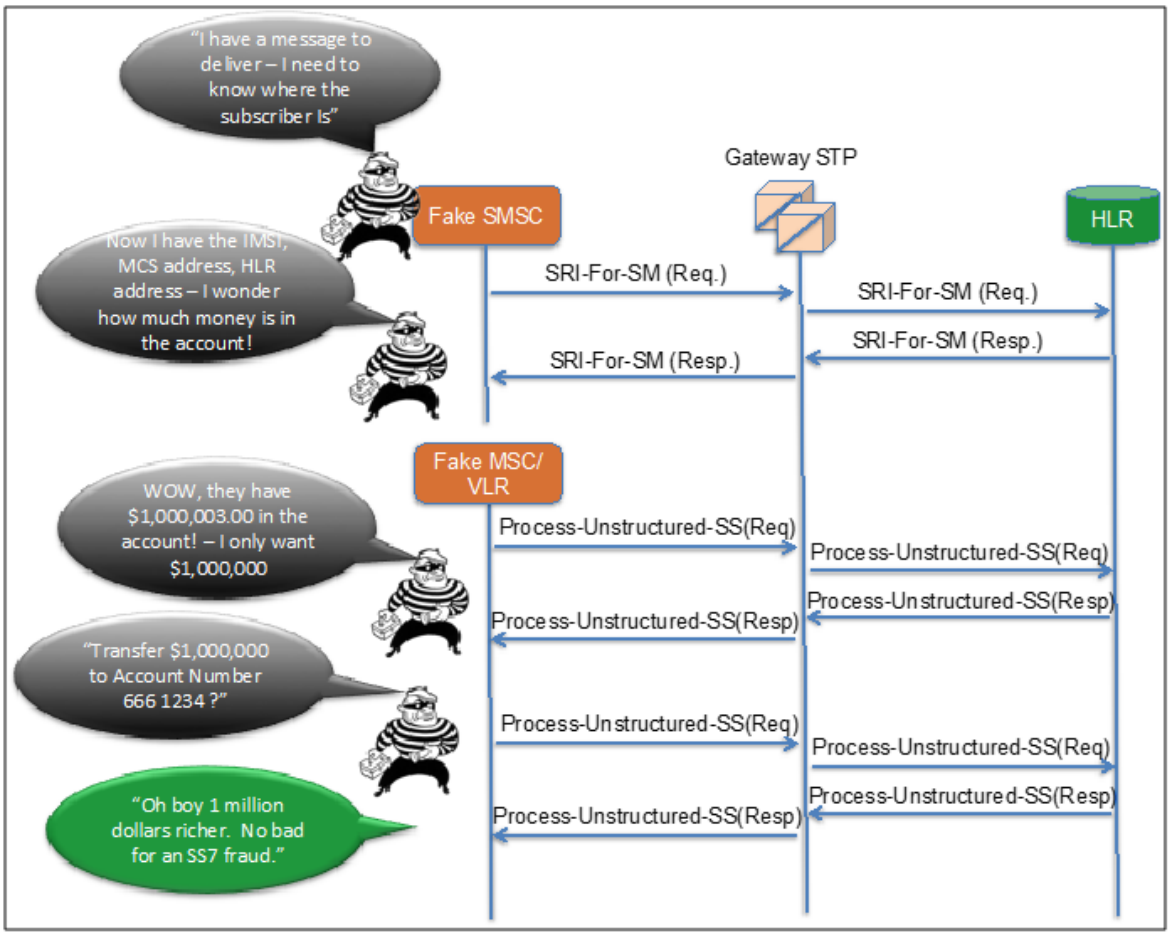
- The IMSI of the target subscriber
- The address of the current serving MSC/VLR
- The Global Title Address of the HLR

Armed with this information the intruder now poses as an MSC/VLR acting on the behalf of the target subscriber. The Fake MSC/VLR constructs a Process-Unstructured-SS (Req.) asking for the current account balance. This message is sent to HLR. The HLR responds with a Process-Unstructured-SS (Response) that includes the account balance requested.

The intruder now poses as an MSC/VLR acting on the behalf of the target subscriber. The Fake MSC/VLR constructs a Process-Unstructured-SS (Req.) asking the transfer of funds to the account

provided in the message.. This message is sent to HLR. The HLR responds with a Process-Unstructured-SS (Response) that includes the confirmation that the process has been completed.

Note: Normally the subscriber would receive an SMS indication the requested funds had been transferred. This indication could alert the subscriber to the attack. However if the intruder coupled this attack with the one described in "Attack 3.3.4 Intercepting SMS Messages" the target subscriber would never receive the SMS message.



USSD Manipulation Call Flow

3.3.5.4 Result of Attack:

The intruder was able to gain the following information:

1. Address of serving MSC/VRL
2. Address of HLR

3. IMSI of Subscriber
4. Account balance in target subscriber's account

The intruder moved funds from the target subscriber account to their own account.

3.3.6 Manipulation of Subscribers Profile in VLR

Any time an intruder has access to the subscriber identity (MSIDN,IMSI) the address of the serving MSC/VLR and the format of the subscriber profile they can alter billing routing allowing:

3.3.8.1. Disruption of the subscriber service

3.3.8.1. The use of the subscriber's mobile station to make fraudulent calls.

3.3.6.1 Purpose of Attack:

This attack is to use a fake subscriber profile to perform financial fraud, disrupt subscriber service, or to set up intrusive interception in an additional attack.

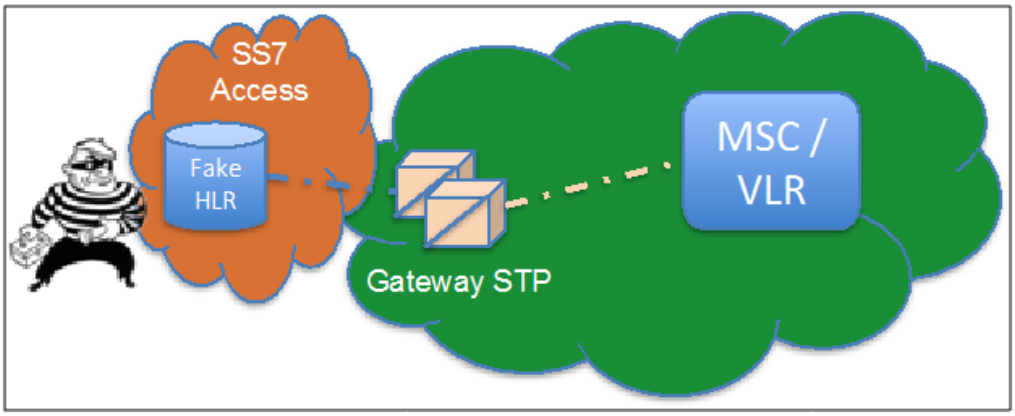
3.3.6.2 Requirements For Attack:

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. Subscriber Number (MSISDN)
4. IMSI of target subscriber (Obtained in Threat 3.3.1)
5. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)

Note: After receiving the subscriber profile information from the attack detailed in 3.3.3 the attacker understands the target subscribers profile information received for the HLR.

The premise for this attack is -- the intruder will pose as an HLR and send a fraudulent subscriber profile to the serving MSC/VLR invoking intruder desired services. These services can include:

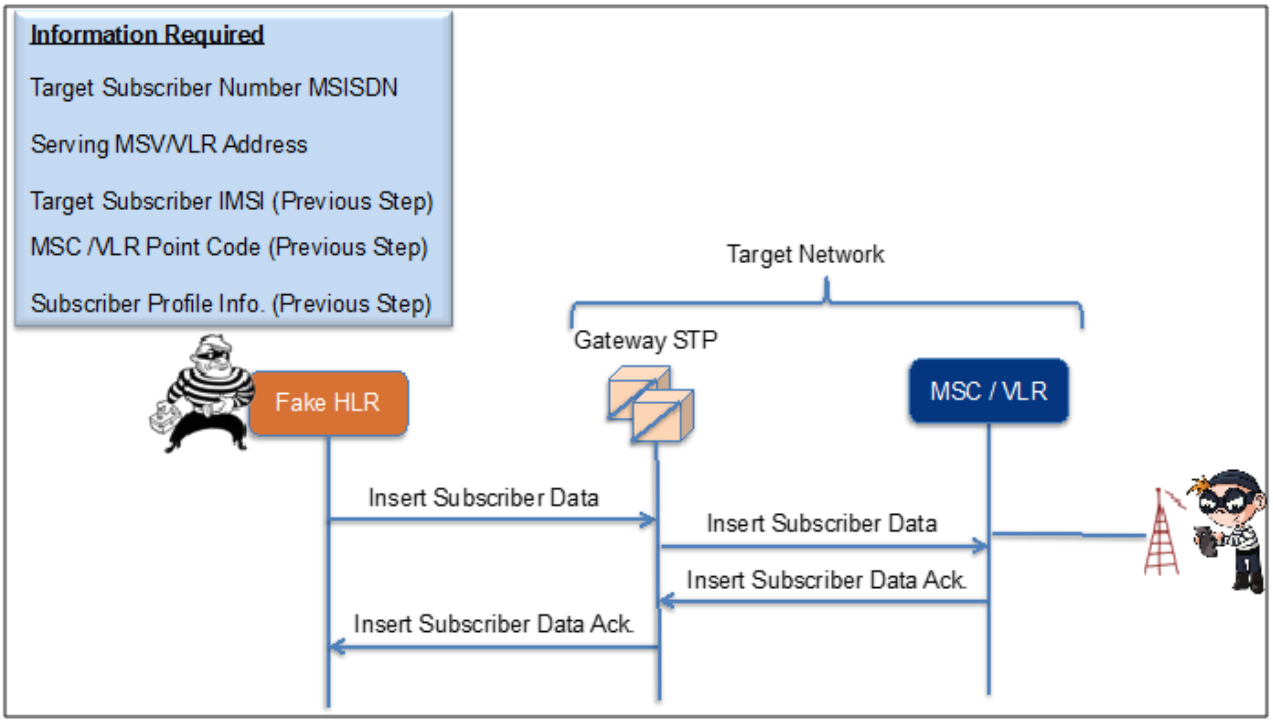
- Bypassing billing services
- Turning on or off call forwarding
- Barring calls to the target subscriber
- And many, many more



Threat Setup

3.3.6.3 Attack Call Flow:

In this scenario the intruder is posing as an HLR sending a fake subscriber profile to the MSC.VLR to affect calling, billing or other subscriber parameters. The intruder posing as an HLR sends an Insert Subscriber Data Message to the MSC/VLR including the fraudulent subscriber profile parameters. Once the Insert Subscriber Data Message is received by the MSC/VLR it responds to the Fake HLR with a Insert Subscriber Data Ack. Message. This message tells the intruder that the process is complete and fraudulent calls can then be made.



Manipulation of Subscriber Profile in VLR Call Flow

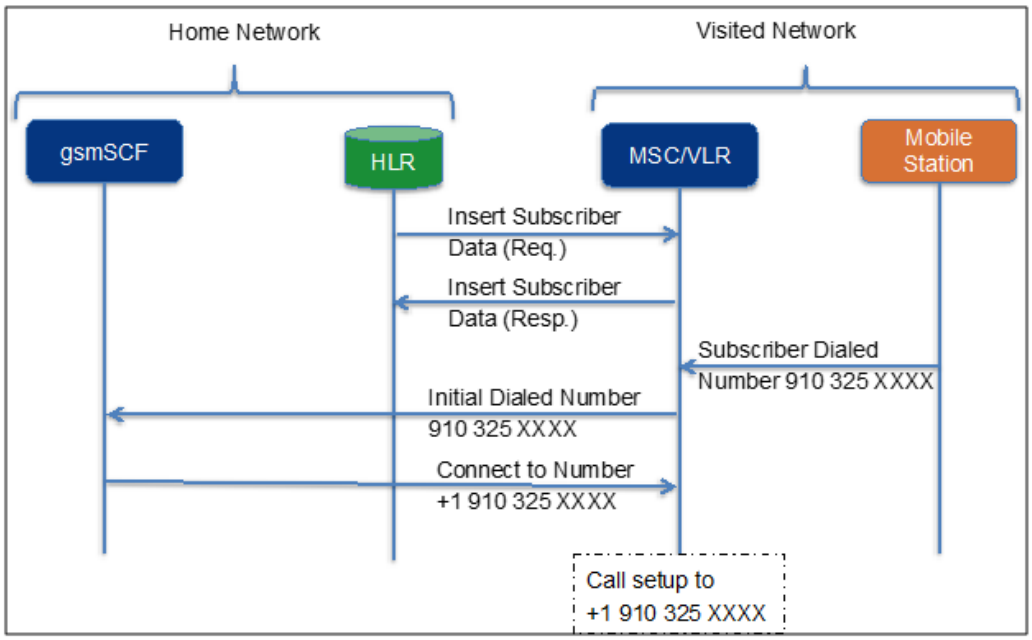
3.3.6.4 Result of Attack:

- The intruder working in concert with a rogue subscriber can place calls bypassing billing.
- The Intruder can use the attack to disrupt the subscriber's service.
- The intruder can use activate call forwarding in this attack as a step toward a Man In the Middle attack -- see the Threat described in 3.3.8

3.3.7 Intercepting and Redirecting Outgoing Calls with CAMEL Application Part (CAP)

Customized Applications for Mobile networks Enhanced Logic Application Part (CAP) is a protocol and logic that allows network operators to define services over and above the standard Global System for Mobile communications (GSM) and Universal Mobile Telecommunication Systems (UMTS) standard services. The CAMEL logic and network is based on the SS7 Intelligent Networks (IN) used in wireline networks. One of the many services typically using CAMEL is Mobile Prepaid service. The GSM Service Control Function (gsmSCF)

implements the CAMEL logic. The gsmSCF is usually located in the subscriber's home network.



CAMEL Dial-Plan Modification

Purpose of Attack:

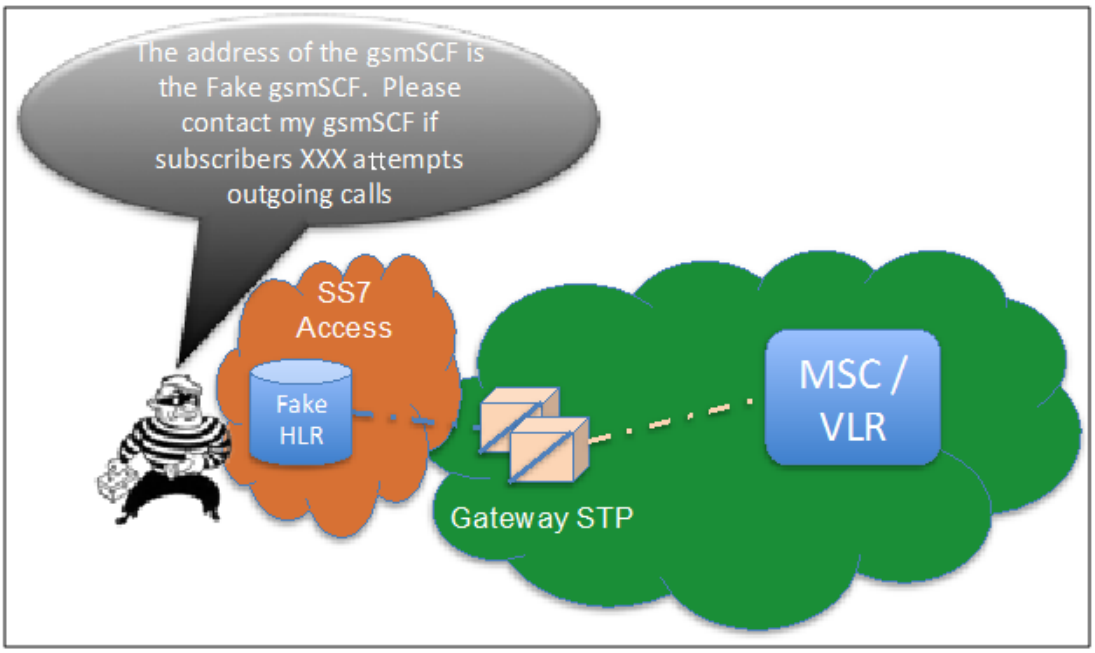
This attack is used to intercept a subscribers outgoing call for the purpose of eavesdropping, including listening and or recording of conversations.

Requirements For Attack:

1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. Equipment for bridging and recording calls
4. Target Subscriber Number (MSISDN)
5. IMSI of target subscriber (Obtained in Threat 3.3.1)
6. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)

Stage 1

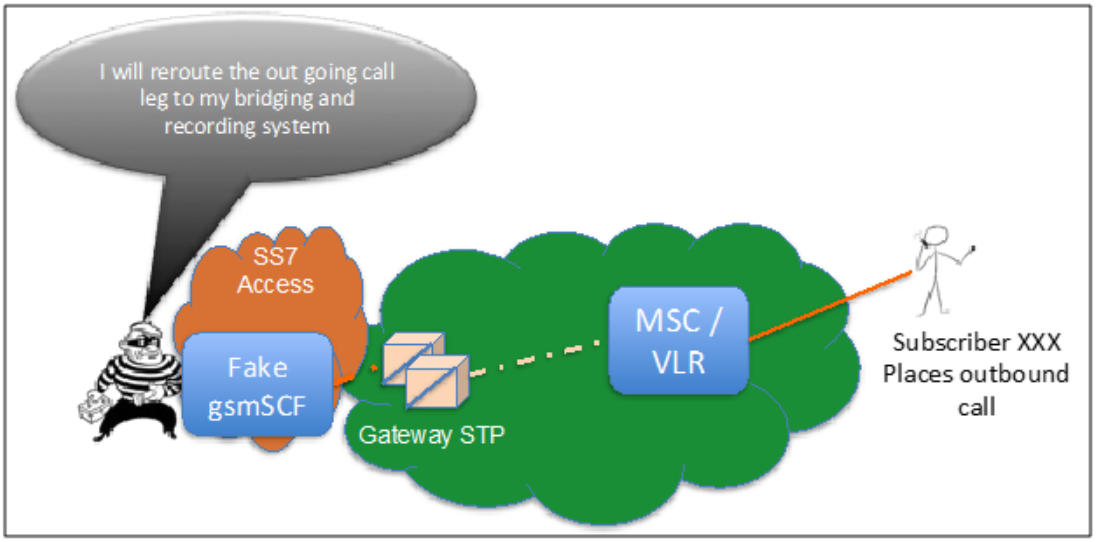
Posing as a Fake HLR acting on behalf of the subscriber has the address of his Fake gsmSCF placed in the VLR. Also the VLR is instructed to contact the Fake gsmSCF while the target subscriber starts to initiate a call.



Stage 1 Threat Setup

Stage 2

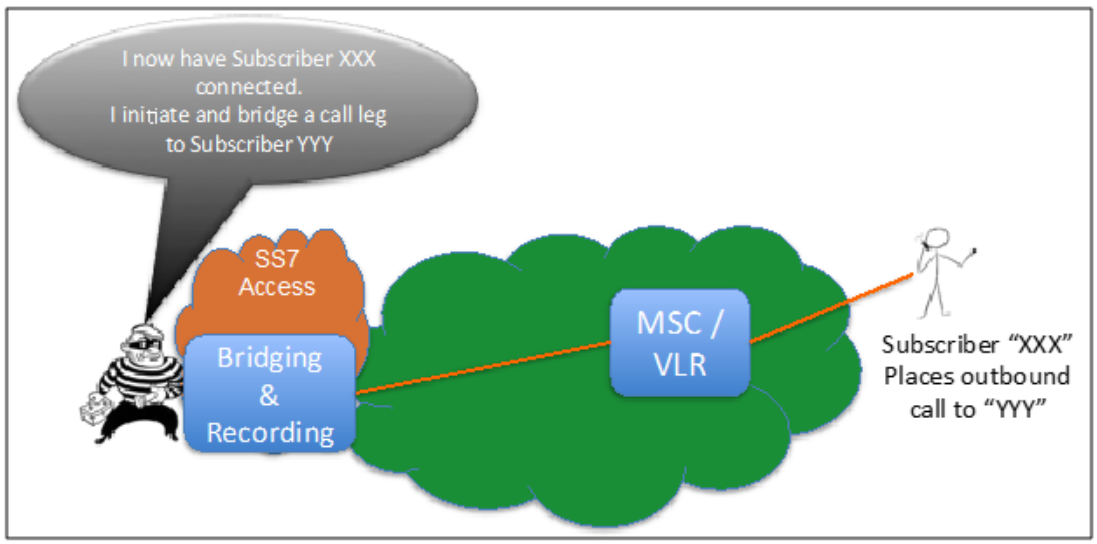
Posing as aFake gsmSCF, the intruder receives a call request from the MSC/VLR acting on behalf of subscriber “XXX” to call “YYY”– the Fake gsmSCF instructs the MSC/VLR to place the call to his eavesdropping system (“ZZZ”) instead.



Stage 2 Threat Setup

Stage 3

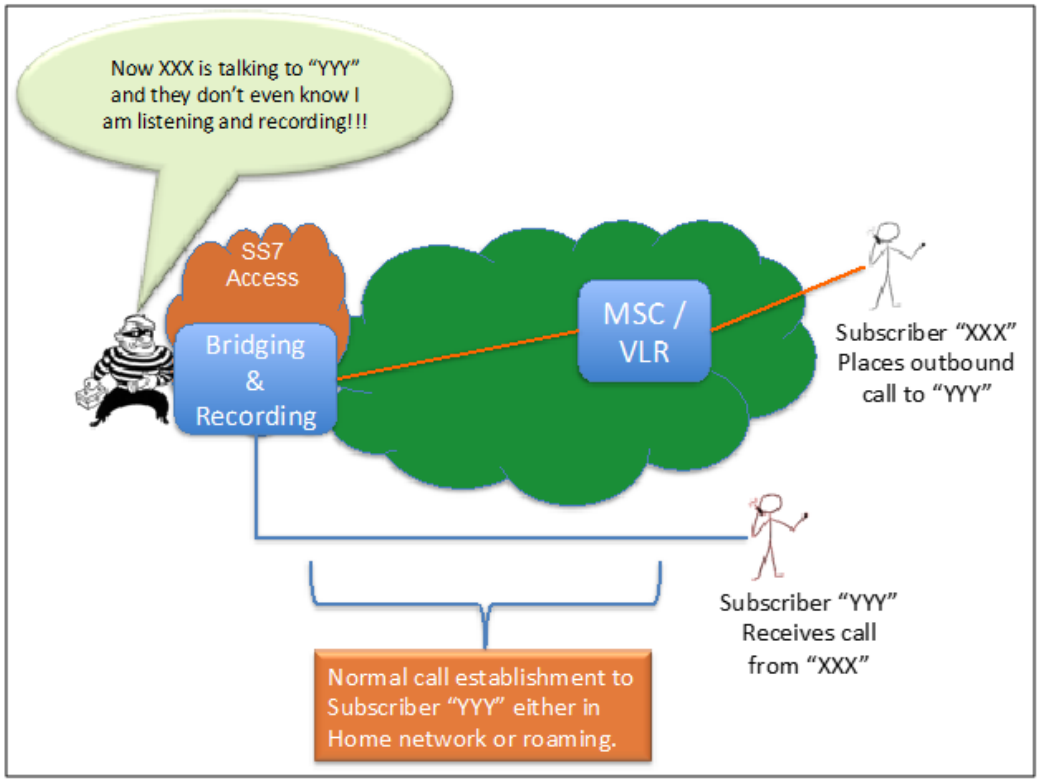
Posing as a Bridging and recording system the intruder receives the call from subscriber “XXX”. The intruder places a call to the original called subscriber (“YYY”).



Stage 3 Threat Setup

Threat Setup Completion

The intruder then bridges these two calls together and is able to listen to and/or record the conversation.



Threat Setup Completion

3.3.7.1 Attack Call Flow:

This multistage threat will allow the intruder to intercept outgoing calls from a subscriber, place a call to the original CALLed subscriber; then bridge the two calls together and listen in or records the calls.

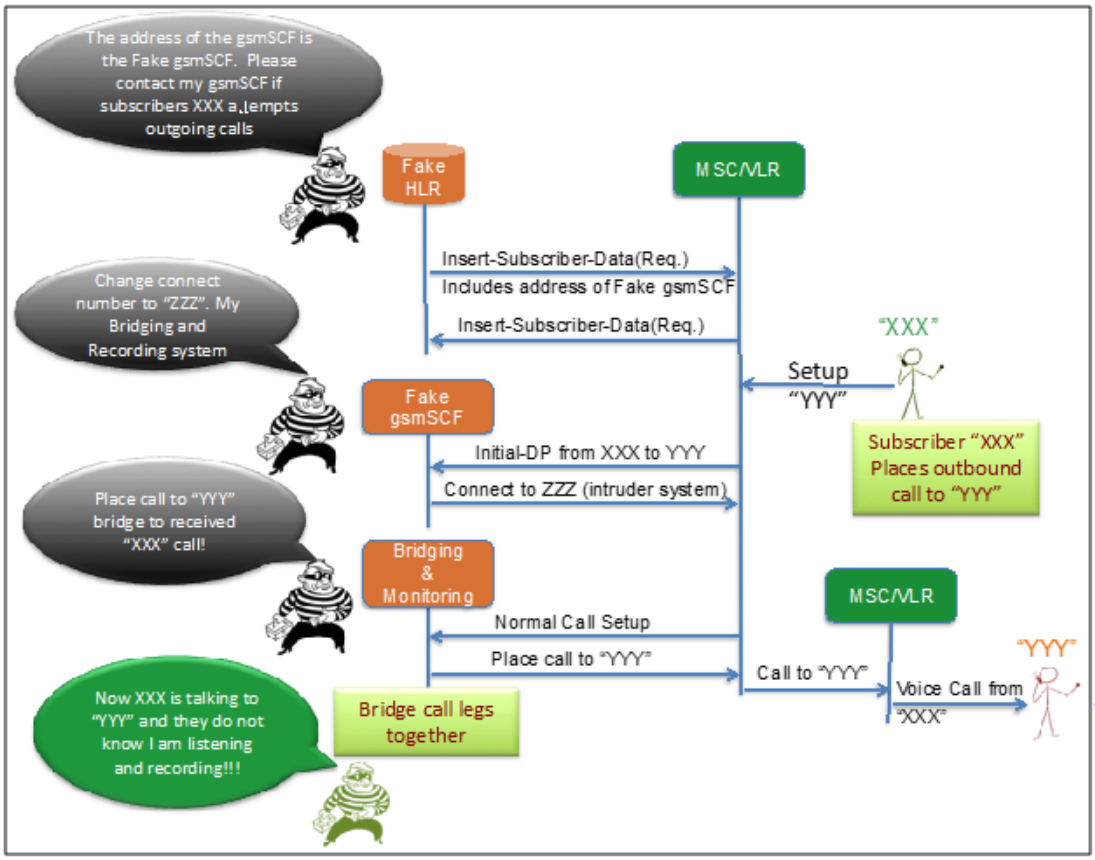
In the first stage the intruder poses as a Fake HLR. The Fake HLR uses the Insert-Subscriber-Data Request to inform the MSC/VLR it should send an indication to the Fake gsmSCF when the target subscriber (XXX) starts to initiate a call. The CAMEL protocol should be used to provide this indication. The Insert-Subscriber-Data Request will contain the address of the Fake gsmSCF and the IMSI of the target subscriber.

In the second stages of this threat the Fake gsmSCF receives the Initial-DP (Decision Point) message from the VLR indicating the target

subscriber is placing a call. This message contains all relevant call information including the CALLing and CALLed subscriber number information. The Fake gsmSCF responds with a Connect Message. The Connect Messages indicates to the MSC that it should send the call to "ZZZ" rather than to the original CALLed subscriber (YYY).

In the next stage the MSC/VLR uses normal call setup procedures to connect the call to ZZZ, which is the intruder's bridging and recording system. Upon receipt of the call from XXX the intruder connects this call leg to the bridging and recording system. The intruder then places a call to YYY, connects it to the bridging and recording system and bridges the two call legs together.

The completion of the previous stages allows the intruder to both record and listen to the conversation between XXX and YYY without their knowledge.



Intercepting and Redirecting Outgoing Calls with CAMEL Application Part (CAP)

3.3.7.2 Result of Attack:

- The intruder is able to redirect outgoing call to an eavesdropping system without the knowledge of the originating party
- The intruder is able to place an outbound call to the original called subscriber.
- Intruder is able to bridge the two calls together and record them without the knowledge of either subscriber.

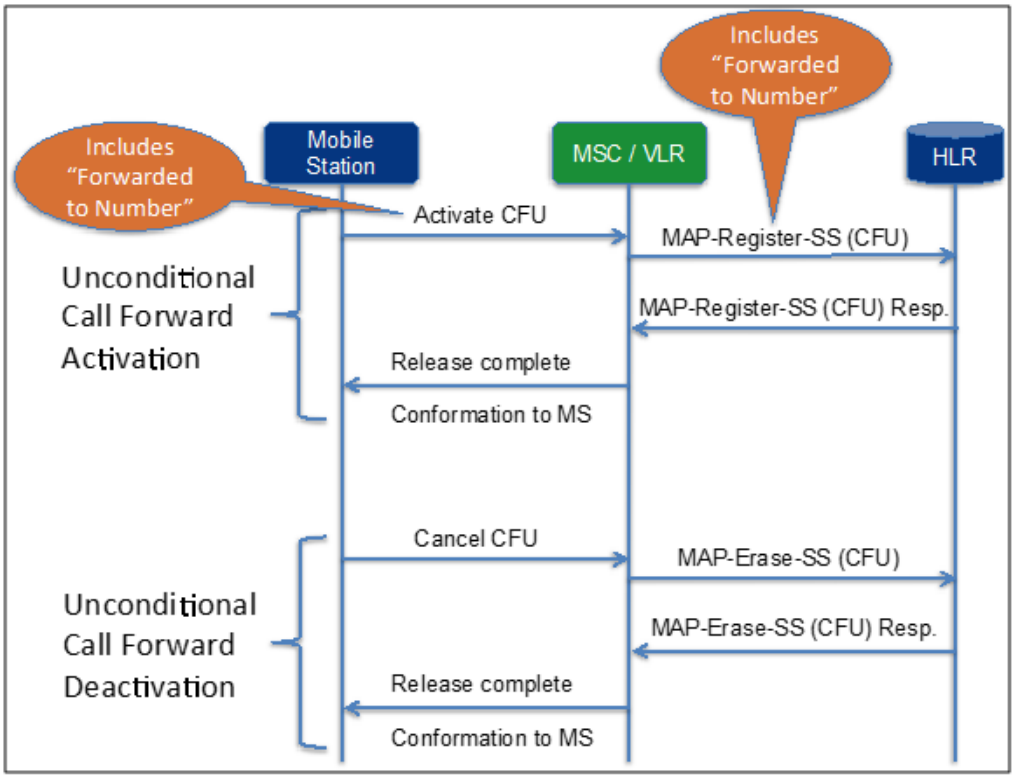
3.3.8 Redirecting Incoming Calls

The threats described in this section use the subscriber supplemental service -- call-forwarding feature. The normal call flow for call forwarding activation and deactivation is shown in the following graphic. In this case the mobile subscriber signals their desire to either activate or deactivate call forwarding using a key sequence – usually * code plus two digits. The serving MSC receives this indication and builds a MAP-Register-SS (CFU) message including

the “Forward to Number” and sends this message to the HLR. The HLR responds with a MAP-Register-SS (CFU) response message. This acknowledgement is received by the MSC, which in turn sends an acknowledgment to the mobile station triggering the conformation tone to the user.

To deactivate call forwarding the user dials a * code plus two digits. The serving MSC receives this indication and builds a MAP-Erase-SS (CFU) message and sends this message to the HLR. The HLR responds with a MAP-Erase-SS (CFU) response message. This acknowledgement is received by the MSC, which in turn sends an acknowledgment to the mobile station triggering the conformation tone to the user.

Parts of the normal call forwarding procedure can be used by an attacker to insert themselves in the middle of a call for nefarious or other fraudulent purposes.



Unconditional Call Forward Activation / Deactivation message flow

3.3.8.1 Redirecting incoming calls for recording

Purpose of Attack:

This attack is used to place the intruder or the intruder devices in the middle of an incoming call so the conversation can be monitored or recorded.

Requirements For Attack:

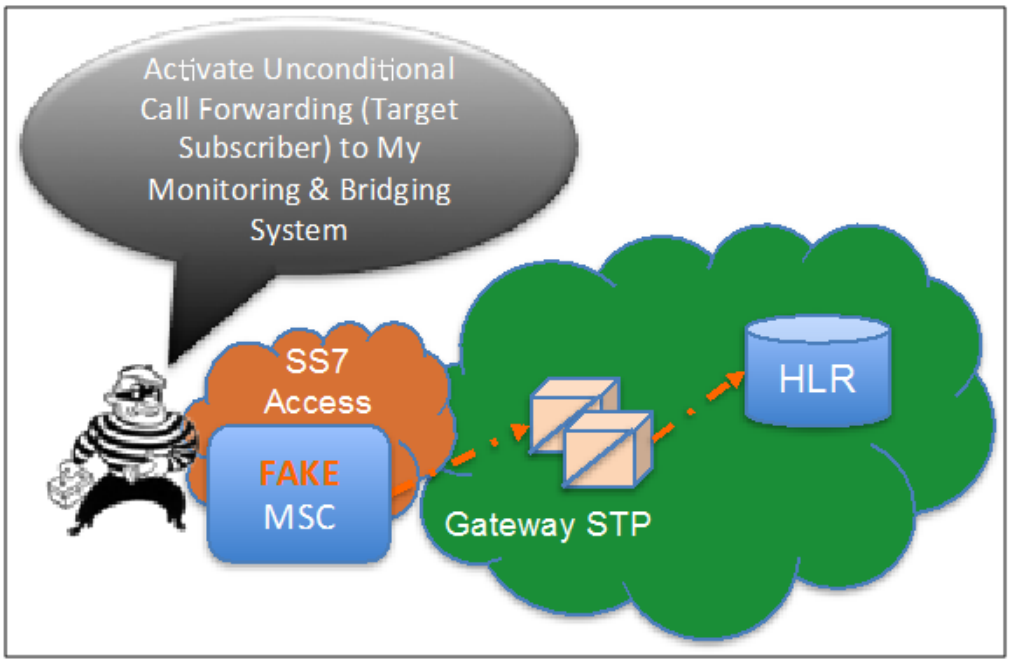
1. SS7 Network Access – fairly easy to obtain
2. SS7 message generation capability – open source and easy to obtain
3. Equipment for bridging and recording calls
4. Subscriber Number (MSISDN)
5. IMSI of target subscriber (Obtained in Threat 3.3.1)
6. Address of Serving MSC/VLR (Obtained in Threat 3.3.1)
7. Address of HLR (Obtained in 3.3.1)

Note: This is a multi-stage attack and relies on information gained in other attacks. Only the stages used directly in this attack will be discussed in this section.

The premise for this attack is:

Stage 1.

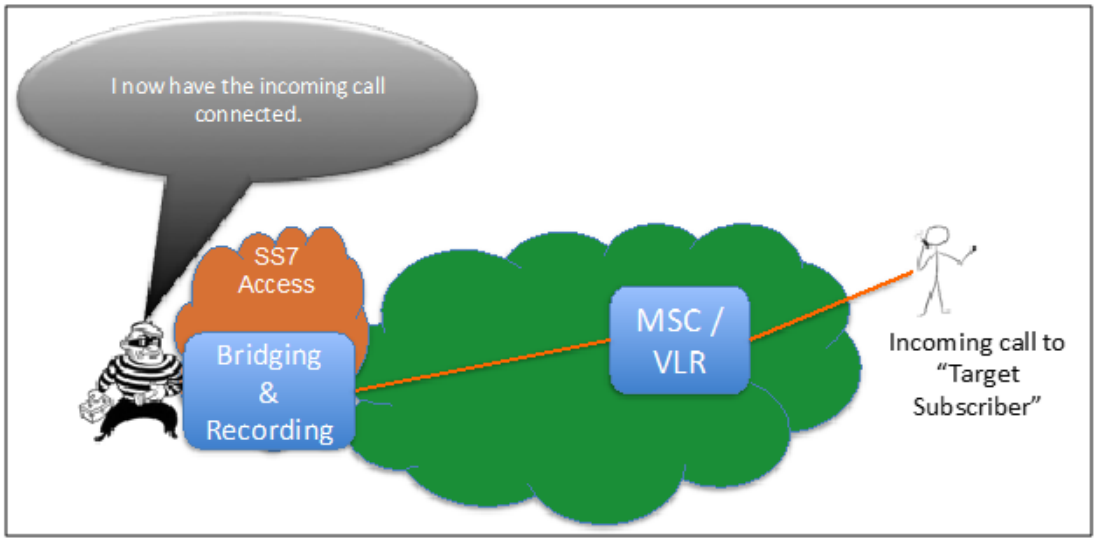
The intruder posing as the serving MSC for the target subscriber will send the Call Forwarding information to the HLR. The "Forward to Number will be the number for the Bridging and Recording Equipment.



Threat Setup Stage 1

Stage 2.

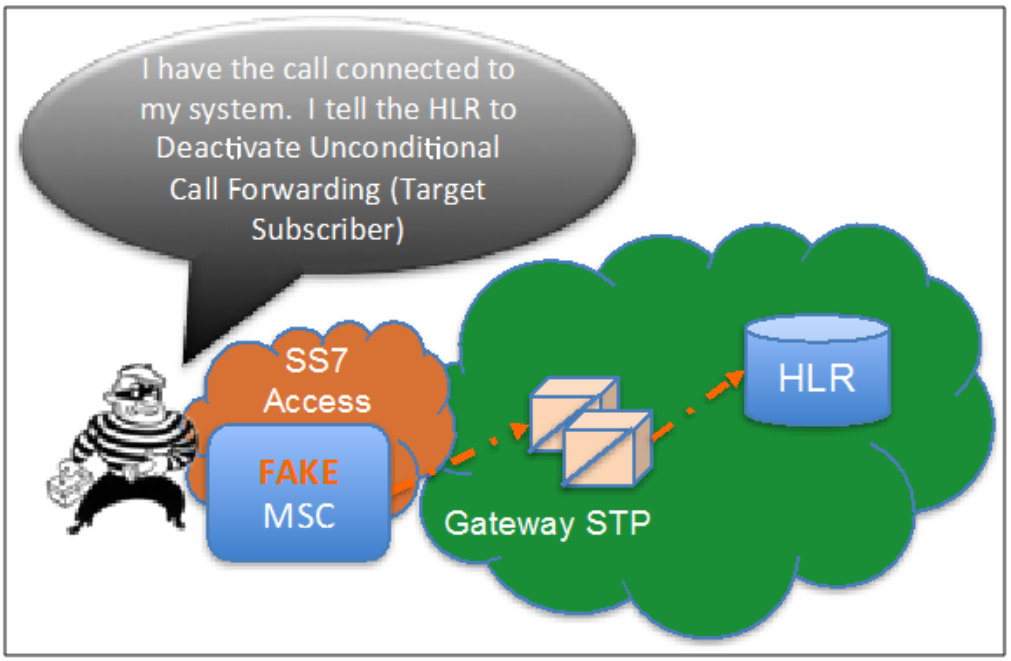
The intruder receives a forwarded call from the target subscriber. This call is connected to the intruder's bridging and recording system.



Threat Setup Stage 2

Stage 3.

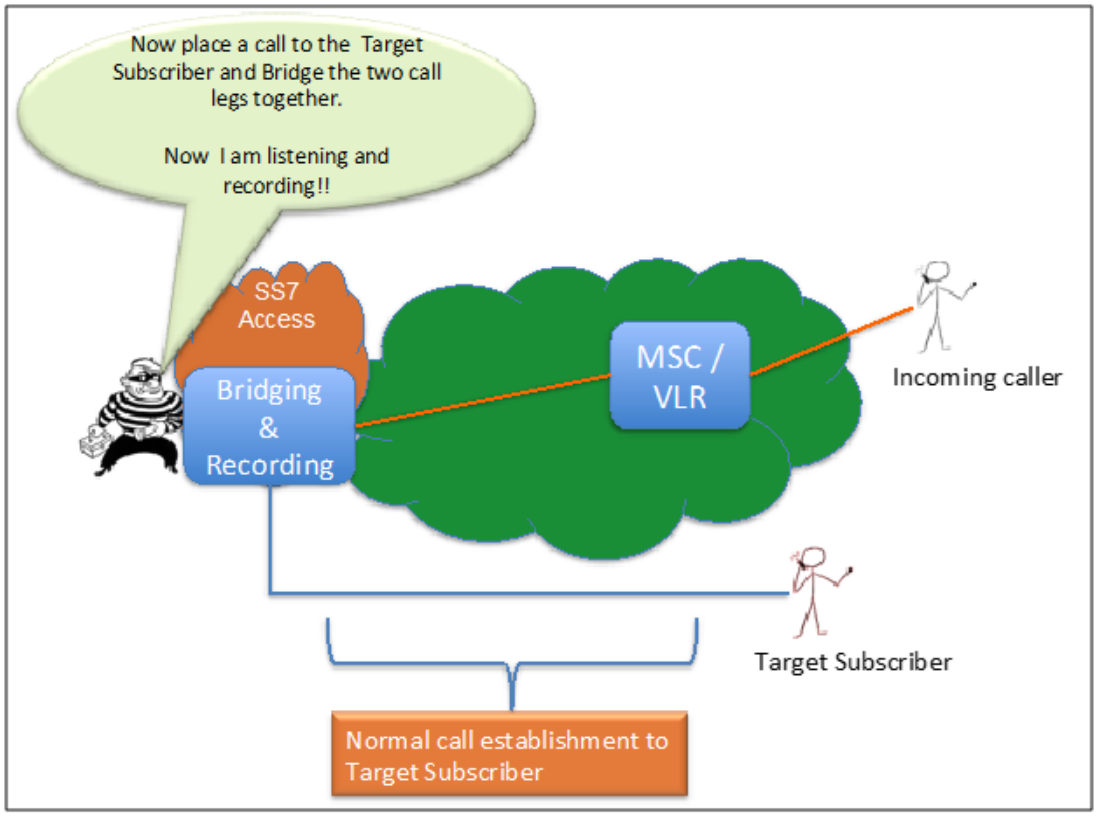
The intruder, acting as the serving MSC/VLR for the target subscriber, sends Cancel Call Forwarding information to the HLR.



Threat Setup Stage 3

Stage 4.

The intruder will place a call to the original CALLed party (Target Subscriber) and bridge the two call legs together through their monitoring and bridging system.



Threat Setup Stage 4

Attack Call Flow:

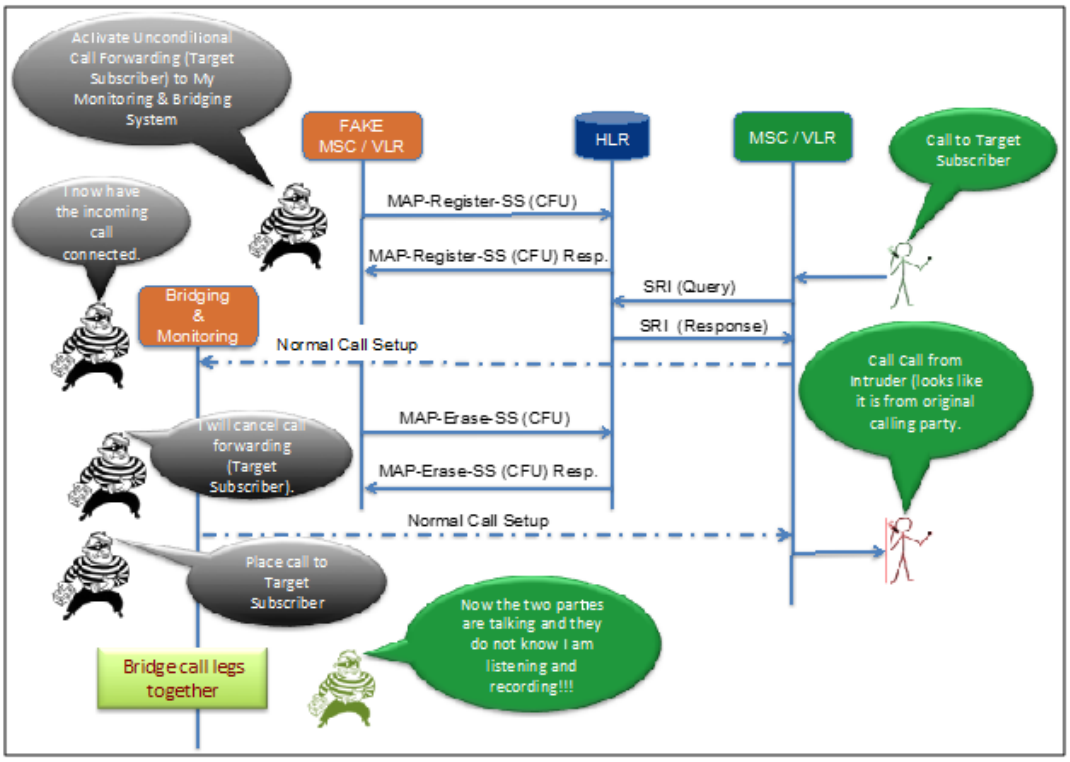
To start this scenario the intruder poses as the Fake Serving MSC/VLR. The intruder sends a MAP-Register-SS (CFU) to the HLR of the target subscriber. This message indicates that the target subscriber has call forwarded their phone unconditionally to the intruders Bridging and Monitoring system.

Upon placing a call (to the target subscriber) the originating party's MSC or Gateway MSC contacts the HLR of the target subscriber to get their current location. The HLR responds with the call forwarding information the intruder has inserted. The call is then routed to the intruders Bridging and Monitoring System.

When the intruder receives the call they use a MAP-Erase-SS (CFU) to cancel the call forwarding information for the target subscriber.

The intruder then places a call to the target subscriber and bridges the two call legs together using the Bridging and Monitoring System.

Now the intruder is in the middle of the call for bridging, monitoring, and recording.



Redirecting Incoming Calls for Eavesdropping

Result of Attack:

- The intruders can place themselves in the middle of a call.
- The intruders can use their position in the call to listen and/or record the conversation.

3.4 Conclusion

It is quite evident that the SS7 protocol and network implementation is open to intrusion and threats for both internal and external threats. Given the vast deployments of SS7 and the voluminous quantity of nodes that implement the SS7 protocol it is too late to implement changes to the protocol and nodal implementation of the protocol. Additionally the security threats are beyond Gate Screening capabilities of network based Signaling Transfer Points (STP). Given the severity of the security issues a need has arisen to implement intelligent, rules based systems that can monitor, develop rules and implement policies to stop or limit the impact of these attacks. These signaling firewalls will be the protection mechanism for the legacy-signaling network until it is totally replaced by LTE/EPC diameter based networks. This could be upwards of 20 years.

4. What to look for in a Signaling Firewall Solution

It seems evident that security in the SS7 network is and will continue to be a big issue. Being that SS7 is the mostly widely deployed signaling methodology in telecommunication history -- changing the protocol at this stage is out of the question. To solve the security issues intelligent security firewalls need to be implemented. These firewalls should address today's threats as well as have the flexibility to address new threats as they arise. The following items should be included in any security solution or security vendor.

4.1 MAP / CAMEL message monitoring

The first step to identifying any SS7 based security threat is monitoring the signaling message traffic. This traffic should be filtered and reported to the operator to alert them to potential threats. Since some of these threats are sporadic and low traffic threats the traffic monitoring should be continuous using real-time or near real-time methodologies. Since there can be quite a large volume of messaging most of which is normal and valid, a comprehensive set of filtering criteria need to be implemented to alert operators to potential threats. This filtering will reduce the amount of operator manual analysis required to identify threats.

4.2 Security threat rules definition and policy enforcement

At the heart of any SS7 security solution is the ability for operators to define rules to be enforced to stop security threats. The definition of rules need to encompass messaging at various levels of the SS7 protocol stack including: MTP3, SCCP, TCAP, MAP and CAP. The ability to develop rules should also include parameters within each protocol stack level. The policy enforcement engine portion of the rules system should provide the ability to Rate Limit, Modify, Drop or Log messages based on individual rules.

4.3 Experience in SS7 / SMS fraud solutions

Quite a few of the SS7 security threats begin with an intruders use of the SMS messaging to gain valuable subscriber and network information – it is

extremely important that any SS7 security vendor have both experience and solutions to address issues concerning SMS security and fraud.

4.4 System Diagnostics

When placing equipment/solutions into the mobile network it is extremely important that they have the ability to self-monitor and report anomalies to system administrators in the operations maintenance and administrations (OA&M) area. This system diagnostics should include hardware, software and any associated databases. Systems diagnostics should also report to the users when resources such processors, memory and disk storage should be added to the system to maintain optimum performance. The system diagnostics insures the services delivered to the operator and subscribers alike are maintained to network standards for reliability.

4.5 Fast, Scalable and Fault Tolerant

The system's hardware, software and database architectures must provide the operators with a solution that meets the real-time requirements of the telecommunications network. Also, these solutions must be able to organically grow to meet the demand of increasing numbers of subscribers and traffic on the network. Finally, these solutions should have fail-over mechanisms, replication and backup methodologies to maintain network standard system availability.

5. Cellusys Signaling Firewall Advantages

The Cellusys signaling firewall is a system that provides complete SS7 protection and traffic monitoring which enables an operator to detect and prevent different threats from occurring on the network. The Cellusys Signaling Firewall provides:

- Full control over Signaling stack from MTP3 to MAP
- Fine-grained filtering to prevent Signaling attack threats but allow valid messaging into the network
- Detailed reporting and alerting of issues
- Flexible pipeline architecture allowing additional modules to be quickly deployed to detect and prevent new attack vectors

i.e. verification of roaming subscriber's location before accepting messages from that location.

5.1 Signaling Firewall - Monitoring

Cellusys Signaling Firewall solution monitors and filters messaging traffic at all levels providing an efficient mechanism of identifying potential threats. This monitoring and filtering capability delivers the ability to quickly identify threats, define and implement rules to stop or minimize any subscriber or network harm these threats would cause.

5.2 Signaling Firewall – Policy Definition and Enforcement

Rules are defined in the firewall to enforce that the network is being used for legitimate purposes and not being abused for malicious intent. A rule is composed of the message parameter criteria and actions to take if matched. The first rule that matches a message is applied and no further rules are processed for that message.

The Cellusys Signaling Firewall solution allows the definition of rules on the SS7 protocol stack form MTP3 through MAP and CAMEL as follows:

- MTP

- SCCP
- TCAP
- MAP
- CAP

Once the rules are defined the policy enforcement engine analyses traffic according to the defined rules. In the event traffic matches a rule the following actions can be defined:

- Rate limit traffic matching a particular rule
- Allow the Message
- Modify the details of the message
- Drop the message
- Log the message

The rules system gives the operator a powerful system that will limit the exposure of subscribers and the rework to outside security threats.

5.3 System Diagnostics

The system diagnostics capabilities of the Cellusys Signaling Firewall solution provides operators with a comprehensive set of tools to monitor the health of the system and quickly pinpoint any portion that may need attention. The monitoring and diagnostics incorporates the ability to monitor clusters of servers providing system functionalities or individual server within a cluster. System resource monitoring provides the operator with timely data that can indicate when these resources need to be increased based on increased utilization or traffic. A graphical User Interface provides a quick visual indication of system health and performance.

5.4 Scalable and Fault Tolerant

The architecture of the Cellusys Signaling Firewall solution is designed to provide operators with a near-real-time, highly scalable fault tolerant solution to the SS7 security issues.

The Cellusys Security Firewall meets the stringent requirements of fault tolerance of telecommunication equipment but more especially it meets or exceeds the reliability standards for any solution providing or protecting operator revenues.

The Cellusys Security Firewall solution delivers the easiest to implement and highest degree of scalability available in the telecommunications industry. Cellusys scalability concepts provide a cost effective solution to today's security threats while allowing operators a flexible rules based system to address new threats as the arise.

6- Glossary

2G	Second Generation
3G	Third Generation
3GPP	Third Generation Project Partnership
AIN	Advanced Intelligent Services
ATI	Anytime Interrogation
C7	CCITT Seven
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CAP	Camel Application Part
CFU	Call Forward Unconditional
CGI	Cell Global Identity
EPC	Evolved Packet Core
GSM	Global System for Mobile Communications
gsmSCF	GSM Service Control Function
GTT	Global Title Translations
HLR	Home Location Register
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISUP	ISDN User Part
LAC	Location Area Code
LTE	Long Term Evolution
M2PA	MTP 2 Peer to Peer Adaption
M2UA	MTP 2 User Adaption
M3UA	MTP 3 User Adaption
MAP	Mobile Application Part
MAP-Erase-SS	MAP Erase Supplemental Service
MAP-Register-SS	MAP Register Supplemental Service
MCC	Mobile Country Code
MNO	Mobile Network Operator
MO-Forward-SM	MAP Mobile Originating Short Message Service
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International Directory Number
MTP 1	Message Transfer Part 1
MTP 2	Message Transfer Part 2
MTP 3	Message Transfer Part 3
PLMN	Public Land Mobile Network
PSI	Provide Subscriber Information
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service

SMSC	Short Message Service Center
SRI-For-SM	Send Routing Information for Short Message Service
SS7	Signaling System Seven
STP	Signal Transfer Point
SUA	SCCP User Adaption
TCAP	Transaction Capabilities Application Part
UL	Update Location
UMTS	Universal Mobile Telecommunication Systems
USSD	Subscribers Unstructured Supplementary Service
VLR	Visitor Location Register
VoLTE	Voice over LTE

Cellusys®

Cellusys founded in 2004 is a privately held company, based in Dublin, Ireland. It provides leading edge solutions for mobile networks including comprehensive Data Solutions, Security Solutions and Roaming Management Solutions.

Dublin, Ireland

- Research & Development
- Signalling Solution & Circuit Switched Engineering

Berlin, Germany

- Research & Development
- Mobile Broadband & Pocket Switched Solutions Engineering

Bangkok, Thailand

- Sales & Technical Support Asia Pacific

Atlanta, USA

- Sales & Technical Presales

Dubai, UAE

- Sales & Technical Presales

www.cellusys.com sales@cellusys.com +353 1 642 5000