2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

We Know Where You Are!

Siddharth Prakash Rao
Department of Computer Science
Aalto University, Finland
siddharth.rao@aalto.fi

Dr Silke Holtmanns
Bell Labs, Nokia
Espoo, Finland
silke.holtmanns@nokia.com

Dr Ian Oliver
Bell Labs, Nokia
Espoo, Finland
ian.oliver@nokia.com

Dr Tuomas Aura
Department of Computer Science
Aalto University, Finland
tuomas.aura@aalto.fi

Abstract: Mobile network technologies require some degree of tracking of user location, specifically user equipment tracking, as part of their fundamental mechanism of working. Without this basic function, features such as hand-over between cells would not work. Since mobile devices are typically associated with a single person, this provides a potential mechanism for user location surveillance. Network operators are bound by strict privacy legislation. However, spying by certain agencies, hackers and even advertisers without the users' or operators' knowledge has become a serious issue. In this article, we introduce and explain all known recent attacks on mobile networks that compromised user privacy. We focus on attacks using the Signalling System 7 (SS7) protocol as the interconnection interface between operators mainly in GSM networks. In addition, we outline a novel evolution of location tracking for LTE networks. One reason these attacks are not widely published or known by the general public is due to the complex and arcane nature of the networks and their protocols. Mobile network interfaces are 'hidden' from users, and therefore the general public's interest in such attacks is much lower compared to other phone vulnerabilities.

The purpose of the paper is to raise awareness about the current location tracking problem in cellular networks, the existing countermeasures and to encourage further research in the area for 5G networks.

Keywords: *location privacy, SS7, mobile networks, interworking, roaming, tracking, diameter*

1. INTRODUCTION

Mobile phones have become a major part of our daily lives and communication. Mobile phone services are based on cellular network technology which requires the operators to keep track of users' movements between cells and networks in order to provide seamless telecommunications services such as network access, messaging, and voice calls direct to the phone. Since personal mobile phone use is nearly ubiquitous, the discourse of location (i.e. Cell ID) information that is collected by the network operators poses a threat to the personal privacy. Disclosure of location information by the operators is strictly controlled by legislation in most countries. However, spying on mobile users by government agencies, hackers, and advertisers without the knowledge of the user or the network operator has become a serious issue.

Cellular location privacy research is related to the disclosure of identifiers in the Radio Access Network (RAN) using so-called IMSI catchers with which attackers can spoof base stations and collect mobile subscriber identifiers over the air. This requires the attacker to set up a base station near the assumed location of the target users. Solutions to this problem are being developed to detect and prevent attacks that use a false base station [3]. It is more practical for the attacker to obtain the location information from the cellular network operators directly.

Signalling System No. 7 (SS7) is a widely used protocol for communication between network elements and between operator networks. It is one of the key protocols to enable roaming and cellular services across operator domains. Although there are newer protocols (specifically, Diameter), SS7 is still widely used between cellular networks, and interoperability will force operators to support it long into the future. SS7 was designed when there were a few state owned operators, which in turn trusted each other. The protocol itself offers little or no protection, nor was it designed to resist attacks using the SS7 signalling networks or SIGTRAN (SS7 over IP).

In 2008 the first location tracking attack was illustrated by Engel in [1]. In 2014 it was proven that an attacker with access to the SS7 network can track users and perform other attacks such as eavesdropping, SMS interception, and fraud [1],[2],[4],[5],[6],[22]. One of those attacks was shown in a live demonstration [7].

In this paper, we discuss the known weaknesses in the mobile communication backend of the networks that may disclose the location of a user. We assume that the attacker has the victim's phone number and SS7 access. We provide message-level details of the attacks that exploit the SS7 protocol in addition to outlining a new Diameter based location tracking attack for LTE networks and discussing the potential countermeasures.

2. BACKGROUND

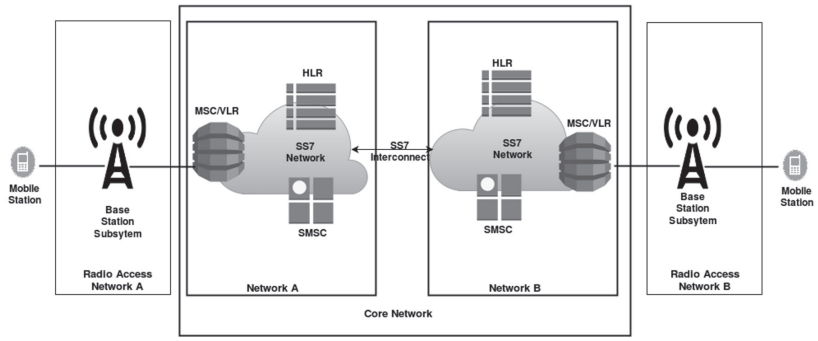
This section gives a brief overview of the SS7 interworking network, the situations where location is intentionally disclosed, and the different levels of accuracy at which the network may reveal the user location.

A. SS7 and interworking network overview

SS7 is a network protocol used worldwide between network elements and between operator networks. It was standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T) more than 30 years ago. SS7 specifies the exchange of information over the signalling networks in Public Switched Telephone Networks mainly to enable the establishment of phone calls across networks. The Message Application Protocol (MAP) which is standardised by the 3rd Generation Partnership Project (3GPP) [8] offers a wide set of additional features for enabling mobility, roaming, SMS, and billing.

The Home Location Register (HLR), Mobile Switching Centre (MSC), Visitor Location Register (VLR), and Short Message Service Centre (SMSC) are some of the key components of the core network (shown in Figure 1) used for the attacks discussed here. These elements are identified by their Global Title (GT), which are used as addresses for routing messages through the SS7 network using the SS7 MAP protocol [8] .

FIGURE 1: CORE NETWORK OVERVIEW



HLR is the central database in an operator's home network. It contains the subscription profiles, service data, and current location of the subscribers of that operator. It maintains the mapping of subscribers' International Mobile Subscriber Identity (IMSI) and their phone numbers, or Mobile Station International Subscriber Directory Number (MSISDN). The VLR stores a copy of the data from HLR for mobile subscribers who are currently in its geographic area, for both local and roaming subscribers. The MSC is responsible for routing calls and SMS text messages to and from the mobile phones in the RAN. The SMSC is responsible for storing, forwarding, and delivering SMS messages.

B. Regular and legitimate location disclosure

The radio network to which the user is currently connected knows the precise location of the cell tower and this then gives the approximate location of the user based on proximity measurements and triangulation. In city areas this is up to 200 m around a given cell tower, and in rural areas up to 35 km with normal equipment or up to 77 km with extended cell range equipment. In densely populated areas, more base stations are deployed and each of them covers a small area, which implies more accurate user location.

This information is revealed by some legitimate services as follows:

- Locate-my-phone services. Network operators offer a service for tracking lost phones with the consent of the phone owner. However, these have not gained popularity due to similar functionality provided by GPS.
- Public safety. In case of emergency or when the user has to be tracked down for safety reasons, officials are given access to location information.

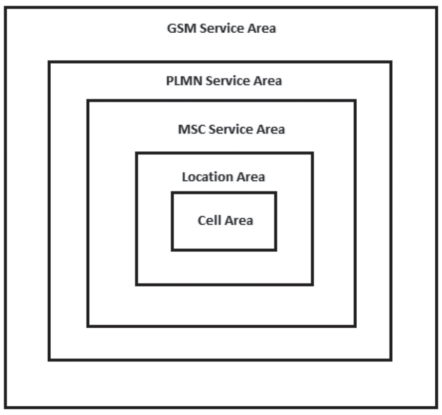
The FCC [9] requires the precise location of the caller for emergency purposes. Access to this level may be protected by local laws and require judicial intervention to obtain. Mobile operators provide the position of the mobile phones as part of the Location Services (LCS). The precise location information is obtained with the Radio Resource LCS Protocol [10] with the help of Gateway Mobile Location Centre (GMLC).

C. Overview of location proximity

To provide cellular services to mobile users, mobile networks have a hierarchical geographic structure [11] (see Figure 2). A cell is the smallest area, and its radius ranges from 100 meters to over 35 kilometres (which is the normal radio coverage of a transmitter). Each cell is identified by the Cell Global Identity (CGI), or Cell ID. When used for positioning, the CGI is typically mapped to the geographic coordinates of the cell tower at its centre.

Several such cells constitute a Location Area (LA). Every time a mobile user moves to a new LA, their location will be updated in the MSC/VLR database. An MSC Service Area comprises several LAs, which are served by the same MSC. HLR stores the information about the MSC that currently serves a particular Mobile Station (MS). Each mobile operator has several MSCs, which together form the PLMN Service area. The overall area with GSM connectivity is called the GSM Service area.

FIGURE 2: GSM GEOGRAPHIC HIERARCHICAL STRUCTURE [11]

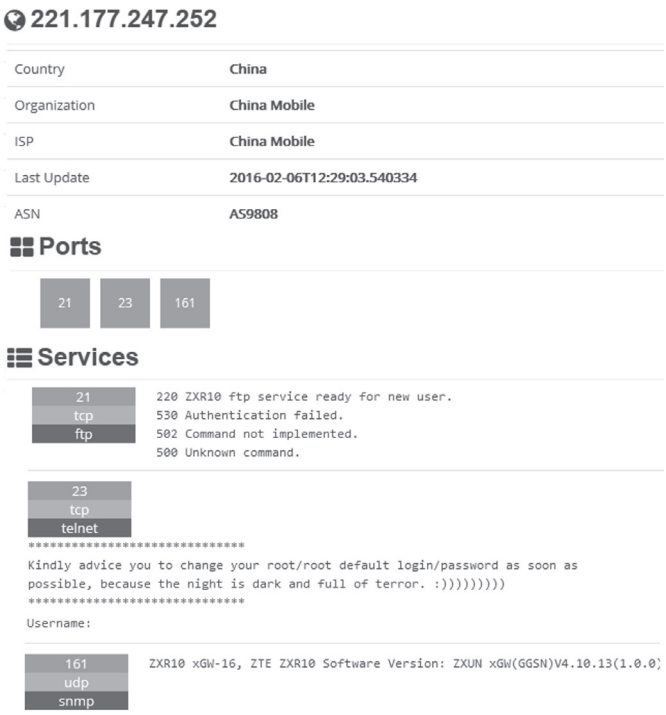


3. LOCATION DISCLOSURE ATTACKS

Attacks from the interconnection network that would reveal the precise location of users were first demonstrated by Engel in 2008 [1] and then, in 2014 [2], more accurately at the Cell ID level. These exploited flaws in the existing specification and implementations. It is possible for an attacker to gain access to the SS7 core network through a compromised edge device or through a badly configured core network node. It might be as easy as searching for a core network node with open ports in an Internet-connected database [12] as shown in Figure 3. Another means of getting into SS7 networks is by gaining connection through an existing provider with insufficient security checks when renting out their SS7 access.

As part of mobility management, network operators have to keep track of the location of the mobile station. This happens even when the mobile is in the idle state, i.e. it is turned on and ready to make or receive messages and calls. The HLR of the mobile phone's home operator needs to know the MSC/VLR via which the mobile can be reached. The MSC/VLR where the mobile is currently roaming needs to be able to page the mobile when a call or message arrives. The mobile phone is identified by its IMSI, which is also used in the mobility management messages between the HLR and MSC/VLR.

FIGURE 3: GGSN VISIBLE ON THE INTERNET (DISCOVERED VIA SHODAN.IO, 11.2.2016)



A. Location disclosure using call setup messages

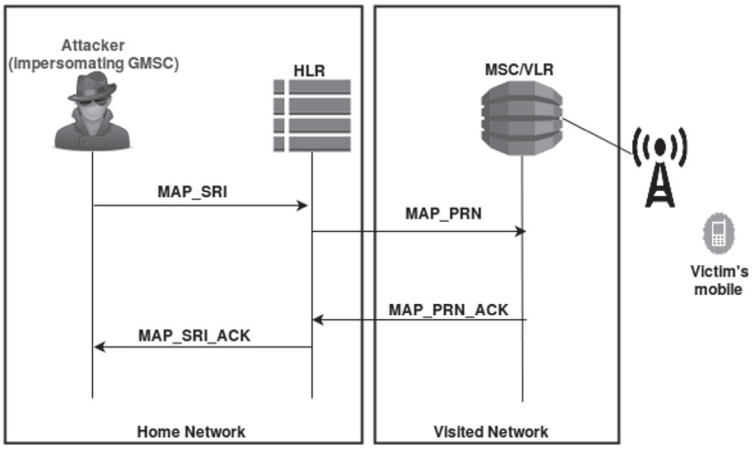
We now describe the normal message flow for a mobile-terminated call when the mobile is roaming in a visited network [13]. The call in this case may originate either from the fixed telephone network or from a mobile subscriber from another operator network.

1. When a call is placed to the mobile user's phone number (MSISDN), the caller's network sends an ISUP IAM (Initial Address Message) message to the mobile user's home network. The message is routed to a Gateway MSC (GMSC) of the mobile's home network based on the MSISDN.
2. The GMSC queries the HLR in the home network for the mobile's current location by sending the MAP Send Routing Information (MAP_SRI) message to the HLR. The HLR keeps track of the mobile's location. We assume that the mobile is roaming in another network.
3. The HLR queries the MSC/VLR in the visited network by sending the MAP Provide Roaming Number message (MAP_PRN).
4. The VLR responds to HLR with the MAP_PRN_ACK message. The response contains the Mobile Station Roaming Number (MSRN), which is a temporary ISDN telephone number assigned by the VLR for the purpose of routing this call.
5. The HLR passes the MSRN back to the GMSC with the MAP Routing Information Acknowledgement MAP RIA message.
6. The GMSC now sends the IAM message to the MSRN to set up the call.
7. This message is routed to the MSC/VLR in the visited network. Since MSC/VLR just assigned the MSRN to the mobile, it knows to which mobile (identified by IMSI and TMSI) the call should be routed. Thus, on arrival of IAM message, it establishes the call connection to the mobile.

Attack using call set up messages. This attack [1] uses the normal message flow of the call set up to learn the approximate location of the victim's phone and therefore of its user. An attacker with SS7 access pretends to be the GMSC and follows the call setup procedure from the point where the GMSC supposedly received the IAM message. The attack message flow, also shown in Figure 4, is as follows:

1. The attacker sends the MAP_SRI message enclosing the victim's MSISDN to the HLR in the victim's home network. In the SS7 network, no authentication is performed. However, the attacker needs to know the Global Title of the HLR to send this message to (but often brute force attacks to operator ranges are performed till an 'HLR is hit').
2. HLR maps the MSISDN to the victim's IMSI and sends MAP_PRN to the VLR at the visited network.
3. The VLR responds with MAP_PRN_ACK, which contains the MSRN (or an error message if the phone is not reachable). The same message contains the IMSI and Global Title of the MSC/VLR that is currently serving the mobile.
4. HLR forwards the information to the attacker, who is impersonating a GMSC, in MAP_SRI_ACK message. This response also contains the Global Title of the VLR/MSC.

FIGURE 4: LOCATION DISCLOSURE USING CALL SETUP MESSAGES



The attacker will not proceed with the call setup to the GMSC. Instead, the attacker has learned the victim's IMSI and the GMSC and Global Title of the VLR of the network where the victim is currently roaming. The latter two disclose the mobile's location with the relatively coarse granularity of the MSC service area.

The MSC service area is typically a region or state of a country. Since the number of mobiles that an MSC can serve is limited, the area served by one MSC is smaller in densely populated areas. The numbering of the MSCs is purely operator specific, but for some operators, the number itself can reveal the geographic area, such as telephone area code of the MSC GT [1]. The GT identifies the country and operator in whose network the mobile is roaming. Another way to discover the location of the GT is to search in a business or residential phone list for phone numbers that have the same prefix as the GT. The addresses listed with these numbers will mostly be in the geographic area of the MSC. The prefix of the MSRN reveals the same kind of information as the GT. The IMSI may be useful for further attacks e.g. fraud, eavesdropping.

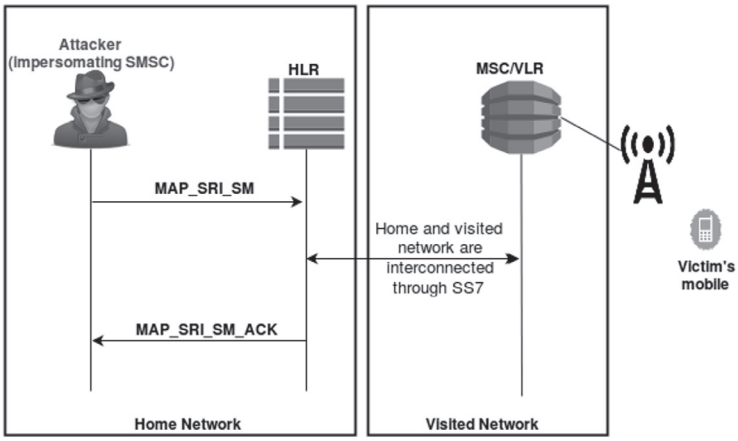
B. Location disclosure using SMS protocol messages

SMS is a service for the transmission of text messages up to 140 bytes. The end-to-end SMS procedure comprises of two parts: in the Mobile Originating Part, the sender submits the SMS to a Short Message Service Centre (SMSC); in the Mobile Terminated Part, the message is delivered from the SMSC to the recipient mobile. The messages are sent over the GSM signalling channels [13].

The message flow of the Mobile Terminated Part is similar to the call setup described above. To deliver the message directly to the destination, the SMSC has to know the IMSI of the recipient mobile and the Global Title of the MSC that is currently serving the recipient. When the SMSC is in the same network as the recipient or a roaming partner, the SMSC obtains the required information from the recipient's HLR:

1. The SMSC sends MAP Send Routing Information for SM MAP_SRI_SM message to the HLR in the recipient's home network.
2. The HLR queries the MSC/VLR in the visited network, where the mobile is currently roaming, with the MAP_PRN.
3. HLR encapsulates the received IMSI and MSC/VLR GT in the MAP Send Routing Information for SM ACK message and sends it back to the SMSC.
4. The SMSC then sends the text message with the IMSI to the recipient MSC/VLR GT, and the MSC/VLR delivers it to the mobile station.

FIGURE 5: LOCATION DISCLOSURE USING SMS PROTOCOL MESSAGES



Attack using SMS protocol messages. Here the attacker impersonates an SMSC and sends signalling messages to learn the IMSI and MSC/VLR GT of the victim [1]. The attack message flow is as follows; it is also shown in Figure 5.

1. Pretending to be an SMSC, the attacker sends the MAP_SRI_SM message to the HLR by enclosing the MSISDN (phone number) of the victim.
2. The HLR thinks that the SMSC needs to send an SMS to the provided MSISDN, and replies with the MAP_SRI_SM_ACK message, which contains the IMSI of the victim along with the GT of the MSC/VLR that is currently serving the victim.

The attacker translates the MSC/VLR GT to the geographic location in the manner described before. However, the success of this attack depends on details of the bilateral SMS roaming arrangement between the network operators.

C. Location disclosure using CAMEL location management function messages

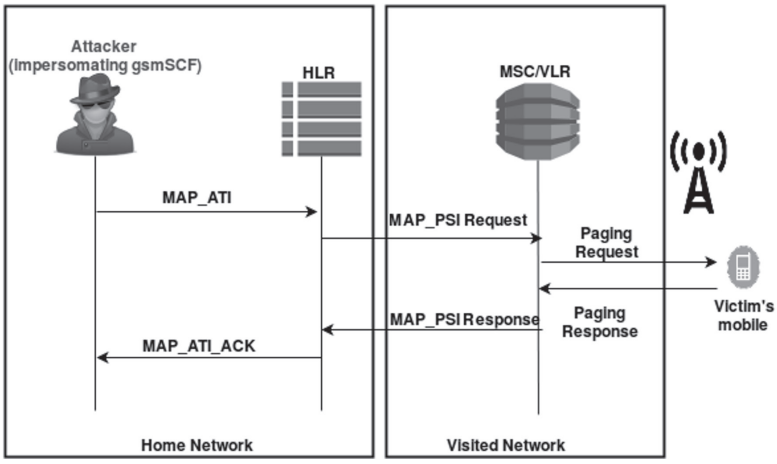
Customised Applications for Mobile Networks Enhanced Logic (CAMEL) [14] is an overlay on MAP. As a part of the network internal location management function, the network providers

can send Any Time Interrogate (ATI) messages to the HLR from CAMEL platforms to obtain the Cell ID of the user. The location information provided in this case is the last known location of the mobile station. The basic message flow of this function [15],[8] is as below:

1. The GSM Service Control Function (gsmSCF) element sends the MAP Any Time Interrogation Request (MAP_ATI) message, which contains the MSISDN, to the HLR of the mobile's home network.
2. The HLR again looks up the mobile's current location in its database based on the MSISDN. It then transmits the MAP Provide Subscriber Information (MAP_PSI) message to the MSC/VLR.
3. The MSC/VLR sends a Paging Request message to the mobile station to look up its current state. The Paging Response message will have the Cell ID of the cellular tower to which the mobile is currently connected.
4. MSC responds to the HLR with the MAP Provide Subscriber Information Response message, which contains the Cell ID and IMSI. If the mobile station responded to the paging, then the age field is set to 0, as the MSC/VLR accurately knows its current location; otherwise the last known Cell ID is sent, with a non-zero age field.
5. The HLR now sends the MAP Anytime Interrogation Response back to the gsmSCF with the subscriber information from the previous step.

Attack using Any Time Interrogation message. Here the attacker impersonates the gsmSCF and sends the MAP_ATI message with the MSISDN of victim to the HLR [B]. The message flow of this attack is shown in Figure 6.

FIGURE 6: ATTACK USING ANY TIME INTERROGATION MESSAGE



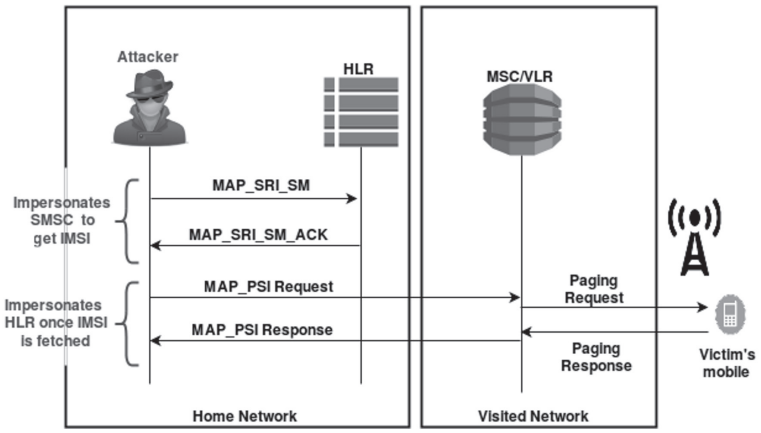
1. The attacker pretends to be a gsmSCF and sends the MAP_ATI request containing the MSISDN of the victim to the HLR.
2. The HLR treats this as a legitimate message from gsmSCF and sends the MAP_PSI request to the MSC/VLR.
3. The MSC/VLR initiates the Paging Request to the victim's phone and receives the IMSI and Cell ID in the Paging Response message.
4. The MSC/VLR then sends the information from the previous step along with the MSC/VLR GT to the HLR in the MAP_PSI response.
5. The HLR forwards this information to the attacker in the MAP_ATI response.

As the result, the attacker now knows the cell of the victim along with the IMSI and the GT of the serving MSC. Here, the attacker would learn victim's location more accurately than in the previous attacks because the Cell ID is retrieved.

Since the MAP Any Time Interrogation message is not an essential function for the network operation and it raises obvious privacy concerns, many network operators filter the message. The filtering can potentially be bypassed by the following hybrid attack.

Hybrid attack using SMS and CAMEL messages. The hybrid attack [6] queries the MSC/VLR directly in order to circumvent the potential MAP_ATI filters. The attacker can send the Provide Subscriber Information request to the MSC/VLR by pretending to be the HLR. For this, the attacker needs to know the victim's IMSI. The attacker needs to discover first the IMSI corresponding to the MSISDN. The message flow for this attack is shown in Figure 7.

FIGURE 7: HYBRID ATTACK USING SMS AND CAMEL MESSAGES



1. The attacker performs the previously described SMS-based attack to learn the IMSI and MSC/VLR GT.
2. The attacker then queries the MSC/VLR with the MAP Provide Subscriber Information MAP_PSI request.
3. As before, after the paging procedure, the MSC/VLR returns the Cell ID to the attacker.

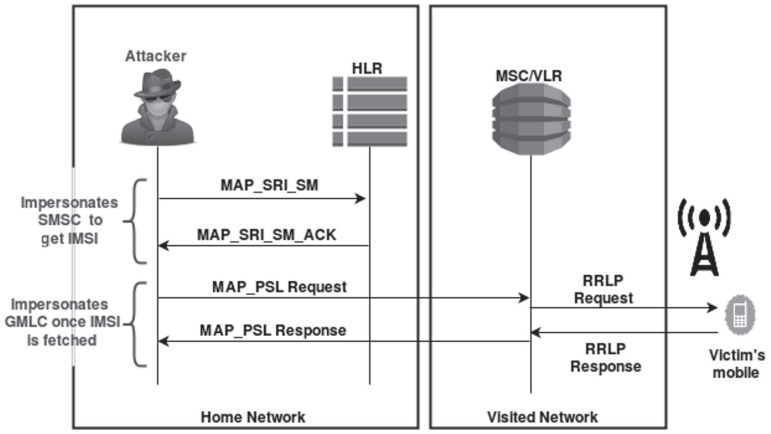
D. Location disclosure emergency location service messages

In situations, governmental bodies have access to location information that is collected from the network [10]. The accurate location is based on triangulation using the angle of signals observed at the cellular towers or the arrival times of the radio signals at the mobile. The triangulation is usually triggered by an emergency call from the mobile station, but it can also be initiated from the network side, such as by law-enforcement officials. The basic message flow of an authorised LCS [16] is as follows:

1. An authorised client can send the MAP Location Service request to a Gateway Mobile Location Centre (GMLC) either at the mobile's home network or at the visited network. The request contains either the MSISDN or the IMSI of the mobile. The authorisation of the client is left to the operator and depends upon local legislation.
2. The GMLC that receives the request sends it to a GMLC in the mobile's home network, which enforces the user's privacy preferences on the request, and then forwards it to the visited network's GMLC. The GMLC may query the HLR at the mobile's home network for the IMSI and routing information with the MAP Send Routing Info for LCS MAP_SRI_LCS.
3. The visited network's GMLC acts as a gateway for external LCS clients to the LCS functions in the radio access network. In 3G networks, the GMLC sends the MAP Provide Subscriber Location MAP_PSL request to the MSC/VLR. This request identifies the mobile station by its IMSI.
4. The MSC/VLR resolves the location request with the help of the radio network and the mobile using one of various positioning methods. It then encapsulates the location report into the MAP Provide Subscriber Location ACK message to the GMLC of the visited network.
5. The GMLC encloses the location information in the MAP Location Service Response and sends it back to SMLC client via the same route as the request was received.

The validation of the request origin and the authorisation are enforced by the GMLCs. Emergency services are allowed to make location requests directly to the GMLC in the visited network. This request is not routed through the GMLC in the home network and can be done without querying the HLR for the IMSI. This allows assistance to users in need also while they are roaming, but brings a way to circumvent control setting in the home GMLC.

FIGURE 8: ATTACK USING LOCATION SERVICE MESSAGES



Attacks using location service (LCS) messages: In this attack [2], the attacker bypasses the authentication at the visited network's GMLC by impersonating the GMLC to the MSC/VLR. The message flow for the attack using LCS messages, also shown in Figure 8:

1. The attacker needs to know the victim's IMSI and MSC/VLR GT. The IMSI can be obtained by MAP_SRI as described above.
2. Now the attacker queries the MSC/VLR in the visited network for the accurate location information. He sends the MAP_PSL request to the MSC/VLR. The MSC/VLR has not means for authenticating this request because the LCS client authentication should have taken place already at the GMLC, which the attacker bypassed with the direct request to the MSC/VLR.
3. The MSC/VLR detects the mobile station's location with one of the various possible methods, such as the RRLP Request to the mobile. It then responds to the attacker with the MAP Provide Subscriber Location Response, which reveals the location of the victim to the attacker.

E. Experiment paradigm

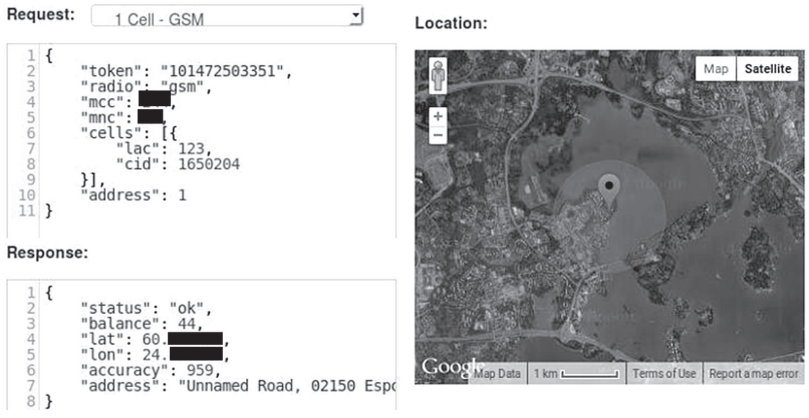
Being one of the network providers, in cooperation with an operator, we had access to the core network honeypot system. Since this honeypot was built using virtualisation of the kernel of actual core network nodes, we used it for confirming the attacks. Using such protected test environments not only avoids disruption of actual telecom services while conducting experiments, but also it helps in practical realisation of feasibility of the attacks on the real infrastructure by continuous monitoring. Our setup had one HLR, SMSC, EIR, and two MSC/VLR (of which we used one of the MSCs as part of home and the other as the visited network's VLR) which was fine-tuned to use our test SIMs. To mimic the actual attack scenarios, we kept specific ports of these elements open so that we could avoid rudimentary steps such as port scanning or topology mapping during our experiments. Core network nodes were connected to

each other using Stream Control Transmission Protocol (SCTP) and some of the SCTP ports were also open to interact with IP Internet. Since attackers use such ports an entry point to SS7, we replicated the same scenario to inject crafted packets from VLR to other elements of home network in our setup. We established SCTP client-server connection over known ports using PySCTP modules, generated SS7 traffic using the Seagull tool, and used Scapy, the packet manipulation tool, to inject false IMSIs and GTs of MSCs into the traffic of regular protocol messages exchanged between the nodes.

Following this, we monitored the packets throughout its journey using Wireshark to track and confirm the practicality of our attacks. Since our setup modelled real world scenarios, we were able to confirm the attacks presented in section 3A, 3B and the hybrid attack in 3C. For legal reasons we were not allowed to use the LCS messages (section 3D) and hence we could not confirm the feasibility of this attack. Furthermore, our test setup rejected answering ATI messages for security reasons and for the same reason we could not confirm the first attack described in section 3C.

The attackers can buy core network access from untrustworthy operators, if not portraying themselves as genuine operators by being virtual operator networks, thereby misusing the loaned infrastructure. In such cases, they can carry out attacks similar to those in our experiments. After gaining access to the core, they can use openly available tools such as SCTPscan (for port scanning), SS7Calc (for topology mapping) and Hydra (to brute force passwords) along with the tools that we used in our setup to exploit the system. Figure 9 demonstrates the mapping of authors' Cell IDs to their latitude and longitude, which is done using an online Application Programming Interfaces (API) [17]. Similarly, in many countries, the coordinates of the cell towers are public information. An attacker can either use such information if available, or use APIs such as[17] to visualise the location of the victim once he retrieves the Cell IDs.

FIGURE 9: MAPPING OF CELL ID USING THIRD PARTY API [17]



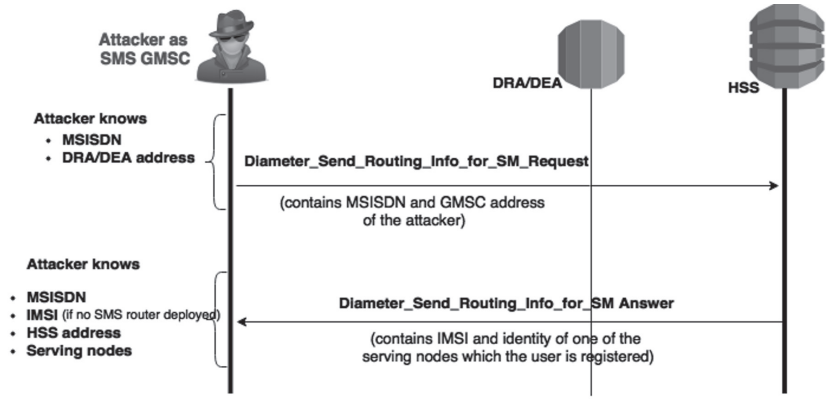
We speculate that the SS7 attackers extensively use SIGTRAN to find their entry point to the core network. Being an adjunct of the SS7 suite, SIGTRAN supports call management and application exemplars of SS7 but over IP and SCTP. SIGTRAN also facilitates adaptation of VoIP networks to the PSTN signalling. Attackers use the open interfaces of SCTP to IP dig deeper into the network.

In our understanding, the attacker would need more time to identify the open ports and map the network periphery, compared to executing the attacks themselves, which takes less time. The major costs of such attacks lie in gaining access (either by buying access or using femtocells) rather than in executing the attacks which depends only on the attackers' skillset and selection of tools. Due to these variable factors, we cannot estimate the economic feasibility of the attacks from an attacker's point of view.

4. EVOLUTION

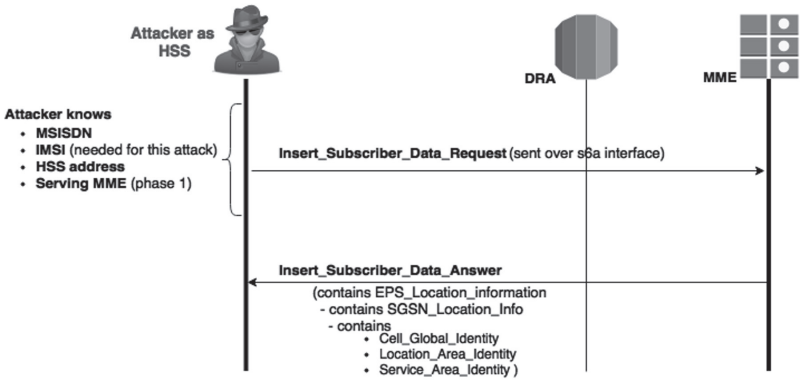
Diameter is the evolution of the SS7 and MAP protocol that is used within and between the 4G Long Term Evolution (LTE) networks. It uses the Diameter Edge Agent (DEA) that resides on the border of the network as the first contact point for messages coming over the interconnection link. In this context, Home Subscriber Server (HSS) is the evolved HLR and Mobility Management Entity (MME) can be considered to be an evolved MSC.

FIGURE 10: IMSI ACQUISITION IN LTE



Based on the existing SS7 attacks, we see the attack evolution in LTE. The potential steps are outlined in Figures 10 and 11 and can be seen as an evolution of the SS7 attack in [1]. First the attacker needs to obtain the users' IMSI and used SMS related protocol messages over the S6c interface. The attacker then starts the real part of the attack where he uses the diameter Insert Subscriber Data (ISD) command that is configured to request the location of the user over S6a interface.

FIGURE 11: LOCATION ACQUISITION IN LTE



This approach mirrors the MAP based Provide Subscriber Information approach for Diameter. LTE roaming interfaces are not yet common, and further practical testing of Diameter-based vulnerabilities are part of our ongoing research.

5. COUNTERMEASURES

One obvious solution to defend the system against the attacks discussed in section 4 is by authenticating the SS7 signalling messages. If SS7 runs over IP, then IPsec should be considered [18]. Another approach is to block or filter messages that give out location, based on the origin of the message. These may not be effective solutions as many of the signalling messages used for the attacks are part of basic communication such as calls and SMS. Filtering these messages might affect the performance of cellular services. Nevertheless, properly deployed filters can help weed out many attacks.

Firstly, the MAP_ATI command should only be used network internally within the operator network, which allows blocking of MAP_ATI requests coming over the interconnection. Secondly, both the MAP_PSI and MAP_PSL messages should be filtered to prevent bypassing of higher-level authentication. Cross-layer checks, in particular for the source address information between the Signalling Connection Control Part (SCCP) transport layer and in the MAP application layer, could help to detect spoofing of signalling messages and detection of an attack.

It is hardest to filter the MAP_SRI and MAP_SRI_SM. Even when these originate from an unknown source, they may be required for normal function of the network, such as call setup or SMS delivery. Fortunately, the attacks that exploit these messages only reveal the mobile's location at the MSC Service Area level [19].

The most promising solution for preventing the leakage of the MSC/VLR and MSRN is called SMS home routing [20], which routes the communication, via the home network without providing any location information to the sender. It requires the MAP Mobile Terminated Forward SM message to be routed always through an SMS router in the home network. Rather than revealing the IMSI of the receiving MS, the MAP_SRI response from the HLR will only contain a 15-digit MT-SMS Correlation ID [20]. This number establishes a mutual relationship between the MAP_SRI_SM and the MAP Mobile Terminated Forward SM messages without revealing the IMSI to the SMS message source. There are, however, some objections to the home routing. First, operators are used to charging more for the so-called transparent mode of SMS delivery where the SMS delivery reports are correctly returned to the sender. Second, some global operators depend on the IMSI in the current SMS delivery reports for the implementation of their billing system. Additional proposed countermeasures can be found in [21].

6. CONCLUSION

The SS7 attacks discussed in this paper make use of the lack of security in signalling protocols to breach mobile user's location privacy, whereas the Diameter attack as an evolution of SS7-based attacks, hints that the vulnerabilities are persistent in newer generations of networks. We have reviewed these attacks and explained how they work on the level of exact protocols and messages. The attacks presented in this paper have been confirmed in a real 3G/LTE network, and this confirmation and evolution of the previous knowledge to LTE networks is one of the main contributions this paper.

The initial attacks described enable an attacker with SS7 access to retrieve the IMSI and the GT of the MSC/VLR based on MSISDN, without alerting of the victim. While the MSC/VLR GT will only disclose the approximate location of the victim, it can be further narrowed down to cell area or better using the attacks presented in later part of section 3. Though Diameter seems to be an improvement over SS7 in terms of security with the use of IPsec or TLS and certificate based authentication, it is possible to port SS7 attacks to Diameter. Additionally, backward compatibility needs to be ensured between these networks, and hence downgrading attacks will remain as a persistent threat to the telecommunication industry.

Telecommunication networks are intricate systems made up of diverse circuitous subsystems, each of which comprises various different technologies. While legacy sub-systems and components are here to stay for many years, it is important to remember that the security of the whole system depends on the security of the weakest link and partner.

REFERENCES

[1] Tobias Engel, 'Locating Mobile Phones using Signaling System 7', 25th Chaos Communication Congress 25C3 (2008), http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.

[2] Tobias Engel (Sternraute), 'SS7: Locate. Track. Manipulate', 31st Chaos Communication Congress 31C3 (2014), http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf.

[3] SR Labs, 'SnoopSnitch,' Security Research Lab, https://opensource.srlabs.de/projects/snoopsnitch.

[4] Karsten Nohl (SR Labs), 'Mobile self-defense' 31st Chaos Communication Congress 31C3 (2014), https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf.
[5] Alexandre De Oliveira et.al. 'Worldwide attacks on SS7 network' Hackito Ergo Summit (2014), http://2014.hackitoergosum.org/slides/day3_Worldwide_attacks_on_SS7_network_P1security_Hackito_2014.pdf.
[6] Sergey Puzankov, Dmitry Kurbatov (Positive Technologies), 'How to Intercept a Conversation Held on the Other Side of the Planet', PHDays (August 2014), http://2014.phdays.com/program/tech/36930/.
[7] Australian TV Channel 9, 60 Minutes Show, 'Special Investigation: Bugged, Tracked, Hacked', (August 2015), http://www.9jumpin.com.au/show/60minutes/stories/2015/august/phone-hacking/.
[8] 3rd Generation Partnership Project (3GPP), TS 29.002, 'Mobile Application Part (MAP) specification,' Release 13, 2015, http://www.3gpp.org/DynaReport/29002.htm.
[9] Federal Communication Commission, '911 Wireless Services', 2015, https://www.fcc.gov/guides/wireless-911-services.
[10] 3rd Generation Partnership Project (3GPP), TS 44.031 'Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP) ', Release 13, 2015, http://www.3gpp.org/DynaReport/44031.htm.
[11] Mouly, M. Pautet, 'The GSM system for mobile communications', Palaiseau, France: Cell & Sys, 1992, pp. 100-472.
[12] Shodan.io, 'SHODAN – search engine for internet connected devices', 2015, http://www.shodan.io/
[13] Learntelecom.com, 'SMS in GSM Network | Learn Telecom', 2010, http://learntelecom.com/sms-in-gsm-network/.
[14] 3rd Generation Partnership Project (3GPP), TS 23.078, 'Customised Applications for Mobile network Enhanced Logic (CAMEL)', Release 13, 2015, http://www.3gpp.org/DynaReport/23078.htm.
[15] C. Pudney, 'Liaison Statement on Restoration of R'96 Any Time Interrogation functionality', 3GPP TSG-SA WG2 meeting #22, 2002.
[16] 3rd Generation Partnership Project (3GPP), TS 23.271 'Location Services (LCS); Functional description; Stage 2', Release 13, 2015, http://www.3gpp.org/DynaReport/23271.htm.
[17] Unwired Labs, 'Unwired Labs Location API - Geolocation API and Mobile Triangulation API, Cell Tower database', Unwired Labs Location API - Geolocation & Mobile Triangulation API, 2015, http://unwiredlabs.com/api.
[18] 3rd Generation Partnership Project (3GPP), TS 33.210 '3G security; Network Domain Security (NDS); IP network layer security', Release 13, 2015, http://www.3gpp.org/DynaReport/33210.htm.
[19] Positive Technologies, 'Signaling System 7 (SS7) security report ', December 2014.
[20] 3rd Generation Partnership Project (3GPP), TR 23.840, 'Study into routing of MT-SMs via the HPLMN', Release 7, 2007, http://www.3gpp.org/DynaReport/23840.htm.
[21] GSMA permanent reference document (PRD) FS.07 'SS7 and SIGTRAN Network Security v1.0' (Currently internal to the GSMA association, but to be released to the public later.).
[22] Rao, Siddharth Prakash, et al. 'Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access.' Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.