User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

Silke Holtmanns
Bell Labs - Nokia Networks
Espoo, Finland
Email: silke.holtmanns@nokia.com

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

Ian Oliver
Bell Labs - Nokia Networks
Espoo, Finland
Email: ian.oliver@nokia.com

***Abstract*—User location tracking attacks using cellular networks have been known since 2008. In 2014, several Signalling System No 7 (SS7) protocol based location tracking attacks were demonstrated, which particularly targeted the cellular roaming in GSM networks. Currently, the mobile network operators are in a gradual process of upgrading to Long Term Evolution (LTE) networks, in addition to replacing SS7 by its successor - Diameter protocol. Though Diameter seems to be an improvement over SS7 in terms of security with the use of IPsec/TLS and certificate based authentication, they still need to communicate with their roaming partners who use less secure SS7. In this paper, we will briefly present the translation of existing SS7 attacks into Diameter-based attacks in LTE networks (under certain assumptions) using Interworking Functions(IWF) - which allows communication between networks that use different protocols. The key contribution of this paper is the the detailed explanation of novel attack vectors to obtain the user location information using IWF and hence, the proof that even new LTE network can be vulnerable to legacy attacks. Furthermore, we will outline some of the potential protection approaches for the attacks that we discuss.**

***Keywords*—Signalling System No.7 (SS7), Diameter, Interworking Funcation (IWF), Location Tracking, Privacy**

I. Introduction

Cellular 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 and it is not possible to provide seamless user experience (i.e. no dropped calls or connections) when the user is moving. Furthermore, the aforementioned user tracking by Mobile Network Operators (MNOs) helps to provide cellular services to subscribers of partner MNOs, which indeed is the generic scenario of ”roaming”. In such scenarios, the inter-operator network connection which is used for exchanging information is often termed as the interconnection. Recently, these interconnections have been exploited to track individual subscribers by hackers, especially when the interconnections are bound by Signalling System No.7 (SS7) protocol. In this paper, we describe attack scenarios again targeting such interconnection networks, however, instead of exploiting the GSM networks like the previously found attacks, we exploit the newer generation of mobile telecommunications technology i.e Long Term Evolution(LTE) or 4G. The fundamental idea of this paper is that – an attacker poses as a roaming partner having an old network (SS7) and therefore, forces the new LTE network to use less secure legacy communication messages. We will first walk through the existing attacks and the related work that use SS7, followed by extending those attacks against LTE networks using the Interworking Functions (IWF). We describe this so-called downgrading attack for illegitimate location tracking. This is the first attack published which downgrades the LTE Diameter security to the level of SS7 security over the interconnection.

ISBN 978-3-901882-83-8

II. Roaming Interconnection

Signalling System No.7 (SS7) is a mobile backend protocol used for interconnectivity between mobile operator networks, which enables roaming and cellular services across operator domains. The protocol is mainly used for communication between the network elements and the networks themselves. It has served its purpose successfully over four decades being a substantial source of income for the service providers and MNOs. In spite of its age, SS7 and its IP version called SIGTRAN continue to be the most commonly used protocols for roaming interconnections till date. In order to provide seamless services to the roaming partners who might have interconnections only over SS7, irrespective of generation of mobile technology (such as GSM, UMTS and LTE), operators are expected to support SS7 protocol. In that sense, all the operators in the world who offer roaming of any type are connected to the older SS7 interconnection network (refer figure 1). Older in this context means that the nodes deployed use the 3rd Generation Partnership Project (3GPP) standards which are older than Release 8.

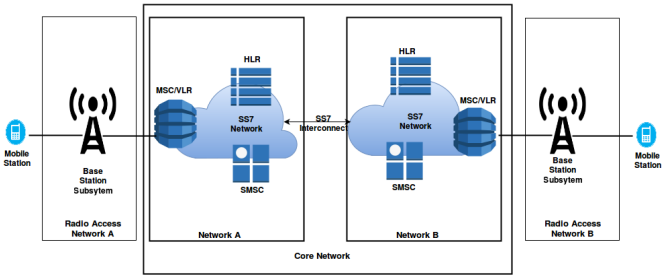

Fig. 1. Two pre-release 8 networks connected via SS7

The Message Application Protocol (MAP) is one of the key applications of SS7 protocol stack which is mainly responsible for the communication between the elements of core network, mobility management and supplementary services. The following elements or nodes of the core network interacts with each other using MAP protocol: (1) Home Location Register (HLR), which contains the subscriber keys and user profile information, (2) Mobile Switching Center (MSC), which manages the user mobility and (3) Visitor Location Register (VLR), which takes care of a user in roaming. Due to the evolution of network technologies and the continuous addition of new services, the MAP specification has grown substantially to support a vast range of services [1].

Unlike the older generation of roaming networks in which subscriber's Home Public Mobile Network (HPMN) (i.e. home network) and Visited Public Mobile Network (VPMN) (i.e. visited network) are connected with SS7 interconnection, the newer LTE networks replaces the SS7 with IP interconnection via the IPX/GRX roaming exchange network. As shown in figure 2, the traffic coming from IPX/GRX interconnection is routed through Diameter Edge Agents (DEA).

As an evolution of HLR, the Home Subscriber Server (HSS) contains the subscriber profiles and it is definitely one of the most important nodes in an LTE network. The Mobility Management Entity (MME) can be seen as the evolution of the MSC, which takes care of the user's mobility management. The home Policy Charging and Rule Function (hPCRF) is the entity that enables billing and thereby collects the charging records for a user. When the subscriber is in a visited network, the same functionality is handled by the visited Policy Charging and Rule Function (vPCRF). The Serving GPRS Support Node (SGSN) handles packet switched data within the network and enables data roaming.

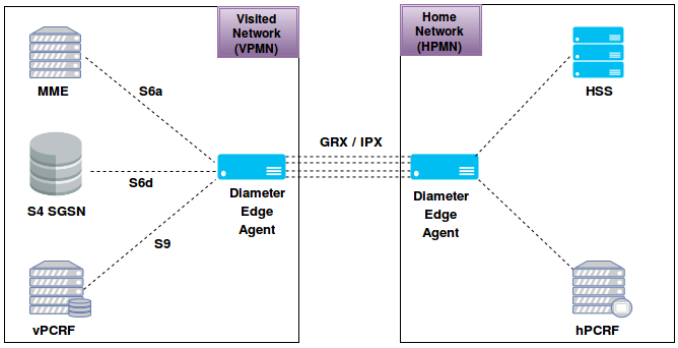

Fig. 2. Diameter roaming implementation between two LTE networks

As mentioned earlier, the upgrade of network (and the supporting infrastructure underneath) from SS7 to Diameter is a gradual process. Most operators update their network infrastructure gradually to avoid service interruption and optimize the return of investment of their infrastructure. During such updates the old equipment are often sold to operators in developing countries, where the capital expenditure is limited and the turnover per user is low. The figure 2 shows the simple direct connection between two operators, both running Diameter. However, the real-life situation is much more complex as shown in figure 3. The number of partners in these cases may scale to around thousand, whose nodes are from different software and hardware releases. The reason for such complex inhomogeneous set-up found in the global interconnection network is either due to the aforementioned gradual update process of supporting network infrastructure or due to limited capital of the operators from developing economies. Irrespective of the reason, such this inhomogeneous set-up provides some interesting attack vectors from security perspective. We describe the exploits using those attack vectors in the subsequent sections.

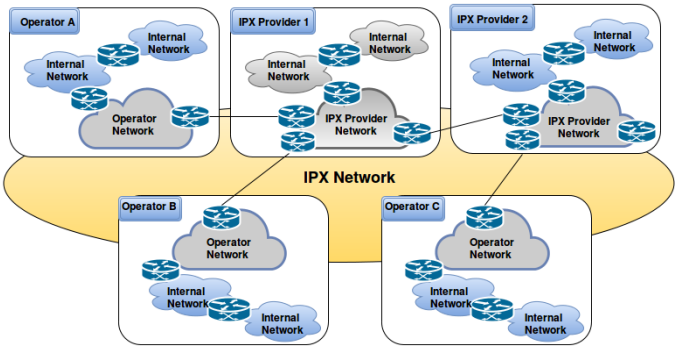

Fig. 3. Roaming hubs and interconnection network

The inhomogeneous set-up simply implies the possibility of existence of nodes within a network that are from different releases and therefore support different protocols. It also implies that the networks towards each other on the roaming interface may use either SS7 or Diameter or the combination of both, depending on the node and the network as outlined in figure 4.

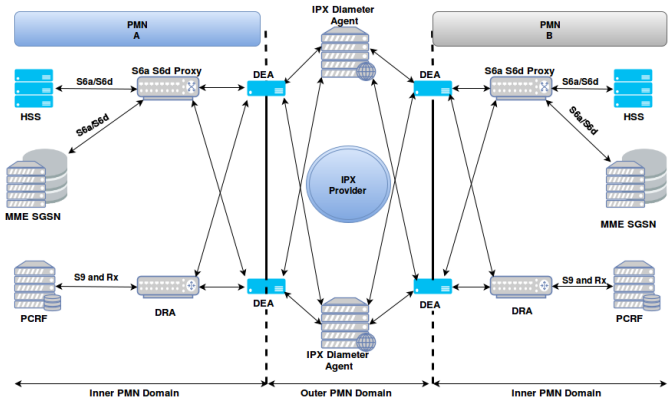

Fig. 4. SS7-Diameter interworking with roaming hubs

For interoperability reasons with their partners, the edge nodes and the nodes themselves have often the ability to translate between Diameter and MAP protocols. Diameter is specified to be secured with NDS/IP [2] (Network Domain Security) security and most commonly IPSec is used as a security protocol. Nevertheless, even the Diameter nodes have

to support partners who run legacy SS7 nodes, where cryptographic security in terms of authentication, confidentiality and integrity is absent.

III. Interworking Function

Usually 3GPP standardizes the functionalities and specifications for communication between nodes belonging to same release. But there are cases, where specific functionality has been standardized to enable interoperability between different releases and technologies. In this realm, the Technical Specification (TS) 29.305 [3] and the non-binding Technical Report (TR) 29.805 [4] describe how Attribute Value Pairs (AVPs) of Diameter and SS7-MAP messages can be mapped to each other. AVPs can be considered as *variables* which often change during cellular communication such as user identity, source of messages etc. Even though this is specified as a feature of mainly edge nodes (e.g. DEA) called Interworking Function (IWF), the way-of-translation is practically deployed on other types of nodes directly to enable interoperability within the operator network, where nodes from different releases are deployed. In such case, where the interworking functionality is used directly at the node, it is often called a multi-domain support scenario. Due to the gradual upgrading within an operator domain, this is a quite common setup as illustrated in figure 5.

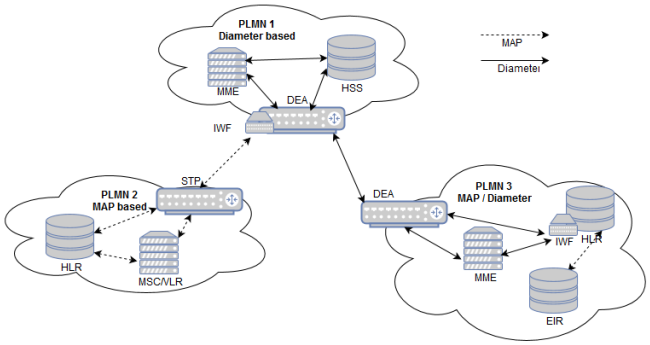

Fig. 5. Three networks with different protocol support

IV. Related Work

Recent successful attacks on SS7 as per [5][6][7][8] and [9] have proven that an attacker with access to the SS7 interconnection network can take control over personal information of the users such as location tracking, billing data and Short Message Service (SMS) messages, in addition to eavesdropping. A detailed explanation about different types of SS7 based attacks can be found in [10] and [11]. We will briefly present only the location-based attacks in this section, followed by investigating in the subsequent sections whether they can be performed on a Diameter network using IWF. On the conceptual level, the idea is to validate whether the Diameter networks are vulnerable to SS7 location attacks by using the IWF for *attack translation*. For all attacks presented in this section we assume that the attacker has access to an SS7 network.

The following location tracking attacks using SS7 are known at the time of writing:

Attack 1: Location disclosure using call setup messages
An attacker here uses the general message flow of a call set up to determine the approximate location of the victim. The attacker with SS7 access pretends to be GMSC (Global MSC), potentially of a partner of the victim's operator, however, the attack may also work with a random GT. The Global Title (GT) uniquely identifies a node in the SS7 network, similar to MAC address in an IP network. The target is a Home Location Register (HLR), the node holding crucial subscriber data.

1) The attacker posing as a GMSC and executes the routine call set up procedure from the point where the GMSC is supposed to receive the Initial Address Message (IAM). At first, he encloses the victim's MSISDN (phone number) in a MAP *Send Routing Information (SRI)* message to the HLR in victim's home network, provided he learns the GT of HLR (It is often found using brute force requests to the GT range an operator holds).
2) The HLR maps the MSISDN sent by the attacker to the International Mobile Subscriber Identity (IMSI), followed by querying the Visitor Location Register (VLR) of victim's visited network by sending MAP *Provide Roaming Number (PRN) Request* to facilitate the call setup. The IMSI is quite important as it is the network internal subscriber identity required by most of the MAP and Diameter commands.
3) The legitimate VLR answers via MAP *Provide Roaming Number* ACK message which in turn contains the IMSI of the victim and the global title of the serving VLR to the HLR.
4) This information is returned via MAP *Routing Information* ACK to the attacker who is impersonating GMSC. The GT of VLR learned here can be used to spot the approximate location of the victim in context.

This attack gives only a rough estimate of the location of a victim, but serves to identify whether he is travelling. Depending on the intention, the travel trajectories could be sufficient for the attacker.

Attack 2: Location disclosure using SMS protocol messages
Similar to the previous attack, the attacker impersonates a Short Message Service Center (SMSC). He pretends to have an SMS waiting for the victim and hence, he requests the MSC/VLR location information in order to deliver it.

1) Pretending to be an SMSC, the attacker sends the MAP *Send Routing Information for SM* (SRI SM) message to the HLR by enclosing the MSISDN of victim.
2) The HLR assumes that the SMSC needs to send an SMS to the provided MSISDN, and thus it replies with the MAP *Send Routing Information for SM* ACK message, which contains the IMSI of the victim along with GT of the MSC/VLR that is currently serving the victim.

Usually, an operator has several MSCs deployed in his network, where each MSC is responsible for a large region. Therefore, this attack allows to identify the region where the victim is currently located, similar to the previously described attack scenario.

Attack 3: Location disclosure using CAMEL location management function messages

The attacker in this scenario exploits the fact that, many network nodes do not check whether a message over the interconnection is internal to the network or otherwise. The *MAP Any Time Interrogation* (ATI) message is usually used within the operator network (i.e. internally), thus, it is not intended to be received over the interconnection network. Nevertheless, Positive Technologies [12] and Tobias Engel [9] showed that the ATI command is often successfully answered by an operator even when it is sent via the interconnection. In spite of the fact that many operators started to block ATI commands coming via interconnection after the public revelation of the aforementioned attacks, it is most likely that not every operator in the world would do the same. In the previously described attacks, the attacker at most can learn the GT of victim's MSC/VLR and hence, the attacker can track down the approximate location of the victim. However, using CAMEL protocol [13] messages, the attacker can narrow down the victim's location accurately to a cell ID, which in densely populated areas can be as accurate as to a street address.

1) The attacker impersonates the GSM Service Control Function (gsmSCF) node and sends a *MAP Any Time Interrogation Request* (ATI) message by encapsulating MSISDN of the victim to the HLR.
2) The HLR considers this as a legitimate message and carries it further by sending *MAP Provide Subscriber Information Request* (PSI) message to MSC/VLR of the victim.
3) The MSC/VLR will initiate the *Paging Request* to receive the Cell ID of the victim.
4) This information is handed over to the HLR via *MAP Provide Subscriber Information Response*, and then back to the attacker via ATI *response* message.

Due to increased risk, many operators started to filter the ATI command as mentioned in the attack in context. However, an attacker can bypass such filters by performing a hybrid attack by executing the SMS protocol based attack to know the MSC GT of the victim, followed by sending MAP *Provide Subscriber Information Request (PSI) message* directly to that MSC as described in the ATI based attack. Since the PSI command has a legitimate usage over the interconnection, it is difficult to filter it.

Attack 4: Location disclosure emergency location service messages

Mobile operators are lawfully bound to provide accurate location information of their subscribers during emergency situations such as accidents (initiated by the subscribers themselves e.g. emergence number 911) or criminal tracking (initiated by the operators on behalf of law-enforcement officials. In case of the latter, the operator initiates an internal network command called *MAP Provide Subscriber Location (PSL)*. This command can be exploited for illegitimate location tracking as per the following attack:

1) The attacker needs to know the victim's IMSI and MSC/VLR GT. He can discover those identifiers through SMS protocol or call setup message based attack as described attack 1 or 2 respectively.
2) Now the attacker queries the MSC/VLR in the visited network for the accurate location information of the victim by sending *MAP Provide Subscriber Location Request (PSL)*. In order to do so, the attacker should bypass the Location Service client (LCS) client (in regular circumstances, law-enforcement authorities are the legitimate LCS clients) authentication at the Gateway Mobile Location Center (GMLC), by directly sending the aforementioned PSL message to MSC/VLR. In turn it leaves the MSC/VLR in context with no means of verifying the actual occurrence of the authentication.
3) The MSC/VLR detects the location of victim's mobile station using one of the various possible methods (e.g. *RRLP Request* [14]).
4) The MSC/VLR then responds to the attacker with the MAP *Provide Subscriber Location Response* message, which contains the Cell ID of the location of the subscriber.

The Cell ID can be mapped to a real location in terms of geographic coordinates of the victim, using publicly available web services such as [15]. In some cases, the LCS message might also reveal the closest GPS coordinates of the victim along with the serving cell ID. However, it is not guaranteed to be as accurate as the GPS information provided by the mobile stations themselves (e.g. using any GPS app on the mobile). It should be noted that the aforementioned attack works only when an operator supports the emergency localization feature.

V. Assumptions for the target LTE networks

We assume that an attacker has access to the roaming interconnection network. For an attacker, there are several ways to gain access to the interconnection network:

- Most operators have a wholesale department or subsidiary which rents out access to third parties and various service providers.
- The roaming network is global and it covers countries or regions where having legal access to subscriber data is allowed due to less strict enforcement of the privacy regulations.
- Compromised or misconfigured nodes that are visible on the Internet (e.g. via Internet-connected database such as Shodan.io [16]), could act as the potential points of entry for the evil hackers. Caskun showed the practical feasibility of attacking nodes of a GRX at the DefCon 2015 [17].
- Insider attack (e.g. via social engineering or bribing) can lead to unauthorized access by criminals.

Further details about *how an attacker gains illegitimate SS7 interconnection* is beyond the scope of this paper. However, we assume that an attacker, depending on skills, resources and motivations, finds a way in. On the technical side, we make some general assumptions especially on the configuration of the operator who is under attack as follows:

- IPSec (as per [2]) is not used between the SS7 and Diameter supporting nodes. In other words, the messages are sent in clear text without any cryptographic protection.
- No IP address filtering is done. It should be noted that, even with white and blacklisting filtering methods, some attacks where the attacker uses a compromised partner node, obtains a valid partner IP or uses messages that do not require an answer, may still work.
- No layer matching (comparison and cross/checking of sender and return addresses of different protocol layers) is done on HSS or DEA. In some cases, a direct connection between the roaming partners is absent; instead, the interconnection is mediated by one or several IPX/GRX providers (see figure 3). It should be noted that, in such cases the layer matching cannot be performed. Even if the layer matching is implemented, some attacks still would work because spoofing at different layers could be possible, which eventually allows an attacker to bypass the controls put in place.
- No sanity check is made at the receiving node e.g. check for a preceding message that would be there in a normal message flow.
- The attacker knows the MSISDN (phone number) of the victim and address of the edge node (e.g. DEA).

To many readers, especially those with IT background, the aforementioned assumptions may sound too wide and unlikely to be realistic. However, in the cellular industry where SS7 interconnection with absolutely no security has been working quite well for more than 30 years, those assumptions are confirmed to be realistic: Indeed, they can be found in many operator networks, if not all. Initially when the SS7 network was designed, the interconnection network was intended to be used only by the trustworthy government owned operators and hence, there was no obligation to provide any security. However, at present, due to changes in regulations and opening of the telecommunication backend to new entrants, the number of stakeholders who are connected to the interconnection network is increasing day by day. In this real, the question who will finance the additional costs and overhead for certificate management is highly debatable.

There are no statistics or public information about the number of operator networks that would fall under the assumptions that we have made, as it is more likely that most of the operators are hesitant to disclose whether they are vulnerable. Furthermore, lack of internal network monitoring and security audits, and the recent revelation of the attacks [17] [12] where the similar configurations were exploited, strengthens our assumptions.

In our attack scenario, the operator that is under attack has a LTE network within which he may use NDS/IP security [2]. However, on the interconnection edge, he has a Diameter Edge Agent (DEA), which is collocating an Interworking Function (IWF) corresponding to [3]. Another scenario that works in the similar manner is where the operator does not deploy a DEA. Instead, he connects the nodes directly to the interconnection link and implements the interworking functionality at that node. Such ”direct connection” of important core network nodes are not often, but we speculate that, in future, with Network Function Virtualization the international operators attempt to optimize the usage of their nodes and eventually end up setting the aforementioned direct connections due to ignorance.

VI. Interworking Attack Scenario

The attacks that we describe in this section are the typical downgrading attacks where the the attackers intentionally lower the strong security of a particular protocol or system to that of a much less secure legacy system. Even though such types of attacks are common in the radio access networks [18], they rarely seen in the core signalling systems. As mentioned before, the general idea is that an attacker pretends to a legacy SS7 network or node, thereby forcing the more secure LTE Diameter network to use SS7 MAP protocols for further communication.

The first step for an attacker is to obtain the IMSI of the victim, as the IMSI is one of the primary user identifier needed for majority of the communication within the interconnection network. There are several ways to obtain the IMSI, but, we present an attack vector which use the IWF and describe the procedure to obtain IMSI based on the knowledge of MSISDN in Diameter-based network.

The attacker starts his attack by querying the targeted victim's network using the MAP SRI SM command. However, the success of this attack is guaranteed only in absence of *home routing* and if the Diameter interconnection of the targeted operator is established over the S6c interface with additional support for IWF. The IWF of the targeted network translates the MAP SRI SM to Diameter Send Routing Info For SM Request (SRR) as depicted in figure 6.

The attacker impersonates as a partner SMSC or an IWF (for the two IWFs scenario) in the querying network and claims only to support legacy SS7 MAP by sending the MAP SRI SM request over the interconnection network.

1) The attacker sends a MAP SRI SM request containing the MSISDN to the targeted victim's network. On the underlying protocol layer that facilitates routing (routing is usually facilitated by the Signalling Connection Control layer i.e. SCCP layer of SS7 protocol stack), the attacker can use his own Global Title Calling Party Address (CgPA), since no layer matching is done between SCCP and rest of the MAP layers. In addition to the aforementioned parameters such as victim's MSISDN and cgPA, the attacker requires Service Centre Address (SCA) and set the SM-RP-PRI priority flag in order to

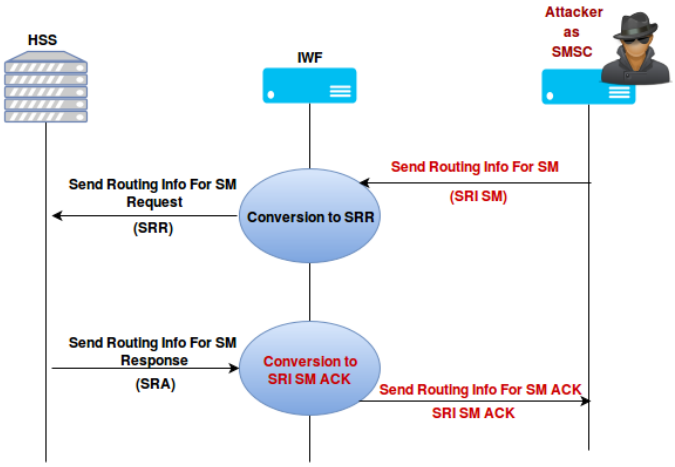

Fig. 6. IMSI disclosure attack using *SRI SM*

craft the MAP SRI SM request command. The attacker can spoof the SCA to hide his identity, whereas the SM-RP-PRI flag enables him to receive relevant information from the HSS of the targeted network even when the victim is not being served by the network in context.

2) The targeted network's IWF receives the MAP SRI SM request and converts it into the Diameter SRR by mapping the received MAP parameters to the corresponding Diameter AVPs. For instance, Diameter AVPs such as SC-Address, MSISDN, and SM-RP-PRI are directly populated based on the corresponding MAP parameters. Whereas the Origin Host/ Realm and Destination Host/Realm AVPs are mapped from the received SCCP CgPA and called party address (CdPA) parameters respectively. More information about these mapping procedures can be found in Annex A.3.5.1 of [3].
3) Once the mapping as described in the previous step is done, the IWF routes the SRR towards HSS of the targeted network via DEA/ DRA. The HSS responds with the Diameter *Send Routing Info For SM Answer (SRA)* command, which contains the IMSI in the User-Name AVP (refer section 5.2.1.1 of [19] for more details) and the nodes currently serving the victim in context. The SRA command is routed back to the IWF again via DEA/DRA.
4) The targeted network's IWF receives the Diameter SRA and converts it into MAP SRI SM response by mapping the received AVPs to the corresponding MAP parameters. The IWF routes the MAP SRI SM response towards the roaming interconnection. If the attack in context is successful, the SRA command contains all the AVPs that an attacker is expecting. In such cases, the IWF populates the MAP SRI SM response by mapping the received AVPs to the corresponding MAP parameters as follow (only the most important parameters are listed):
   - **IMSI** is populated with the value contained in the SRA User-Name AVP.
   - **Network-Node-Number** is populated with the value contained in either of SRA MME Number for MT SMS, MSC-Number, SGSN-Number, or IP-SM-GW-Number AVPs. This field contains the nodes which are currently serving the victim and hence, it can be used by the attacker to launch further attacks or to estimate the rough location either based on MSC or MME number.
   - **Origin and destination Host/Realm** AVPs are mapped to SCCP CgPA of the targeted network's HSS address and SCCP CdPA of the attacker's network address (i.e. the actual GT which enables the attacker to receive the response) respectively.
5) Furthermore, the IWF of the targeted network will send the MAP *Inform Service Center* message to the attacker to confirm the completion of the requested information delivery. However, from the point of view of the attacker, this message is rudimentary, since he would have already received the desired information such as the targeted victim's IMSI, serving node address and possibly the address of the HSS

The aforementioned IMSI retrieval attack is crucial, as the IMSI is used a priori to launch the actual location tracking attacks. This is mainly due to the extensive use of IMSI in Diameter based communication, instead of just the MSISDN or Mobile Station Roaming Number (MSRN) in SS7 based networks. There exist several other ways of obtaining the IMSI, such as using false base station, WLAN access point and EAP-AKA protocol. However, we omit further description about those methods, as they are beyond the scope of this paper.

We now investigate how the four SS7 based location tracking attacks can be extended over a Diameter based network using the Interworking Functions.

Attack 1: Location disclosure using call setup messages The MAP SRI has no direct mapping to Diameter, as is there is no specific entry in the 3GPP standards regarding how the IWF should handle it. This in turn forces the attacker to directly submit the request command in context to the HSS, hoping that the HSS would support a multi-domain scenario. However, the operators rarely connect their HSS directly to the interconnection network, and hence, the success chances of this attack is very unlikely.

Attack 2: Location disclosure using SMS protocol messages using *SRI SM* As mentioned before in the preparation step of an attacker to retrieve IMSI of the victim, the MAP SRI SM message sent to an IWF node retrieves the information about the serving node along with IMSI. Since this attack follows the exact same set of steps of the IMSI disclosure attack, we would skip the repetition of the same. The serving node information in terms of the SRA MME Number for MT SMS in the network configuration of our presumed scenario provides a coarse-grained estimate of the victim's location, specifically at the granularity of MME serving area.

Attack 3: Location disclosure using CAMEL location management function messages

Diameter has no direct mapping of the MAP Any Time Interrogation (ATI) command in IWF related specifications. However, an attacker can perform the hybrid attack of using MAP PSI command as described below, provided he has successfully retrieved the IMSI and serving node information.

1) An attacker poses as an IWF himself (say IWF2) and opens a *MAPv2* channel by sending a *MAP PSI* request to the target network's IWF (say IWF1). This request contains the IMSI and serving node information (i.e. the destination MME serving the victim) which he has previously obtained. In addition to that, the attacker must include the parameters such as *Invocation identity* (which can be a random value) and *Requested Information* (which is set to retrieve *Location information*) [20] [13] in the *MAP PSI* command that he uses for the attack.
   Optionally, the *Requested Information* parameter can include sub-parameters like *Active Location Retrieval requested* and *Location Information in EPS supported*, to obtain more fine-grained location details from the targeted network. The attacker can also request information such as subscriber state, the International Mobile Station Equipment Identity (IMEI), and software version of the victim. For many attackers, the IMEI along with software version is probably one of the most interesting information to have, as they might enable the attackers to launch device specific targeted attacks.
2) The receiving IWF1 of the attacked network converts the *MAP PSI* request into a *Diameter Insert Subscription Data Request (IDR)* as per the mapping guidelines provided in [4] and [3]. During this mapping, the IWF populates *User-Name* AVP based on the IMSI contained in the MAP PSI request and sets the *IDR-flag* to value '3' (this indicates that the location information is requested), along with generating a *Session ID*. The IDR message is then directed to MME/SGSN.
3) The MME/SGSN replies to the IDR command using *Diameter Insert Subscription Data Answer (IDA)* over the SGd/Gdd interface as specified in [21]. Depending on the information requested, the IDA message includes the *EPS User State* and *EPS Location information* AVPs, which contains the subscriber (victim) state and cell ID respectively.
4) On the receipt of IDA message, the IWF 1 translates that into *MAP Provide Subscriber Data Info Ack (PSI ack)* message as per the guidelines specified in the section 8.11.2 of [1]. In particular, the translated PSI ack contains the location information (Cell ID or GPRS information) and subscriber state (if it was requested in step 1).

A variant of the attack in context is when the attacker poses as home-HLR of the victim and sends the MAP *Insert Subscriber Data* command instead of PSI. Even in this case, the MAP specific messages will be translated [11] into IDA/IDR to finally return the MAP *Insert Subscriber Data Ack* (ISD) containing the victim's subscription data.

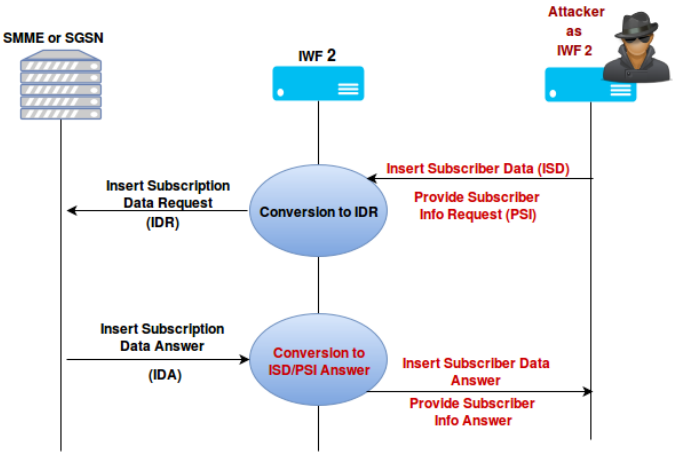

Fig. 7. Location disclosure attack using *MAP PSI*

Attack 4: Location disclosure emergency location service messages

The 3GPP standards for IWF (i.e. [4] and [3]) does not specify the procedures for handling MAP PSL command and hence, the direct mapping to Diameter specific command is not possible. Even if there were relevant specifications, the maximum achievable accuracy of the location is similar to that of the location information retrieved using *PSI command*.

VII. Countermeasures

Interworking with legacy equipment cannot be discontinued without serious service interruption, however, there are several measures which can be deployed in order to improve the security of the interconnection as we describe below:

The first line of defence is the protection of the IMSI, specifically by deploying the home routing for SMS based communication messages, as it makes the IMSI retrieval via the interconnection network much harder. The second layer of defence is to improve the Interworking Function with security features. The Interworking Function should have some additional layers of security, in particular we suggest:

1) Basic SS7 filter or firewall that that effectively verifies whether a message is:
   - network internal or to be received via the interconnection.
   - communicated within the GT range of a contract partner.
   - for an outbound roamer who is actually roaming.
2) Whitelisting of partners and the protocols that they use i.e. an LTE-only partner should use Diameter and not suddenly send a MAP message.
3) Implement NDS/IP security over the Diameter Edge Agents with roaming hubs and with partners who has direct connection along with support for Diameter.

4) AVP specific filtering and modifications e.g. dummy location in MAP PSI over the interconnection.

Diameter security is much closer to the traditional Internet security, which deploys IP based firewalls. In addition, The operators should validate whether the origin realm AVP belongs to one of their partners, and if not, such messages should be either discarded or filtered for further analysis. For the routing level security, the routing need to be based on the origin identity and not on the hop-by-hop identity between nodes to avoid the attack outlined in [22].

VIII. Conclusion

Telecommunications is an intricate system made up of diversified, circuitous subsystems with a multiplicity of different technologies. The complexity increases even further in the worldwide interconnection network which connects operators for the purpose of roaming, as such interconnection contains all possible kinds of legacy systems. Therefore, even the fully fledged LTE operators deploy Interworking Functions to be able to communicate with their partners with legacy technologies. This paper takes the existing SS7 based location tracking attacks into consideration and further investigates the behaviour of the attacks, when they are run against the interconnection nodes with Interworking Function support. Even though some of the attacks fail to harm the LTE networks, the successful attacks that we described, prove the feasibility of translation of legacy attacks on the newer protocols or networks which are believed to be secure. Furthermore, the Interworking functionality may be potentially used to launch other type of attacks such as Denial of Service against a subscriber by using Cancel Location or Purge commands, which is part of our ongoing research.

In conclusion, we argue that the newer generation of mobile networks are vulnerable to legacy attacks. The attacks described in this paper not only outlines a novel evolution of legacy attacks, but also it appeals to be relevant to the current state of telecommunication industry, where the operators are gradually upgrading to networks along with LTE roaming. While, those operators continue to be vulnerable by still supporting some SS7 functionalities until all their roaming partners fully upgrade their networks, the proposed countermeasures are expected to make them relatively secure.

Acknowledgment

The authors would like to thank the GSMA RIFS group members for their drive to improve the security of the global interconnection network and in particular, Looi Kwok Onn for spotting some technical hurdles and suggesting measures to overcome them.

References

[1] 3GPP, "Mobile Application Part (MAP) specification," 3rd Generation Partnership Project (3GPP), TS 29.002, Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/29002.htm

[2] 3GPP, "3G security; Network Domain Security (NDS); IP network layer security," 3rd Generation Partnership Project (3GPP), TS 33.210. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33210.htm

[3] 3GPP, "InterWorking Function (IWF) between MAP based and Diameter based interfaces," 3rd Generation Partnership Project (3GPP), TS 29.305, Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/29305.htm

[4] 3GPP, "InterWorking Function (IWF) between MAP based and Diameter based interfaces," 3rd Generation Partnership Project (3GPP), TR 29.805, Jul. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/29805.htm

[5] T. Engel, "Locating mobile phones using signalling system 7," in *25th Chaos communication congress*, 2008.

[6] K. Nohl, "Mobile self-defense," in *Vortrag auf dem Chaos Communication Congress 31C3, Hamburg*, 2014.

[7] A. De Oliveira and P.-O. Vauboin, "Worldwide attacks on ss7 network," *FTP: http://2014. hackitoergosum. org/slides/day3_Worldwide_attacks_on_SS7_network_P1security_Hackito_2014. pdf*, 2014.

[8] S. Puzankov and D. Kurbatov, "How to intercept a conversation held on the other side of the planet," 2014. [Online]. Available: http://2014.phdays.com/program/tech/36930/

[9] T. Engel, "Ss7: Locate. track. manipulate," in *FTP: http://events. ccc. de/congress/2014/Fahrplan/system/attachments/2553/or iginal/31c3-ss7-locate-track-manipulate. pdf*, 2014.

[10] S. P. Rao, "Analysis and mitigation of recent attacks on mobile communication backend," 2015.

[11] S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura, "Unblocking stolen mobile devices using ss7-map vulnerabilities: Exploiting the relationship between imei and imsi for eir access," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1171–1176.

[12] "Signaling system 7 (ss7) security report." [Online]. Available: http://tinyurl.com/SS7-Security-report

[13] 3GPP, "Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase X; Stage 2," 3rd Generation Partnership Project (3GPP), TS 23.078, Sep. 2007. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23078.htm

[14] 3GPP, "Functional stage 2 description of Location Services (LCS)," 3rd Generation Partnership Project (3GPP), TS 23.271, Sep. 2007. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23271.htm

[15] "Open cellid." [Online]. Available: http://opencellid.org/

[16] "Shodan: The search engine for internet of things." [Online]. Available: https://www.shodan.io/

[17] O. Coskun, "Why nation-station malware targets telco networks," 2015. [Online]. Available: http://www.slideshare.net/merCokun1/defcon23-why-nationstatemalwaretargettelcoomercoskun-51440112

[18] D. Fox, "Der imsi-catcher," *Datenschutz und Datensicherheit*, vol. 26, no. 4, pp. 212–215, 2002.

[19] 3GPP, "Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)," 3rd Generation Partnership Project (3GPP), TS 29.338.

[20] 3GPP, "Basic call handling; Technical realization," 3rd Generation Partnership Project (3GPP), TS 23.018, Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23018.htm

[21] 3GPP, "MME Related Interfaces Based on Diameter Protocol," 3rd Generation Partnership Project (3GPP), TS 29.272, Sep. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/29272.htm

[22] C. Bonnet, "From ss7 to diameter security," 2015. [Online]. Available: http://www.slideshare.net/zahidtg/from-ss7-to-diameter-security