# Mobile Subscriber Profile Data Privacy Breach via 4G Diameter Interconnection

Silke Holtmanns*, Ian Oliver and Yoan Miche

*Nokia Bell Labs, Security Research, Karakaari 3, 02610 Espoo, Finland*
*E-mail: silke.holtmanns@nokia-bell-labs.com; ian.oliver@nokia-bell-labs.com; yoan.miche@nokia-bell-labs.com*
**Corresponding Author*

Received 08 September 2017;
Accepted 05 October 2018

## Abstract

The interconnection network (IPX) connects telecommunication networks with each other on the globe. The IPX network enables features like voice and data roaming with your mobile device while traveling. Designed as a closed network it is now opening and unauthorized entities now misuse the IPX network for their purposes. The majority of the IPX still runs the Signalling System No 7 (SS7) protocol stack, while the more technically advanced operators roll out and deploy Diameter based LTE roaming. SS7 is known to suffer from many attacks. The first attacks using the Diameter protocol appeared. We will show how an attacker can breach the subscriber's privacy by deducting the subscriber profile from the Home Subscriber Service (HSS) and use the obtained information. The subscriber profile contains all key information related to the users' subscription e.g. location, billing information, MSISDN etc. We will close with a recommendation how to prevent such an attack.

**Keywords:** SS7, Diameter, IPX, security.

*Journal of ICT, Vol. 6_3,* 245–262. *River Publishers*
doi: 10.13052/jicts2245-800X.634

**List of Abbreviations:**

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AVP | Attribute Value Pair |
| CSG | Closed Subscriber Group |
| DEA | Diameter Edge Agent |
| DoS | Denial of Service |
| HLR | Home Location Register |
| HSS | Home Subscriber Service |
| Id | Identity |
| IDA | Insert Subscription Data Answer |
| IDR | Insert Subscription Data Request |
| IMSI | International Mobile Subscriber Identity |
| IPX | Internetwork Packet Exchange/Interconnection Network |
| ITU | International Telecommunication Union |
| LTE | Long Term Evolution |
| MAP | The Message Application Protocol |
| MDT | Mobile Drive Test |
| MME | Mobility Management Entity |
| MSC | Mobile Switching Center |
| NMT | Nordic Mobile Telephony |
| SGSN | Serving GPRS Support Node |
| SM | Short Message (commonly known as SMS) |
| SMSC | Short Message Service Center |
| SRA | Send Routing Information for SM Answer |
| SRR | Send Routing Information for SM Request |
| SS7 | Signalling System No 7 |
| ULA | Update Location Answer |
| ULR | Update Location Request |

## 1 Introduction

It is taken for granted that we can use our phone for data and calls when being abroad and travelling. We rarely consider what happens in the background when we switch on our phone after our arrival in another country. You actually connect to a network that knows at that point of time nearly nothing about you, still in the end you can make calls, receive text messages, access your cloud data, e-mail and social networks and are being charged on your home-network bill, even if the operator you connect you has never seen you before.

**Figure 1** Simplified IPX Network.

**Figure 2** Old NMT Advertisement from Siemens.

This all is possible because operator networks communicate through a private signalling network, the Interconnection Network or IPX network. All network operators are connected through it with each other, sometimes directly, sometimes indirectly via service providers. There are hundreds of (mobile) network operators in the world, so below there is very simplified view of the network:

The IPX network is a private network and not the Internet. To understand the security issues related to it, we go briefly into the evolution and history of the IPX network. The first roaming network was the Nordic Mobile Telephone Network (NMT) between Norway, Finland, Sweden and Denmark [1] in 1981.

At that time most network operators were state owned and there was trust between the partners. The Nordic countries had a long history of cooperation and therefore the main goal was to enable services for their users using a closed network. They designed protocols and messages to serve that goal. The Signalling System No. 7 (SS7) [2] is a network signalling protocol stack used worldwide between network elements and between different types of operator networks, service providers on the interconnection. It was standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T) more than 35 years ago and consists out of various protocol layers, like the ISO-OSI stack, but not the same. At that point of time, security was not the main design criteria, as the usage of SS7 was envisioned to be used only in a closed network between trusted partners.

## 2 Background

### 2.1 SS7 Briefer

SS7 specifies the exchange of information over the signalling networks mainly to enable the establishment of phone calls across networks i.e. to enable roaming. Over the time the usage of the protocol has been extended to accommodate many services. The Message Application Protocol (MAP) is the most important application protocol in the SS7 stack. MAP is standardised by the 3rd Generation Partnership Project (3GPP) [3] offers a wide range of additional features for enabling mobility, roaming, SMS, and billing.

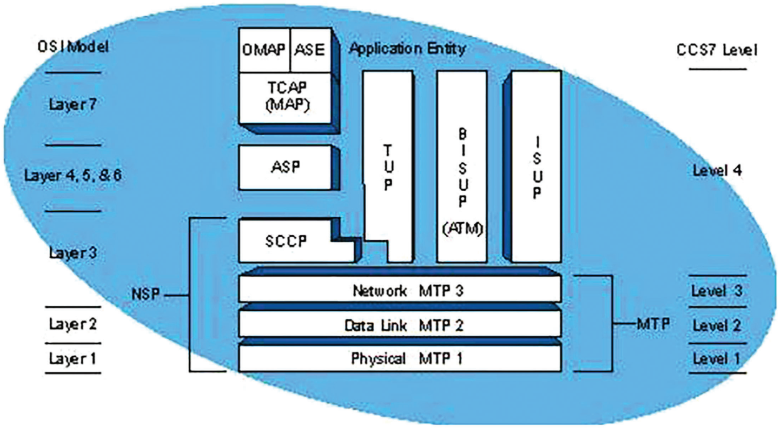

**Figure 3** SS7 Stack and comparison to ISO-OSI Model.

*Source:* [32].

The MAP protocol is currently the most used protocol for Interconnection application messages, but the long term Long Term Evolution (LTE) replacement Diameter is appearing for 4G and 5G Interconnection communication. But LTE is not only more bandwidth on the radio link, it is also a major evolution of the core network and the messages and protocols therein.

## 2.2 Diameter Background

Diameter is the evolution of the SS7 (and its IP variant SIGTRAN) and MAP protocol that is used within and between the 4G LTE networks. LTE uses the Diameter protocol for communication between the network elements inside a network and between networks. In a Diameter based network architecture all elements are connected via an IP interface. The network nodes use either the newer the Diameter base protocol specified in IETF RFC 6733 [4] or the one defined in RFC 3588 [5]. The 3GPP specifications that specifies the telecommunication specific usages of the Diameter protocol has already moved from RFC 3588 to RFC 6733, but of course in the deployments many nodes still support the older version of the protocol. In Diameter each interface has its own application interface specification which is defined separately in a different 3GPP specification document and defines the application specific additions to the base protocol.

Mobile network operators often connect directly only to very few of their partners. To their other partners, they connect via interconnection service provider. Therefore, a communication between two networks can traverse many intermediate nodes in the interconnection network. Network operators, also chose the route a message travels based on aspects like quality and costs, this implies, that a route chosen today for an outbound roamer can be different then the route chosen tomorrow. Below a simplified connection between two LTE enabled networks:

Mobile network operators usually deploy a Diameter Edge Agent (DEA) that resides on the border of their network and is the first contact point for messages coming over the interconnection link. The underlying connection channel terminates in the DEA and the network topology is “hidden” behind the DEA. The most important nodes from security point of view are the Home Subscriber Server (HSS) which holds the subscriber profile information and the and Mobility Management Entity (MME) which takes care of the user’s mobility (often combined with a Visited Location Register VLR). These two are the key core network nodes for the users’ mobility and personal data. 3GPP envisioned for those potentially untrusted interfaces over the

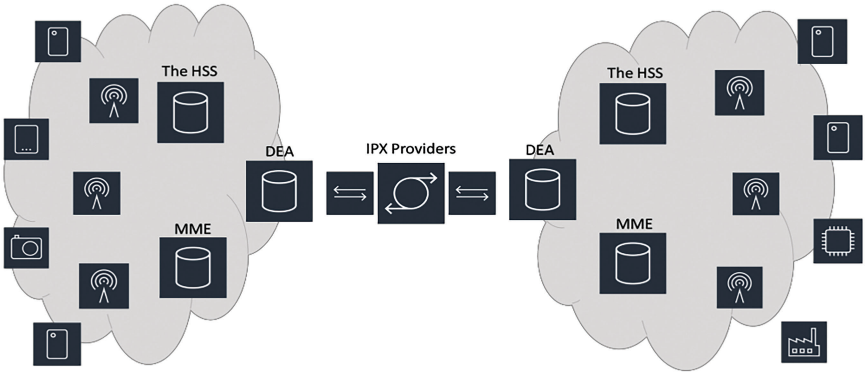

**Figure 4** Connection between two LTE Networks.

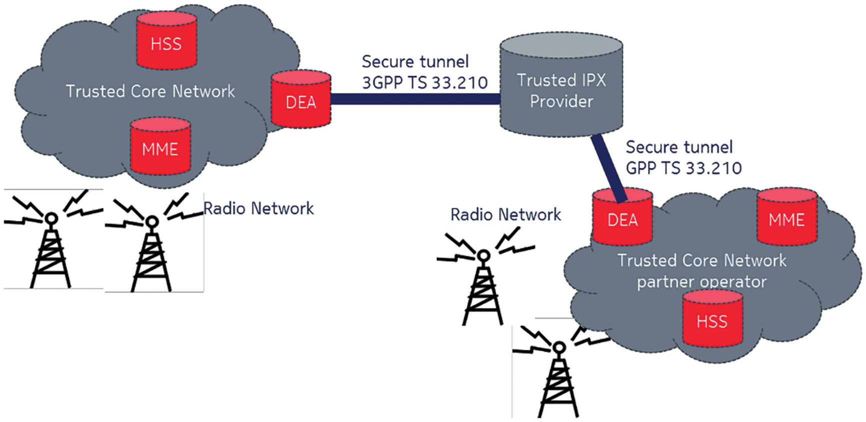

**Figure 5** Interconnection between LTE operators using diameter with NDS/IP.

interconnect to use IPSec or alternatively TLS (see TS 33.210 Network Domain Security/IP [6]).

The practical issue is that even if IPSec is implemented in many core network nodes, it is commonly not used. The reason for that are manifold. Since this is an international network, the question of the trusted root certificate, revocation list, key generation etc becomes a political one. In addition, there are Interconnection Service Providers i.e. messages often traverse several "hops" between the operators. And some operators just don't have the financial resources or expertise to secure their network communications. Beside one needs to recognize, that in the beginning, there were no security costs, as the network was fully closed and secure, and then "suddenly" potential security costs are required and there is no clear return of investment for those. For any operational team in an operator it is difficult to obtain financial and human resources for this kind of extensions. A small group of experts identified a potential vulnerability in exploitation of SS7 by entities that have unauthorized access to the interconnection network was identified very early [30] and 3GPP standardization took measures to counter those threats by drafting MAP Security (MAPSec) TS 33.200 [31], but that never found a wide deployment base and took off.

The most commonly used diameter-based interface for roaming is the S6a/S6d interface between HSS and MME as specified in 3GPP TS 29.272 [7]. Without it, there is no roaming possible, so switching it of is not an option. Diameter is the core network protocol for LTE and is constantly extended. Even if Diameter is a different protocol than the MAP protocol, the underlying functional requirements e.g. authenticating the user to set up a call etc there are many similarities in the messages used for Diameter and the SS7 MAP protocol messages. Still, there is not a one-to-one mapping for each MAP message to each Diameter command and vice versa. The 3GPP has defined some basic degree of interworking between the SS7/MAP protocol and Diameter in the technical report TR 29.805 [8] which is more of a technical study character or in the technical specification TS 29.305 [9]. There exist attacks which exploit this kind of interworking [10], but we will not go into that topic in this article. The messages used in this article are ones that differ to a large degree from their corresponding MAP counterparts.

## 3 Recent Security Research Results

The first widely publicly known attack was presented in 2008 by Tobias Engel [11] and consisted out of a coarse location tracking attack on MSC or country level. It was a SS7 MAP based attack. It was then very quiet up to 2014, when a string of major SS7 attacks were published and their practical feasibility demonstrated:

- Location Tracking [12–14, 27]
- Eavesdropping [13, 14]
- SMS interception [13, 14]
- Fraud [13, 14]
- Denial of Service [13, 14]
- Credential theft [14]
- Data session hijacking [15, 16]
- Unblocking stolen phone [17]

- One-time password theft and account takeover for Telegram, Facebook, Whatsapp [18, 19]

Recently the first interconnection vulnerabilities were published for the 4G diameter protocol.

- Location tracking [20]
- Denial of Service [21]
- SMS interception [22]

There is a constant evolution and fine tuning of those attacks ongoing e.g. in [28] and [29] many of the above attacks were refined and the Insert Subscriber Data command features exploited to modify and extract data. This article can be seen in the spirit of the further refinements and extensions of those attacks, where we will work out the details of [29].

The main obstacle for an attacker is to gain access to the closed and private Interconnection network. But the legal rules for network operators for renting out access to the interconnection to service providers differ between countries, also some nodes are attached and visible on the internet for example using shodan.io. Therefore, attacker with sufficient technical skills or financial resources have found ways to breach the privacy of the network. Since this is a worldwide problem of many different players, standardization of security is of uttermost importance to obtain a feasible security system. The GSMA Association has provided their members with a set of protection measures for SS7 and issued in summer 2017 diameter interconnection security rules to help their members countering this threat.

## 4 Mobile Subscriber Profile Attack

We have to make some assumption on the network configurations. Those assumptions, even if they seem to be quite generous, can be found to in many real-world network deployments and are quite common. The first assumption is that the network does not have any filtering functionalities or a diameter firewall deployed at the edge of the network, typically represented by a Diameter Edge Agent (DEA). Secondly, that the attacker is in possession of the phone number i.e. the MSISDN and has access to the Interconnection network.

### 4.1 IMSI Retrieval

The first step for an attacker is to obtain the user's International Mobile Subscriber Identity (IMSI). The IMSI is the key subscription identifier inside the core network, not the MSISDN.

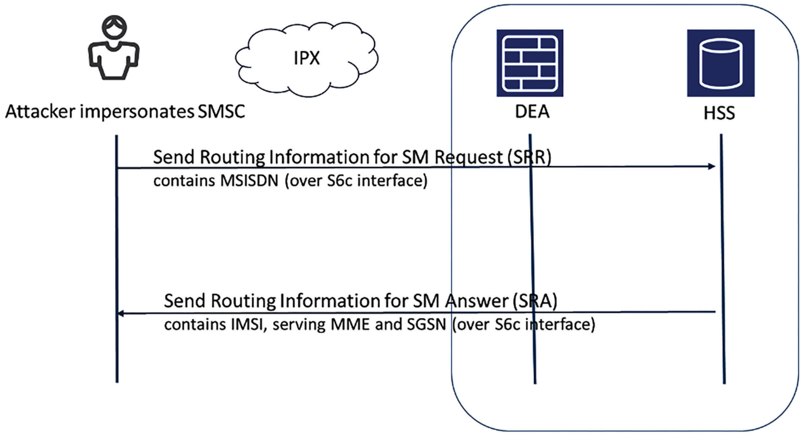
IPX
Attacker impersonates SMSC
DEA
HSS
Send Routing Information for SM Request (SRR)
contains MSISDN (over S6c interface)
Send Routing Information for SM Answer (SRA)
contains IMSI, serving MME and SGSN (over S6c interface)

**Figure 6** IMSI Retrieval using SMSC impersonation.

There are several ways of doing that. One can set up a false base station and just call all devices in the area to send them their IMSI. Even if 3GPP is currently studying how to protect the IMSI, we can assume that this will be a common way to obtain the IMSI for many years to come. Alternatively, a WIFI access point which is able to issue a EAP-SIM call to the device. We will focus on how to obtain the IMSI via the Interconnection, as we assume that the attacker does not want to travel to his victim. The attacker impersonates a SMSC Short Message Service Center i.e. he claims to have a SMS for a user and he wants to deliver it and needs therefore the "contact details" as he is only having the phone number (MSISDN). This is a quite common and valid roaming scenario, where a user sends a SMS to a user from another network.

For that purpose, the attacker sends a Send_Routing_Information_For_SM Request (called SRR) to the Home Subscriber Server (HSS) of the user. The message is send not directly to the HSS, but to the DEA of the home operator of this user. This message contains the MSISDN (phone number) of the user. The DEA relays the SRR message to the HSS (so not to reveal the HSS address) and the HSS will provide via the DEA in a Send_Routing_Information_For_SM Answer (SRA) the IMSI and the serving nodes for the user i.e. serving MME and SGSN.

## 4.2 Subscriber Profile Retrieval

The attacker is now in possession of the IMSI of the user, the serving MME and SGSN. It should be noted, that between the IMSI acquisition and the actual

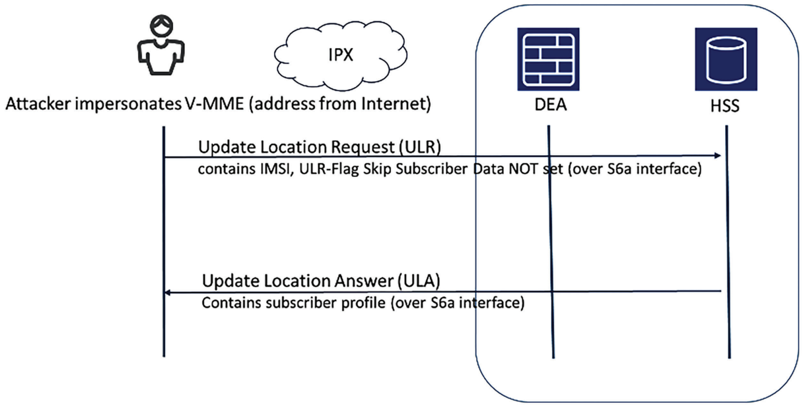
IPX
Attacker impersonates V-MME (address from Internet)
DEA
HSS
Update Location Request (ULR)
contains IMSI, ULR-Flag Skip Subscriber Data NOT set (over S6a interface)
Update Location Answer (ULA)
Contains subscriber profile (over S6a interface)

**Figure 7** Profile extraction using ULR.

attacks might elapse a large time. The IMSI is embedded into the users UICC card (commonly called SIM card) and does not change during the lifetime of the card, only with replacement of the card it changes.

For the subscriber profile retrieval, the attacker performs a location update i.e. the attacker claims, that this user has "landed" in his network, this is a typical roaming scenario. For this he makes a diameter Location Update Request (ULR) over the S6a interface according to 3GPP TS 29.272 [7]. In this location update request he does NOT set the ULR-Flag "Skip subscriber data", in a normal roaming scenario this indicates to the HSS that the MME requests a fresh copy of the subscriber profile for synchronization purposes. The HSS then send in an update location answer (ULA). This answer then contains the requested subscriber profile.

We will later on elaborate new cases what this subscriber profile contains and what it implies if an attacker gets hold of the subscriber profile. In a nutshell, it described the key attributes for a subscription. We assume, that once an attacker holds a complete subscriber profile of a user of one operators he can deduct the structure of the profile and by that figure out, what are "nice" items to modify for another subscription. Each operator supports different services for his users and has different features deployed therefore each subscriber profile looks somewhat different.

A subtle attacker would reset the MME back (assuming again that the edge does not properly differentiate between internal and external messages). Even if not strictly needed for the profile extraction and modification, it helps the attacker to stay unnoticed.

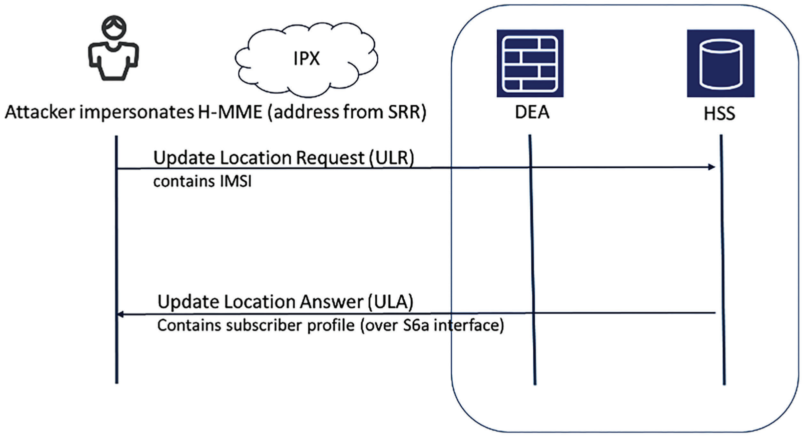
IPX
Attacker impersonates H-MME (address from SRR)
DEA
HSS
Update Location Request (ULR)
contains IMSI
Update Location Answer (ULA)
Contains subscriber profile (over S6a interface)

**Figure 8** Setting back the MME entry to “old home MME”.

## 4.3 Subscriber Profile Modification

We assume that the attacker has the IMSI of a subscriber and wants to modify the subscriber data stored in the MME. A typical scenario would be that he wants to change the settings so that he has more rights and can use more services or become member of a closed subscriber group. He can also set for another subscription the Proximity Service (ProSe) discovery settings differently and by that the target user can then be traced. In either case, the mechanism is the same. There are two “flavours” to that attack. If the user is roaming, then the attack has high chances of succeeding. The attacker would impersonate the Home-HSS, but due to roaming the visited network would only see the DEA address of the home net-work (which can be spoofed by setting the origin realm and origin host), as the message answer does not really need to go through it is no issue to spoof the origin. The DEA address can be found from IR.21 documents on the internet or brute forcing the operator ranges.

The other flavour is, if the attacker tries to modify the profile of the user while the user is in his home network. There the attacker would need to know the address of the home-HSS (potentially again from IR.21), but that address is “less public” then for example a DEA address. But on the other hand operators tend to use ranges of address blocks for their nodes, so a brute force try-and-error may yield the desired result. Also, the network would not even have the lowest of all checks i.e. it does not check, if a message arrives on the interconnection edge which claims to come from an internal node. Therefore,

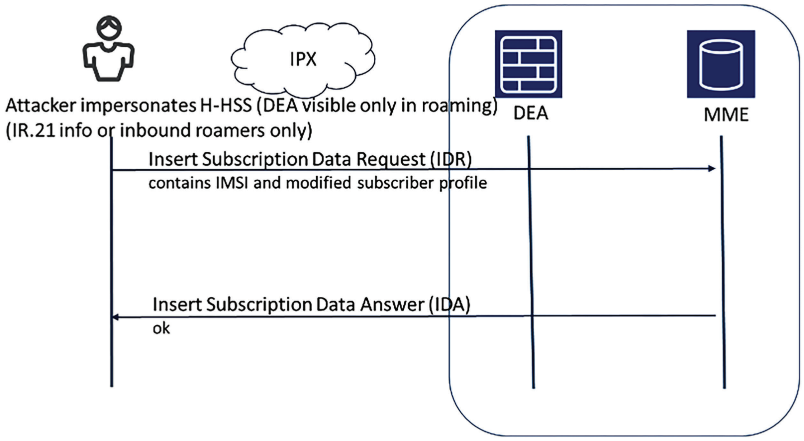
IPX
Attacker impersonates H-HSS (DEA visible only in roaming)
(IR.21 info or inbound roamers only)
DEA
MME
Insert Subscription Data Request (IDR)
contains IMSI and modified subscriber profile
Insert Subscription Data Answer (IDA)
ok

**Figure 9** Subscription Profile Placement in MME.

the attack is considered harder, when the target user is not roaming. The modified profile would stay active until the MME synchronizes again with the HSS and indicates that it would need a fresh profile.

## 5 Subscriber Profile

We saw how an attacker can extract a subscriber profile from an HSS and places a potentially modified profile into the MME. The Subscriber Data Attribute Value Pair (AVP) is of type grouped, which means, there are many “subitems”, some of them are in turn also of type grouped. Many of those items can be used for DoS against the user, basically changing the settings to something strange, so that the user would not have a properly working access. Since a simple DoS is possible using a Purge or Cancel Location message [21] or [28], we assume that the attacker had a more sophisticated attack in mind like changing the profile to obtain some fraud or similar things. The following items could be interesting for an attacker to modify. It should be noted, that some of them are features, that are quite new and therefore not commonly deployed yet.

**Closed Subscriber Groups (CSG)** are intended to be used for groups which require special security like fire brigade, rescue workers, police or similar. If in the update location the fake MME includes an equivalent PLMN id list, the HSS returns not only the subscriber data but also the Closed Subscriber Group List for that IMSI [7] 5.2.1.1.3. In [7] 5.2.2.1.2 it is described how using a IDR command with CSG replaces the existing Closed Subscription Data stored in the MME. I.e. an attacker may exploit this to add himself to a closed group by adding the CSG-Id.

**Proximity Security (ProSe)** is a security concept for local means of communication and intended for public services usage (e.g. governments). The ProSe Subscription Data is also part of the Subscription Data. The ProSe Subscription Data contains sub-AVPs [7] and 3GPP TS 29.344 [23] that describe how a device can be discovered locally i.e. could be potentially misused for local tracking.

**Mobile Drive Test (MDT)** was designed as method to get data from the terminal to discover coverage holes in a network. For this a consent was introduced, as it basically allows also close tracking of the user. The MDT-User-Consent is part of the subscription data [24] TS 32.422. The flag modification might be combined with another attack.

**MSISDN** i.e. phone number is also part of the subscriber profile. The effects of changing this entry in the MSISDN needs still further study, but potentially poses quite a fraud and impersonation risk. Those risks need to be validated in detail.

**Access Point Node (APN)** configuration is used for data access and the impacts of changing that to another address (beside the obvious DoS if changed to a non-valid address) need to be studied further.

The subscription data also contains the charging characteristics [7] and TS 29.061 [25]. The modification of those may hinder proper charging of the user and result in a potential fraud scenario.

## 6 Protection Measures

In a normal roaming case, the visited MME would need to obtain some subscription information, but since not all fields that are mentioned in the subscriber profile are need in a roaming case a firewall can filter the outgoing traffic to suppress those not needed AVPs e.g. closed subscriber group etc.

Another simple method is to validate the authenticity of the request. Is this an internal request arriving at the edge? Is this MME address really belonging to a roaming partner and is the same as usual? Can the outbound user really travel that distance since the last location update? The MME should not accept IDR messages for its own subscriber coming from the DEA. Of course, the long-term goal should be to really set-up an IPSec based secure communication with the partners, but there are many non-technical obstacles on that road. This kind of knowledge needs to be implemented in a Signalling aware firewall at the edge of the network. The GSMA organization established a working group and is driving to identify attack vectors and related countermeasures for 4G and 5G Interconnection Security to stop these kind of attacks. This work is also contributed to this effort.

## Acknowlegdements

This work has been supported by the finish DIMECC CyberTrust Project and the EU Horizon 2020 project SCOTT Secure Connectable Trusted Things.

## References

[1] International Telecommunication Union (ITU) - T, Signalling System No.7 related specifications, https://www.itu.int/rec/T-REC-Q/en

[2] Nordsveen Arve M., Norsk Telemuseum, 'Mobiltelefonens historie i Norge' (2005). https://web.archive.org/web/20070213045903/http://telemuseum.no/mambo/content/view/29/1/

[3] 3rd Generation Partnership Project (3GPP), TS 29.002, 'Mobile Application Part (MAP) specification,' v14.3.0, Release 14, (2017). http://www.3gpp.org/DynaReport/29002.htm

[4] Internet Engineering Task Force, IETF RFC 6733 'Diameter Base Protocol', October 2012. https://tools.ietf.org/html/rfc6733

[5] Internet Engineering Task Force, IETF RFC 3588, 'Diameter Base Protocol', September 2003. https://tools.ietf.org/html/rfc3588

[6] 3rd Generation Partnership Project (3GPP), TS 33.210, '3G Security, Network Domain Security (NDS), IP Network Layer Security' v14.0.0 Release 14 (2016). http://www.3gpp.org/DynaReport/33210.htm

[7] 3rd Generation Partnership Project (3GPP), TS 29.272, 'Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol', v14.3.0, Release 14 (2017). http://www.3gpp.org/DynaReport/29272.htm

[8] 3rd Generation Partnership Project (3GPP), TR 29.805, 'InterWorking Function (IWF) between MAP based and Diameter based interfaces', v 8.0.0, Release 8 (2008). http://www.3gpp.org/DynaReport/29805.htm

[9] 3rd Generation Partnership Project (3GPP), TS 29.305, 'InterWorking Function (IWF) between MAP based and Diameter based interfaces', v 14.0.0, Release 14 (2017). http://www.3gpp.org/DynaReport/29305.htm

[10] Holtmanns, S., Rao S., and Oliver, I. (2016). 'User Location Tracking Attacks for LTE Networks Using the Interworking Functionality', IFIP Networking Conference, Vienna, Austria.

[11] Engel, T. (2008). 'Locating Mobile Phones using Signaling System 7', 25th Chaos Communication Congress 25C3. http://berlin.ccc.de/∼tobias/25c3-locating-mobile-phones.pdf

[12] Engel, T. (2014). 'SS7: Locate. Track. Manipulate', 31st Chaos Computer Congress 31C3. http://berlin.ccc.de/∼tobias/31c3-ss7-locate-track-manipulate.pdf

[13] Positive Technologies, 'SS7 Security Report', 2014. https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf

[14] Nohl, K. (2014). SR Labs, 'Mobile self-defense', 31st Chaos Communication Congress 31C3. https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

[15] Nohl, K., and Melette L. (2015). 'Chasing GRX and SS7 vulns', Chaos Computer Camp. https://events.ccc.de/camp/2015/Fahrplan/system/attachments/2649/original/CCCamp-SRLabs-Advanced_Interconnect_Attacks.v1.pdf

[16] Positive Technologies, 'Mobile Internet traffic hijacking via GTP and GRX', (2015). http://blog.ptsecurity.com/2015/02/the-research-mobile-internet-traffic.html

[17] Rao, S., Holtmanns, S., Oliver, I., and Aura, T. (2015). '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.

[18] Fox-Brewster, T. (2016). Forbes, 'Hackers can steal your facebook account with just a phone number'. http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#6860b09b8fa7

[19] Fox-Brewster, T. (2016). Forbes, 'Watch as hackers hijack WhatsApp accounts via critical telecoms flaw'. http://www.forbes.com/sites/thomasbrewster/2016/06/01/whatsapp-telegram-ss7-hacks/#7ca2999d745e

[20] Rao, S., Holtmanns, S., Oliver, I., and Aura, T. (2016). 'We know where you are', IEEE NATO CyCon, In *8th International Conference on Cyber Conflict*, 277–294.

[21] Kotte, B., Holtmanns S., and Rao, S. (2016). 'Detach me not – DoS attacks against 4G cellular users worldwide from your desk', Blackhat Europe. https://www.blackhat.com/eu-16/briefings.html#detach-me-not-dos-attacks-against-4g-cellular-users-worldwide-from-your-desk

[22] Holtmanns, S., and Oliver, I. (2017). 'SMS and One-Time-Password Interception in LTE Networks', IEEE ICC Conference, Paris.

[23] 3rd Generation Partnership Project (3GPP), TS 29.344, 'Proximity-services (ProSe) function to Home Subscriber Server (HSS) aspects' v14.1.0, Release 14, (2017). http://www.3gpp.org/DynaReport/29344.htm

[24] 3rd Generation Partnership Project (3GPP), TS 32.422, 'Telecommunication management; Subscriber and equipment trace; Trace control and configuration management,' v14.0.0, Release 14, (2017). http://www.3gpp.org/DynaReport/32422.htm

[25] 3rd Generation Partnership Project (3GPP), TS 29.061, 'Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)' v14.3.0, Release 14, (2017), http://www.3gpp.org/DynaReport/29061.htm

[26] Telecom Dictionary, SS7 Stack, http://www.telecomdictionary.com/Telecom-Dictionary-SS7-Protocol-Stack-Definition.html

[27] Puzankov, S. (2017). Positive Technology, 'Stealthy SS7 Attacks', IEEE Network and Systems Security (NSS), International Workshop on 5G Security.

[28] Mashukov, S. (2017). Positive Technology, 'Diameter Security: An Auditors Viewpoint', IEEE Network and Systems Security (NSS), International Workshop on 5G Security.

[29] Holtmanns, S., Oliver, I., and Miche, Y. (2017). Nokia Bell Labs, 'Subscriber Profile Extraction and Modification via Diameter Interconnection', IEEE Network and Systems Security (NSS), International Workshop on 5G Security.

[30] ETSI, (1998). SMG27, 'Status Report from SMG10 to SMG27', Annex D, http://www.qtc.jp/3GPP/GSM/SMG_27/tdocs/P-98-0531.pdf

[31] 3rd Generation Partnership Project (3GPP), TS 33.200, '3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security,' v1.0.1, Release 4, (2001). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2275

[32] Telecom Dictionary, 'SS7 Protocol Stack' http://www.telecomdictionary.com/Telecom-Dictionary-SS7-Protocol-Stack-Definition.html

## Biographies

**Silke Holtmanns** is a security expert at Nokia Bell Labs and research new attack vectors and mitigation approaches. She holds a PhD in Mathematics and her current research area combines data analytics, penetration testing and privacy. The creation of new and the investigation of existing security attacks using SS7, Diameter and GTP protocols via the Interconnect lead to new countermeasures for 4G/5G networks. She is also actively supporting the evolution of 5G intereconnection security in 3GPP. The identfied countermeasures using techniques combine monitoring, filtering, and advanced protection with machine learning. As an expert on existing and future attack patterns for interconnection security, she provides advice to our company, customers, standard boards, and regional and national regulating governmental bodies e.g. US FCC or EU ENISA. Recently, she started investigating potential risk areas of 5G, which has a different architecture and design concept compared to the previous releases.

She serves as a regular organizer and editor for workshops and special issues. She has over 18 years experience in mobile security research and standardization with strong focus on 3GPP security and GSMA. She is rapporteur of ten 3GPP specifications and editor of the GSMA Interconnection Diameter Signalling Protection document.

**Ian Oliver** works for Nokia Bell Labs as a senior security researcher specialising in high-integrity and trusted Network Function Virtualisation, and on occasion the more theoretical underpinnings of privacy and privacy engineering. He also holds a Research Fellow position at the University of Brighton working with the Visual Modelling Group on diagrammatic forms of reasoning and semantics.

Prior to that he worked as the privacy officer for Nokia Services and for eleven years at Nokia Research Centre working with Semantic Web, UML, formal methods and hardware-software co-design. He has also worked at Helsinki University of Technology and Aalto University teaching formal methods and modelling with UML. He holds over 40 patents in areas such as The Internet of Things, semantic technologies and privacy, as well as numerous papers in these areas. He is the author of the book: Privacy Engineering – A Data Flow and Ontological Approach. (www.privacyengineeringbook.net)

Ian lives in Sipoo, Finland with his wife, two children, dog and cat. https://www.bell-labs.com/usr/ian.oliver

**Yoan Miche** was born in 1983 in France. He received an Engineer's Degree from Institut National Polytechnique de Grenoble (INPG, France), and more specifically from TELECOM, INPG, on September 2006. He also graduated with a Master's Degree in Signal, Image, Speak and Telecom from ENSERG, INPG, at the same time. He has worked in the Information and Computer Science (ICS) lab of Aalto University as a postdoc for 4 years, after obtaining his D.Sc. from INPG (France) and Aalto University (Finland). He is currently a Cybersecurity Researcher at Nokia Bell Labs, Finland.