Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

# New Attack Vectors for Mobile Core Networks

**Silke Holtmanns**

Mobile network operators connect towards each other through the private interconnection network (IPX). This closed private network enables international calls, data, messages and many other services across network and country borders. It connects billions of users and Internet of Things devices. In the last years, evidence arose that the network has been misused for various kind of attacks. We will introduce the foundations of the interconnection network, give the security background. Outline existing attacks and describe a new charging attack. Various activities are ongoing to improve the security of the IPX network, which we will describe. We close with an overview of potential risk areas for 5G core networks.

**Keywords:** IPX, SS7, interconnection, diameter, charging, 4G, 5G, mobile network

Citation: Holtmanns, S. (2019). New attack vectors for mobile core networks. *Magdeburger Journal zur Sicherheitsforschung*, *18*, 943–951. Retrieved August 5, 2019, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_064_Holtmanns_MobileCoreNetworks.pdf

# 1 Introduction

When we travel abroad, we assume that our phones connect us with our loved one and we can use data, receive messages and make calls. When we arrive in the country of our choice and switch on the phone, we often do not think what happens in the background before we can obtain and use the local network operator services.

Depending on your destination, the network you connect to has never seen you before. It has no preknowledge about the subscriber, it is not aware if you have a pre-paid or post paid subscription, it doesn't have the cryptographic credentials to protect the air interface and it can't authenticate you. Still in the end we can make calls etc and are charged on our home-network bill. To achieve this the communication network operators 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 (called IPX providers). Those network operators are competing with each other, they belong to different political systems and are in many cases independent of each other, still they cooperate and connect through the IPX. This network spans the whole globe and there are large undersea cables connecting the continents with each other, so Figure 1 shows a very simplified view of the network.

The first roaming network was the Nordic Mobile Telephone (NTM) Network 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 main goal was to enable services for their users and to enlarge the offerings. They built a system that was working nicely and served that goal securely in this specific setting.

The networks connected to each other using the Signalling System No. 7 (SS7) protocol stack between network elements and between different types of operator networks, service providers on the interconnection and within operator networks. In this closed private network no additional security was needed. SS7 was standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T) [2] and consists out of various protocol layers, similar to the ISO-OSI stack. The system turned out to be a huge success. The IPX network and the services running over it have expanded rapidly and now there are about 2000 entities in the IPX network.

Today, the IPX network uses SS7 and its IP version SIGTRAN heavily for control traffic. User data traffic uses the GPRS Tunnelling Protocol (GTP). But with upcoming 3G/4G network deployments also the interconnection between operators take more and more place using the diameter protocol.

# 2 Existing Attacks

About 10 years ago the first publicly known attack was presented by Tobias Engel [3] and consisted out of a coarse location tracking attack on MSC (Mobile Switching Center) or country level if a user was abroad. It was a SS7 Message Application Part (MAP) based attack. It was then very quiet up to 2014 and the following years, when a string of SS7 attacks were published and their practical feasibility demonstrated. Also, attackers started to exploit the IPX for criminal gains:

- Location Tracking on CellID level [4], [5], [6]
- Eavesdropping [5], [6]
- SMS interception [5], [6]
- Fraud [5], [6]
- Denial of Service [5], [6]
- Credential theft [6]
- Data session hijacking – GPRS Tunneling Protocol [7], [8]
- Unblocking stolen phone [9]
- OTP (One Time Password) theft and account takeover for Telegram, Facebook, Whatsapp or banking TANs [10], [11], [12], those attack were usually part of a larger attack

Those researchers showed potential attack vectors, that those attack vectors were exploited can be seen by the attack in [10] where fraudsters used it or in [13], [14] where entities were caught or in [15] where a service company offers this kind of activity as a service.

# 3 Existing Attacks for Diameter

When a new mobile generation appears, usually the radio part is updated first to provide the users with more bandwith, then the core network nodes are upgraded. The last part to be updated is the communication between the operators i.e. the IPX. In 2014, most of the IPX communication still took place using SS7 or its IP version SIGTRAN. Slowly the industry moved toward 3G/4G diameter based IPX communications. Even if diameter is a different protocol, the underlying functional design ideas are similar in many cases. Therefore, researchers together with the industry were evaluating the diameter protocol for potential misusage and countermeasures. Here some of the findings:

- Interworking and bidding down attacks [16]
- Location tracking [17], [18]
- Denial of Service [19], [20]
- Fraud [21], [22], [23]

The IPX network is not an open network, where every script kid can just send messages to. It is still a private network. A potential attacker has to gain access to the IPX network first to perform attacks. In the EU to encourage competition, operators have to offer the

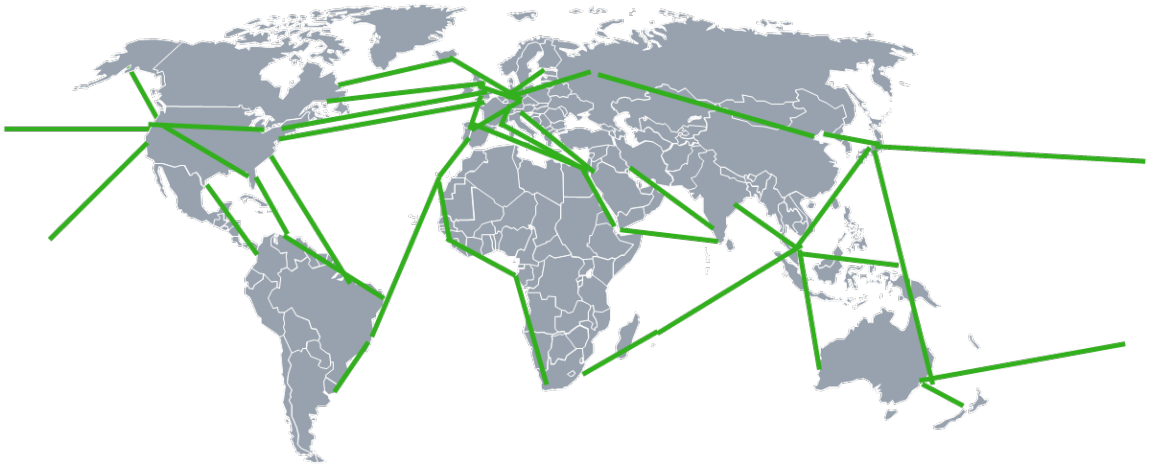

Figure 1: Major Interconnection Links

services that they have themselves for their customer also to potential virtual operators. The idea is to reduce the threshold and avoid anti-competitive behavior. From a practical point of view, an operator has no good possibility to validate up-front if the potential B2B customer is a legitimate virtual operator or a fraudster. Therefore, an attacker can »just« rent access.

Another entry point is offered by nodes that are connected to the IPX AND the Internet. Those kinds of nodes are visible on search engines like Shodan.io or can be found through scans of the Internet. Classical attack routes like exercising pressure e.g. political, bribing, social engineering or similar also exist. In all cases, the attacker needs to have sufficient telecommunication technical skill and financial resources. In addition, attack software is not as widely available as for example for Internet type of attacks, where tools like Burp or Metasploit make attackers and security engineers lives easier.

The operator community GSMA is a good example of an industry that changes. Today, GSMA has a CVE program and a working vulnerability management process and several specifications outlining how to protect networks against the known attacks. Also, their cooperation with the security research community is very constructive. But still there are many operators out there and not all of them are diligent when it comes to securing their networks.

## 4 New Attack Vectors for 4G

For our research we used a Nokia internal emulator, which allowed us to realistically test attack scenario without accidentally damaging a real running operational network. This kind of emulators are normally used for interoperability tests between network nodes e.g. for new software releases. We used the nodes marked in pink in Figure 2.

The following nodes are relevant related to our attack:

- User Equipment (UE) the mobile terminal
- Enhanced Node B (eNB) the antenna
- Mobility Management Node (MME)
- Home Subscriber Service (HSS)
- Serving Gateway (SGW)
- Packet Gateway (PGW)
- Policy and Charging Rule Function (PCRF)

With regard to the interface, the S9 interface is the one relevant for our attack. The S9 interface is a diameter based roaming interface between two networks. It is used to exchange charging related control information, in particular the Policy Charging Control (PCC) information. The PCC defines everything about your subscription:

- Data type
- Data rates
- Whatever cellular service you can think off
- Defines how to handle you and what to grant you »service flow filters«
- Usually identified by a string

In Figure 3 we have the case of a roaming scenario where a finnish subscriber visits Austria.

The terminal UE connects to the serving network eNB and then the MME, SGW are involved in setting up the communication. The home PGW and HSS are involved in the set-up. The first S9 communication (after setting up the basic communication) would be the Charging Control Request (CCR), where the visited network would enquire about the subscription details of the subscriber from the home network. The answer would be in the Charging Control Answer (CCA).

In addition, on that interface the home network has the possibility to make a Re-Authentication Request (RAR) message with a Re-Authentication Answer. This message is for example used when some things with regard to the subscription change, while the user is abroad.

We will show now how those messages can be mis-

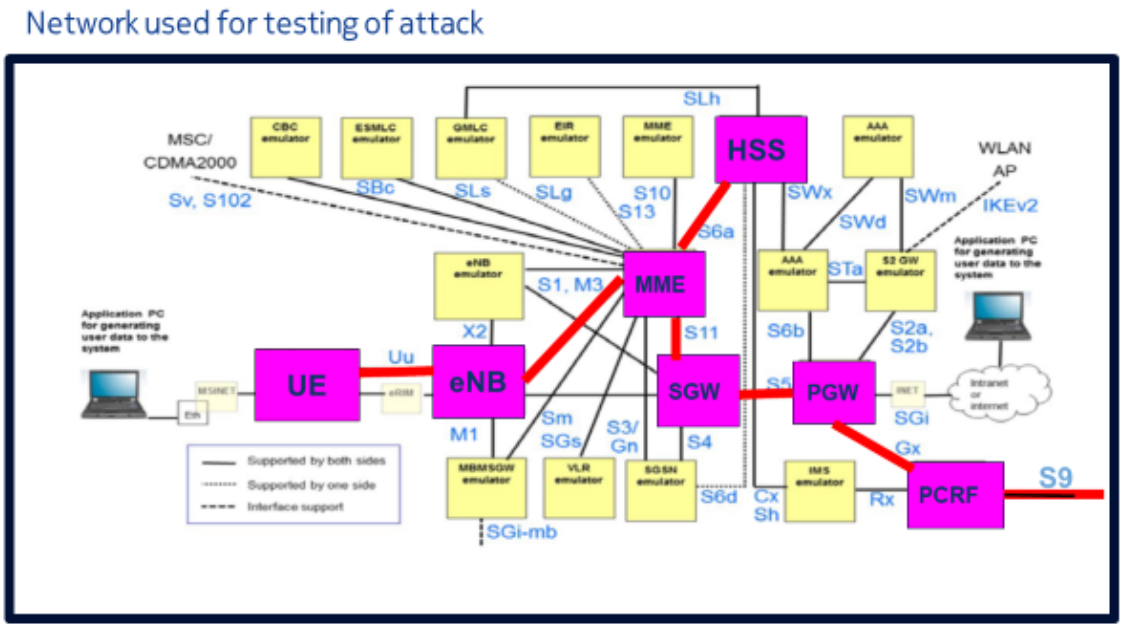


Figure 2: Core Network Simulator

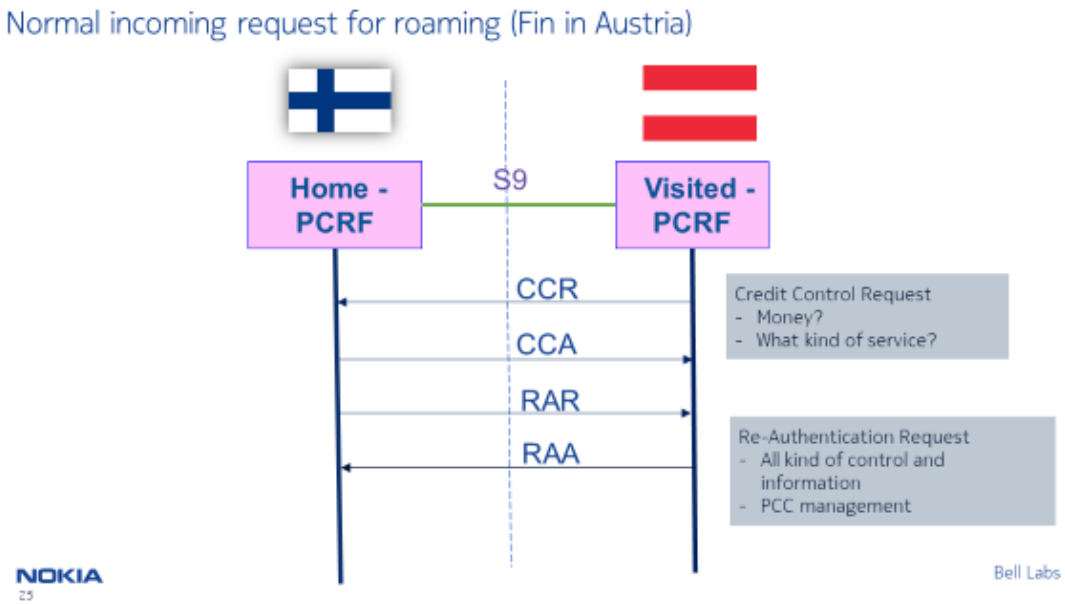


Figure 3: Normal roaming flow on S9

used to influence the type of service a user gets. The attack has two steps:

1. to obtain the PCC of a »good subscription« to know the format
2. to change a low value subscription into a good subscription

Of course, for a DoS scenario one can just change the subscription into a »no service« type of subscription, but we will focus on the fraud case.

In the first step the attacker poses at the home network and request the PCC via a RAR message. This kind of approach assumed basically that the receiving network does not make any sanity check (see Figure 4).

If the user is roaming, then such a RAR request has better chances of getting through. But for that the attacker would need to know, to which network the users roamed to.

The attacker is now in possession of a PCC from a good subscription e.g. data flatrate from an IoT device. The next step is to use the PCC obtained to update a »cheap subscription« with good terms, as shown in Figure 5.

For this the attacker poses again as home network and sends a RAR request. If the receiving operator is doing proper data handling, then the request should not go through, because

1. it is coming from own network
2. the user is its own subscriber

There are some routing tricks and double entry approaches possible to fool a potential filtering, but those strongly depend on the implementation of the filtering. But as said before, not all network operators are diligent to really validate those details at the network edge. An alternative approach can be taken, when the user is not in his home network (see Figure 6).

In this case the attacker poses as home network while the subscription is roaming. This is an interesting case from fraud perspective, as the attacker may sell an »upgrade« for a subscription to a user who goes to a high-cost country.

Those attacks illustrate how important it is to validate requests that arrive at the network edge via various means e.g. velocity check, validation of origin host and realm, realm/host based routing etc. GSMA has some specific specifications dedicated to that topic for their members e.g. IR.88, FS.19.

# 5 Risk Areas for 5G Core Network Security

5G offers improved security and privacy on the air interface. It also harmonized authentication for non-cellular access. It also allows virtualization of network functionalities including security filtering functions.

The 5G core network architecture introduces the concept of a Service Based Architecture (SBA). Each network node offers their data and information as a service resource, which can be requested from other nodes through HTTP Rest APIs. The Home Network, called HPLMN and the Visited Network (VPLMN) communicate via the edge proxy (SEPP) to exchange data related to charging, security, user identity, mobility etc using the SBA bus (red in Figure 7). The SEPP is a newly introduced architectural node, which improves the 5G security architecture compared to the 3G and 4G, where de-facto often a security filtering node was in the communication path, but it was not official part of the 3GPP architecture (Figure 7).

While this offers a large degree of flexibility in terms of extensibility and deployment, it has the drawback, that it requires careful configuration to avoid unauthorized data access, modifications or deletions. By definition a communication bus each entity can communicate with each other entity on the bus. The SBA uses the standardized REST API, which is well-known from web services. It will be a big challenge not only to ensure the correct authentication of all entities, but also if they are authorized to perform a certain action on a given resource.

# 6 Conclusion

Mobile networks connect towards each other through the Interconnection Network. Every user and cellular enabled device is connected to it through the local operator. Through this networks attacks have been performed using the legacy protocol SS7. The newer 3G/4G diameter protocol offers similar functionalities as the SS7 protocol. In an insufficiently protected case, attacks can also be performed using the diameter protocol and may lead to charging fraud and Denial of Service attacks. The presented attacks could be in particular being bad for IoT devices, where no user is directly involved. Countermeasures exist and can be deployed but require diligence and attention to details.

The upcoming 5G Core Network has a very flexible Service Based Architecture which uses HTTP and REST API. The usage of those protocols requires security expertise to harden it against unauthorized data access. We outlined some potential risk areas and how to approach them.

# 7 Acknowledgments

The research was partially funded by the SCOTT project. The SCOTT project has received funding from the European Union's Horizon 2020 research and innovation program under the grant agreement No 737422.

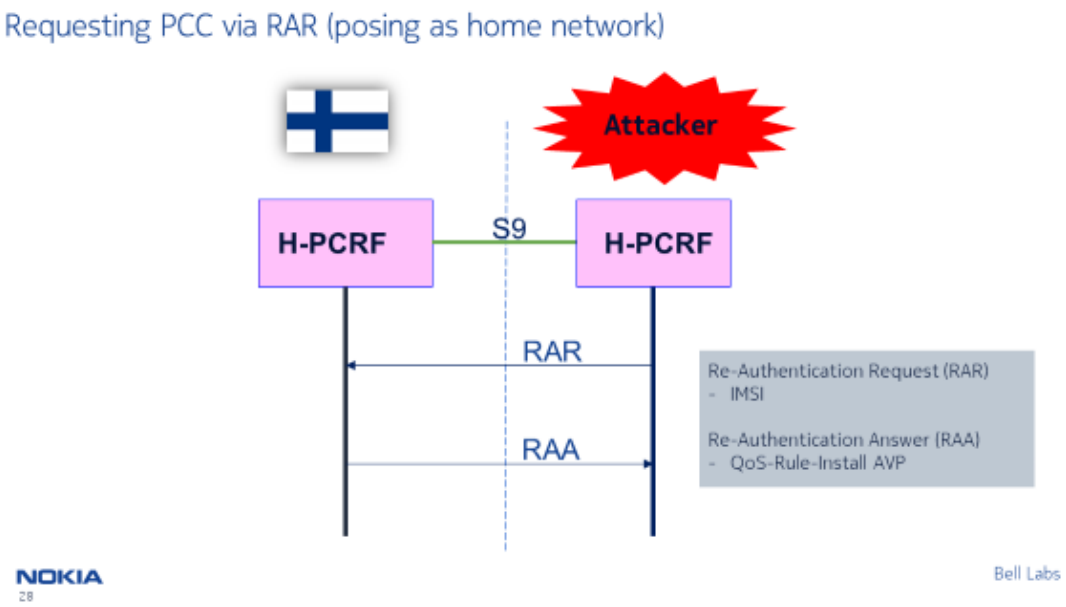


Figure 4: Acquisition of PCC

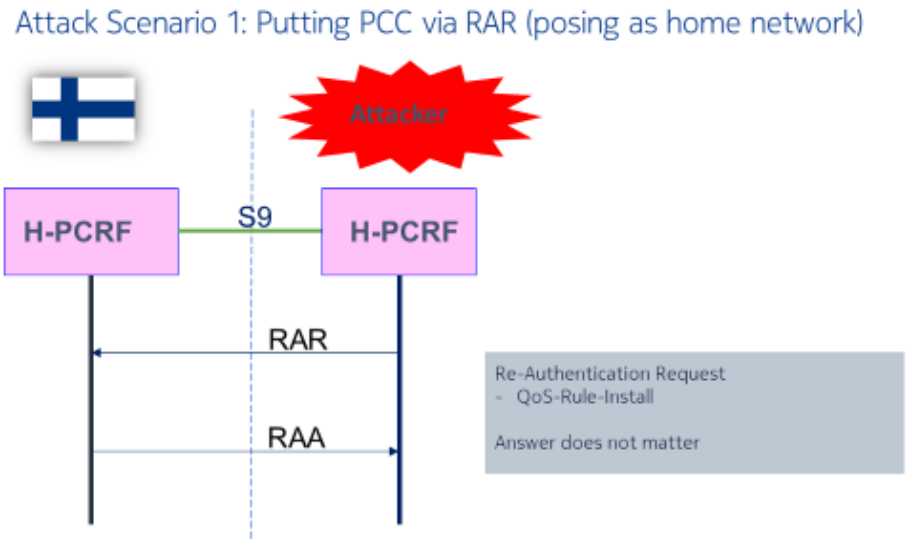


Figure 5: Variant 1 for updating PCC

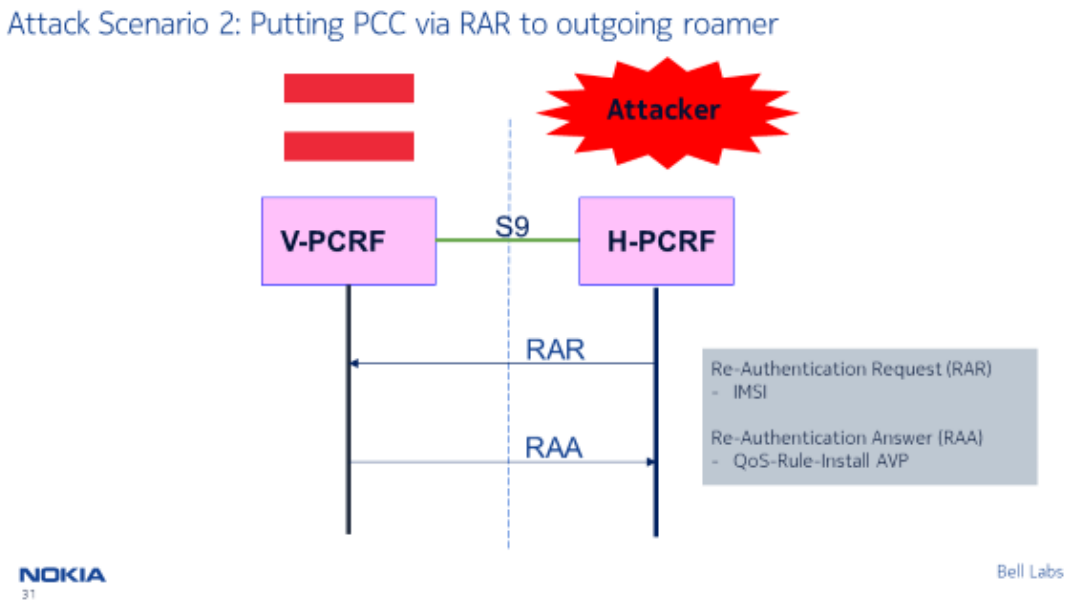


Figure 6: Alternative 2 of updating PCC

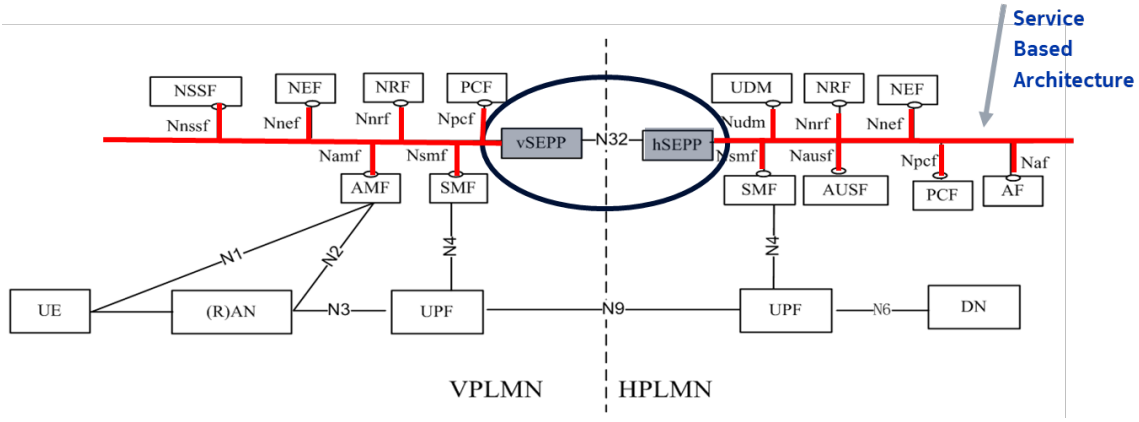


Figure 7: Service Based Architecture – Roaming Scenario

## 8 About the Author

Dr Silke Holtmanns is a distinguished member of technical staff and security specialist at Nokia Bell Labs. She researches new attack vectors and mitigation approaches. The creation of new and the investigation of existing security attacks using SS7, Diameter and GTP via the Interconnect lead to new countermeasures for 4G/5G networks. Her focus lies on the evolution and future of security for mobile networks. For 5G she investigates potential risk areas coming from the combination of IT security and signaling threats. As an expert on existing and future attack patterns for interconnection security, she provides advice and input to customers, standard boards, and regional and national regulating governmental bodies e.g. in US FCC and EU ENISA. She has over 18 years of experience in mobile security research and standardization with strong focus on 3GPP security and GSMA. She is rapporteur of ten 3GPP specifications and of the GSMA Interconnection Diameter Signalling Protection document. She is (co)-author of more than 70 security publications.

## 9 References

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

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

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

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

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

[6] [24] K. 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

[7] [25] K. Nohl, L. Melette, ' Chasing GRX and SS7 vulns', Chaos Computer Camp, 2015, https://events.ccc.de/camp/2015/Fahrplan/system/attachments/2649/original/CCCamp-SRLabs-Advanced_Interconnect_Attacks.v1.pdf

[8] [26] Positive Technologies, 'Mobile Internet traffic hijacking via GTP and GRX', 2015, http://blog.ptsecurity.com/2015/02/the-research-mobile-internet-traffic.html

[9] S. Rao, S. Holtmanns, I. Oliver, T. Aura, '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.

[10] Mathew J. Schwartz, BankInfoSecurity, »Bank Account Hackers Used SS7 to Intercept Security Codes«, https://www.bankinfosecurity.com/bank-account-hackers-used-ss7-to-intercept-security-codes-a-9893 (5.5.2017)

[11] [21] T. Fox-Brewster, Forbes, 'Hackers can steal your facebook account with just a phone number', 2016, http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#6860b09b8fa7

[12] T. Fox-Brewster, Forbes, »Watch as hackers hijack WhatsApp accounts via critical telecoms flaw«, 2016, http://www.forbes.com/sites/thomasbrewster/2016/06/01/whatsapp-telegram-ss7-hacks/#7ca2999d745e

[13] R. Gallagher, The Intercept, »Operation Socialists – The Inside Story of How British Spies Hacked Belgian's Largest Telco«, (2014), https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

[14] Corelan Team, S. Kho, »On Her Majesty's Secret Service – GRX & A Spy Agency«, (2014) https://www.corelan.be/index.php/2014/05/30/hitb2014ams-day-2-on-her-majestys-secret-service-grx-a-spy-agency/

[15] [20] T. Fox-Brewster, Forbes, 'For$20M, These Israelian Hackers will spy on any phone on the planet', 2016, http://www.forbes.com/sites/thomasbrewster/2016/05/31/ability-unlimited-spy-system-ulin-ss7/#5b43b75a7595

[16] [11] S. Holtmanns, S. Rao, I. Oliver, 'User Location Tracking Attacks for LTE Networks Using the Interworking Functionality', IFIP Networking Conference, Vienna, Austria, 2016.

[17] [27] S. Rao, S. Holtmanns, I. Oliver, T. Aura, 'We know where you are', IEEE NATO CyCon, 8th International Conference on Cyber Conflict (2016), pp 277-294

[18] Positive Technologies, »Diameter vulnerabilities exposure report, 2018«, 14.6.2018, https://www.ptsecurity.com/ww-en/analytics/diameter-2018/

[19] [28] B. Kotte, S. Holtmanns, S. Rao, »Detach me not - DoS attacks against 4G cellular users worldwide from your desk«, Blackhat Europe 2016, https://www.blackhat.com/eu-16/briefings.html#detach-me-not-dos-attacks-against-4g-cellular-users-worldwide-from-your-desk

[20] S. Mashukov, »Diameter Security: An Auditor's Viewpoint«, Journal of ICT Standardization, Volume 5, Issue 1, 2017, pp 53-68 https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/3

[21] S. Holtmanns, I. Singh, »4G—Who is paying your cellular phone bill?«, DefCon'26 2018 (Aug), Las Vegas, USA, https://www.defcon.org/html/defcon-

26/dc-26-speakers.html#Holtmanns

[22] S. Holtmanns, J. Ekman, C. McDaid, "Mobile Data Interception from the Interconnection Link", 34C3 Chaos Computer Congress 2017, Leipzig, Germany, (Dec 2017), https://www.youtube.com/watch?v=iNr1KjaR0jM

[23] D. Mende, H. Schmidt, »Attacking NextGen Roaming Networks«, Blackhat Europe (2017), https://www.blackhat.com/eu-17/briefings.html#attacking-nextgen-roaming-networks