Interconnection Security Standards – We Are All Connected

Silke Holtmanns

Nokia Bell Labs, Karakaari 13, 01620 Espoo, Finland
E-mail: Silke.holtmanns@nokia.com

Received 20 September 2016;
Accepted 19 October 2016

Abstract

The interconnection network is a private network that connects all operators of the world. It enables calls, data and many other services across network and country borders. It connects billions of users and also now an increasing amount of Internet of Things devices. Recently, it has been shown that this network can be severely hacked. We will describe the active protection standardizing and what are the threats that we all face.

Keywords: SS7, MAP, interconnection, security, diameter, GSMA.

1 Introduction and History of Interconnection

We are all taken it for granted that we can use our phone for data and calls when being abroad. We rarely consider what happens actually 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 etc and are being charged on your home-network bill. 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 (Figure 1):

Journal of ICT, Vol. 4_1, 1–18.
doi: 10.13052/jicts2245-800X.411

Figure 1 Simplified interconnection network.

It was a long road till today's large Interconnection network which enables data roaming, calls, SMS. We will explain the road, which also explains the security approach of the whole system and is a needed background to understand the standardization in this area.

The first roaming case was the so called Nordic Mobile Telephone Network between Norway, Finland, Sweden and Denmark [3] 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. They designed protocols and messages to serve that goal. The Signalling System No. 7 (SS7) is a network signalling protocol stack used worldwide between network elements and between different types of operator networks, service providers on the interconnection and within operator networks. It was standardised by the International Telecommunication Union, Telecommunication Standardisation Sector (ITU-T) more than 35 years ago [1] and consists out of various protocol layers, similar to the ISO-OSI stack. In short, at that point of time, security was not the main design concern, as the usage of SS7 was considered to be only in a closed network between trusted partners.

2 SS7 Background

2.1 SS7 and Interworking Network Overview

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 more and more services. The Message Application Protocol (MAP) which is standardised by the 3rd Generation Partnership Project (3GPP) [8]

offers a wide range of additional features for enabling mobility, roaming, SMS, and billing. The MAP protocol is currently the most used protocol for Interconnection messages, the long term replacement Diameter is appearing, but currently far from being the main protocol on the Interconnection network.

We will give now a brief example how two non-LTE networks can connect to each other e.g. for roaming. The Home Location Register (HLR), Mobile Switching Centre (MSC), Visitor Location Register (VLR), and Short Message Service Centre (SMSC) are some of the key components of the core network (shown in Figure 2). These nodes are key nodes, when it comes to security and to the existing attacks using the interconnection network. These elements are identified by their Global Title (GT), which are used as addresses for routing messages through the SS7 network using the SS7 MAP protocol [8]. They can be seen as something roughly similar to a MAC address or IP address of a computer.

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

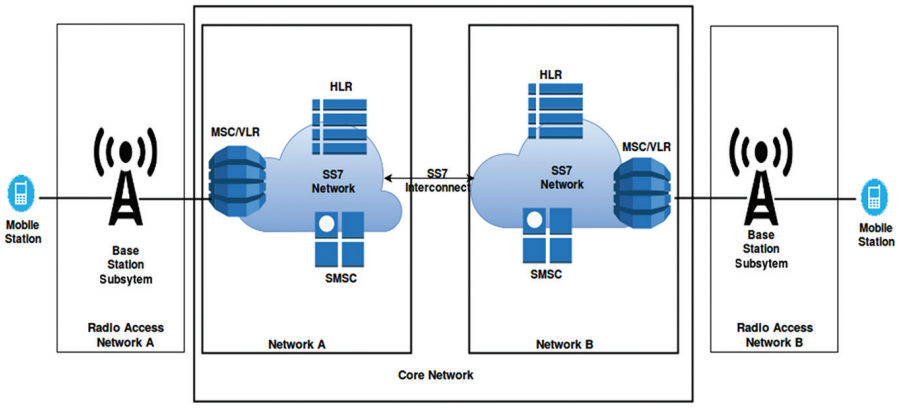

Figure 2 Simple interconnection between two non-LTE networks using SS7.

Today, more and more operators offer Long Term Evolution (LTE) services to their users. But LTE is not only more bandwidth on the radio link, it is also an evolution of the core network and the messages and protocols therein.

3 Diameter Background

Diameter is the evolution of the SS7 and MAP protocol that is used within and between the 4G LTE networks. LTE uses the Diameter protocol for communication between the network elements. In a Diameter based network architecture all elements are connected via an IP interface. The network nodes all support the Diameter base protocol specified in IETF RFC 6733 [9]. RFC 6733 now gradually replaces the earlier RFC 3588 [10] in the 3GPP specifications, which is at the time of writing an ongoing process. In Diameter each interface has its own application interface specification which is defined separately in a different specification document and specifies application specific additions to the base protocol.

To connect two LTE diameter based operators together, often an IPX or interconnection service provider is used. Operator networks usually deploy a Diameter Edge Agent (DEA) that resides on the border of the network as the first contact point for messages coming over the interconnection link. In this context, Home Subscriber Server (HSS) is the evolved HLR and Mobility Management Entity (MME) can be considered to be an evolved MSC (Figure 3).

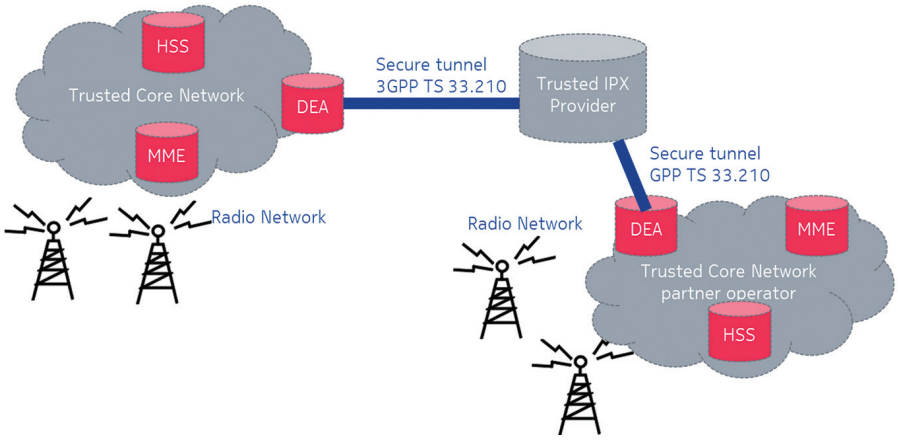

Figure 3 Interconnection between LTE operators using diameter with NDS/IP.

Diameter based communication can be secured using Network Domain Security NDS/IP as specified in 3GPP TS 33.210 [12] i.e. IPSec. We will elaborate on this later on.

Below are some examples, of Diameter using application interfaces by 3GPP:

- S6a/S6d between the Home Subscriber Server (HSS) and Mobile Management Entity (MME) TS 29.272 [5]
- Sh between an IP Multimedia Subsystem (IMS) application server and the HSS TS 29.329 [6]
- S9 between the Policy and Charging Rule Function (PCRF) and the visited PCRF TS 29.215 [7]
- S6c between the HSS and the central SMS functions TS 29.338 [4]
- SGd between MME and SMSC TS 29.338 [4]

Some of those interfaces are actually not intended to be used over the interconnection network and are just operator network internal e.g. Sh is a network internal interface and should not be visible or accessible from outside of the operator network, the S9 interface is intended for be used for roaming and similarly the S6c and SGd are not really inter-operator interfaces. But one has to remember that the interconnection network is a grown organism, one operator merges with another, an operator acquire subsidiaries in another country, network planning is optimized to safe opex etc. Therefore, there have been cases where due to bad configuration, company internal network optimization between subsidiaries or unclear or missing security domain separation or separation was actively bypassed, those interfaces were accessible to some degree from the interconnection network.

Diameter is the core network protocol for LTE and is constantly extended also for 5G and the list above gives only a snapshot of the key interfaces that deploy Diameter. Also note, that the documents provided only give an overview of Diameter for that application, but each of the specifications above references other specifications to enable the whole service.

Even if Diameter is a different 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 [13] or in the technical specification TS 29.305 [14]. Those documents outline, how messages are converted and the Attribute Value Pairs

(AVPs) are mapped, so that a Diameter enabled network node, can communicate with a SS7/MAP node to provide basic services. Some of the attacks later on exploit this kind of interworking [11]. From a standardization point of view, this implies, that the assumption to have a homogenous interconnection infrastructure worldwide with an equal level of security is just an utopia and legacy attacks have to be taken into practical consideration when designing new system.

4 Recent Security Breaches of Interconnection

The first publicly known attack was presented in 2008 by Tobias Engel [17] 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 [15, 23, 24]
- Eavesdropping [23, 24]
- SMS interception [23, 24]
- Fraud [23, 24]
- Denial of Service [23, 24]
- Credential theft [24]
- Data session hijacking [25, 26]
- Unblocking stolen phone [16]
- One time password theft and account takeover for Telegram, Facebook, Whatsapp [21, 22]

Those attacks were not only of theoretical nature, as revelations in [18, 19] and advertisements of "service" companies in [20] or from the darknet (see Figure 4) showed.

Recently the first vulnerabilities were published for the diameter protocol e.g.

- Interworking attacks [11]
- Location tracking [27]
- Denial of Service [28]

The main obstacle for an attacker is to gain access to the 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 (e.g. via shodan.io).

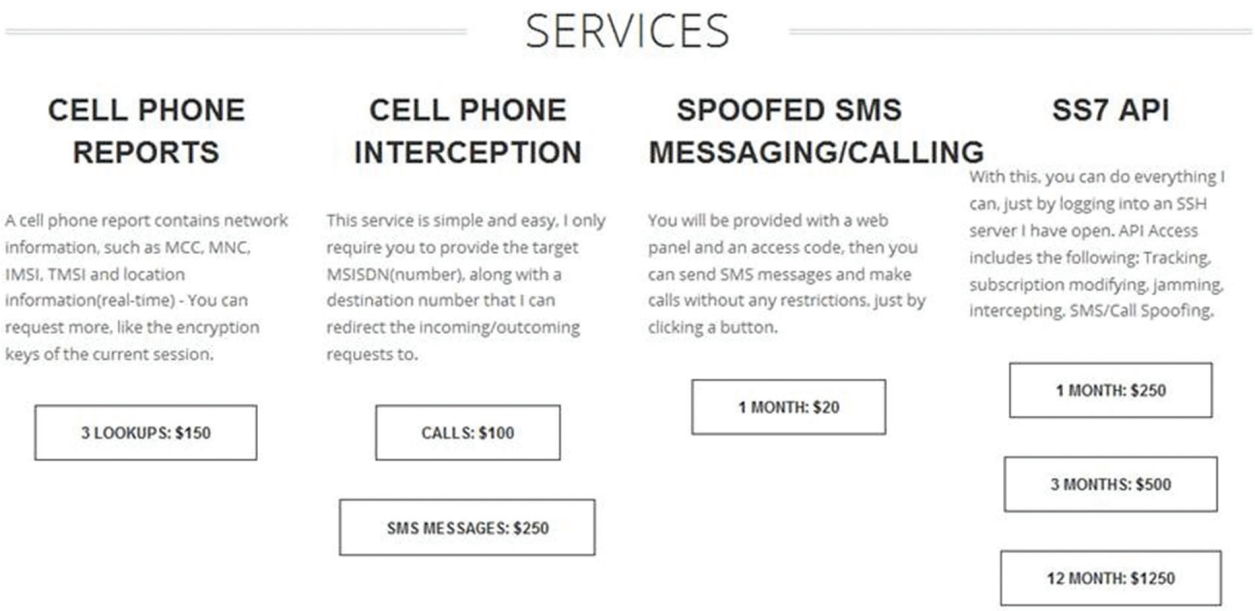

Figure 4 SS7 Interception service offering.

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. We now give an overview where the security standardization for Interconnection is at the time of writing.

5 Security Standardization Activities for Interconnection

5.1 3GPP

The 3rd Generation Partnership Project (3GPP) has defined many key mobile standards e.g. GSM, UMTS, LTE and its security. Their focus lies on the operator network itself and the interfaces between nodes, radio equipment and devices. One of the underlying fundamental problems of the Interconnection network is that it was built on trust and that this trust model no longer applies. In technical terms, that means, that there commonly is no authentication, authorization, confidentiality or integrity protection of messages. One obvious approach is to use IPSec for that purpose.

3GPP assumes that an operator deploys for IP based security on not trustworthy interfaces called Network Domain Security (NDS/IP) as specified in 3GPP TS 33.210 [29]. For diameter-based interfaces it is assumed, that they would be secured using this IPSec specification. IPSec is commonly implemented in new network nodes, but it requires the corresponding support for certificate and credential management. But sad reality is, that the usage is not common as would be desirable. The reasons are manifold (Figure 5):

- Legacy – old nodes may not support IPSec
- False sense of security – interconnection closed network and considered safe
- Political issues – who would be trustworthy enough to issue a root certificate
- Complexity – many parties in different legislations have to be provisioned with PKI infrastructure, management of issuing, revocation etc
- Costs – who will take the costs for the establishment of a world-wide PKI
- Lack of expertise – many operators just don't have the expertise for security, in particular in countries with low turnovers per user

Even with IPSec deployed for securing the communications between operators and service providers, it is not a silver bullet for the problems mentioned before. However, it would narrow down the possibilities for an attacker

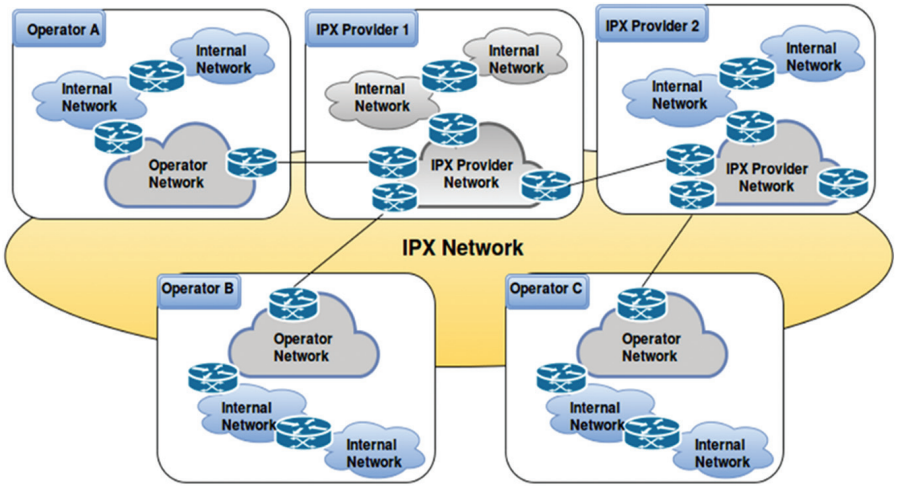

Figure 5 Simplified IPX network.

substantially to breach the security of the interconnection network and could be an important piece in the puzzle to defend attacks and narrow the attack space. But IPSec would NOT provide protection against the following threats:

- Many operators use roaming hubs to offer a maximum number of roaming partners to their customers in particular this is done for low-volume connections.
- IPSec could only be used in a Hop-by-Hop fashion, i.e. there is no assurance that ALL legs of the communication would use IPSec.
- The messages may even transfer via several roaming hubs and the security would only be hop-by-hop and it would not be possible to reliably verify that more than the last leg is secure.
- Due to different legal settings in some countries operators are not too strict with their security checks and rent out interconnection access via their wholesale business.
    - IPSec or TLS does not help against potentially misbehaving "tenants"
    - The incentive to "check" upon well-paying tenants is pretty low
- Nodes might be compromised
    - Due to bad configurations (i.e. visible on Internet and found via shodan.io or other tools)
    - Software problems (i.e. classical bugs)

- Insider attacks (e.g. bribing)
- Governmental pressure

Another technical issue is that the SS7 stack uses the SCCP and MTP protocols and has a different protocol stack, therefore deploying IPSec is quite challenging and requires major changes to a large existing infrastructure. Also for the IP version of SS7 i.e. SIGTRAN IPSec support would require a major effort to upgrade the network worldwide.

Even with all those limitations, deployment of IPSec would be strongly desirable for the now evolving 4G and 5G networks, as there is a technology evolution in the progress and upgrade also in security could be done in the same migration process. Currently, an attacker can impersonate another operator even in direct messages using the Global Title of the operator the attacker wants to impersonate.

MAPSec

3GPP specified in 2007 in TS 33.200 [30] SS7 MAP Security called MAPSec, but that specification has not been practically used or deployed. It is still available for Release-7 (2007) and has never been properly updated or debugged and with the evolution of the system since then its practical relevance can be debated. It is mentioned here for completeness sake:

Node Hardening

Interconnection security is a puzzle and so are the protection measures. One approach is to reduce the amount of potential entry points for an attacker by harden nodes against attacks. 3GPP has been working the recent years on specifying hardening for network nodes, so that their security can be tested and certified. This kind of hardening would reduce the attack space for an attacker substantially and would offer better protection for the network infrastructure in general from unauthorized usage (e.g. fraud). The specifications are:

- TS 33.117, General Security Requirements [31]
- TS 33.116, Security Assurance Specification for MME [32]
- TS 33.250, Security Assurance Specification for PGW [33] (early work)

Interconnection Security

Recently 3GPP Security Group (SA3) started a new work item (NSA), which also encompasses diameter based interconnection security. At the time of writing, the draft working document contains a suggestion how to establish trust in the long run. The approach starts with a group of operators that have a common “level” of security, which would include rules on network hardening,

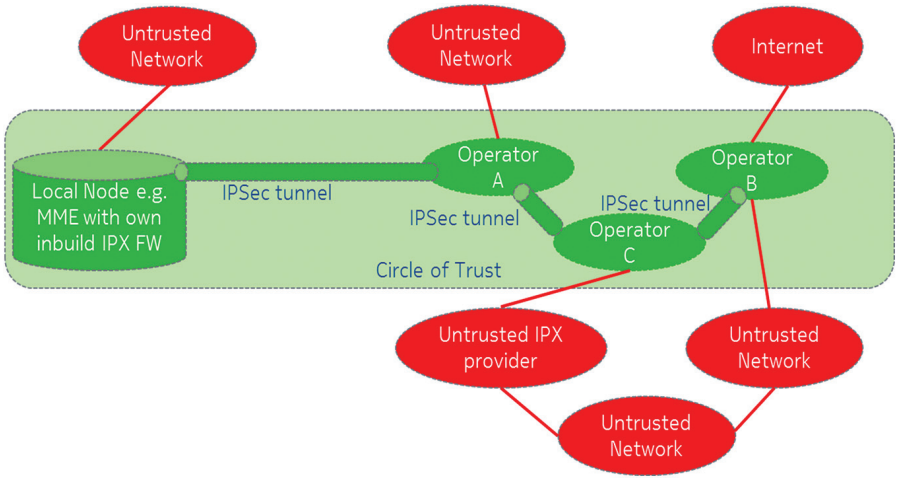

Figure 6 Potential 3GPP interconnection approach.

deployment of IPSec, deployment of signaling firewalls at the perimeters of the trusted group and rules for renting out access to third parties. The members of the circle could then trust each other to a reasonable degree and know the trustworthiness of the arriving messages (Figure 6).

In the very long run, those circles may even merge or acknowledge each other security level. The work is currently in an early study phase and hopefully evolves.

5.2 ITU

The ITU has designed the SS7 protocol stack and therefore, due to the recent security incidents, the ITU had in June 2016 a workshop in SS7 Security [2], where they identified that there is a security problem with SS7. The workshop was exploring the problem space on a general basis.

The outcome was that they wanted to investigate the topic further, but a concrete timeframe or deliverable list is not known to the authors. A follow-up meeting is planned for 2017, but it is unclear, if the ITU will be able to attract a critical mass of experts and contributors and if they will be able to provide detailed specification in the right time-window.

5.3 GSMA

The GSMA Association (http://www.gsma.com/) is an industry trade organization that represents all GSM operators worldwide. The GSMA also provides

services and guidelines to enable roaming and other services. For example, GSMA hosts a database where operator can store information on their network topologies, such as global titles and IP addresses of network elements, so that roaming partners can configure more easily the roaming interfaces and messages to provide seamless roaming experiences to their customers. GSMA is not a standardization body in the classical sense, still they have documents outlining how "communication is done". This also covers also Interconnection security aspects and its security.

GSMA has several dedicated technical and legal working groups, including the Fraud and Security Group (FASG), the Network group, the Packet group and the Wholesale Agreements and Solutions (WAS) Group. The GSMA RIFS sub-group authors a range of SS7 and diameter signaling security related documents in response to the attacks presented in 2008 and 2014, which tackle different aspects of the signaling security problem.

Those documents are GSMA internal and accessible to members only, therefore no exact reference is given and companies that have access can find those documents in the GSMA internal tool easily with the given information below. We will provide here a snapshot on what industrial standards exist and describe on high-level what they offer in form of practical mitigation. The GSMA documents are member-only documents, but most all GSM operators that are members and therefore have access to these documents. Here a brief description of the corresponding documents and their status (August 2016). Those documents are quite detailed and go deep into the signaling messages and protocols. It should be noted, that at the time of writing, some updates are ongoing and under review.

FS.11 (SS7 Monitoring Document)

Formal Title: SS7 Interconnect Security Monitoring Guidelines

Status: Version 1.0, November 2015, but further improvements are ongoing

This document describes how to monitor SS7 traffic for potential attacks. The first step in improving signalling related security is to evaluate, what state the network is in. The main question is, is it under attack, how hard, what kind of attacks. This document describes how to effectively monitor traffic, how long, how to classify incoming MAP messages that are arriving on the interconnection interface. It also goes into suspicious SMS activities. Based on this document an operator can determine, if a message arrives at the interconnection interface, if it is prohibited, unauthorized, suspicious or otherwise "strange".

FS.07 (SS7 Filtering Document)

Title: SS7 and SIGTRAN Network Security

Status: Version 2.0, October 2015, but further improvements are ongoing

This document provides substantial background how to handle SS7 messages on the edge of the network. It describes the handling of the whole SS7 stack, while putting emphasis on the MAP protocol level, where attacks are most common. It allows an SS7 and SIGTRAN security analysis and provides a set of countermeasures that can be deployed i.e. filtering rules and other security approaches. The Annex contains the attacks known to the community and gives a risk list for mobile operators.

Firewall Rule Document

Title: Recommended Signaling Firewall Rules and Data Sharing

Status: Version 0.10 (August 2016)

This document contains details on how to configure an SS7 firewall or an edge node to stop unauthorized messages and attacks from success. This document is work in progress but already quite mature. The results of it will be incorporated into FS.11. The document contains rules for all MAP v2/3 messages and provides countermeasures for the currently known SS7 attacks. A similar countermeasure section is roadmapped for Diameter. Due to the recent SS7 attacks many companies now claim that they have some sort of SS7 firewall, but the quality of those differs substantially. This document intends to clarify the functionality of what a properly working SS7 firewall should be able to do. It goes down to rule level in pseudo code to illustrate the logic how to filter. Message type: Category 2 messages coming from the home network of a subscriber.

IR.88 (LTE) and IR.82 (SS7) – GSMA Interconnection Security

Title: IR.82 Security SS7 implementation on SS7 network guidelines

Status: Version 4.0, March 2016

This document outlines general security measures for SS7 security, which include for example SMS specific security measures and many SS7 stack related security measures. It should be seen as a toolbox for operators, as not every measure mentioned in this document can be deployed in every network. This document is constantly evolved to keep in synchronization with FS.07 and FS.11.

Title: IR.88 LTE and EPC Roaming Guidelines

Status: Version 3.0, February 2016

This document outlines LTE related security measures and also contains data related security aspects. The GTP (GPRS Tunneling Protocol) security currently is under revision due to [25] and similar publications [38]. It is the LTE counterpart to the IR.82. It contains a toolbox for security for Diameter, SCTP, GTP and interface specific recommendation e.g. S6a, S9, S8. It also tackles legacy interworking, SMS security and charging and policy related security aspects.

Diameter Security Permanent Reference Document

Title: Diameter Roaming Security

Status: Version 0.16, August 2016

This documents studies the potential Diameter related Interconnection attacks and countermeasures. It covers aspects like routing attacks, DoS, location tracking and other types of diameter based interconnection attacks. The work to identify potential future threats is already quite mature and formal review has taken place, but due to the nature of the work future extensions are expected.

5.4 Other Activities

Not only consumers got worried about SS7 and mobile interconnection network security. In US the TV show CBS 60 minutes showed the live (authorized) hack of a senator [34]. This has caused that the Federal Communication Commission set up a working group investigating the interconnection security [35]. The vulnerability of the interconnection is a concern for national security [36].

The Nordic countries have teamed up and provided together with their local operators a security guideline for SS7 [37].

6 Conclusion

SS7 is the glue that keeps mobile networks together. It faces quite some security challenges due to recent attacks and revelations. The improvement of this running system is an extremely complex task, not only from technical and financial perspective, but also from political angle.

As the security improves, also the attacks will get more sophisticated. Therefore, it is assumed, that even with recent developments, the network will still be under attacks in the future with the successor protocol diameter. Diameter will be one of the key enablers for Internet of Things cellular communication and therefore be a tempting target. If those attacks are successful, and how to prevent them is further research and standardization.

References

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

[2] International Telecommunication Union (ITU) – T. (2016) *ITU Workshop on SS7 Security*. Available at: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx

[3] Arve, M., and Norsk Telemuseum (2005). *Mobiltelefonens Historie i Norge, Norsk Telemuseum, Mobiltelefonens Historie i Norge.* Available at: https://web.archive.org/web/20070213045903/http://telemuseum.no/mambo/content/view/29/1/

[4] 3rd Generation Partnership Project (3GPP). *TS 29.338 Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs), v12.5.0*. Available at: http://www.3gpp.org/DynaReport/29338.htm

[5] 3rd Generation Partnership Project (3GPP) (2015). *TS 29.272, Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol, v13.2.0*. Available at: http://www.3gpp.org/DynaReport/29272.htm

[6] 3rd Generation Partnership Project (3GPP) (2014). *TS 29.329, Sh Interface Based on Diameter Protocol, Protocol Details, v12.5.0.* Available at: http://www.3gpp.org/DynaReport/29329.htm

[7] 3rd Generation Partnership Project (3GPP) (2015). *TS 29.215, Policy and Charging Control (PCC) Over S9 Reference Point; Stage 3, v13.2.0*. Available at: http://www.3gpp.org/DynaReport/29215.htm

[8] 3rd Generation Partnership Project (3GPP) (2015). *TS 29.002, Mobile Application Part (MAP) specification*. Available at: http://www.3gpp.org/DynaReport/29002.htm

[9] Internet Engineering Task Force (2012). *IETF RFC 6733 Diameter Base Protocol*. Available at: https://tools.ietf.org/html/rfc6733

[10] Internet Engineering Task Force (2003). *IETF RFC 3588, Diameter Base Protocol*. Available at: https://tools.ietf.org/html/rfc3588

[11] Holtmanns, S., Rao, S., Oliver, I. (2016). "User Location tracking attacks for LTE Networks using the interworking functionality," in *Proceedings of the IFIP Networking Conference*, Vienna.

[12] 3rd Generation Partnership Project (3GPP) (2016). *TS 33.210, 3G Security, Network Domain Security (NDS), IP Network Layer Security v12.2.0.* 2012. Available at: http://www.3gpp.org/DynaReport/33210.htm

[13] 3rd Generation Partnership Project (3GPP) (2016). *TR 29.805, Inter-Working Function (IWF) between MAP Based and Diameter Based Interfaces, v 8.0.0*. Available at: http://www.3gpp.org/DynaReport/29805.htm

[14] 3rd Generation Partnership Project (3GPP) (2016). *TS 29.305, InterWorking Function (IWF) between MAP Based and Diameter Based Interfaces, v 13.2.0*. Available at: http://www.3gpp.org/DynaReport/29305.htm

[15] Engel, T. (2014). "SS7: Locate. Track. Manipulate," in *Proceedings of the 31st Chaos Computer Congress 31C3,* Berlin. Available at: http://berlin.ccc.de/∼tobias/31c3-ss7-locate-track-manipulate.pdf

[16] Rao, S., Holtmanns, S., Oliver, I., Aura, T. (2015). "Unblocking stolen mobile devices using SS7-MAP vulnerabilities: exploiting the relationship between IMEI and IMSI for EIR access," in *Trustcom/ BigDataSE/ISPA*, Vol. 1 (New York, NY: IEEE).

[17] Engel, T. (2008). "Locating Mobile Phones using Signaling System 7," in *Proceedings of the 25th Chaos Communication Congress 25C3*. Berlin. http://berlin.ccc.de/∼tobias/25c3-locating-mobile-phones.pdf

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

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

[20] Fox-Brewster, T., and Forbes (2016). *For$20M, These Israelian Hackers will Spy on Any Phone on the Planet*, 2016. Available at: http://www.forbes.com/sites/thomasbrewster/2016/05/31/ability-unlimited-spy-system-ulin-ss7/#5b43b75a7595

[21] Fox-Brewster, T., and Forbes (2016). *Hackers Can Steal Your Facebook Account with Just a Phone Number*. Available at: http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#6860b09b8fa7

[22] Fox-Brewster, T., and Forbes (2016). *Watch as Hackers Hijack WhatsApp Accounts via Critical Telecoms Flaw*. Available at: http://www.forbes.com/sites/thomasbrewster/2016/06/01/whatsapp-telegram-ss7-hacks/#7ca2999d745e

[23] Positive Technologies (2014). *SS7 Security Report*. Available at: https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf

[24] Nohl, K., and Labs, S. R. (2014). "Mobile self-defense," in *Proceedigs of the 31st Chaos Communication Congress 31C3, Berlin*. Available at: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

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

[26] Positive Technologies (2015). *Mobile Interent Traffic Hijacking via GTP and GRX*. Available at: http://blog.ptsecurity.com/2015/02/the-research-mobile-internet-traffic.html

[27] Rao, S., Holtmanns, S., Oliver, I., and Aura, T. (2016). "We know where you are," in *Proceedings of the 8th International Conference on Cyber Conflict: IEEE NATO CyCon*, Washington, DC, 277–294.

[28] Kotte, B., Holtmanns, S., and Rao, S. (2016). *Detach Me Not – DoS attacks against 4G Cellular Users Worldwide from Your desk, Blackhat Europe 2016*. Available at: https://www.blackhat.com/eu-16/briefings.html#detach-me-not-dos-attacks-against-4g-cellular-users-worldwide-from-your-desk

[29] 3rd Generation Partnership Project (3GPP) (2012). *TS 33.210, 3G Security, Network Domain Security (NDS), IP Network Layer Security' v12.2.0*. Available at: http://www.3gpp.org/DynaReport/33210.htm

[30] 3rd Generation Partnership Project (3GPP) (2007). *TS 33.200, 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) Application Layer Security, v7.0.0*. Available at: http://www.3gpp.org/DynaReport/33200.htm

[31] 3rd Generation Partnership Project (3GPP). *TS 33.117, Catalogue of General Security Assurance Requirements, v2.0.0*. Available at: http://www.3gpp.org/DynaReport/33117.htm

[32] 3rd Generation Partnership Project (3GPP) (2016). *TS 33.116, Security Assurance Specification (SCAS) for the MME Network Product Class, v2.0.0*. Availble at: http://www.3gpp.org/DynaReport/33116.htm

[33] 3rd Generation Partnership Project (3GPP) (2016). *TS 33.250, Security Assurance Specification for PGW Network Product Class, v0.1.0.* Available at: http://www.3gpp.org/DynaReport/33250.htm
[34] Alfonsi, S. (2016). *Hacking Your Phone CBS 60 Minutes*. Available at: http://www.cbsnews.com/news/60-minutes-hacking-your-phone/
[35] Finkle, J., and Volz, D. (2016). *FCC Studies Technology Behind 60 Minutes Hack of Congressman*. Available at: http://www.reuters.com/article/us-usa-cybersecurity-phones-idUSKCN0XH2MC
[36] Lieu T. (2016). *Letter to Congress of the United States*. Available at: https://lieu.house.gov/sites/lieu.house.gov/files/Lieu%20FCC%20Letter%20SS7.pdf
[37] Ficora (2016). *Ficora Calls for a Single Information Security Level for Mobile Network in the Nordic Countries*. Available at: https://www.viestintavirasto.fi/en/ficora/news/2016/ficoracallsforasingleinformationsecuritylevelformobilenetworkinthenordiccountries.html
[38] Coskun, O. (2015). *KPN, Why Nation-State Malware Target Telco Networks, DefCon 23*. Available at: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Omer-Coskun-Why-Nation-State-Malwares-Target-Telco-Networks-UPDATED.pdf

Biography

S. Holtmanns is working in Nokia Bell Labs as a Security Expert. She has over 16 years of mobile communication security experience (Ericsson Research, Nokia Research, Nokia Mobile Phones, Nokia Networks). In her 10 years of 3GPP Security she contributed in the creation of 3G and 4G Security. She has written over 50 security articles, book chapters and a book. Her research interests today focus on interconnection (diameter/SS7) and Network Function Virtualization (NFV) security. For interconnection security she is active in the GSMA association to develop protection methods and specify them. She serves as a matter expert for operator customers and also for governments on SS7 and diameter security and its evolution.