WARSAW UNIVERSITY OF TECHNOLOGY

DISCIPLINE OF SCIENCE: INFORMATION AND COMMUNICATION TECHNOLOGY /
FIELD OF SCIENCE: ENGINEERING AND TECHNOLOGY

Ph.D. Thesis

German Peinado Gomez, M.Sc.

Development of a Risk-based Security Framework for Mobile Networks interconnection applied in Roaming Service Level Agreements within the 5G context

Supervisor
prof. dr hab. inż. Jordi Mongay Batalla, Professor

WARSAW 2025

Acknowledgements

First, I would like to express my sincere gratitude to my supervisor, Prof. Jordi Mongay Batalla, who motivated me to start this journey, and whose guidance and unwavering support have been instrumental in the successful completion of the Ph.D. program and dissertation.

I would also like to express my appreciation to the Warsaw University of Technology, an institution that has provided me with a stimulating environment to pursue my research.

Special thanks are owed to my esteemed colleagues and friends, Dr. Liliann Miche, Dr. Silke Holtmanns and Dr. Anja Jerichow, for their expert insights, patience and collaborative spirit.

I am also deeply grateful to my company Nokia (Poland), and my department Nokia Standards. The opportunities provided by my company have allowed me to explore real-world implications of my research. In addition, they supported my research from the beginning of the journey with time and resources.

Lastly, I wish to extend my heartfelt thanks to my family, my wife, my children and my parents. Without their tremendous understanding and encouragement in the past years, it would be impossible for me to complete my study.

Streszczenie

Operatorzy sieci komórkowych łączą swoje sieci w celu świadczenia usług roamingu w oparciu o umowy o gwarantowanym poziomie usług (SLA) bezpośrednio z operatorami równorzędnymi lub za pośrednictwem pośredników roamingowych. Umowy SLA zawierają klauzule bezpieczeństwa, które są przekładane na wymagania bezpieczeństwa w połączeniach międzysieciowych. Podczas gdy architektura bezpieczeństwa w sieciach mobilnych piątej generacji (5G), w porównaniu z poprzednimi generacjami, wprowadziła znaczące ulepszenia w nowym paradygmacie bezpieczeństwa end-to-end, stan bezpieczeństwa w połączeniach między sieciami mobilnymi nie może być uważany za statyczny i zależny tylko od polityk zawartych w dokumentach umownych. Wręcz przeciwnie, stan bezpieczeństwa w tym kontekście wymaga ciągłego dostosowywania się do stale rozrastającego się ekosystemu połączeń międzysieciowych i krajobrazu zagrożeń, z jednoczesnym wzięciem pod uwagę nieuniknionego współistnienia, od początku istnienia sieci komórkowych, trzech stosów protokołów (ang. protocol stacks) , tj. SS7 (2G/3G), Diameter (4G) i HTTP/2 (5G).

Głównym celem niniejszego badania było zbudowanie struktury bezpieczeństwa opartej na ryzyku (ang. risk-based), zdolnej do przewidywania głównych kwestii bezpieczeństwa i reagowania na zmiany poziomu bezpieczeństwa połączeń międzysieciowych ustanowionych między równorzędnymi operatorami sieci komórkowych i/lub pośrednikami roamingu. Aby to osiągnąć, opracowałem cztery elementy składowe połączone w kompleksowy cykl życia (ang. lifecycle) zabezpieczeń. Po pierwsze, zaprojektowałem dynamiczny mechanizm oceny ryzyka zarówno na poziomie wiadomości jak i sekwencji, przy użyciu wiedzy eksperckiej i technik data mining zastosowanych do strumieni danych. Jako punkt odniesienia do obliczania ryzyka przyjąłem Common Vulnerability Scoring System. Po drugie, zaproponowałem nowatorskie podejście do określania wskaźnika zaufania dla sieci mobilnych w roamingu, z pomiarem ryzyka jako głównym elementem wejściowym. Po trzecie, wprowadziłem koncepcję profilowania bezpieczeństwa w połączeniach międzysieciowych 5G, jako katalizator wdrożenia nowego paradygmatu bezpieczeństwa end-to-end w 5G. Wreszcie, zaprojektowałem nową metodę dynamicznego tworzenia i egzekwowania polityk bezpieczeństwa w interconnection gateways, działających jako punkty egzekwowania (ang. enforcement points), poprzez ulepszenie obecnej struktury 5G Policy Control, i ustalając bezpieczeństwo faktycznym elementem jakości sieci.

Ramy bezpieczeństwa zostały zweryfikowane na podstawie teoretycznego *key use case*, takiego jak śledzenie lokalizacji, oraz na podstawie anonimowego śladu rzeczywistego ruchu sygnalizacyjnego Diameter w roamingu 4G między dwoma operatorami w Azji. Aby zademonstrować adekwatność nowych metod w systemie 5G, przedstawiłem kilka procedur zgodnych z rzeczywistą standaryzacją 5G-Advanced, pomimo tego że obawy związane z prywatnością i bezpieczeństwem dostępu do danych sygnalizacyjnych w połączeniach międzysieciowych utrudniają szeroko zakrojone eksperymenty akademickie w tej dziedzinie.

Słowa kluczowe: sieci mobilne, bezpieczeństwo, roaming, połaczenia międzysieciowe, signalizacja, SLA, 3GPP, 5G, 4G, Diameter, HTTP/2, IPX, zarządzanie ryzykiem, data mining, security enforcement, wskaźnik zaufania, profilowanie bezpieczeństwa.

Abstract

Mobile Network Operators interconnect their networks to provide roaming services based on Service Level Agreements (SLAs) directly with peers or through roaming intermediaries. The SLAs include security clauses that are translated into security requirements in the interconnection links. Whilst the security architecture in the fifth generation of mobile networks (5G), in comparison with previous generations, has introduced significant advancements towards a new end-to-end security paradigm, the security posture in the interconnection of mobile networks cannot be considered static and solely dependent on policies part of contractual documents. On the contrary, the security posture in this context requires a continuous adaption to the ever-growing interconnection ecosystem and threat landscape, considering the unavoidable coexistence of the three protocol stacks since the beginning of the mobile networks, i.e., SS7 (2G/3G), Diameter (4G) and HTTP/2 (5G).

The primary aim of this research was to build a risk-based security framework capable of anticipating major security issues and reacting to changes in the security level of the interconnection links established between peer Mobile Network Operators and/or roaming intermediaries. To achieve this, I have developed four building blocks, connected to form a comprehensive security lifecycle. Firstly, I have designed a dynamic risk evaluation mechanism at both message and sequence levels using expert knowledge and data mining techniques applied to data streams. As a baseline for computing the risk, I have adopted the Common Vulnerability Scoring System. Secondly, I have proposed a novel approach to determine a trust score for Mobile Networks in roaming context, with risk measurement as the main input. Thirdly, I have introduced the concept of security profiling in 5G interconnection as a catalyzer to implement the new security end-to-end paradigm in 5G. Finally, I have designed a new method to dynamically create and enforce the security policies in the interconnection gateways, acting as enforcement points, by enhancing the current 5G Policy Control framework, making security an actual quality element of the network.

The security framework has been validated with a theoretical key use case such as location tracking, as well as with an anonymized trace of real Diameter signaling traffic between two operators in Asia. Several procedures following the actual 5G-Advanced standardization are provided to demonstrate the adequacy of the novel methods in the 5G system, even when privacy and security concerns to access the signaling data in interconnection hinder wide academic experimentation in this field.

Keywords: mobile networks, security, roaming, interconnection, signaling, SLA, 3GPP, 5G, 4G, Diameter, HTTP/2, IPX, risk management, data mining, security enforcement, trust score, security profiling.

Table of Contents

1 Theme of the dissertation

Mobile Network Operators (MNOs) are interconnecting their networks based on Service Level Agreements (SLAs) directly with peers or through roaming intermediaries (e.g., IP Exchange providers, Roaming Hubs, etc.). SLAs in the contracts govern the conditions of interconnection, including legal, business, and technical clauses, being security a crucial part of those. Thus, SLAs include security clauses translated into security requirements to be applied in interconnection links. The context of this dissertation is Security in the Service Level Agreements (SSLAs) in the interconnection of telecommunication mobile networks, considering the coexistence of different schemas and corresponding protocol stacks such as SS7 in 2G/3G, Diameter in 4G and HTTP/2 in 5G.

1.1 Problem Statement and Objectives

The field of Security in mobile networks has seen remarkable advancements across the last generations, which obviously include the interconnection and roaming services between networks as basic and required functionality in every generation. Specifically in this context of interconnection and roaming, 5G has introduced a new security paradigm, moving the hop-by-hop approach in 2G/3G and 4G towards new end-to-end protection mechanisms. However, despite these developments, specific challenges are persistent, i.e., they remain unresolved firstly by current 5G standardization and subsequently, by industry implementations. In this regard the following **challenges** are highlighted:

- During the negotiations of SLAs, a.k.a. roaming agreements, in relation to security considerations/clauses, the MNOs must expose how they are protecting their subscribers and network from attacks impacting the visitor. What are the criteria for establishing more stringent or laxer security clauses in SLAs during this process? In a broader sense, what are the key factors impacting the trust relationship between operators?
- SLAs often have notions of quantifiable Key Performance Indicators (KPIs), such as those used to measure Quality of Service (QoS) type of parameters. Achieving reliable measurements of Security in the (roaming) SLAs between interconnected MNOs remains a challenge that neither standardization bodies like 3GPP (3rd Generation Partnership Project) nor industry groups like GSMA (Global System for Mobile Communications Association) have addressed yet.

- In previous generations (2G/3G/4G), and currently in 5G networks, the provision of security policies in the interconnection gateways is considered a *manual* process by standardization and industry forums, excluding all the advantages of automation. This can be observed in standards and industry documents such as:
    - 3GPP SA3 TS 33.501 [1] (clause 13.2.3.5, Provisioning of the policies in the SEPP): "The SEPP shall contain an interface that the operator can use to *manually* configure the protection policies in the SEPP."
    - GSMA NG.113 [2] (clause 6.5.6, 5G Roaming Security Architecture Overview): "Operators *manually* provision SEPPs with a protection policy based on bilateral agreements…"
- Network operations are exhaustive and complicated in mobile networks, focused on ensuring the availability of the services. The efficiency and agility in network operations can be used as excuses to relax security requirements, and consequently avoid potentially required sophisticated security protection mechanisms. Specifically, the new end-to-end application layer security paradigm introduced in 5G has been questioned by the industry due to, among other factors, the inherent complexity in the negotiation of very granular security policies. Indeed, GSMA, as the main representative of the industry, established the 5G Mobile Roaming Revisited (5GMRR) Task Force a few years back with the mission to define a scalable, usable, and secure solution for 5G mobile roaming.
- Risk management is a very complex task in telecom networks, more so in interconnect links which are out of the control of the operator. Even if the industry and regulators mostly recommend the use of the standard ISO/IEC 27005:2022 [3] as a framework, concrete mechanisms to compute the risk in interconnection are still a gap in the majority of the mobile networks.

The core **problem** addressed in this dissertation is that the security posture in the interconnection of mobile networks to provide roaming services cannot be considered static and dependent on the policies part of contractual documents. On the contrary, the security posture in this context requires a continuous adaptation to the ever-growing interconnection ecosystem and, consequently, the threat landscape.

Addressing this problem is currently essential as per the co-existence of the three schemas of interconnection at present and in the near future. While previous research, standardization, and development have addressed different security aspects in interconnection, the current

approaches are limited to addressing the challenges described above and upcoming use cases in 5G-Advanced and 6G, where even subscription plans can be related to security added value services and corresponding tenants (e.g., owner of a critical infrastructure). Those might require different levels of security (e.g., per slice) and the ability to react to security incidents.

This research seeks to address this problem by building a security framework capable of anticipating major issues and reacting to changes in the security level of the interconnection links established between peer MNOs and/or with roaming intermediaries. The main **objectives** of the proposed security framework are the following:

- To evaluate and compute dynamically the risk in the interconnection signaling links across all technologies.
- Based on the risk computation, to determine a trust score per interconnected operator, acting as a basis of the MNO decision making criteria in establishing security policies in interconnection.
- To overcome the operational complexities introduced by the superior level of security in 5G by simplifying and automating the configuration and implementation of security policies in the new end-to-end security paradigm.
- To provide a suitable mechanism for enforcing the security policies in the interconnection gateways by reusing 5G Core capabilities.
- To incorporate the outcomes of this framework as security analytics in interconnection within the existing network analytics framework specified in 5G [4].

1.2 Theses of the Dissertation

The following theses were defined in this research:

Thesis 1.

The trust between MNOs when providing roaming services, reflected in security clauses in SLAs, needs to be continuously evaluated by measuring and controlling the risk level in interconnection signaling links, across the three technologies coexisting today in the mobile networks, i.e., SS7 (2G/3G), Diameter (4G) and HTTP/2 (5G).

Thesis 2.

The operational complexity introduced by the new end-to-end security paradigm in 5G when granular security policies are to be agreed between MNOs (more in general, roaming stakeholders) based on risk and trust measurements, should be significantly reduced by introducing the concept of security profiles.

Thesis 3.

A unified 5G policy framework should provide an effective security enforcement schema, flexible to create new security policies, and agile to react to the constantly changing environment across the end-to-end mobile network architecture.

1.3 List of Research Publications and Granted and Applied Patents

In order to demonstrate the aforementioned theses, I have developed a novel security framework for MNOs' interconnection. The description of the building blocks of the framework and related procedures have been published in six research papers (and one more submitted paper), and the Intellectual Property Rights of specific related mechanisms have been protected by three patents (two granted and one applied).

Fig. 1.3-1 represents the conceptual map of the developed security framework (which will be fully specified in Sections 3-7), containing the main building blocks (marked with numbers from 1 to 4) that support the three theses above. More details of the schema itself are provided in Chapter 3. The building blocks have been specified and validated in the research publications and patents, as explained below.

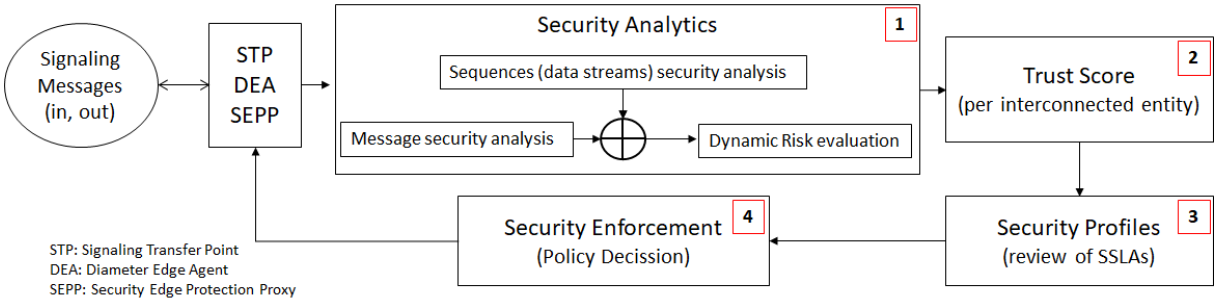

Figure 1.3-1: Security Framework Overview

Research Publications

1. Silke Holtmanns, Ian Oliver, Yoan Miche, Aapo Kalliola, Gabriela Limonta, and German Peinado Gomez, "5G Security – Complex Challenges," in Wiley 5G Ref, John Wiley & Sons, Ltd, 2019, pp. 1–15. DOI: 10.1002/9781119471509.w5GRef161 [5].
   - The article sets the scene of 5G security space, dividing it into several subtopics. One subtopic explicitly refers to the need to measure security in 5G networks and recommends following a risk approach promoted by the industry, pre-standardization research projects, and early regulations. It motivates the development of the **building block 1** of our schema already from the beginning of the research, and has contributed to Chapter 4 of this dissertation.
2. Jordi Mongay Batalla, Luis J. de la Cruz Llopis, German Peinado Gomez, Elzbieta Andrukiewicz, Piotr Krawiec, Constandinos X. Mavromoustakis and Houbing Herbert Song, "Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-

Criteria Decision Making" in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 5, pp. 3496-3512, May 2024, https://doi.org/10.1109/TITS.2023.3325908 [6].

- The paper discusses the security assurance approach that the automotive sector would require to the 5G network for the secure communication of the Intelligent Transport System applications, including the enhancements introduced in Interconnection Security. The article reviews the entire 5G Security architecture and is the baseline of subchapter 2.1.3 of this dissertation.

3. Jordi Mongay Batalla, Elżbieta Andrukiewicz, German Peinado Gomez, Piotr Sapiecha, Constandinos X. Mavromoustakis, George Mastorakis, Jerzy Żurek, and Muhammad Imran, "Security Risk Assessment for 5G networks - national perspective". IEEE Wireless Communications, vol. 27, no. 4, pp. 16-22, Aug. 2020. DOI: 10.1109/MWC.001.1900524 [7].
   - The article presents a security risk assessment for 5G networks based on the ISO 27005 standard [3] from a National perspective. It motivates and inspires the development of **building block 1** of our schema from a regulator perspective.
4. German Peinado Gomez, Jordi Mongay Batalla, Yoan Miche, Silke Holtmanns, Constandinos X. Mavromoustakis, George Mastorakis and Noman Haider, "Security policies definition and enforcement utilizing policy control function framework in 5G", Computer Communications, Vol. 172, Pp. 226-237, Apr. 2021, DOI: 10.1016/j.comcom.2021.03.024 [8].
   - The article corresponds entirely to **building block 4** of the schema, i.e., the enforcement of the security policies in the corresponding signaling gateways of interconnection. In addition, the article proposes the enhancement of the actual Network Analytics function in 5G to cover security analytics use cases. In Chapter 7 and subchapter 8.5 we provide more details on how this concept can be developed for security analytics in interconnection as depicted in the schema above.
5. R. M. Dhanasekaran, Jing Ping and German Peinado Gomez, "End-to-End Network Slicing Security Across Standards Organizations," in IEEE Communications Standards Magazine, vol. 7, no. 1, pp. 40-47, March 2023, DOI: 10.1109/MCOMSTD.0005.2200055 [9]
   - The article reviews the status quo in standardization with regard to end-to-end network slicing security. The topic is not in the scope of this dissertation, but it has been proposed as a candidate for **further research** in the context of security in interconnection.
6. Andreas Andreou, Constandinos X. Mavromoustakis, Houbing Herbert Song, German Peinado Gomez, and Jordi Mongay Batalla, "Transforming ageing in the metaverse:

embracing virtual communities for enhanced well-being and empowerment". Adv. Metaverse Wirel. Commun. Syst., pp. 457–494, doi: 10.1049/PBTE112E_ch16 [10].

- The article is the chapter 16 of a book titled “Advanced Metaverse Wireless Communication Systems”, and among other aspects, provides privacy and security considerations to apply in the metaverse as a key service of future mobile networks.

7. German Peinado Gomez, Jordi Mongay Batalla, Liliann Miche, Andrzej Bęben and Constandinos Mavromoustakis, "A Dynamic Risk Evaluation Mechanism for Mobile Networks Interconnection Signaling" (Status: **Submitted and under review**).
   - The article presents a new mechanism for evaluating and measuring the risk in interconnection between MNOs, including the formal mathematical model. It constitutes the baseline of the entire **building block 1**.

Patents

1. German Peinado Gomez, Anja Jerichow, Chaitanya Aggarwal, “Security enforcement and assurance utilizing policy control framework and security enhancement of analytics function in communication network.” Patent No. (Granted): US 12,126,658 B2. Date of Patent: Oct. 22, 2024, https://patents.google.com/patent/US12126658B2/en [11].
   - The patent describes the mechanism deployed in **building block 4** of the schema.
2. Anja Jerichow and German Peinado Gomez, “Apparatus, method, and computer program of protecting communications between networks using predefined security profiles.” Patent No. (Granted): US 12,192,208 B2. Date of Patent: Jan. 7, 2025 [12].
   - The patent corresponds to **building block 3** of the schema. It proposes to use security profiles to simplify and automate the negotiations of security mechanisms between MNOs in interconnection.
3. Borislava Gajic, German Peinado Gomez, Saurabh Khare, and Tejas Subramanya, “Method and apparatus for determining and utilizing a trust indication in mobile networks,” US20230413029A1,Dec.21,2023, https://patents.google.com/patent/US20230413029A1/en [13]
   - The patent corresponds to **building block 2** of the schema. It proposes a mechanism to determine and utilize a trust indication in mobile networks, and one of the relevant use cases is interconnection.

1.4 Methodology Overview

The research conducted in this dissertation has required the use of methods in the field of telecommunications and security. Specifically, I have utilized the following techniques and steps during the process:

1. Analysis of the 5G security architecture specifications in standardization bodies such as 3GPP (Working Group SA3) and official documentation generated in industry relevant organizations such as GSMA (Fraud and Security Group). Sound knowledge and experience in security architectures in previous mobile generations (2G/3G/4G) are assumed, considering that there are always updates in security mechanisms due to the ever-changing threat landscape, which has motivated significant research and development in the last years.
2. Analysis of scientific literature and technology, extending the scope of standardization in the fields of Security Management, Risk Management and Interconnection/Roaming services between MNOs. The analysis has been complemented by my own experience in the field, having been involved in the design of several security projects in interconnection delivered by my actual employer.
3. Data analysis and preparation: Study and classification of all possible information elements exchanged in interconnection in SS7 (2G/3G), Diameter (4G), and HTTP/2 (5G). The signaling data formats and contents provide the hints on how to define a risk-based computation in the interconnection links.
4. High-Level Design of the security framework, addressing the objectives indicated in subchapter 1.1. I.e., how the different building blocks are placed in the overall solution which is proposed to resolve the problem.
5. Low-Level Design of each building block of the security framework, including a mathematical model in the case of the dynamic risk evaluation mechanism, as it is the cornerstone of the overall framework.
6. Validation of the framework. As explained more in detail in Chapter 9, a practical validation of the framework would require access to a massive amount of data in several interconnection links, with the privacy regulatory constraint that the signaling data in those links contains subscriber sensitive information, such as PII (Personal Identifiable Information) or location. After multiple unsuccessful attempts to obtain relevant real data from several operators, I finally got a real trace containing a few messages in 4G Roaming (note that 5G Standalone roaming services are not available at the time of

writing this dissertation) that was conveniently anonymized and used to apply the designed mechanisms to evaluate the risk. For the building blocks 2, 3, and 4 of the framework described in Chapter 3, I have designed a set of possible procedures and enhancements to be implemented in the current 5G architecture. Note that in the case of building block 3, i.e., Security profiles, the actual 3GPP standardization has already implemented those as part of the specifications in 5G-Advanced.

1.5 Thesis Structure

The rest of the dissertation is organized as follows.

Chapter 2 summarizes the state of the art, starting with a review of the security architectures in Mobile Networks interconnection, which includes all generations. Afterwards a review of the existing literature is provided, including standards and scientific publications, on the actual topics of the dissertation.

Chapter 3 provides an overview of the proposed Security Framework for interconnection, showing how the building blocks of the overall schema are part of a security lifecycle-oriented architecture.

Chapter 4 provides a new dynamic risk evaluation mechanism for mobile networks interconnection. To explain the mechanism, I introduce a mathematical notation that will be used in the description of the model, and afterwards, the two main threads, i.e., message security analysis and sequence security analysis, are described in separate subchapters. Finally, the chapter describes in detail how to compute the risk by adapting the Common Vulnerability Scoring System (CVSS).

Chapter 5 proposes an approach to determine a trust score for mobile networks interconnection in 5G by enhancing the existing Network Analytics functionality.

Chapter 6 describes a new concept (patented), which has already been accepted in standardization, to optimize the configuration and negotiation of security policies in 5G by the definition of security profiles.

Chapter 7 introduces a new method of enforcing security policies in the 5G Core network by reusing the existing Policy Control framework in 5G. Complementarily, a concrete enhancement of the actual Network Analytics functionality to cover Security Analytics is proposed.

Chapter 8 explains the validation of the concepts and methods explained in previous chapters.

Chapter 9 describes the limitations of the research and encourages us to continue with the research in some specific areas.

Chapter 10 provides a concise summary of the overall research.

2 State of the Art

This chapter explores the current state of the art in mobile networks interconnection architectures, focusing on the key advancements and challenges relevant to the Security aspects of those architectures, and taking into consideration the co-existence of three different schemas/protocol stacks used for providing roaming services, i.e., SS7 in 2G/3G networks, Diameter in 4G networks, and HTTP/2 in 5G networks.

The discussion begins with a high-level exploration of the key security aspects in each of the interconnection schemas present in the mobile network architectures, outlining the main contributions in each generation. Subsequently, the chapter delves into the main themes of the dissertation, providing an analysis of the existing methods and technologies currently used in mobile networks, specifically on:

- Risk management
- Trust definition and measurement
- Security policies and profiling
- Security enforcement

Note that each of the chapters of the dissertation provides an introductory section, which discusses more details about the references, existing work, and motivation of the new approaches and proposed solutions.

2.1 Review of security architectures in mobile networks interconnection

This subchapter summarizes the main security aspects considered and specified in each of three schemas of interconnection, which are currently deployed and co-coexist in mobile networks. It is intended to set up the research scene and assumes a solid understanding of mobile network architectures as standardized by 3GPP.

2.1.1 2G/3G Signaling Roaming Security Architecture (SS7)

Signaling System No. 7 (SS7) is a set of telecommunications signaling protocols developed more than four decades ago to facilitate the communication in a trusted environment within and between fixed networks, a.k.a. Public Switched Telephone Networks (PSTNs). The protocol stack does not provide security mechanisms per se. The protocol suite was extended in the 1990s and 2000s to support 2G and 3G mobile generation networks and hosts several services.

For example, to implement roaming services, pre-paid subscriptions, or short messages (SMS), the Mobile Application Part (MAP) [14] and the CAMEL Application Part (CAP) [15] protocols were added to SS7. Nevertheless, the basic structure and signaling architecture has stayed the same, even though the global SS7 network has grown from a few hundred carriers in a "supposed" trusted network to thousands of service providers and network operators, opening the overall ecosystem to multiple stakeholders (e.g., IPX providers, Roaming Hubs, etc.). Despite the massive growth of SS7 interconnections, security policies and corresponding frameworks were still missing. In the 2000s, IETF (Internet Engineering Task Force) defined a suite of protocols named SIGTRAN (Signaling Transport) [16] to enable the transport of signaling traffic over IP, and more specifically for our context, also published a RFC with security considerations for SIGTRAN protocols [17], defining IPsec or TLS as security transport mechanisms for SIGTRAN protocols.

2G/3G Core Network elements such as Home Location Register (HLR), Visitor Location Register (VLR), and Mobile Switching Center (MSC) process MAP and CAP requests via SS7 interconnection points, mostly without any verification of their legitimacy. This factor has been the main cause of multiple incidents: fraud, denial of service, call interception, data theft, spam, etc., reported even by generalist press [18] [19] [20] [21] [22]. Multiple specialized security companies and researchers have published and reported the security flaws and vulnerabilities of the old protocol suite [23] [24] [25] [26]. Many of those companies and researchers, in alignment with the telecom industry, have been strongly recommending during the last decade mitigations related to the deployment of application layer firewalls with capabilities of inspection and enforcement at MAP and CAP levels.

GSMA in FS.11 [27] provides a high-level set of guidelines to monitor SS7 traffic and establish some useful associated firewall rules and data sharing capabilities intended to protect the signaling interfaces of the Core networks. In annex B.5 of [27] several implementations of the firewall in the signaling architecture are suggested. Based on my own experience in the field during the last decade, out of those implementations the overlay model has been selected by the majority of the operators due to its flexibility at the cost of incrementing the signaling flows in the network, and in combination with capabilities of acting as a passive message monitoring.

In the Fig 2.1.1-1 I have adapted the Figure 2 of annex B.5 of [27] to represent the firewall overlay model with passive message monitoring capabilities.

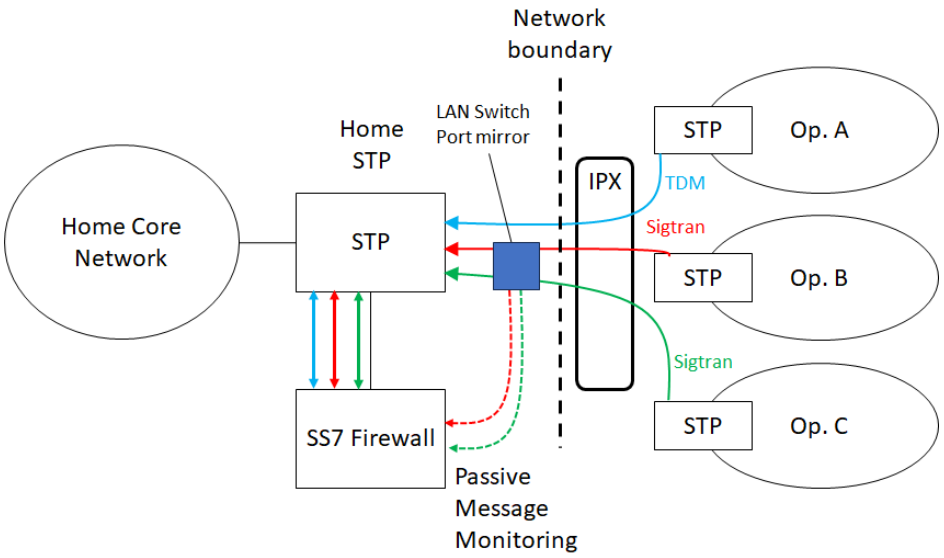

Fig. 2.1.1-1: SS7 firewall overlay model with passive message monitoring (adapted from Figure 2 of GSMA FS.11 [27])

This architecture enables the firewall to act as both passive and active nodes simultaneously, whereas managing the filtering can be easily done via software configuration, i.e., the detection rules can be configured in permissive or enforcing mode. The transport of signaling links via SIGTRAN allows the deployment of simple LAN switches to perform port mirroring of the traffic. Passive message monitoring enables the learning of the security device (note that most firewalls include or are connected to a security analytics platform). Additionally, this architecture enables a smart redirection of only suspicious messages towards the firewall, optimizing the STP performance.

2.1.2 4G Signaling Roaming Security Architecture (Diameter)

Diameter protocol was originally defined by IETF in RFC 3588 [28], and nowadays maintained in RFC 6733 [29]. Diameter was adopted as a signaling protocol for the control plane in 4G for internal and external communications in interconnection as specified in 3GPP TS 23.401 [30]. SCTP (Stream Control Transmission Protocol) (IETF RFC 9260 [31]) was adopted to transport the Diameter signaling messages. The Figure 2 of GSMA FS.19 [32] official document provides a good illustration of the Diameter architecture in interconnection that we reproduce here for convenience in Fig. 2.1.2-1.

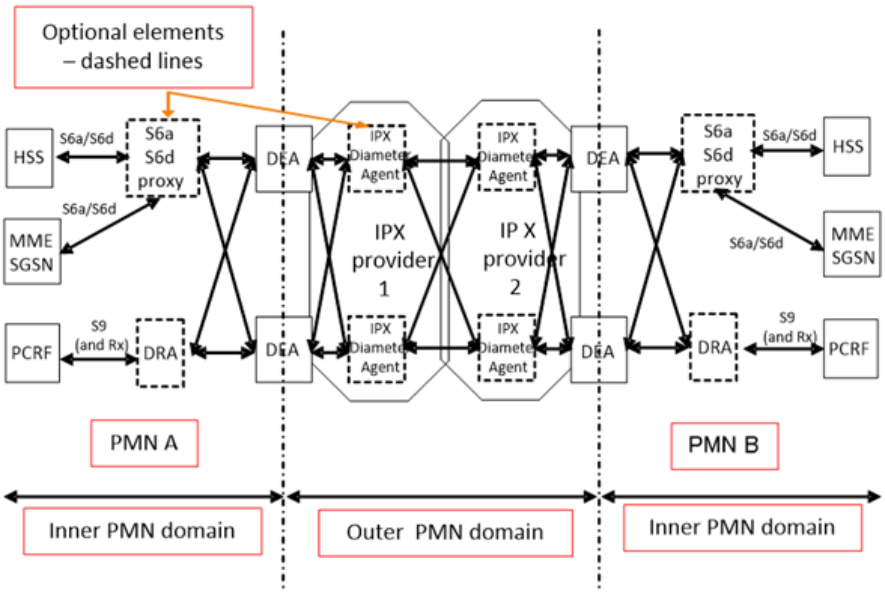

Fig. 2.1.2-1: End-to-End Diameter Architecture in Interconnection (extracted from GSMA FS.19 [32])

Note that, although 4G networks use a different signaling protocol than 2G/3G networks, they still need to interface with those networks and convert SS7 messages into equivalent Diameter ones.

The adoption of a new protocol did not solve the major security challenges in SS7. Even though Diameter incorporated some security features such as the support for encryption transport protocols (TLS, DTLS, IPsec), enabling secure communication between nodes, it has the same architectural constraints as the original SS7, let it be for backward compatibility or for reasons to not reinvent the logic of signaling just because a new protocol was required. For example, there is no end-to-end security concept as such, but just hop-by-hop security mechanisms on lower layers and it requires additional security measures. As a result, many of the threats and vulnerabilities found in SS7 continue to exist in Diameter, e.g., user tracking, billing fraud, call interception, Subscriber DoS, etc. Thus, the Diameter security strategy has evident synergies with the one discussed for SS7 signaling. All the knowledge built up in SS7 definitely helps in Diameter protection, e.g., velocity checks are needed in the same manner as in SS7. Also, the same sources for threat detection and monitoring used for SS7, such as GSMA, threat intelligence databases, etc., are still valid for Diameter based networks.

In addition, the adoption of the protocol itself introduces new vulnerabilities that can be cataloged as follows:

- Diameter **Routing** vulnerabilities

    - Automatic peer discovery, if used, may allow native rogue IP connectivity to the local or global Diameter network.
    - If DNS is used to resolve DEA IP addresses, known DNS attacks can be easily introduced into this domain (e.g., DNS poisoning).
    - Hop-by-Hop routing. In Diameter, unlike in MAP, the receiver does not reply to the requestor but to the previous node. As a consequence, an attacker can fake its sender ID (origin-realm and origin-host) with an authorized one and get the response to its query since the answer will be routed not according to the sender ID used by the attacker in the query but using the same Hop-by-Hop ID found in Diameter requests.
- Diameter **Functional** vulnerabilities
    - Update Location Requests (ULR) to HSS can be sent addressing a range of subscribes, not only single subscribers, and consequently a subscriber DoS attack can also target a range of subscribers. For example, the subscriber's HSS updates the information in its database according to the ULR parameters and sends a CancelLocation to the previous MME, making all the subscribers with valid IMSI become unreachable, and consequently, data sessions are interrupted.
- Diameter **Protocol** vulnerabilities
    - Diameter message manipulation, Attribute Value Pair (AVP) doubling. Diameter messages can be manipulated to contain AVPs of the same kind (same AVP id) even though the specification clearly says it's illegal to do so.

Furthermore, as a matter of fact, in LTE roaming MNOs often neglect to deploy secure protocols to protect Diameter signaling messages and rely on a trust model based on peer-to-peer relationships with roaming partners and intermediaries.

3GPP did not standardize a security architecture for Diameter signaling per se, either for internal interfaces or for external interfaces used in interconnection. Nevertheless, GSMA worked to establish a series of security guidelines/recommendations for interconnection of LTE networks, captured mainly in IR.88 [33], FS.21 [34] and FS.19 [32] official documents.

In addition to the use of secure transport protocols for Diameter, the GSMA recommendations suggest the deployment of Diameter signaling firewalls in interconnection, either integrated into the DEAs or as standalone security devices, with certain screening types of functionalities. Otherwise, the security mechanisms are to be applied in the Core Network elements, such as

the MME, which is operationally cumbersome. The following bullets summarize some of those key security functionalities expected to be implemented in the Diameter signaling firewalls:

- Imposing sanity checks on each protocol layer, blocking, for example, double AVPs, Diameter messages that should not appear on the interconnection interface, certain command codes, etc.
- Anti-spoofing mechanisms for all Diameter applications, for example, by checking originating and destination hosts and realms.
- Blocking messages not related to roaming scenarios. For example, Applications/Command-Codes that are not allowed on roaming links.
- Checking the relation of specific messages to outbound roaming subscribers only, not home-registered subscribers. For example, Application/Command-Codes that are allowed only for VPLMN to HPLMN traffic.
- Plausibility and Velocity checks, i.e., correlation of last seen Location Update to Origin Host/Realm of the message, comparison of the received Origin-Host/Realm with previously stored data, etc.
- Stateful message flow check, i.e., if certain messages are not sent, a subset of messages is immediately denied since the use case is not valid.
- Validating parameters using Allowed/Block/Grey lists and cross-checking multiple message parameters. For example, HPLMN only permits Update Location requests only from known MMEs in the VPLMN.
- Overload protection and throughput control. Limiting message rates to protect the upstream network.

The possible deployments of the Diameter firewalls are described in Annex B.7 of [32]. They are analogous to the SS7 firewall deployment modes. Fig. 2.1.1-1 in the previous subchapter can be reused simply by removing the TDM links, and replacing STP for DEA and SS7 Firewall for Diameter Firewall.

In short, the Diameter messages exchanged between MNOs do not have any native integrity or confidentiality protection within the protocol itself. With the introduction of security transport mechanisms such as IPsec, TLS, or DTLS, hop-by-hop protection is provided. Protocol screening and firewalling functionalities are to be provided either integrated in the DEA or in a separate security device in the perimeter of the Core Network.

Additionally, GSMA FS.19 [32] Annex D provides some guidelines on what to protect (i.e., interfaces, AVPs), where to protect (i.e., Edge of the network), and how to protect (i.e., authentication, integrity and confidentiality protection) the end-to-end exchange of Diameter messages within the IPX ecosystem by adding integrity, authentication, and confidentiality protection measures to the protocol itself. This so-called Diameter End-to-End Signaling Security (DESS) solution is complementary to the Diameter firewall approach described above. DESS is aligned with the 5G security framework in interconnection depicted in subchapters 2.1.3 and 6.2 of this document, and consists of two phases:

- DESS Phase 1 (Signature) – Authentication and Integrity protection (the implementation details are provided in D.3.4.3 and Annex E of [32].
- DESS Phase 2 (Encryption) – Confidentiality protection on top of DESS Phase 1 (not developed).

As per our knowledge, just a few global operators have recently implemented DESS phase 1 in addition to the firewall functionalities (e.g., Deutsche Telekom Global Carrier [35]).

2.1.3 5G Security Architecture

3GPP Working Group SA3 specifies the security architecture, i.e., requirements, features, and procedures, for the 5G system in TS 33.501 [1]. This specification is focused on securing the 3GPP specified interfaces. Furthermore, as explained in section IV of [6], to build a comprehensive security framework at network layer in 5G, the following main areas are to be considered:

- Standard security architecture (3GPP)
- Non-formally standardized security best practices and schemas
- Security operations
- Security assurance of the network elements and the systems building the architecture

In Fig. 2.1.3-1 I depict a schematic overview of the 5G network security architecture, where the main security elements and features have been highlighted. Please note that the schema does not include all Network Functions (NFs) specified for the 5G system.

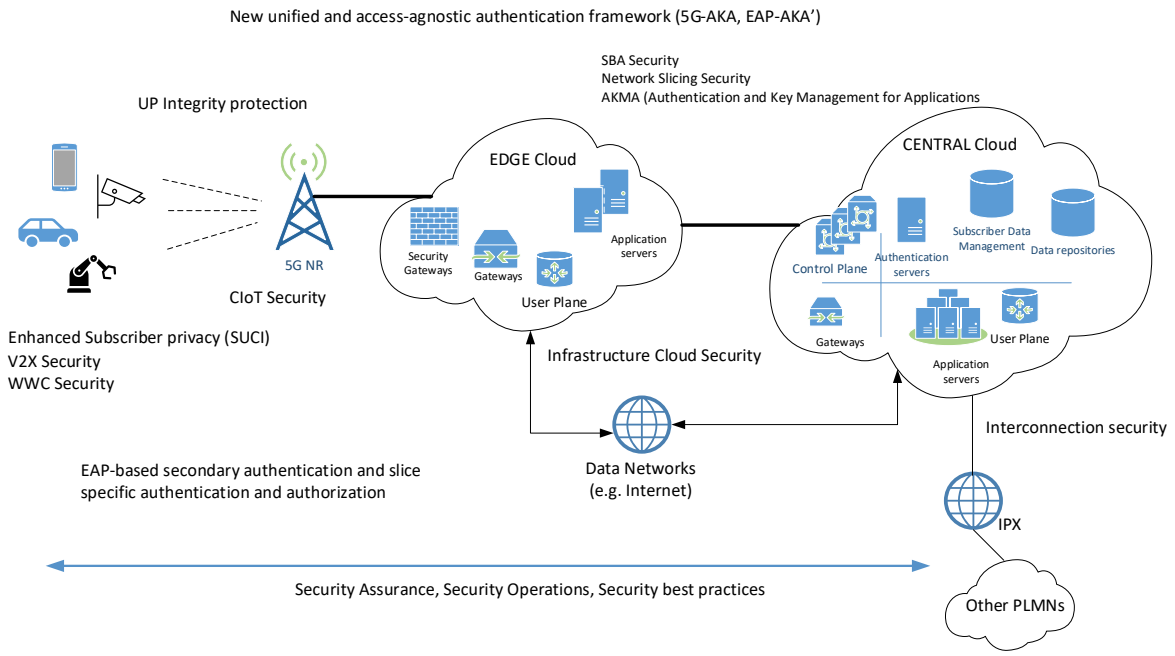

Fig. 2.1.3-1: Schematic overview of the 5G network security architecture

The foundational features defined by 3GPP in 5G have been the following:

- **New Unified and Access-Agnostic Authentication Framework**: The 5G system supports two main authentication methods: 5G-AKA (Authentication and Key Agreement) and EAP-AKA' (Extensible Authentication Protocol for AKA). Both mechanisms can be applied for 3GPP as well as for non-3GPP access, and both provide assurance to the home network that the User Equipment (UE) is present in the visited network, which brings a significant improvement in Home Public Land Mobile Network (HPLMN) control in roaming scenarios. Besides EAP-AKA' other EAP methods, such as EAP-TLS, can be implemented, for example, in non-public networks and vertical industries (e.g., in the authentication of Wi-fi devices).
- **Enhance Subscriber Privacy**: 5G enhances the privacy posture in previous mobile network generations, preventing the SUPI (Subscription Permanent Identifier) from being sent in clear over the air interface. In a public network, SUPI contains an IMSI (International Mobile Subscriber Identity). There is a specific schema to encrypt a SUPI in case it has to be transmitted from the UE to the network, building a new identifier known as SUCI (Subscription Concealed Identifier). The UE computes the SUCI by encrypting (Elliptic Curve Integrated Encryption Scheme, ECIES) the individual part of the SUPI (MSIN: Mobile Subscriber Identification Number) with a public key pre-

provisioned in the UE. The network decrypts the SUCI using the Subscription Identity De-Concealing Function (SDIF). Note that mostly the 5G-GUTI (Globally Unique Temporary Identifier) is used over the air, and there are stringent requirements for frequent allocation of a new GUTI.

- **User Plane (UP) Integrity Protection in Radio Access Network**: UP integrity includes both confidentiality (encryption) and integrity protection and is mandatory to support and optional to use in the Radio Access Network (RAN). This means that the use of integrity protection will be negotiated between the UE and the network. The negotiation is done per PDU (Protocol Data Unit) session, and the Session Management Function (SMF) is in charge of sending the policy decision down to the gNB (5G base station), where the policy gets applied on a Radio Bearer-specific basis.
- **Service Based Architecture (SBA) Security**: Two basic security mechanisms have been standardized to protect the service-based interfaces of SBA (both mandatory to support, but optional to use):
    - TLS with client and server certificates (a.k.a. mutual TLS) between all NFs.
    - Token-based authorization schema for service requests to network functions based on OAuth 2.0 framework. NRF (Network Repository Function), acting as OAuth authorization server, authorizes NFs to use services provided by other NFs, exposed by APIs, according to predefined policies.

  In addition, new service communication models have been introduced between consumers and producers in SBA. Specifically, a new component named SCP (Service Communication Proxy) enables indirect communication for NF-NF interactions, acting as a trusted intermediary with certain delegated functions. SCP can assume functions of services discovery and selection of instances providing those services on behalf of the consumer, as well as routing functions. In addition, a concept of Client Credentials Assertions (CCA) has been added to enable end-to-end authentication by signed tokens on the NF consumer side. These mechanisms enable the support of service mesh architectures.
- **Enhancements for Interconnection Security**: The 5G system introduces a new entity named SEPP (Security Edge Protection Proxy) for signaling interconnection between operators. All roaming control traffic is routed via the SEPP and the N32 interface to the SEPP of the other PLMN. Two end-to-end protection mechanisms have been specified, TLS at network layer and PRINS (PRotocol for N32 INterconnect Security)

at application layer for JSON (Java Script Object Notation) information elements on N32. The SEPPs have the capability of security negotiations, i.e., selecting the protection mechanism and, in the case of PRINS, applying granularly encryption, integrity protection, and authentication at Information Element (IE) level.

Further details of the enhancements for Interconnection Security introduced in 5G, namely 5G Signaling Roaming Security architecture, are provided in subchapter 6.2 of the present document. The reason for placing most of the contents of the state of the art related to 5G Signaling Roaming Security architecture in chapter 6 is to facilitate the justification and correct understanding of the new concept of security profiles in that context.

2.2 Review of risk management frameworks in mobile networks

Mobile networks connect with each other very often through the Internet Protocol Exchange (IPX) Network to provide roaming services. As those networks are independent of each other and act in different jurisdictions, there is no central authority to secure the overall system. The standard security risk evaluation framework EN-ISO/IEC 27005 [3] allow us to evaluate the risks related to 5G networks with a concrete methodology, although it would need to be complemented with several techniques to provide a consistent management of the risks related to roaming. Reference [5] discusses the need for a comprehensive and regular risk management approach in 5G networks as a prerequisite to provide efficient security measures based on asset's criticality. It also confirms the support by Regulations, particularly in the European Union (EU), with the reform of the EU data protection rules, the entry into application of the General Data Protection Regulation (GDPR) [36], and especially with the recent regulation known as EU CSA (Cyber Security Act) [37]. GDPR broadens the relevance of risk, as it is explicitly based on the notion of a risk-based approach, whereas EU CSA in clause (49), part of the initial assumptions, clearly indicates the need to establishing risk management-based approaches and measuring the security:

"*Efficient cybersecurity policies should be based on well-developed risk assessment methods, in both the public and private sectors. Risk assessment methods are used at different levels, with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public-sector and private-sector organizations will increase the level of cybersecurity in the Union. To that end, ENISA should support cooperation between stakeholders at Union level and facilitate their efforts relating to the establishment and take-up of European and international*

standards for risk management and for the measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems."

In 2017, the 5G ENSURE program (EU-funded project for the development of 5G networks) through one of the deliverables referenced as 5G-ENSURE D2.3 Risk Assessment, Mitigation and Requirements [38] took the first steps toward the definition of a risk assessment and mitigation methodology for 5G. The study was based on EN-ISO/IEC 27005 [3], and especially on its simplification represented by NIST (National Institute of Standards and Technology) SP-800-30 [39].

J.M. Batalla et al. in [7] introduced a risk assessment and risk mitigation methodology applicable to specific aspects of 5G network security. The proposed methodology was based on [3] and responded to the requirements and expectations of the European Commission for the report elaboration on EU coordinated risk assessment of 5G network security [40].

These references represent a baseline for the implementation of a risk framework in 5G mobile networks. However, although the interconnection/roaming context is briefly mentioned, it is not the focus of any of those works and subsequently, not meritoriously treated. Nevertheless, a common denominator is that the interconnect network is considered a critical point in the network, rated as moderately to highly sensitive.

More recently, ENISA elaborated an analysis of standardization requirements in support of cybersecurity policy in 5G [41]. There, risk management, specifically "Sector-specific governance and risk management", is identified as a gap in standardization, outlining that the existing literature related to risk assessment is not specific to 5G and/or does not identify and evaluate risks consistently. Moreover, the analysis recommends fostering the maturity and completeness of the identification and assessment of the risk of the 5G ecosystem. Specifically in interconnection/roaming, a major gap is identified in the section of "Monitoring, auditing, and testing" in relation to event correlation for 5G roaming.

Finally, in most countries worldwide mobile networks are considered a critical national infrastructure. The Network and Information Systems Directive (NIS2), issued by the European Union in December 2022, classifies MNOs as a type of entity within sectors of high criticality, referring to them as "providers of public electronic communications networks" [42]. Within the remit of NIS2, MNOs are explicitly required to implement more rigorous security mechanisms

across their networks, including the signaling systems used for interconnection. Cybersecurity risk management measures and reporting are key aspects of NIS2 regulation. Along the same line, the Government of the United Kingdom (UK) defines critical infrastructure as "those facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends". Furthermore, within this critical infrastructure, the UK National Cyber Security Centre (NCSC) has identified the international signaling plane as a high-risk area in its security analysis for the telecoms sector [43].

Chapter 4 of the document addresses specifically the risk management in signaling interconnection/roaming by proposing a dynamic method risk evaluation mechanism, intended to support risk management frameworks in 5G networks.

2.3 Review of trust score in mobile networks

European Telecommunications Standards Institute (ETSI) defines security and trust guidance for NFs [44]. ETSI's guidance adheres to the principles of zero trust design by emphasizing that compliance and state measurements must be continuously monitored in order to evaluate the level of trust of an NF. Trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfill specific responsibilities. Trust is considered to be dynamic, thus it is expressed in assurance levels based on specific measures that identify when and how a relationship or transaction can be relied upon. Trust measures may include different assurance elements, such as identity, attribution, attestation, and non-repudiation. Some of the parameters for trust evaluation in Network Functions Virtualization (NFV) are geographical location, jurisdiction/regulatory location (public/private), logical (network) location, hardware/software capabilities, provenance and history, chain of trust, security of network, appropriate use of encryption techniques, etc.

The National Institute of Standards and Technology (NIST) published in 2020 a special document named "Zero Trust Architecture" (NIST SP.800-207) [45], with the target of improving the security posture of the enterprise networks. The Zero Trust Architecture (ZTA) is to be built according to seven principles that are listed here for convenience:

1. All data sources and computing services are considered resources
2. All communication is secure regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy – including the observable state

of client identity, application/service, and the requesting asset

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

One of the critical logical components of the architecture is the Policy Engine (PE). The PE is responsible for the ultimate decision to grant access to a resource for a given subject. In order to make a decision, it will feed a Trust Algorithm, described as well in [45], with multiple and different kinds of data, internal (e.g., internal security policies) or external (e.g., Threat Intelligence sources). Those sources are conveniently evaluated/weighted by the Trust Algorithm according to the implementer's criteria. Among the variations described in the NIST publication, the one based on score, i.e., the computation of a confidence level, has been considered in our dissertation, referred to as “trust indication” or “trust score”, and computed based on a dynamic risk evaluation, as detailed in Chapters 4 and 5 of this dissertation. The trust score is used to select and apply security policies in the interconnection gateways, i.e., Policy Enforcement Points (PEP) in ZTA lingo, eventually modifying the established Security SLAs with roaming stakeholders, peers, or IPX providers. Those aspects are discussed in chapters 6 and 7.

3GPP SA WG3 (Security and Privacy) standardization group has studied the applicability of ZTA principles in 5G network, specifically in 5G Core, in Releases 18 (TR 33.894 [46]) and 19 (TR 33.794 [47]), and it is expected that the next releases, including 6G, will be designed with those principles in mind. In the following table 2.3-1, I compare briefly both NIST SP 800-207 versus 3GPP security specifications as of today:

Tab. 2.3-1: NIST SP 800-207 versus 3GPP Specifications

	NIST SP 800-702	**3GPP Specifications**
Scope	Enterprises	Cellular networks

Protection Target	Enterprise data and services	The cellular network, confidential network and user data (including user traffic, and location)
Security Mechanisms	Authentication + authorization of access requests based on a trust algorithm Cryptographic traffic protection Continuous diagnosis & mitigation Gathering threat intelligence	Authentication of user equipment and network entities Authorization of access to network services and resources Cryptographic traffic protection Many feature-specific mechanisms
Level of specification	General approach, some more details on important mechanisms	Down to the bit level as required to ensure interoperability

There are multiple elements of the 3GPP 5G security architecture that reduce the need for implicit trust, such as primary and secondary authentication, authorization for use of services, three different security associations between UE and different parts of the network, three independent security algorithm sets, mechanisms to control the security policy to be applied for user traffic on the radio interface, network slice specific authentication and authorization, etc.

The security mechanisms are available for all interfaces of the architecture, but of course, 3GPP, as a standardization organization, cannot force MNOs to use them. In the following schema (Fig. 2.3-1), adapted from 3GPP TS 23.501 [48], I summarize and place the security mechanisms in the overall 5G architecture, including the ones specified between 5G Network Functions. Specifically in interconnection, the following mechanisms have been standardized (more details are provided in subchapter 6.2):

- Interconnection control plane
    - Mutual authentication of SEPPs using TLS based on client and server certificates
    - Traffic protection using TLS and PRINS (involves Java script object notation encryption and signatures)

- Interconnection user plane
    - IKEv2/IPsec like for other non-service-based interfaces
    - IPUPS (Inter PLMN User Plane Security) to discard rogue incoming packets

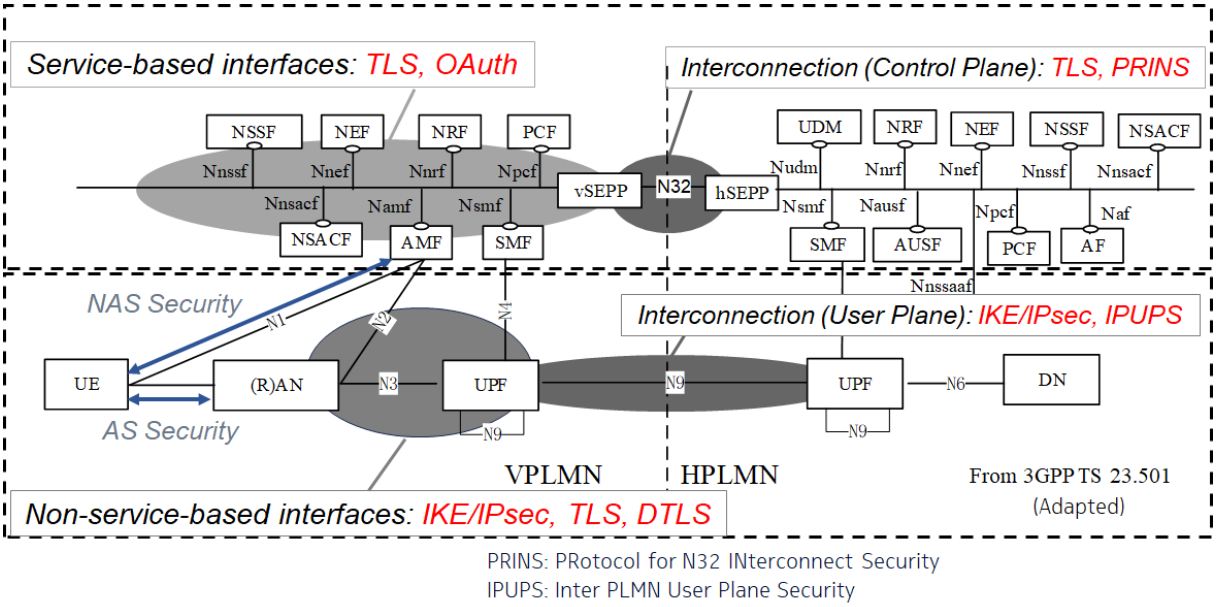

Fig. 2.3-1: Security Between 5G Network Functions (adapted from 3GPP TS 23.501 [48])

Therefore, the 3GPP 5G security architecture is never built on perimeter security but comprises securing all the external and internal interfaces properly, building on mutual authentication, authorization and cryptographic protection. The 3GPP security architecture comprises many layers of protection, reducing the need to trust single components (e.g. base stations) or peering networks.

Finally, since Release 16 3GPP has specified enhancements to the 5G System to support network data analytics services [4]. The NF supporting those analytics is the NWDAF (Network Data Analytics Function). There have also been security studies related to those data analytics services and NWDAF, and some solutions, proposed as part of those studies, described the functionality of detection of anomalous NF behavior by the NWDAF. However, the functionality itself has not been finally standardized by 3GPP in 5G. In those preliminary studies (e.g., TR 33.866 [49], TR 33.738 [50]) the proposed solutions have not indicated the level of a broader and "longer term" trust, i.e., whether the NF can be considered as trustable or not based on statistics and predictions regarding its potential abnormal behavior, as well as on security and risk considerations. Furthermore, currently there are no standardized means for maintaining such trust indication and utilizing it in the most efficient way.

2.4 Review of security policies and profiles in mobile networks

The establishment of security policies in mobile networks has been considered an operational issue that must be fixed by each MNO in their own networks. Whereas security requirements, functionalities, protocols, and procedures are usually defined for mobile networks by standardization bodies like 3GPP (e.g., TS 33.501 [1]), the translation of those to concrete security policies is generally left to implementation. Nevertheless, in the specific scenario of signaling interconnection/roaming, the industry group GSMA Fraud and Security Group (FASG) has elaborated a set of security policies to be implemented in signaling firewalls, e.g., annex B.3 of FS.11 [27] for 2G/3G (SS7 firewalls) and annex B.3 of FS.19 [32] for 4G (Diameter firewalls). SEPP rules and guidelines for SEPP network implementation in 5G networks will be part of future versions of FS.36 [51].

There is no formal definition of security profiles or profiling, but rather, there are particular adoptions of the term in the literature. In standardization, several specifications have used the term to specify which algorithms and parameters are to be used in a protocol or protocol suite. The intention is to facilitate the interoperability and consistent security level in standardized interfaces. For example, 3GPP TS 33.210 [52] profiles IPsec in clause 5.2, TLS 1.3 in clause 6.2.2, etc.

GSMA provides a set of templates and guidelines for international roaming agreements to facilitate interoperability and consistency between MNOs. These templates are part of the AA and BB series documents and include SLAs for different aspects of roaming services, including Security. Among them, we highlight the following ones:

- AA.12 (“Standard Template for International Roaming Agreement”) [53] establishes the general terms and conditions between operators for roaming, and includes references to security obligations that operators must fulfill to ensure secure and reliable roaming operations.
- AA.13 (“International Roaming Agreement – Common Annexes”) [54] details the expectations of potential common annexes in the SLA. Among them we find the technical security aspects under annex C.5.2, data privacy aspects in C.6, and fraud prevention aspects in C.7.
- BA.51 (“Roaming Service Level Agreement Guidelines”) [55] provides guidelines for MNOs, Roaming Hub providers, and IPX providers to optimize the roaming services by using end-to-end SLAs.

Thus, the security policies and profiles are to be documented in the International Roaming agreements between operators, which may use the referred GSMA templates or other similar ones crafted for the same purpose.

The Chapter 6 of the dissertation addresses the security policies definition and profiling in 5G networks in interconnection/roaming scenarios, with new concepts to be applied in the new end-to-end Application Layer Security framework.

2.5 Review of security enforcement in mobile networks

The reference [8] discusses the security enforcement in mobile networks and introduces a new concept by reusing the policy control function framework in 5G [56]. The concept of considering security as a dimension of QoS in networks has been commonly accepted for many years by the telecommunications industry. However, from an enforcement perspective, the implementation of security policies and QoS parameters in the network differ significantly in mobile networks so far. This is because, until the arrival of 5G, security had been only regarded as an add-on feature, whereas QoS always represents the key measurement parameter of the network. In contrast, in 5G security has been considered an essential part of the overall architecture and built into it natively. On the other hand, in 5G, the PCF provides a single framework for defining any type of policies in the network and for delivering related policy rules to the other control plane network functions as relevant per each function.

The procedures related to the enforcement of security policies in 5G are specified in TS 33.501 [1]. Except for the air interface between the UE and NG-RAN, the security enforcement in the User Plane in the rest of the network is configured locally and statically per network segment without a consistent end-to-end policy across the entire network.

The challenge of applying QoS principles to security enforcement and how to enable quantification of security characteristics in the network currently does not have an existing unified approach. Traditionally, security enforcement mechanisms have been static and exclusively preventive, for example, the policies deployed in firewalls in the perimeter, i.e., in sGi (EPC) and N6 (UPF) core network interfaces towards Internet or in general Data Networks. In contrast, QoS profiles can be dynamically established by the SMF in the 5G access network. QoS profile is well defined as the set of QoS parameters applied to a QoS flow (QoS flow is the finest granularity of QoS differentiation in a PDU session). Such parametrization is quantitative, i.e., it can be measured with numerical digits. For example, the QoS identifier is a

parameter represented by a scalar used as a reference to 5G QoS characteristics such as scheduling, weights, admission thresholds, etc. There are even pre-configured standardized values. The SMF manages QoS flows with rules, associating traffic filters with QoS policies coming from the PCF. Currently, the 3GPP 5G policy control framework mainly focused on QoS, and QoS rules can be enforced to the UE either through Session Management (SM) signaling over N1 from the SMF (via the AMF), or directly on the UPF over N4 interface.

The evolution of security management systems such as SIEM (Security Incident and Event Management) to SOAR (Security Operations, Automation, and Response) attempts to cope with the challenge of automatically and intelligently reacting to security incidents through the design and implementation of security workflows in the enterprise network. Extended Detection and Response (XDR) technologies are currently the most sophisticated solutions that unify multiple security layers and offer a more comprehensive and automated approach to threat detection and response by using Artificial Intelligence (AI). All those technologies require a high grade of customization and adaptation of interfaces and patching of data to convert it into "something digestible" by the tools.

Chapter 7 of the dissertation proposes a new concept that enables the specialized security management systems (e.g., SIEM, SOAR, XDR, etc.) to enforce in a standardized way (i.e., avoiding customizations) security policies and profiles across the entire 5G network by improving the Policy Control framework and current Network Analytics. Furthermore, subchapter 8.5 provides the guidelines to adapt the concept to interconnection.

3 Security Framework Overview

This chapter reviews the motivation for the development of a new Security Framework for the interconnection of mobile networks and outlines its main design principles by showing how the main building blocks of the Framework, described in detail in subsequent chapters, are connected and operate in unison.

3.1 Introduction

As introduced in the Theme of the dissertation, the overall context of this research is Security in the Service Level Agreements (SSLAs) in the interconnection of telecommunications mobile networks, considering the coexistence of different protocol stacks in each generation, i.e., SS7 in 2G and 3G, Diameter in 4G and HTTP/2 in 5G. In Figures 3.1-1 and 3.1-2, I represent the actual situation in most operators with licenses in 2G/3G/4G/5G and the associated protocol stacks to be maintained in interconnection.

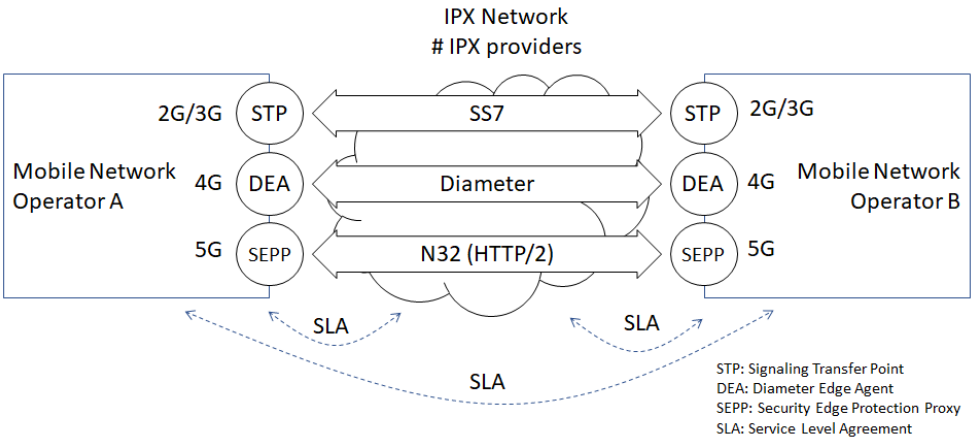

Fig. 3.1-1: Coexistence of all mobile network generations in interconnection

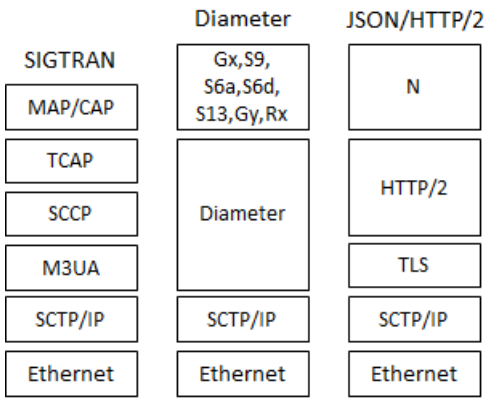

Fig. 3.1-2: Protocol stacks in interconnection

When discussing the current situation of interconnection in previous chapter, we argued that the security posture is not static in any network environment; instead, it requires continuous adaptation based on a constant and dynamic risk evaluation. Although interconnection signaling standards were initially specified on the assumption that all links between operators could be trusted, the reality is that there have been multiple security breaches in those links since SS7 times and afterwards with Diameter in 4G [20] [57]. Those breaches have had severe consequences for MNOs and their subscribers, such as fraud, privacy issues, bad reputation, and penalties. Different types of agents have been behind them:

- Intelligence communities that use mobile networks for VIP tracking and eavesdropping.
- Dark service companies that use interconnection links to make money (e.g., fraud, SMS interception, location tracking offerings, etc.).
- Military / Law enforcers that use mobile network data for target localization.
- Etc.

5G introduces a new end-to-end security paradigm supported by new standard protocols that add a new application security layer. However, at the time of writing this dissertation, 5G roaming interconnection has barely been deployed, and it is widely assumed that it will still coexist with SS7 and Diameter protocol stacks for many years. Furthermore, there is no reason to think the cited breaches will disappear with the new 5G protocols and that the attackers and above-mentioned agents will stop their activities. In addition, the security landscape is continuously changing, and the operators are expected to adapt accordingly their defenses, starting with measuring and controlling the risk levels.

Those factors have motivated the Security Framework that I propose for interconnection in this dissertation.

3.2 High-level Schema of the Proposed Framework

The proposed framework evaluates each interconnection link based on the dynamic message exchange. The messages in the interconnection links have different risks associated with the information contained in the message, the procedures that they support, and others. Moreover, the framework also considers the message sequences exchange as a whole and not only the single packets. This is because single messages do not provide full information on the risk (note that every single message is allowed and important for the proper functioning of the roaming services). However, repetition of risking messages or the concatenation of specific messages

may show a higher risk of the overall message exchange. Based on the dynamic evaluation of the message exchange risk, the framework gives a score to individual interconnection links and decides on the security policies to be enforced as per that interconnection peer.

Fig. 3.2-1 represents the high-level schema of the security framework that I have designed and conceptualized as a security lifecycle-oriented architecture.

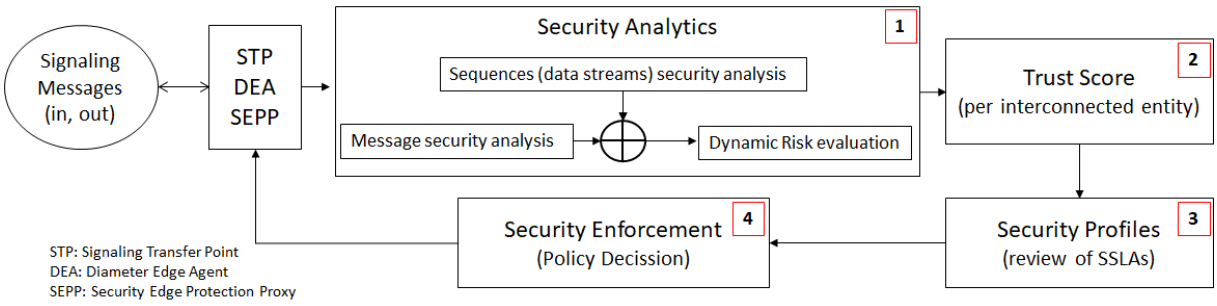

Figure 3.2-1: Security Framework Overview

The main building blocks of the schema are:

1) Security Analytics – Dynamic Risk evaluation
2) Trust Score (per interconnected entity)
3) Security Profiles (review of SSLAs)
4) Security Enforcement (policy decision)

I have designed the schema to be valid and implementable across the actual protocol stacks in interconnection in each of the existing mobile generations, to some extent becoming "agnostic" to the technology itself. Therefore, it should be applicable as well to the upcoming 6G mobile generation, still in pre-standardization stage at the time of writing this dissertation.

It can be safely assumed that all inbound and outbound signaling messages in interconnection traverse the signaling gateways, which are placed in the perimeter of the Mobile Core network, namely Signaling Transfer Points (STPs) in case of 2G/3G, Diameter Edge Agents (DEAs) in case of 4G, and SEPP (Security Edge Protection Proxy) in case of 5G. Those gateways act as bastions of the network, where security policies and protection mechanisms can be enforced (e.g., the establishment of secure tunnels such as IPsec to transport SIGTRAN or Diameter, activation of TLS for HTTP/2, encryption of specific Information Elements, etc.).

A copy of the signaling traffic (input) is required to be processed by the first building block named **Security Analytics** in our schema. The copy can be done by the signaling gateway itself

if such a feature is available in the system, or via internal or even external taps (physical or virtual). The Security Analytics block is responsible for performing a dynamic risk evaluation, firstly, by analyzing and weighting a set of preselected relevant security and privacy attributes at message level, and secondly, by analyzing from security and privacy viewpoints the sequence patterns in the signaling traffic, which has been modeled as data streams. The outcome is the measurement and computation of the risk, for which I have taken and adapted the Common Vulnerability Scoring System (CVSS) [58]. Please refer to Chapter 4 for a detailed description of the proposed Security Analytics building block of the schema.

The measurement of the risk is one of the key factors (there could be others not specifically studied in this dissertation) to build a **Trust Score** per interconnected entity to the MNO. In the sample procedure provided in subchapter 8.3, this indicator (e.g., a scalar value) is part of a proposed enhancement in the actual Network Data Analytics Function (NWDAF) of 5G, although other options could also be suitable. The trust score can be computed in an aggregated mode per VPLMN. Please refer to Chapter 5 for a detailed description of the proposed Trust Score building block of the schema.

The Trust Score should serve as a key input for the continuous review of the SSLAs. The concept of **Security Profiles** in interconnection has been created in 5G context to facilitate the negotiations of protection mechanisms and security policies between MNOs when Application Layer Security is selected. The elaboration of Security Profiles for previous mobile generations is certainly possible, but they are not part of the present dissertation. Therefore, the third building block of the schema is reduced to the review of SSLAs in case of 2G/3G/4G, but without the possibility to use Security Profiles for the interconnection links. Please refer to Chapter 6 for a detailed description of the proposed Security Profiles building block of the schema.

Once the risk measurements have been computed, the trust score has been determined, and the security policies/profiles have been selected, the next step in the framework is the **Security Enforcement**. This building block has been crafted by enhancing the actual Policy Control and Network Analytics frameworks standardized in 5G. The main purpose is to be capable of dynamically establishing security policies over the corresponding interconnection signaling gateways, or alternatively attached security platforms, such as signaling firewalls. Please refer to Chapter 7 for a detailed description of the proposed Security Enforcement building block of the schema.

4 A Dynamic Risk Evaluation Mechanism for Mobile Networks Interconnection Signaling

This chapter focuses on the proposed mechanism for a dynamic risk evaluation in the interconnection of mobile networks and it corresponds to the first building block of the overall security framework. The system receives a copy of the signaling traffic (modeled as data streams) from the interconnection signaling gateways, and provides the computation of a risk index, which is the main key factor in determining the trust score.

Subchapter 4.1 (Introduction) reviews the motivation for developing a dynamic risk evaluation mechanism in the context of interconnection of mobile networks. Subsequently, subchapter 4.2 firstly introduces a mathematical notation which will be used in the entire chapter to describe the risk evaluation mechanism. Exchanged signaling messages and sequences are accordingly modeled to facilitate the identification of critical security attributes and patterns. Afterwards, I propose two primary security analyses that constitute the baseline of the risk evaluation mechanism, i.e., the analysis of the individual messages based on expert knowledge and applied to a series of stepwise ordered filters, and the analysis of sequence patterns based on data mining over data streams type of techniques. Next, subchapter 4.3 proposes a computation of the risk by applying the principles and available tools of Common Vulnerability Scoring System (CVSS) [58] to this specific environment. To the best of our knowledge, this is the first work that adapts CVSS to mobile networks interconnection environment. While a few documents in the industry, such as [51], have indicated the possibility of adapting a framework like that, none has addressed the challenges associated with it, making our adaptation a novel contribution.

Note that under Chapter 8, the subchapter 8.1 presents the validation of the overall mechanism by applying it to a theoretical Location Tracking use case, and the subchapter 8.2 provides a more practical validation over a real traffic diameter trace in interconnection between two operators in Asia.

4.1 Introduction

Risk management is a complex task in telecommunications, especially in interconnection links, which are out of the operator's control. Security events, from mere sensitive and suspicious messages to sophisticated attacks over a period (e.g., APT (Advanced Persistent Threats)), are usually unforeseen, thus, changes in risk levels may occur without any predefined pattern. Consequently, a dynamic (“online”) risk evaluation should be the cornerstone of any security

framework capable of reacting automatically to changes in the risk level of the interconnection links.

This research proposes a new mechanism to address and compute the risk evaluation in the roaming context. Note that we do not pursue the design of a new Intrusion Detection System (IDS) for accurate attack detection. The ultimate target is rather to support the building of a trust score/index per operator by a dynamic computation of the risk in the interconnection links that enables the selection among different security profiles, which are translated into concrete policies to be enforced in the interconnection gateways (i.e., STP in 2G/3G, DEA in 4G and SEPP in 5G) and/or attached signaling firewalls.

The mechanism consists of two primary security analyses:

1) Individual message analysis.

2) Sequence analysis.

Security analysis at the message level is performed using expert knowledge. GSMA FASG in different Functional Specifications (FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines [27], FS.19 Diameter Interconnect Security [32], FS.36 5G Interconnect Security [51]) has depicted an initial rough risk estimation per possible message interchanged between operators in the different schemas of interconnection. That risk estimation is based on the possibility of misuse of certain messages that may become part of potential attack vectors such as interception, fraud, spam, DoS (Denial of Service), or Location tracking. Complementarily, the proposed security analysis presented in this dissertation structures the risk evaluation in different steps, where each message is filtered based on several criteria (e.g., origin, protocol conformance, category, security sensitivity, etc.). The risk is computed in every step, contributing to the link's overall risk evaluation (interconnection interface). Basically, the concept is that a deterministic analysis per exchanged message evaluates a set of pre-selected features/fields of the message relevant to the security analysis.

Most of the applications used in telecommunications, and signaling in interconnection is not an exception, use data that cannot be modelled as persistent tables but rather as transient data streams that evolve over time. Data streams are stochastic processes in which events occur continuously and independently. In the context of signaling traffic in interconnection, the received/sent data is (to some extent) regulated by specified protocols and standard procedures (3GPP TS 29.573 “5G System; Public Land Mobile Network (PLMN) Interconnection; Stage

3" [59]). Therefore, even if the events are independent, there are identified sequence patterns of messages that need to be considered, i.e., the "time" variable is introduced in the analysis as sequences of messages subject to well-defined standards. The proposed security analysis of sequences in signaling traffic is intended to evaluate the appearance and frequency of specific critical sequence patterns from a risk viewpoint, which would allow, for example, fetching the IMSI, getting the location, or modifying the subscriber data, among others. The analysis should also be able to find rare patterns in the signaling and identify those conveying sensitive information, such as privacy-related data or charging subscriber data. Data mining techniques applied to data streams are proposed for this sequence security analysis.

The methodology assumes that different algorithms can be used in the proposed model for sequence pattern mining in data streams and for extracting meaningful statistics, that are used for further security analysis, out of the exchanged signaling messages. Therefore, for the designed filters and metrics, a different set of algorithms can be tested and selected by an implementer of the mechanism. The specialized security company Adaptive Mobile reported during a virtual event organized by GSMA FASG (FASG #19 [60]) that 0.04% of the traffic in interconnection (just considering SS7 links) is irregular/suspicious, and out of it, 1.37% is malicious, with the majority related to location tracking. These numbers, coming from the field, have oriented our study towards techniques that enable us to harvest very specific and meaningful information for security analysis, out of the signaling data streams. Those are known as *data stream mining* techniques [61].

Note that, although the methodology is perfectly valid for all three existing technologies in interconnection, in this dissertation, I have detailed the application of the methodology in 4G and 5G related technologies, thus neglecting the details on SS7 used in previous generations. The reasons are conciseness, i.e., most of the security issues in Diameter used in interconnection have been inherited from SS7, and relevance, progressively the services currently provided by SS7 signaling will be migrated to Diameter or HTTP/2, together with the network's transformations in the next future.

4.2 Dynamic Risk Evaluation Mechanism

Fig. 4.2-1 summarizes the main components of the mechanism that I propose for a dynamic ("online") evaluation of the risk in interconnection links. They are organized in two threads that finally contribute to the overall computation of risk and that correspond to the two primary analyses already mentioned:

- Thread-1: Message analysis supported by expert knowledge.
- Thread-2: Online sequences security analysis on data streams.

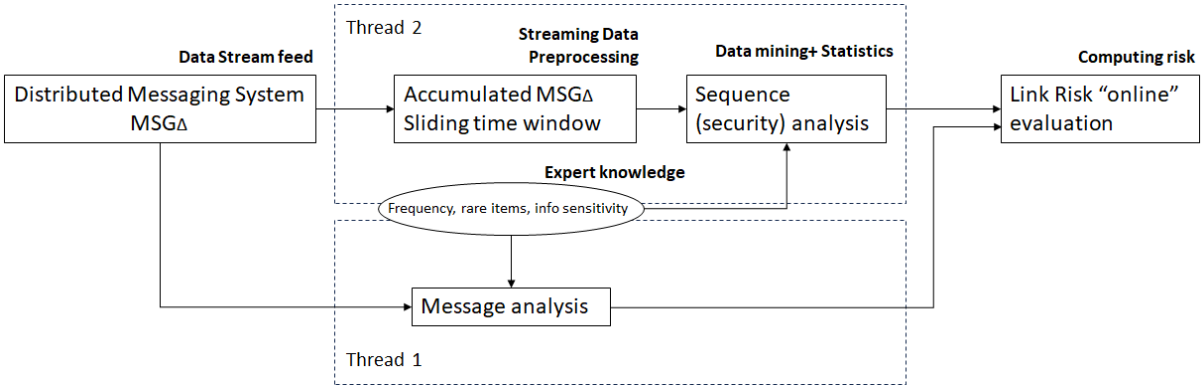

Fig. 4.2-1: Risk evaluation building blocks schema

After introducing a basic mathematical notation required for the modeling of the mechanism, the following subchapters explain the design of both threads and the components of the entire evaluation.

4.2.1 Mathematical notation

Let's denote $\mathcal{I}$ the set of all possible messages in interconnection:

$\mathcal{I} = \{i_1, \dots, i_n\}$

i_i: Unit of information in signaling, i.e., a signaling message.

- In 4G: Diameter standardized messages.

- In 5G: HTTP/2 standardized messages.

> Note: Both schemas, 4G and 5G, are independent. $\mathcal{I}$ refers to all possible messages in Diameter or (exclusive) in HTTP/2, depending on whether the clause in the chapter relates to 4G or 5G signaling.

The signaling messages count with a set of attributes (a.k.a. features) relevant to the security analysis that are represented as:

$A = \{A^{(1)}, \dots, A^{(d)}\}$

$A^{(j)}, j \in \{1..d\}$ is a discrete random variable for a particular attribute *j* over all messages under analysis.

$a_i^{(j)}$ is the value of attribute *j* in the message *i*.

$\mathbb{X}^{(j)}$ is the set of all possible values for a particular attribute $A^{(j)}$, so $a_i^{(j)} \in \mathbb{X}^{(j)}$.

A dataset X of N messages under analysis is represented as:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} a_1^{(1)} & \cdots & a_1^{(d)} \\ \vdots & \ddots & \vdots \\ a_N^{(1)} & \cdots & a_N^{(d)} \end{pmatrix}$$

One row corresponds to one signaling message characterized by 'd' (security) attributes:

$x_i = \left(a_i^{(1)}, \dots, a_i^{(d)}\right), a_i^{(j)} \in \mathbb{X}^{(j)}$.

One column represents the values of an attribute across N messages. Note that for simplicity we abuse the notation and use $A^{(j)}$ for the set of N realizations of the random variable corresponding to each of the N messages.

A sequence Y of signaling messages is represented as a mapping function f between $\mathbb{N}$ and $\mathcal{I}$, so we can write:

$f : \mathbb{N} \to \mathcal{I}$ to be that mapping.

We can write the elements of the sequence as $Y = (y_k)_{k \in \mathbb{N}}$ with $y_k = f(k), k \in \mathbb{N}$. Then, a subsequence of $Y = (y_k)_{k \in \mathbb{N}}$ is any sequence Z of the form $Z = (y_{k_l})_{l \in \mathbb{N}}$ where $(k_l)_{l \in \mathbb{N}}$ is a strictly increasing sequence of positive integers defined by the function ϕ with $\phi : \mathbb{N} \to \mathbb{N}$ being a strictly increasing mapping.

The subsequence Z can be represented as:

$$Z = \left(z_1, \dots, z_j, \dots z_m\right)$$

A sequence pattern, also known as a sequential pattern, is a recurring subsequence or motif within a set of sequences. Sequence patterns are discovered through data mining algorithms that aim to identify meaningful subsequences within the data set. Let's define a sequence pattern of signaling messages S as a tuple:

$$S = (s_1, \dots, s_i, \dots s_n)$$

Where s_i is the $i - th$ signalling message of the sequence pattern.

A transaction is defined as a tuple of a transaction identifier (t_{id}) and a sequence pattern (S):

$$t = (t_{id}, S)$$

If $Z \subseteq S$ (i.e., Z is a subsequence of S), then t contains Z, i.e., Z occurs in t.

In general, a data stream is a countably infinite sequence of elements used to represent data elements made available over time [62]. More formally, a data stream can be defined as an infinite sequence of transactions, i.e.:

$D = [t_1, \dots, t_m)$, where t_i, $i \in [1..m]$ is the ith transaction in the data stream.

For simplicity reasons, along the dissertation, we will mostly use the notation $x_1, x_2, \dots, x_t, \dots$ to represent the input data stream, where x_t (signaling message) arrives sequentially at the time t, and describes an underlying function $F[i]$ for $i \in [1, N]$, which we would like to query for our security analysis. Formally, Muthukrishnan [63] describes three data stream models based on how $x_i's$ characterize F:

- Time series: $x_t = F[t]$
- Cash Register: $x_t = (j, c_t), c_t \geq 0$ to mean $F_t[j] = F_{t-1}[j] + c_t$, where F_t is the state of the signal after seeing the tth item of the stream. Note that $F_t[j'] = F_{t-1}[j']$ for all $j' \neq j$.
- Turnstile: As Cash register, but no restriction on c_t (i.e. c_t could be negative).

The first "Time series" model treats every element x_i in the stream as a new independent vector entry, i.e., each element is to be processed individually. The processing of each message in the data stream to investigate a few selected attributes is the main purpose of the proposed individual message analysis based on expert knowledge of the methodology. Nevertheless, the computation of the risk also comes from the monitoring and identification of specific messages

and sequence patterns of signaling messages within the data stream under analysis to measure the appearance, frequency, and potential anomalies (rare items), which weigh the overall risk factor. The "Cash Register" model fits our sequence analysis application and $F[j]$ represents in this case a security/privacy critical message or a category of those (e.g., user identifiers, location, authentication info, etc.).

4.2.2 Expert knowledge applied to message analysis

Each signaling message of the input data stream is to be analyzed individually, i.e., given an input data stream $x_1, x_2, \ldots, x_t, \ldots; x_t = F[t]$, where F is the signal to be queried at the time t, the value of the variable t $(time)$ itself is not relevant for the computation of the risk at message level; it is instead a simple identifier of the message.

Fig. 4.2.2-1 represents the overall schema that I propose for individual signaling message analysis. The schema consists of a sequential series of filters intended to calibrate the inherent risk of the individual message based on certain predetermined features (e.g., origin, protocol conformance, etc.) and selected statistics (heuristics) over values conveyed in the message and related to security-sensitive information (e.g., privacy, charging, location, etc.). Every step in the analysis contributes to the risk at message level.

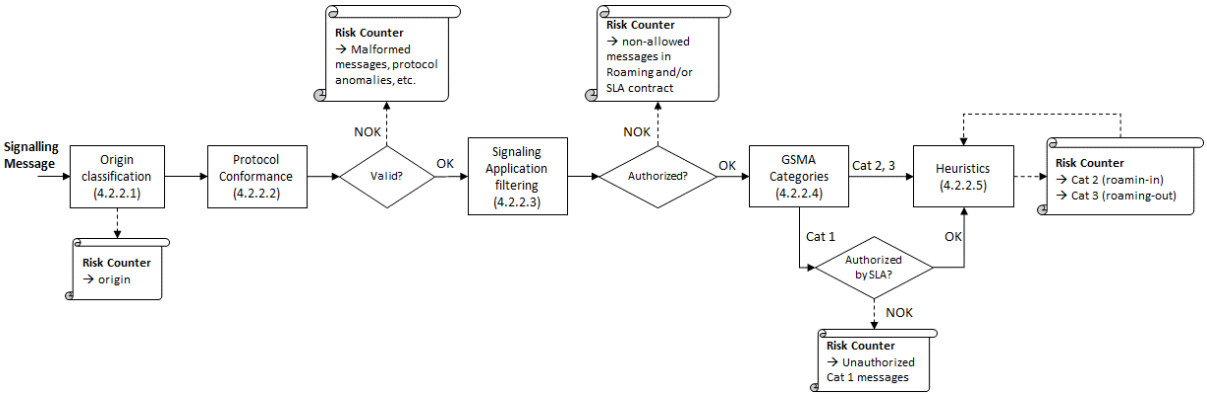

Fig. 4.2.2-1: Individual security message analysis

The following clauses describe each of the steps of the model and the corresponding key attributes in the signaling messages studied in the model that contribute to the quantification of the risk in the interconnection interfaces.

More attributes and filters can be easily added to the model, always looking at the improvement in accuracy or performance versus the cost of increasing the complexity. The design of the overall schema should remain the same.

4.2.2.1 Origin-based classification

The origin of the message in the interconnection link impacts the risk index as per different types of trust relationships with roaming partners and/or roaming intermediaries (e.g., IPX providers, Roaming Hubs). I propose a categorization of four types of origins that are relevant for the security analysis:

- Type 1: Fully Trusted Operators (*FTO)*. MNOs with bi-lateral direct connection.
- Type 2: High-Medium Trusted Operators (*HMTO*). Roaming intermediaries with a formal agreement, and MNOs indirectly connected with the home operator via those "trusted" intermediaries with explicit roaming agreements (SLA).
- Type 3: Low-Medium trusted operators (*LMTO*). MNOs indirectly connected via roaming intermediaries, in principle trusted for the home operator, but *without* an explicit roaming agreement with the home operator, i.e., there is no SLA between the interconnected MNOs.
- Type 4: Non-trusted operators (*NTO*). Roaming intermediaries and MNOs indirectly connected with the home operator *without* roaming agreements in any case.

A mobile operator (PLMN) is identified by MNC (Mobile Network Code) and MCC (Mobile Country Code) according to ITU-T Recommendation E.212 [64]. Both identifiers are 3-digits long string of numbers. GSMA PRD IR.88 ("EPS Roaming Guidelines") [33] and [2] recommend implementing access control mechanisms such as access lists with the allowed roaming partner networks. The access lists are mathematically represented as follows:

$$FTO = \{(MNC_i, MCC_j), \dots, (MNC_k, MCC_l)\}$$

$$HMTO = \{(MNC_m, MCC_n), \dots, (MNC_o, MCC_p)\}$$

Note: FTO and HMTO access lists are generally declared by the operators in the GSMA RAEX IR.21 database [65] and preconfigured in the operator's interconnection gateways (DEA, SEPP).

$$LMTO = \{(MNC_r, MCC_s), \dots, (MNC_t, MCC_v)\}$$

Note: The operator may not know this LMTO list upfront, i.e., the list of MNOs reachable through their "trusted" roaming intermediary (e.g., IPX provider), but without an explicit roaming agreement (SLA). In this case, it is required to make a filter of the message at IP

network level to ensure it comes from their known intermediary, and then verify that the MNC and MCC values are not included in HMTO.

$NTO = \Omega \setminus \{FTO, HMTO, LMTO\}$

Ω = {any (MNC, MCC) codes}

The roaming partner's identification should be consistent in the network and signaling layers and across all fields that convey the identifiers in the message.

For example, in 4G, AVP 296 (Origin-Realm), AVP 264 (Origin-Host), and AVP 1407 (Visited-PLMN-Id) in diameter signaling convey MNC/MCC information. AVP 296 and AVP 264 are mandatory attributes in every message, whereas AVP 1407 is to be used in ULR (Update Location Request) and AIR (Authentication Information Request) messages. Thus, given a message x_i characterized by a series of attributes relevant to security analytics: $x_i = \left(a_i^{(1)}, \ldots, a_i^{(d)}\right)$, let's assume that the first three attributes correspond to the origin PLMN identifiers, i.e.:

$a_i^{(1)}$: (MNC, MCC) $data\ included\ in\ AVP\ 296$

$a_i^{(2)}$: (MNC, MCC) $data\ included\ in\ AVP\ 264$

$a_i^{(3)}$: (MNC, MCC) $data\ included\ in\ AVP\ 1407$

The consistency check related to the origin of the message is: $a_i^{(1)} = a_i^{(2)} \left(= a_i^{(3)}\right)$.

If $a_i^{(1)} = a_i^{(2)} \neq a_i^{(3)}$, it means that the message arriving at the home network has been filtered in the middle by some intermediary, i.e., the visited PLMN does not correspond to the origin of the diameter message.

In 5G, the MNO is identified by the FQDN of the SEPP, which should carry the 5G Core network domain as a suffix (in the trailing part), i.e., '5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org' [66]. The X.509 v3 certificate used for peer authentication includes this identifier, also used in the N32-c handshake service for security capability negotiation between SEPPs ('/n32c-handshake/v1/exchange-capability').

Whereas in 4G the consistency check is done by comparing data PLMN Ids values in certain AVPs of the message, in 5G, the consistency check is done by comparing the PLMN Ids

received in N32-c during the security capability negotiation (SecNegotiateReqData content) versus the information in the X.509 v3 certificate used for peer authentication.

If the consistency check fails, the risk associated with the message is automatically medium-high. Let's note $R(x_i)$: Risk per message x_i.

$\forall\, x_i \; and \; \forall j, such \; that \; a_i^{(j)} \; contains \; (MNC, MCC)$

$If \; a_i^{(j)} \in \{FTO\} \rightarrow R(x_i) + \emptyset$, i.e., the risk is not incremented since the PLMN is trusted.

$If \; a_i^{(j)} \in \{HMTO\} \rightarrow R(x_i) + \delta$, i.e., a small increment of risk due to interconnection through a roaming intermediary.

$If \; a_i^{(j)} \in \{LMTO\} \rightarrow R(x_i) + \delta'$, i.e., significant increment of risk due to lack of SLA.

$If \; a_i^{(j)} \in \{NTO\} \rightarrow R(x_i) + \delta''$, i.e., it is a high-risk message that should be rejected.

The outcome of the filter is a classification of the message based on the trust in the Origin (O) of the message.

O: $\{FTO, HMTO, LMTO, NTO\}$

4.2.2.2 Protocol conformance

Before further classification of the message, the model introduces a low-layer filtering or sanity check of the message based on expert knowledge, which is potentially complemented by AI/ML techniques.

The techniques to detect anomalies, e.g., syntax failures, non-compliance with standards, missing attributes, invalid inputs, etc., in the messages used in the standardized signaling protocols are out of the scope of this dissertation. Those techniques may be deterministic (based on "if-then" rules) and/or AI/ML-based (e.g., unsupervised clusters). The deterministic analysis would require massive work of compiling all possible use cases out of the multiple IETF RFCs, 3GPP specifications, GSMA official documents, etc. On the other side, there are no available autoencoders for signaling data as defined by 3GPP, whose specifications are implemented in ASN.1. Alternatively, a tremendous amount of signaling data would be required to be capable of replicating it with a certain level of accuracy and reliability. Privacy restrictions in the

acquisition of that data, and the lack of 5G roaming implementations at the time this dissertation is written, make this work a very difficult task to accomplish at present.

The filter (e.g., anomaly detector) shall provide a categorization of messages depending on their protocol conformance level. The number and type of categories can be determined by implementers, for example:

- type 0: no incompliances were found.
- type 1: messages that cannot be decoded.
- type 2: messages with incorrect attributes (e.g., AVPs in diameter).
- type 3: repeated attributes according to standard.
- type 4: missing attributes according to standard.
- ….
- type Q: to be defined.

The output of the filter can be represented as follows:

$$P = \begin{pmatrix} p_{1,1} & \cdots & p_{1,Q} \\ \vdots & \ddots & \vdots \\ p_{N,1} & \cdots & p_{N,Q} \end{pmatrix}$$

$p_{i,j} = \delta\ (x_i\ is\ type\ j)\ \ Kronecker\ delta$

$$\delta\ (x_i\ is\ type\ j) = \begin{cases} 0\ if\ x_i\ is\ not\ type\ j \\ 1\ if\ x_i\ is\ type\ j \end{cases}$$

One row of P represents the type of malformations found in the message x_i. For example, the vector: $(p_{i,1} \ldots p_{i,Q}) = (0 \ldots 0\ 1\ 1\ 0\ 0)$ indicates that message x_i includes protocol non-conformances of types 3 and 4.

Every type of non-conformance might have an associated risk level that contributes to the computation of the overall risk index per message. Only certain types of non-protocol conformance messages will deserve further security analysis, which is subject to the implementation of the methodology. For the rest of the non-protocol conformance messages, the analysis can stop in this filtering layer, and the associated risk will be high.

4.2.2.3 Signaling application filtering

Not all mobile network core signaling applications/interfaces are acceptable and standardized for use in roaming context. However, certain implementations can include them in the interconnection for various reasons, for example, two roaming partners may have an agreement to provide location services that require exposing certain application Ids (in case of diameter/4G) or APIs (in case of HTTP2/5G), in principle designed to be internal to the Mobile Core network. Some of those applications/interfaces are more critical than others due to the inherent risks of the conveyed messages and the level of exposition of sensitive data (e.g., privacy, location).

In 4G, the specification 3GPP TS 29.230 [67] lists the Application IDs assigned by IANA to all 3GPP diameter applications. The specification 3GPP TS 23.401 [30] defines the 4G roaming architecture and corresponding interfaces. Similarly, in 5G, the specification 3GPP TS 23.501 [48] defines the 5G roaming architecture and corresponding interfaces/APIs and services that will traverse the N32 signaling interface in PLMN interconnection.

From a security viewpoint in interconnection, I propose the following classification:

1) Allow list: Interfaces used in Roaming as per standard specifications (e.g., S6 a/d in 4G, N8 in 5G).
2) Delay list: Interfaces in Allow list or Block list depending on whether the interface is used/agreed between roaming partners, i.e., they are subject to a specific contract and SLA (e.g., S13 in 4G, N17 in 5G).
3) Block list: Rest of interfaces.

The notation used for modeling the filter is as follows:

Be $a_i^{(j)}$ the attribute j of the message x_i that identifies the used application/interface.

Be I_i the interface i allowed in roaming, $i \in \{1, \dots, m, \dots, n\}$, being n the number of all possible interconnection interfaces in a particular schema, 4G or 5G.

$I_i, i \in \{1 \dots m\}$ represents the interface i contained in the Allow list.

$I_l, l \in \{m+1 \dots n\}$ represents the interface l contained in the Delay list.

$AL = \{I_1, \dots, I_m\}$ is the Allow list.

$DL = \{I_{m+1}, \dots, I_n\}$ is the Delay list.

$BL = \Omega \setminus \{AL, DL\}$ is the Block list.

Be $Op_i = (MNC_i, MCC_i)$ a unique identifier of a MNO, $C_{i,j} = \{I_l \in DL\}$ is a set of allowed non-standardized roaming interfaces included in a contract between Op_i and Op_j.

The following classification rules based on interfaces are proposed as a practical example:

$If\ a_i^{(j)} \in AL \rightarrow$ no risk, Allow list

$If\ a_i^{(j)} \in C_{i,j} \rightarrow$ low risk, Delay list

$If\ a_i^{(j)} \in DL \setminus C_{i,j} \rightarrow$ medium risk, Delay list

$If\ a_i^{(j)} \in BL \rightarrow$ high risk, Block list

4.2.2.4 GSMA message categorization

GSMA in FS.21 (Interconnect Signaling Security Recommendations) [34] defines three categories of messages:

1) Category 1 (Cat 1): Interface unauthorized messages at the interconnection level. They should only be received within the same network unless there is an explicit bilateral agreement between two operators.
2) Category 2 (Cat 2): Messages that should only be received from inbound roamers' home networks. These messages are not intended to target the operator's home subscribers.
3) Category 3 (Cat 3): messages authorized to be sent on interconnection between operators related to outbound roamers.

The operator may re-classify the messages based on bilateral agreements. For example, a particular Cat 2 message can be re-classified to Cat 1 and become an unauthorized message for a particular PLMN. And vice versa, one original Cat 1 message might be allowed if it is re-classified into Cat 2 or Cat 3 based on the context. The final categorization will depend upon several factors collected in SLA between operators, identified by $C_{i,j}$, i.e., it can ultimately vary based on the roaming peer identity, thus on the previously described origin-based classification.

In 4G (Diameter), the attribute of the message used to determine the categorization of the message is the Command Code included in the Diameter message header, which is used to

determine the action that is to be taken for a particular message. The Command Code (CC) values have been allocated by IANA and collected in [67]. Note that each command Request/Answer pair is identified with a Command Code, and the sub-type (request or answer) is differentiated by the 'R' bit in the Command Flags field of the Diameter header. Tab. 4.2.2.4-1 presents a sample of the standardized Diameter Command Codes (not a complete list):

Tab. 4.2.2.4-1: Sample of Diameter Command Codes

CC	'R'	Command name	Abbr.
300	set	User-Authorization-Request	UAR
300	clear	User-Authorization-Answer	UUA
301	set	Server-Assignment-Request	SAR
301	clear	Server-Assignment-Answer	SAA
303	set	Multimedia-Auth-Request	MAR
303	clear	Multimedia-Auth-Answer	MAA
304	set	Registration-Termination-Request	RTR
304	clear	Registration-Termination-Answer	RTA
305	set	Push-Profile-Request	PPR
305	clear	Push-Profile-Answer	PPA
….		…..	…..

Be $a_i^{(j)}$ the attribute j of the message x_i that identifies the Command Code $\langle CC \rangle$ value in the signaling message, $a_i^{(j)}$ can take any value in $\mathbb{X}^{(j)}$ (complete set of possible command code values, flagged with 'R' bit in Diameter header):

$$a_i^{(j)} = (\langle CC \rangle, 'R')$$

e.g., $a_i^{(j)} = (RTR\ (304), Request{:}\ Set)$

In 5G (HTTP/2), the attribute of the message used to determine the categorization of the message is the combination of the path (URI), Operation type (HTTP method), and Operation

Id (action triggered by the message) that can be found within the following N32 messages: N32fReformattedReqMsg (it contains the JOSE protected request message from the sending NF and may contain modifications to be applied to the message) and N32ReformattedRepMesg (it contains the JOSE protected response message from the sending NF and may contain modifications to be applied to the message).

> Note: Multiple stage 3 specifications in 3GPP describe every API in the 5G system. The following repository is publicly available: https://forge.3gpp.org/rep/all/5G_APIs [68].

For a 5G HTTP/2 signaling message x_i, $a_i^{(j)}$ is built as:

$$a_i^{(j)} = (path, Operation\ type, OperationId).$$

e.g., $a_i^{(j)} = (/\{ueId\}/registrations/amf-3gpp-access, PUT, 3GppRegistration)$.

In general, the assignment of the category can be implemented by a simple lookup table supported for example by [32] in 4G, and [51] in 5G, which takes as an input $a_i^{(j)}$ and delivers the corresponding category (Cat 1, Cat 2, Cat 3) as an output value. In special cases, for example, specific IMSIs/SUPIs or sets of IMSIs/SUPIs belonging to personalities or critical slices, or specific SLAs with selected roaming peers, specific lookup tables with the corresponding reclassification of messages should be created ad-hoc.

A Cat 1 message obviously increases the risk of the link if it appears in interconnection. It can be allowed based on specific SLA and, consequently, part of a specific allowed list for example in 5G of interfaces/URIs/HTTP method/operations in roaming that needs to be verified before any other processing. If a Cat 1 message is not authorized, i.e., it is not included in the allowed list of messages among two operators, it should be blocked and tagged as a high-risk message.

Fig. 4.2.2.4-1 represents an example of a Cat 1 message over N35 in 5G roaming, and therefore, it implies a high risk if it appears in interconnection, since the N35 interface between UDM and UDR is, by default, an internal interface in the 5G Core Network. The Cat 1 message of the example is an invocation of an API in the UDR through the following path (URI): "/subscription-data/{ueId}/authentication-data/authentication-subscription".

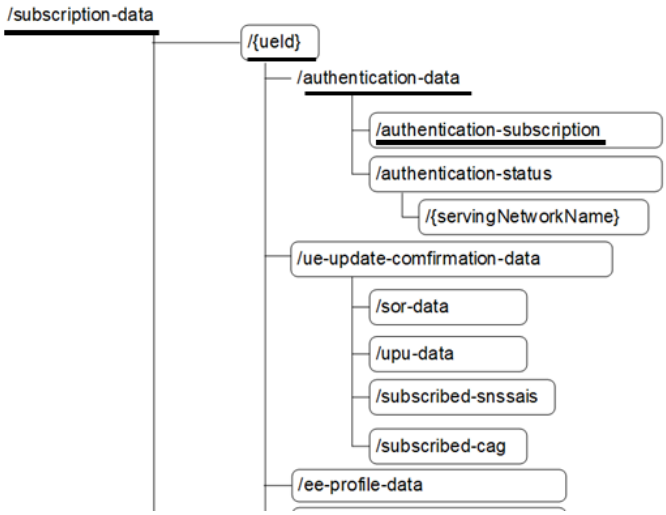

Fig. 4.2.2.4-1: Cat 1 message (N35): authentication subscription data

The message consists of:

- Operation type: Get
- Operation Id: "QueryAuthSubsData". This operation in this message retrieves a UE's authentication subscription data, i.e. it leaks sensitive data such as encrypted Ki, protectionParamterId, SQN, etc…

4.2.2.5 Heuristics

Further security analysis of signaling messages at the application layer is proposed based on different heuristic types of mechanisms, such as:

- Appearance of predetermined sensitive Information Elements in the messages (e.g., IMSI, location, etc.), relevant in the overall risk estimation as they can be misused/abused to perpetrate different kinds of attacks (e.g., tracking, interception, fraud, etc.).
- Detection of well-known inconsistencies within the signaling message at different layers.
- Analysis of error messages in 5G.

Other mechanisms are also possible. Note that these mechanisms are not intended to detect with precision a particular attack or fraud in interconnection, but rather to contribute to the computation of the trust index, corresponding to logical interfaces with a particular roaming partner, by estimating the risk of the exchanged messages.

4.2.2.5.1 Sensitive Information Elements

In the signaling message, several Information Elements (IEs) are considered sensitive from a security viewpoint since they convey critical information that, if compromised or abused, may

be used to perpetrate different types of attacks against the privacy of roaming users such as location tracking, frauds, denial of service attacks, etc.

Below is a non-exhaustive list of sensitive AVPs in the 4G/Diameter schema that can appear in several signaling messages:

- User-Name (AVP code= 1): Contains normally the IMSI of the user.
- User-ID (AVP code= 1444): Contains the leading digits of an IMSI, normally an IMSI range that identifies a set of users.
- MSISDN (AVP code= 701): MSISDN is a public identifier that can be easily obtained. In certain cases, the Command Code of the signaling message allows the use of this information as an input parameter (e.g., Send_Routing_Info_for_SM_Request, CC = 8388647) with the aim of getting more information about the user (e.g., IMSI, location, etc.). In general, all messages that populate this AVP have an inherent security risk.
- Subscription-Data (AVP code= 1400): Contains the information related to the user profile, with multiple nested critical AVPs (e.g., location information).
- IDR-Flags (AVP code= 1490): In IDR (Insert-Subscriber-Data-Request) messages, it contains a bit mask that indicates a variety of needs to the MME and HSS nodes (3GPP TS 29.272 [69]) related, for example, to Location, Local Time Zone, etc.
- DSR-Flags (AVP code= 1421): In DSR (Delete-Subscriber-Data-Request) messages, it contains a bit mask that indicates a variety of needs to the MME and HSS nodes related basically to the removal of some data of the HSS user profile stored in the MME.
- NOR-Flags (AVP code= 1443): In NOR (Notify-Request) messages, it contains a bit mask related to availability, memory usage, and messaging.
- Cost-Information (AVP code= 423): In CCA (Credit-Control-Answer) message, it contains the cost information of a service.
- Charging-Rule-Install (AVP code= 1001): in RAR (Re-Auth-Request) and CCA (Credit-Control-Answer) messages, it is used to activate, install, or modify Policy and Charging Control (PCC) rules as instructed from the PCRF to the PCEF. Please note that those messages are to be conveyed in S9 interface, which can be optionally enabled between operators based on specific SLA, i.e., typically in the Delay list mentioned above.
- Granted-Service-Unit (AVP code= 431): In CCA (Credit-Control-Answer) message, it contains the volume and/or time threshold for usage monitoring control purposes.

Each implementation of the proposed mechanism may include its own list of sensitive AVPs, and they would be considered as any other attribute $a_i^{(j)}$ of the message in the model. Reference [32] provides a Diameter AVP risk estimation that can be used as a baseline. That estimation is based on heuristics of well-known and/or analyzed-by-the-industry possible vulnerabilities that can represent a risk per message.

A more accurate and complex implementation variant may also consider weighing the risk per message with different criteria depending on the concrete information contained in the AVP, e.g., privacy, charging, etc.

In 5G/HTTP/2 schema, clause 6.1.5.3.5 of [59] classifies the IEs (IeType enumeration) used in the HTTP/2 messages defined by URI and HTTP method:

- UEID (*UEID*): IE of type user equipment (UE) identity (e.g., SUPI).
- LOCATION (*LOCATION*): IE carrying location information.
- KEY_MATERIAL (*KEY*): IE carrying keying material.
- AUTHENTICATION_MATERIAL (*AUTH*): IE carrying authentication material like authentication vectors and Extensible Authentication Protocol (EAP) payload.
- AUTHORIZATION_TOKEN (*AUTHZ*): IE carrying authorization token.
- OTHER (*OTHER*): IE carrying other data requiring encryption (still considered sensitive)
- NONSENSITIVE (*NONSENSITIVE*): IE carrying information that is not sensitive (although by default not modifiable unless explicit agreement)

The security focus is put on UEID, LOCATION, KEY_MATERIAL, AUTHENTICATION_MATERIAL and AUTHORIZATION_TOKEN. Out of approximately five thousand IEs subject to be exchanged in roaming, approximately 15% can be matched to one of the "security focus" categories. Based on the 3GPP technical specifications per each Interface/API/Service, annex A of [51] provides a mapping of IEs to IeType, which can be used as a baseline for the implementations of the mechanism. Obviously, it will finally depend on the implementations about how to weigh the risk per IeType. The appearance of such attributes in the messages increases the risk of the message by a factor δ that needs to be determined.

Applying the proposed notation, the following example can be used in 5G context:

Be the signaling message x_i a vector of security attributes s.t. $x_i = \left(a_i^{(1)}, \dots, a_i^{(d)}\right)$.

Be IE the set of 3GPP predefined IeType enumeration to specify accordingly the protection policy:

$$IE = \begin{Bmatrix} UEID, LOCATION, KEY, AUTH, AUTHZ, OTHER, \\ NONSENSITIVE \end{Bmatrix}$$

$$IE_{Sec} \subset IE, IE_{Sec} = \{UEID, LOCATION, KEY, AUTH, AUTHZ\}$$

Be $IE_{Sec_{UEID}}$ a subset of the security attributes of the message categorized as $UEID$:

$IE_{Sec_{UEID}} = \{a^{(j)}\}, j \in \{1..u\}$, i.e. assuming there are u IEs categorized as $UEID$

Be $IE_{Sec_{LOCATION}}$ a subset of the security attributes of the message categorized as $LOCATION$:

$IE_{Sec_{LOCATION}} = \{a^{(j)}\}, j \in \{1..l\}$, i.e. assuming there are l IEs categorized as $LOCATION$

Be $IE_{Sec_{KEY}}$ a subset of the security attributes of the message categorized as KEY :

$IE_{Sec_{KEY}} = \{a^{(j)}\}, j \in \{1..k\}$, i.e. assuming there are k IEs categorized as KEY

Be $IE_{Sec_{AUTH}}$ a subset of the security attributes of the message categorized as $AUTH$:

$IE_{Sec_{AUTH}} = \{a^{(j)}\}, j \in \{1..c\}$, i.e. assuming there are c IEs categorized as $AUTH$

Be $IE_{Sec_{AUTHZ}}$ a subset of the security attributes of the message categorized as $AUTHZ$:

$IE_{Sec_{AUTHZ}} = \{a^{(j)}\}, j \in \{1..z\}$, i.e. assuming there are z IEs categorized as $AUTHZ$

$If\ \exists\ a_i^{(j)} \in x_i\ s.t\ a_i^{(j)} \in\ IE_{Sec_{UEID}}\ or\ a_i^{(j)} \in\ IE_{Sec_{LOCATION}}\ or\ a_i^{(j)} \in IE_{Sec_{KEY}}\ or\ a_i^{(j)} \in\ IE_{Sec_{AUTH}}\ or\ a_i^{(j)} \in IE_{Sec_{AUTHZ}}$ the risk associated with the message $R(x_i)$ is incremented by a factor δ.

Be m the count of the vector components (i.e., message attributes) belonging to any of the above subsets of security attributes, the overall computation of the risk associated with the message $R(x_i)$ and derived from the sensitive IEs, will be a function of $m, R(x_i) = f(m)$.

Certain implementation variants could decide to apply a different risk factor δ per category (UEID, KEY, etc.).

Statistics on the appearance rate of the IEs in the exchanged messages would also be highly recommended for the overall estimation of the risk in the signaling links, but they would require an offline analysis, which is out of the scope of this mechanism.

4.2.2.5.2 Detection of inconsistencies

Further analysis of the signaling message at different levels, i.e., network layer vs. application layer, supports the potential detection of inconsistencies in the conveyed information that appears in different places of the message.

Cat 2 messages are especially prone to inconsistencies between information related to the home network of UEs in lower layers and the information embedded in the signaling application messages in specific IEs. As described earlier, the messages under this category are not intended to target home subscribers, but in principle only inbound roaming subscribers. The key filtering parameter in this message category is the subscriber identifier (i.e., SUPI, SUCI, IMSI, MSISDN, etc.), that can be compared against its source (Home PLMN).

Some examples of detection (filtering) rules against well-known inconsistencies, studied by telecom industry groups like GSMA, signaling firewall vendors, etc., are the following:

- [4G, 5G] Cross-checking of MNO information in the IMSI against the MNO information in other parts of the message.
- [4G] Cross-checking of the realm part of OriginHost AVP with the AVP OriginRealm.
- [4G] In Cat 2 messages, the cross-checking of value inside the Visited-PLMN-Id AVP (if present) with the MCC and MNC of the home operator of the roaming-in user inside the OriginRealm AVP.
- [5G] In N8 (UDM → AMF) interface, "Namf_MT" API, path "/ue-contexts/{ueContextId}", we can compare the MCC and MNC of the SUPI included in {ueContextId} of the operation "Provide Domain Selection Info" against the source NF address of the message to ensure that only the Home PLMN of the subscriber is asking for that information.
- [5G] Other cross-checks, such as parameters in the exchanged certificates vs. relevant IEs in the message within N32-f (e.g., MCC, MNC).

Next, I provide a generic cross-checking rule of certain parameter(s) (e.g., MCC-MNC) across different places in the message using the same notation as in the previous section.

x_i is represented by a series of preselected attributes, s.t. $x_i = \left(a_i^{(1)}, \dots, a_i^{(d)}\right)$.

Be $a_i^{(j)}$ an attribute containing the IMSI, which is a string of concatenation of digits (up to 15): $MCC\ (3\ digits)||MNC\ (2-3\ digits^*)||MSIN(up\ to\ 10\ digits)$.

(*) The length of the MNC, two or three digits, depends on the value of the MCC.

Let's introduce a simple notation for substrings. The substring of a starting at position i (inclusive) and ending at position j (exclusive) is denoted by $a[i,j)$. In our example, $a_i^{(j)}[0,3): MCC;\ a_i^{(j)}[3,5): MNC\ (if\ MNC\ consists\ of\ 3\ digits)$, i.e., MNC/MCC is the IMSI prefix.

Other attributes of the message, such as Origin-Realm AVP in Diameter or Originating Host Information Element in HTTP/2, used to identify the node that originates the message, include as well the MNC/MCC information. Thus, the cross-checking consists simply of, case by case, extracting the MNC/MCC substrings and comparing them with $a_i^{(j)}[0,3): MCC;\ a_i^{(j)}[3,5): MNC$.

If the analysis of the message matches one of those rules, the risk will be increased by a factor/delta that can be predetermined per inconsistency, type of inconsistency (if a classification of inconsistencies is implemented), or even more generally by a common factor (to be determined) to any kind of inconsistency.

Signaling firewalls can detect and block inconsistencies. The proposed mechanism does not preclude any implementation option, provided that the impact on the risk is accordingly computed due to those findings.

4.2.2.5.3 Analysis of Error Messages

In 5G Core, SEPP responds to an error situation with a proper response code/message. The analysis of such error messages is useful information in security-related analytics and, therefore, relevant when measuring the associated risk.

N32 error messages are standardized in clauses 6.1.6 and 6.2.6 of [59]. Three types of errors are identified based on the layer under analysis, i.e.:

- General (HTTP/2 connection error and stream errors as specified in RFC 9113 [70])
- HTTP/2 protocol errors (HTTP status codes applicable in SBI interfaces). When an error occurs that prevents the NF/NF service acting as an HTTP server from successfully

fulfilling the HTTP request, the NF/NF service shall map an application error to the most similar 4xx/5xx HTTP status code as defined in clause 5.2.7.2 of 3GPP TS 29.500 [71] (HTTP status codes applicable in SBI interfaces). Please refer to Table 5.2.7.2-1 of that specification: Protocol and application errors common to several 5GC SBI API specifications (HTTP server).

- Application errors:
    - N32-c: Errors related to the handshake API messages.
    - N32-f: The types of error while processing N32-f messages.

If the received message x_i corresponds to one of these Error messages, the risk will be increased by a factor/delta that can be predetermined per type of error.

4.2.3 Online sequences security analysis on signaling data streams

For the characterization of the Security Analytics model, an important factor to be considered is that an operator is interconnected to multiple operators directly, as well as via IPX network, through different types of intermediaries, so-called IPX providers, to provide roaming services. Thus, the data, and particularly the signaling data, to be analyzed comes from multiple sources, and it flows at high speed in a dynamic and time-changing environment that is also subject to seasonality impacts. For example, roaming traffic in touristic destinations duplicates its volume during summertime. In this environment the security analysis should perform continuous processing of the incoming data to support the continuous online risk evaluation.

The signaling data is characterized as data streams in each of the interconnection links of the MNO network. Therefore, the proposed Security Analytics model uses data stream models, and accordingly, it needs to be implemented as a Data Stream Management System. Working on data stream models does not preclude the analysis of data stored in conventional storage platforms and treated as any other kind of static data. Working with Data Stream Management Systems implies the use of techniques for storing summaries or synopses of information, which implies dealing with a trade-off between the size of those summaries and the capacity to provide precise answers that the proposed model needs to cope with.

In this context, I propose the use of data mining techniques applied to data streams in the processing of incoming data and sequence analysis. More specifically, I have identified three main tasks to be part of the security analysis over the data streams:

1) Identification of specific (well-known) critical sequences (patterns) associated with highly sensitive data from a security/privacy viewpoint.

2) Failures and anomaly detection by the identification of rare items/sequences and changes in normal distributions of messages.

3) Statistical analysis of data, which is encapsulated in AVPs in Diameter and IEs in HTTP/2 messages, with particular security sensitivity (e.g., privacy, location) across the signaling messages.

To accomplish these tasks, I propose a methodology that consists of three key processes: streaming data preprocessing, data mining, and statistical analysis.

4.2.3.1 Streaming data preprocessing

With new data constantly arriving even as old data is being processed, the amount of computation time per data element must be optimal. Since we are typically limited to a certain amount of memory, approximating high-quality answers based on a limited amount of data should be good enough and provide an acceptable level of accuracy. It is not generally feasible to make several passes over the data in the streaming setting, whereas it is crucial that this limited amount of data representation is processed on the stream directly, i.e., in one pass.

I propose two approaches to be adopted for streaming data preprocessing for the context of this dissertation: data reduction and sliding windows. In both cases, the data structures are to be maintained incrementally, however, it is not practical to store all data to execute "a posteriori" queries that refer to past data. This type of query requires techniques for storing summaries or synopsis information about past data. The main problem to solve is to what extent the data streams can be summarized so that accurate estimations can be provided on the underlying signal [72].

For data reduction, the most common techniques include sampling, synopsis and histograms, and wavelets. The following paragraphs explain the main concepts behind these techniques.

Sampling basically consists of selecting a subset of data to be analyzed at periodical intervals, and it is used to compute statistics over the stream with certain expected accuracy. Many different sampling methods have been proposed (e.g., random sampling, distinct sampling [73], universe sampling, etc.), as well as sampling algorithms (e.g., reservoir sampling [74]) intended to obtain approximate answers that support the statistical analysis. Independently of the selected

method, a lot of samples are required for complex and sophisticated analysis, else valuable information can be lost. Sampling is useful to slow down data and works on basic aggregates, but it is not a suitable solution when the target is to monitor complex problems and/or anomalies.

Synopsis (e.g., sketches) and histograms (e.g., V-Optimal, Equi-Width, End-Biased, etc.) are summarization techniques that can be used to approximate the frequency distributions, statistics, or solutions to specific queries in a data stream. Sketches are compact data structures that summarize the data stream by approximating various statistical properties, such as frequency counts, moments, or quantiles of the data distribution. A V-Optimal histogram is a type of histogram optimized for variable-width bins, where the bin widths are adjusted dynamically to efficiently capture the distribution of data points while minimizing error or approximation.

A wavelet is a mathematical function that is used to decompose or analyze signals and data into different frequency components at different scales. Wavelet coefficients are projections of the given signal (set of data values) onto an orthogonal set of basis vector, and the choice of basis vector determines the type of wavelets [75]. Wavelets analysis, i.e. multi-resolution analysis including time and frequency, are popular in streaming applications, since most signals can be represented using a reduced set of coefficients. Some work on how to compute the top wavelet coefficients in the data stream models has been done, among others, by Y. Matias et al. [76], showing how to dynamically maintain the top wavelet coefficients efficiently as the underlying data distribution is updated, or by Gilbert et al. [77] to find the best *B*-term Haar wavelet representation.

The other approach proposed for streaming data preprocessing is sliding windows. The intuition of sliding windows is basically a moving subset of data points that traverses over the entire data stream, capturing localized segments of data at each step. The final computed trust score per link/operator will consider the past analysis, but during the pure online risk evaluation over the data streams, we are only interested in the recent past. The easiest solution is the sliding windows of fixed size. There are several windows models in the literature; for example, reference [75] defines two basic types:

- Sequence-based, i.e., the size of the window is defined in terms of the number of observations.
- Timestamp-based, i.e., the size of the window is defined in terms of duration.

A basic mathematical notation on sliding windows is presented here with the purpose of illustrating a few functions that will be used afterwards in the validation of the mechanism.

Let's denote a data stream as D. A window $\mathcal{W}$ is the set of all transactions in a data stream D between the ith and the jth transaction (j > i).

The size of $\mathcal{W}$ is $|\mathcal{W}| = j - i$.

Whenever a new transaction z is observed and inserted into the window, another element $z - |\mathcal{W}|$ is forgotten.

The count of a sequence Y in a window $\mathcal{W}$, i.e., the number of transactions in $\mathcal{W}$ that contains Y, can be represented as $count_{\mathcal{W}}(Y)$.

The support of a sequence Y can be computed as:

$$Support_{\mathcal{W}}(Y) = \frac{count_{\mathcal{W}}(Y)}{|\mathcal{W}|}$$

Be two sequences S and T, the support of an association rule $S \longrightarrow T$ in a window $\mathcal{W}$ is the proportion of transactions in $\mathcal{W}$ that contains $S \cup T$. The confidence of an association rule $S \longrightarrow T$ is the proportion of transactions in a window $\mathcal{W}$ containing S that also contains T.

Tsang et al. [78] defines an itemset as rare when its support falls below a threshold called minimum frequent support (minFreqSup). With the aim of differentiating between rare and noisy itemsets, a noise filter threshold to eliminate noisy itemsets is also defined, and it is called minimum rare support (minRareSup).

An itemset Y is a rare itemset in a window $\mathcal{W}$ if:

$$minRareSup < Support_{\mathcal{W}}(Y) \leq minFreqSup$$

4.2.3.2 Data mining

Once the streaming data has been pre-processed, the security analysis of the produced summaries is performed with the support of data mining techniques and algorithms.

I propose the use of data mining techniques and algorithms in the security analysis with the following targets:

1) Find known sequences related to security-sensitive use cases (e.g., fetching the IMSI, retrieving the location, etc.) that will impact the risk index. It should be feasible to build a dictionary of security critical, but also valid sequences, which are part of standard procedures and well-known by the industry.

2) Find rare "suspicious" known sequences with proof points that become attack vectors. In the telecommunications industry, programs like GSMA CVD (Coordinated Vulnerability Disclosure) and 3GPP CVD support the identification of those sequences.

3) Find rare non-predetermined sequences, basically anomalies and outliers in the normal distributions of signaling messages, with focus on security and privacy-related features/parameters.

When dealing with massive datasets or streaming data, we need sublinear algorithms in time and space (memory usage) capable of processing such vast information, i.e., algorithms whose running time or memory usage grows slower than linearly with the size of the input. In other words, as the input size increases, the resource requirements of sublinear algorithms increase at a rate less than or equal to O(n), where n is the size of the input.

Specifically in the context of data streams, sublinear algorithms are used to process data sequentially in a single pass, using a sublinear space, for example, approximate counting, frequency estimation, sketching, etc. The ultimate objective is to craft sublinear space data structures that optimize the resources required to process information provided as data streams in interconnection signaling interfaces and, consequently, be capable of responding to different types of queries dynamically and efficiently with an acceptable grade of accuracy.

It is also important to choose algorithms that can handle the dynamic nature of data streams while adapting to changes over time. Due to the continuous change in the streaming data, the problem of concept drift inherently appears (the shift in the underlying distribution of examples arriving from a data stream is known as concept drift). In contrast with typical batch data, it is important to note that the data elements in the stream can only be accessed in the sequence in which they arrived from the stream.

Sequential pattern mining was first introduced by Agrawal and Srikant in 1995 [79]: "Given a set of sequences, where each sequence consists of a list of elements and each element consists of a set of items, and given a user-specified min_support threshold, sequential pattern mining is to find all frequent subsequences, i.e., the subsequences whose occurrence frequency in the

set of sequences is no less than min_support". In the literature, multiple data mining algorithms can be found to mine sequence patterns from static databases, such as GSP (Generalized Sequential Patterns) [80] or PrefixSpan (Prefix Projected Sequential pattern Mining) [81]. They respectively correspond to the two main approaches to the problem of sequence pattern mining: Apriori-based and Pattern-growth methods. In Apriori-based sequence pattern mining algorithms the main idea is to generate candidate sequential patterns from frequent sequences of increasing lengths and then prune the candidate set using the Apriori property, which states that if a sequence is infrequent, all of its supersets must also be infrequent. In addition to GSP, other algorithms follow the same idea, such as SPADE (Sequential PAttern Discovery using Equivalence classes) [82], SPAM (Sequential PAttern Mining), etc. In contrast, Pattern-growth methods grow patterns recursively from smaller existing ones, typically using compact data structures such as prefix trees or projected databases. Another popular Pattern-growth algorithm is FreeSpan (FREquEnt pattern-projected Sequential PAtterN mining) [83]. These sequential pattern mining techniques and algorithms have been originally designed for static databases. Nevertheless, they can be adapted to handle data streams through various mechanisms, such as sliding windows, aiming to limit the amount of data considered at any given time. Sequential patterns are then mined within these windows, allowing the algorithm to process only a portion of the stream at once. This should be an acceptable approach in the context of the dissertation.

Generally, the volume of data in real-world data streams like mobile network signaling traffic is usually too huge to be efficiently mined, so approximate answers for mining tasks are acceptable. Methods and algorithms for mining sequential patterns on data streams have been proposed by researchers in the last years. Among others, I highlight the following proposals and make a few observations (in chronological order) on their adequacy in our context:

- Manku and Motwani in [84] proposed a set of algorithms for computing approximate frequency counts of elements in a data stream and also addresses the problem of maintaining association rules, which is useful when mining sequences related to each other by standard protocol associated call flows in signaling. However, the algorithms are quite focused on finding frequent elements, whereas our main task is to find rare items that have a risk impact.
- Karp, Papadimitriou, and Shenker in [85] proposed an alternative algorithm to identify from a very long sequence of symbols (or tuples) coming from a large alphabet those symbols whose frequency overcomes a certain threshold. Thus, the same limitation as the previous proposal applies when used for security purposes.

- Metwally, Agrawal, and El Abbad in [86] were more precise than previous authors and proposed a solution to compute frequent and mainly top-k elements in data streams, extending the solution to be able to answer continuous queries about those elements. The ordering of the most frequent elements in data streams already provides useful information in the security analysis of data streams in our telecom context, but only at message level (i.e., element level).
- Raissi, Poncelet and Teisseire in [87] introduced a new approach called SPEED (Sequential Patterns Efficient Extraction in Data streams) to identify sequential patterns in a data stream, demonstrating that traditional approaches for mining sequential patterns were not valid when applied to data streams. SPEED can be useful in the identification of well-known sequential patterns impacting the risk in the interconnection links. The application of this approach in a real scenario would require a careful design of the batch duration values.
- Lee, Jing and Agrawal in [88] described a new algorithm derived from Karp et al. [85], and intended for mining frequent itemsets in a stream. Basically, it is a new one-pass algorithm for streaming which has deterministic bounds on the accuracy.
- Kumar and Rao in [89] proposed a scheme (Frequent Pattern Retrieval algorithm) based on the Frequent Patterns tree approach and a sliding window model to extract significant information, i.e., patterns, from data streams. It provides better outcomes in terms of runtime and memory use than previous works on the theme.
- Krishnamoorthy and Karthikeyan in [90] resolved the frequent pattern mining task for data streams applying association rule mining methodology.

The security analysis I propose in this dissertation does not preclude the use of any particular algorithm intended to mine specific sequential patterns on signaling data streams, and it is not in the scope of this article to make an experimental evaluation of them by measuring times of response, efficiency, or other parameters.

In addition to mining specific sequential patterns on signaling data streams, the mining and detection of significant changes in the normal distribution of messages, for example, changes in the average number of signaling messages, including location information, might indicate potential security issues, anomalies, or outliers, that would impact the risk evaluation. The ADWIN (ADaptive sliding WINdow) [91] is a popular change detector and estimator algorithm using an adaptive size sliding window. The authors of ADWIN developed a time- and memory-efficient version of this algorithm called ADWIN/2. ADWIN/2 basically monitors a sliding

window of data and dynamically adjusts its size based on the characteristics of the incoming data. It aims to detect changes or drifts in the data distribution by monitoring statistics like means and variances in the windowed data. When it detects a significant change, it triggers an alert, indicating that the underlying data distribution has shifted.

As indicated earlier in the dissertation, I have proposed CVSS [58] score calculation to compute the risk evaluation. CVSS requires specifying certain metrics, and for that purpose I have selected frequency counts, rare items, anomalies, and information security sensitivity (more details are provided in subchapter 4.3). To extract that information from the data streams, I propose to look initially at the above-mentioned data mining algorithms. The selection of the algorithms above does not have an experimental basis, but it serves the main purpose of the described mechanism. Future implementers are kindly invited to test those and other similar algorithms, and accordingly select the most suitable for their environments.

4.2.3.3 Statistical analysis

The aim of the statistical analysis in the proposed mechanism is to compute and maintain a set of relevant statistics in an online fashion. I.e., when analyzing the sliding windows, it is important to include not only the detection of rare sequences but also the statistical analysis of sensitive information elements across the set of signaling messages included in the window. Generally, there is always a compromise between the size of the summaries and the accepted accuracy to provide answers to queries that involve past data.

In 2002, Datar et al. [92] addressed the problem of maintaining statistics over data streams with respect to the last N data elements seen so far, and showed that, using a multiplicative overhead of $O\left(\frac{1}{\epsilon}\log N\right)$ in memory and a $1+\epsilon$ factor loss in accuracy in their algorithm, many techniques to work for sliding windows models could be adopted, such as histograms, hash tables, sum, averages, etc. Later Arasu and Manku (2004) [91] presented various algorithms for approximate counts and quantiles, considering both fixed-size and variable-size sliding windows. Many other approaches to the problem have been developed since then due to the fact that very often applications naturally generate data streams as opposed to data sets.

One may be interested in computing different types of statistics over the data stream. Nevertheless, this dissertation considers just what I judge as the most important one in the proposed security analysis, i.e., *frequency counts.*

In order to count the number of occurrences of "risky" messages and/or information elements in a data stream, I have selected the sketch construction and corresponding algorithm Count-Min Sketch, presented by Cormode and Muthukrishnan (2005) [93] for estimating frequencies. Count-Min Sketch works by using a set of hash functions to map elements to different positions in an array. Each hash function provides an index in the array, and the corresponding counters at those positions are incremented when an element is encountered. This allows the Count-Min Sketch to estimate the frequency of elements even if they are rare. We don´t really need to have a precise calculation of the number of risky messages, but in the large amount of data received in interconnection in data streams, some level of error in the estimation can be certainly tolerated. Mathematically, a count-min (CM) sketch is represented by a two-dimensional matrix of w $(width) \times d$ $(depth)$ in size, that I have adapted from the original paper in Fig. 4.2.3.3-1. Given a desired probability level (δ) and an admissible error in our approximation (ϵ), the optimal size of the data structure is the following (please refer to the original paper in [93] for further details in the mathematical justification):

$w = \lceil 2/\epsilon \rceil$ and $d = \lceil \ln(1/\delta) \rceil$

Given as an input a data stream of **n** data items (i.e., signaling messages): $x_1, x_2, \ldots, x_n$, each x_i from a universe $\mathcal{I}$, each row of the CM matrix initialized to zeroes, is associated with a hash function $h(.)$ that maps every data item x in the stream to a column in the matrix in the interval $[1 \ldots w]$:

$$h_1 \ldots h_d : \{1 \ldots n\} \rightarrow \{1 \ldots w\}$$

Each cell is then a counter, and when an update c_t of item x_t arrives at time t, c_t is added to each cell indicated by the corresponding hash function in its row.

$$c_{1,h_1(x_t)}(t) = c_{1,h_1(x_t)}(t-1) + c_t$$

$$c_{2,h_2(x_t)}(t) = c_{2,h_2(x_t)}(t-1) + c_t$$

$$\ldots \qquad \ldots$$

$$c_{d,h_d(x_t)}(t) = c_{d,h_d(x_t)}(t-1) + c_t$$

Please note that in our context c_t is always positive, and for the purpose of frequency counts, it is equal to 1. The notion of time itself does not add relevant information to our security analysis.

Instead, the sequence, i.e., the count of items, does matter. Therefore, we will simplify the notation from here by removing the variable t.

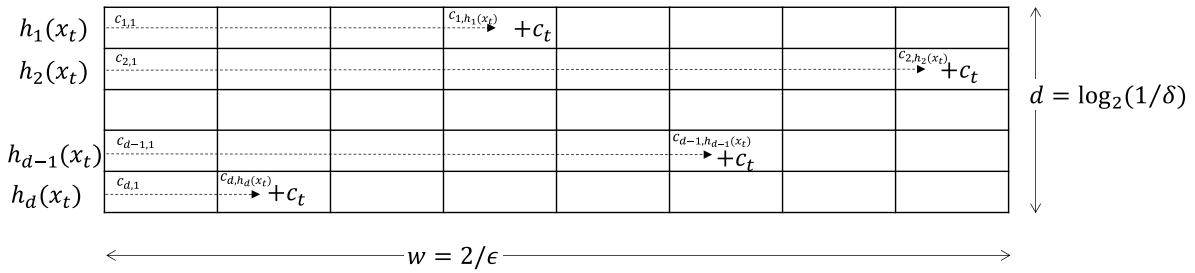

Fig. 4.2.3.3-1: Count-min sketch matrix (adapted from Fig.1 of [93])

f_x: $frecuency\ count, i.e., true\ count\ of\ element\ x$

The answer to a point query provided by the data stream, denoted as $Q(x)$ in count-min algorithm, is computed as an approximation to the real number of occurrences by applying the count-min sketch claim:

Be $\hat{f}_x$: $estimated\ frequency\ count\ of\ element\ x$

$\hat{f}_x = \min\left(c_{1,h_1(x)}, c_{2,h_2(x)}, \dots, c_{d,h_d(x)}\right)$

Or alternative notation could be $\hat{f}_x = \min\left(CM\left[j, h_j(x)\right]\right)$, where $j \in \{1 \dots d\}$

$\hat{f}_x \leq f_x + \epsilon \times n\ with\ probability\ (1-\delta)$

To optimize the **count-min** sketch algorithm we need to make certain choices:

- Choose the length of the stream (**n**) to apply the algorithm.
- Choose the affordable error upper limit, i.e. $\hat{f}_x - f_x \leq \boldsymbol{\epsilon} \times n$
- Choose the probability in a determined range, i.e., $1 - \boldsymbol{\delta}$

Note that the complexity of the sketch will obviously increase with the demanded accuracy.

The statistics of interest in our mechanism are limited to certain messages considered security or privacy sensitive, such as those containing permanent user identifiers (e.g., IMSI), location, authentication vectors, etc. The security classification of the messages can be implemented in multiple ways, for example, based on the IE types carried in the messages as defined in [59]. Each preselected category of the selected classification in the analysis can be considered a new dimension (distinct key) in the statistics of the data stream. In other words, we can consider the stream data under analysis as multi-dimensional. For example:

$\widehat{f_x} \rightarrow Estimated\ frequency\ count\ of\ messages\ carrying\ IMSI\ data$

$\widehat{f_y} \rightarrow Estimated\ frequency\ count\ of\ messages\ carrying\ location\ data$

$\ldots etc.$

Finding heavy-hitters in count-min sketches can be also helpful in the risk evaluation. For example, by defining a specific threshold (T) for a certain category we can set up the following straightforward rule:

$$If\ \min(CM[k, h_k(x)]) \geq T\ , where\ j \in \{1 \ldots d\}, the\ risk\ is\ incremented\ by\ \delta\ (to\ be\ defined)$$

To adapt count-min sketch for a sliding window, we need to ensure that the counts reflect only the elements within the current window. This can be achieved by using a method to decrease the counts of expired elements efficiently. Those methods in the literature are known as time-decay models.

A relevant deployment aspect in relation with the statistics is that our security analysis application in order to evaluate the risk can be distributed across several links/sites in the network. In certain implementations, the applied statistics needs to take this "distribution" factor since it is not always possible to centralize the data in one place up front. That means the model requires the composition of the synopses captured in each link/site.

Papapetrou et al. [94] approached the problem of complex query answering over distributed, high-dimensional data streams in the sliding window models by introducing a new sketching technique termed ECM (Exponential Count-Min) sketch. ECM merges Count-Min sketching with tools for sliding window statistics such as exponential histograms under data stream cash register models. Basically, ECM allows to maintain the monitored frequency counts of the stream items (signaling messages) within the sliding window range. In ECM, a point query is a combination of an item identifier x and the query range defined as number of arrivals (count-based sliding windows). Please consult reference [94] to find all the details of the ECM structure corresponding to the computation of the answer to the queries, aggregation of exponential histograms, etc.

4.3 Risk computation

The risk is continuously being evaluated and accumulated in every step of the security analysis at both message and sequence levels to finally result in a quasi-real-time risk score per interconnection link, which subsequently contributes to building a trust index per interconnected operator used for providing roaming services. The scheme in Fig. 4.3-1 provides a conceptual representation of the dynamic risk evaluation at the different levels proposed in the mechanism.

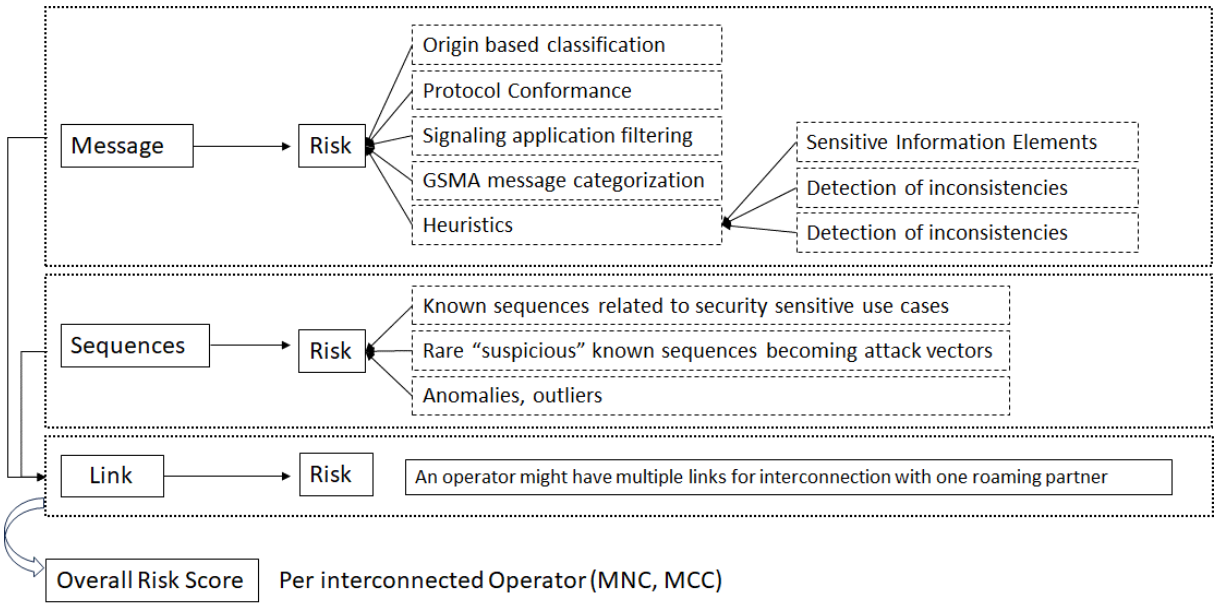

Fig. 4.3-1: Conceptual representation of the dynamic risk evaluation at different levels

The contribution from component of the scheme to the risk at message and sequence levels can be computed in multiple ways. In this dissertation I propose to use the principles of CVSS [58] as a baseline of the risk computation. CVSS is an open framework to assess and communicate the severity of a vulnerability relative to other vulnerabilities. It is de facto a standard methodology in the IT industry, owned and managed by FIRST.Org, that it is widely used in multiple environments. However, there is no formal CVSS-based scoring applied to the telecom domain at the time of writing this dissertation. It is not in the scope of this dissertation to elaborate exhaustively on the formalization of the CVSS framework for the telecoms sector. The intention is rather to guide a possible implementation of the CVSS framework that facilitates a computation of the risk in a dynamic telecom environment such as the signaling interconnection.

CVSS is composed of four metric groups: Base, Threat, Environmental, and Supplemental. Since the system under security analysis is basically an interconnection signaling link, the organization maintaining the system and the consumer of CVSS are the same entity, i.e., the MNO. For that reason and to avoid unnecessary complexities in the adopted framework there is no need to consider the Environmental metric group separately, i.e., considerations around security controls and weights assigned to the different metrics can be taken into account directly in the Base metric group in our proposal. A Supplemental metric group is a set of new optional metrics that describe and measure additional extrinsic attributes of a vulnerability. It does not have an impact on the calculation of the CVSS score, and therefore, for similar reasons provided in the case of the Environmental metric group, our proposal prescinds this metric. Thus, using the nomenclature proposed by FIRST, our methodology is focused on CVSS-BT (Based on Threat metrics).

The *Base metric* group consists of the following metrics and possible values (please refer to the CVSS framework [95] for a detailed description):

- Attack Vector (AV): Network (N)

(Justification in our context: In all vulnerability situations described in the mechanism, the threats are executed remotely)

- Attack Complexity (AC): Low (L), High (H)
- Attack Requirements (AT): None (N), Present (P)
- Privileges Required (PR): None (N), Low (L), High (H)
- User Interaction (UI): None (N)

(Justification in our context: In all vulnerability situations described in the mechanism, the threats can be exploited without interaction from any human user other than the attacker)

- Confidentiality Impact (VC): High (H), Low (L), None (N)
- Integrity Impact (VI): High (H), Low (L), None (N)
- Availability Impact (VA): High (H), Low (L), None (N)

The *Threat metric* measures the current state of exploit techniques. The main threat intelligence knowledge base in the telecom signaling environment is provided by GSMA Coordinated Vulnerability Disclosure (CVD) [96], which has a restricted access to GSMA members. In addition, GSMA members can consult other documents, such as [51], to get a basic

understanding of the potential attacks and recommended mitigations. There are also several specialized agents in the industry, such as signaling firewall vendors, that have built their own threat intelligence databases, although the access is typically subject to commercial agreements. Some of those agents publish regular summary reports describing new vulnerabilities and attack vectors.

The possible values for the Threat metric are Not Defined (X), Attacked (A), Proof-of-Concept (P), and Unreported (U).

The CVSS score can be used to compute risk by combining it with additional contextual factors specific to the environment. In our methodology, the following two factors are proposed (others can be easily added by implementers if needed):

- Data Sensitivity (DS): how sensitive the data exchanged in the signaling messages is. For example: highly sensitive (H) (e.g., privacy subscriber data such as IMSI, location; security information like authentication material), moderately sensitive (M) (e.g., public subscriber identifiers such as MSISDN), low sensitive (L) (e.g., operator public identifiers such as PLMN ID).
- Potential Impacts of the Vulnerability (PIV): In contrast with the impacts evaluated to compute the CVSS base metric, this factor is intended to express the impact of the vulnerability in terms of:
    - regulation (PIV_reg): a regulatory or legal breach that might lead to fines, disciplinary actions, etc.
    - reputation (PIV_rep): damage to the image of the operator.
    - finance (PIV_fin): financial loss.
    - operations (PIV_ope): loss or reduction of the operational service.

  Each of those impact categories can be scored as high (H), moderate (M), or low (L), and weighted accordingly to compute the overall PIV:

$$PIV = PIV_{reg} * w_{reg} + PIV_{rep} * w_{reg} + PIV_{fin} * w_{fin} + PIV_{ope} * w_{ope}$$

  Where $w_{reg}, w_{rep}, w_{fin}, w_{ope}$ are the weights assigned to each impact category.

Consolidating the above-described CVSS metrics and contextual factors, for a vulnerability i, the risk factor can be computed as follows:

$CVSS_i = Base\ Score_i + Threat\ Metric_i$ [95]

$$CF_i = W_{DS_i} * S_{DS_i} + W_{PIV_i} * S_{PIV_i}$$

where CF_i represents the overall contextual factor for the vulnerability i, W_{DS_i} and $W_{PIV_i}$the weights assigned to Data Sensitivity and Potential Impact of the Vulnerability factors, and S_{DS_i} and S_{PIV_i} the given scores to both factors respectively.

$$R_i = CVSS_i * CF_i$$

where R_i is the risk factor associated with the vulnerability i. R_i provides a nuanced understanding of the risk posed by the vulnerability, considering both intrinsic characteristics and context.

The next step in the risk evaluation of the link is to aggregate the individual scores into a single metric that reflects the overall risk posture of the link under evaluation.

In the Tab. 4.3-1 I craft a model of CVSS-BT computation for each individual score considered in the mechanism. Please note that the provided model has been provided as a reference, and it does not prevent an implementer from modifying the evaluation of the metrics, as well as the necessary manual finetuning in the column “Corrected”.

Tab. 4.3-1: MODEL OF CVSS-BT COMPUTATION ADAPTED TO THE PROPOSED DYNAMIC RISK EVALUATION MECHANISM

	Filters	Vulnerabilities	AV	AC	AT	PR	UI	VC	VI	VA	Threat	CVSS	Corrected	Rating
Signaling Message	1. Origin based classification (section 4.2.2.1)	Fully Trusted (FTO)	N	-	-	-	-	-	-	-	-	0	-	None
		High-Medium Trusted (HMTO)	N	L	N	N	N	N	N	N	X	0	3[1]	Low
		Low-Medium Trusted (LMTO)	N	L	N	N	N	L	L	L	X	6.9	-	Medium
		Non Trusted (NTO)	N	L	N	N	N	H	H	H	X	9.3	-	Critical
	2. Protocol conformance[2] (section 4.2.2.2)	type 0	N	-	-	-	-	-	-	-	-	0	-	None
		type x (generic)	N	L	P	N	N	N	H	H	X	8.3	-	High
	3. Signaling application filtering (section 4.2.2.3)	Allow list (AL)	N	-	-	-	-	-	-	-	-	0	-	None
		Delay list (DL)	N	H	P	N	N	N	N	N	X	0	3[3]	Low
		Block list (BL)	N	H	P	N	N	H	H	H	A	9.2	-	Critical
	4. GSMA message categorization (section 4.2.2.4)	Cat 1	N	L	N	N	N	H	H	H	A	9.3	-	Critical
		Cat 2	N	-	-	-	-	-	-	-	-	0	-	None
		Cat 3	N	-	-	-	-	-	-	-	-	0	-	None
	5. Heuristics[4] (section 4.2.2.5)	Sensitive Information Elements	N	L	N	N	N	L	L	L	A	6.9	-	Medium
		Inconsistencies	N	L	N	N	N	L	L	L	U	5.5	-	Medium
		Error messages	N	L	N	N	N	L	L	L	X	6.9	-	Medium
Sequences	6. Known security sensitive sequences (section 4.2.3.2)	Valid sequences	N	-	-	-	-	-	-	-	-	0	3.9[5]	Low
		Rare “suspicious”/attack sequences	N	H	P	N	N	H	H	H	A	9.2	-	Critical

[1] HMTOs are connected via an intermediary to the operator.
[2] An implementation can define several types of non-conformances with distinct levels of severity.
[3] The messages included in Delay list are subject to SLAs between operators, thus the score can be considered low, but not null as in Allow list.
[4] An implementation can define several types of sensitivity, (e.g., privacy, location, etc.), inconsistencies, and error messages, and assign a specific risk weight per each type.
[5] Even if the sequences are valid, they include messages with security and/or privacy relevancy.

	7. Rare non-predetermined sequences (section 4.2.3.2)	Anomalies, outliers	N	L	N	N	N	L	L	L	U	2.7	-	Low
	8. Statistical analysis of messages (section 4.2.3.3)	#critical messages ≥ threshold	N	L	N	N	N	L	L	L	X	6.9	-	Medium

A simple average of individual scores would be a naïve and inaccurate method of aggregation. Therefore, several options might be considered:

- Weighted Average: Each score is multiplied by a weight (w) reflecting its importance. The contextual factor (CF) can be used for that purpose, i.e., $w_i \equiv CF_i$

$$Overall\ Score = \frac{\sum_{i=1}^{n} w_i \times CVSS_i}{\sum_{i=1}^{n} w_i}$$

where n is the number of vulnerabilities under evaluation, which in our model to illustrate the methodology is 19 (# rows of Tab. 4.3-1).

- Maximum CVSS score: The overall risk might be dominated by the most severe vulnerability.

$$Overall\ Score = \max(CVSS_1, CVSS_2, \dots, CVSS_n)$$

- Aggregated Impact calculation: A method that considers the cumulative impact of all vulnerabilities. One approach is to use an exponential scale to give more weight to higher scores.

$$Overall\ Score = \log_{10}\left(\sum_{i=1}^{n} 10^{CVSS_i}\right)$$

New vulnerabilities can be easily and dynamically added to the methodology by maintaining running sums of the weighted scores and the total weights. Thus, when a new vulnerability is added, the sums are updated, and the overall score is recalculated.

$Weighted\ Sum\ (WS) = \sum_{i=1}^{n} w_i \times CVSS_i$, the sum of the products of each CVSS score and its weight.

$Total\ Weight\ (TW) = \sum_{i=1}^{n} w_i$, the sum of all weights

$$Overall\ Score = \frac{WS}{TS}$$

Given a new vulnerability: $CVSS_{new}, w_{new}$, the previous parameters are to be updated, i.e.:

$$WS_{updated} = WS + (CVSS_{new} \times w_{new})$$

$$TW_{updated} = TW + w_{new}$$

$$Overall\ Score_{updated} = \frac{WS_{updated}}{TS_{updated}}$$

The overall risk factor (overall vulnerability score weighted by predetermined contextual factors) is dynamically managed and updated when, in the interconnection link under evaluation, new security sensitive messages arrive, and new security sensitive sequences are mined and found.

Finally, with the aggregation of the risk factors in all links of interconnection with an operator, an overall risk score per operator through which the HPLMN can provide roaming services can be easily computed.

The development of this dynamic risk evaluation mechanism for mobile networks interconnection responds to the need exposed in **Thesis 1** of the dissertation, i.e., provides an efficient mechanism to measure and control the risk level across all technologies. Please note that the model has been detailed at message level for Diameter (4G) and HTTP/2 (5G), but it is of course perfectly applicable to "old" SS7. This Chapter provides the overall risk score, which is the basis for building a trust score per roaming peer and/or roaming intermediary. The trust score is treated in the next chapter and completes the response to the **Thesis 1**.

5 Trust score for Mobile Networks in Roaming

This chapter presents an approach to building a trust score for mobile networks to be used in roaming agreements and, subsequently, in the definition and enforcement of security policies described in chapters 6 and 7, respectively. Determining a trust score per roaming peer (and/or Roaming intermediary), taking as an input the dynamic measurement of the risk in interconnection links, should support the MNO in the task of deciding on the security policies/profiling to enforce in those links.

Subchapter 5.1 (Introduction) discusses the motivation for the creation of a trust score for Mobile Networks at present. Subchapter 5.2 details the fundaments used to assemble a trust score per MNO (and/or Roaming intermediary) connected in roaming. The concept of assembling a trust score in this context has been developed during my research, and protected under a patent application that I have coauthored [13].

Note that under Chapter 8, subchapter 8.3 shows an example procedure of the proposed trust score for mobile networks in roaming, which could be part of future standardization.

5.1 Introduction

There are multiple use cases where the trust indication per NF, or set of NFs, is needed within a single operator network as well as across multiple operator networks, such as Federated Learning, Non-Public Networks (NPN), or VPLMNs (Visited PLMN), where the trust indication is based on the messages exchanged between the HPLMN and VPLMN. Multiple factors may be taken into account by the HPLMN when building the trust score per VPLMN (roaming/interconnection peer): risk per received message (i.e., a message with privacy information (e.g., IMSI, location) or charging info implies a risk); messages and/or sequences of messages being part of an attack (e.g., DoS, interception) or fraud; confidence in analytics data exchanged between operators; logs from signaling firewalls; etc.

The network could certainly benefit from the continuous monitoring of the trust indicator of the VPLMNs by using it to prioritize or deprioritize the PLMN list configuration, modifying accordingly the service level agreements and/or dynamically adopting security measures to cope with the security risk(s), visible for the HPLMN by the lowering of the trust indicator in a particular VPLMN. For example, if operator-A in country-A has established an agreement with each of the three operators in country-B (VPLMN-B1, VPLMN-B2, VPLMN-B3), then

based on different roaming and billing aspects, operator-A can configure the UE with a priority list of country-B VPLMNs. Thus, when UE lands in country B, based on the priority list, a certain VPLMN is selected by the UE. Currently, this information is provisioned in the UE via the SoR (Steering of Roaming) procedure defined in TS 33.501 (clause 6.14) [1]. However, the continuous evaluation of the security posture and trust of the NF(s) of the VPLMN(s) are currently not considered by operator A to prioritize the connectivity through a particular VPLMN, i.e., the most 'secured and trusted' one.

There have been some intents to evaluate trust for telecom networks by relevant industry players. The whitepaper on Zero Trust and 5G – Realizing zero trust in networks [97] builds upon ETSI specification [44] such that multiple parameters can be taken into consideration for evaluating trust that are relevant for telecom networks. Examples include geographical location, NF location, software capabilities (such as patch level, software versions…), execution history of an instance, configuration compliance (compliance with security policies), and the appropriate use of encryption techniques. The whitepaper mentions the notion of trust score associated with NF instance. Such trust score is based on parameters such as NF current configured state, image version and compliance level. The trust scores may have three different ranges on a scale of 0-100: low confidence (<50), medium confidence (51-79), and high confidence (>=80). Based on the trust score evaluation, further actions may be taken, such as terminating the NF and replacing it. However, such scores are based on static parameters and do not consider a dynamic evaluation of the security posture and trustworthiness of the NFs, taking into account variables like abnormal behavior, statistical data, and fundamentally the risk level.

5.2 Determining a trust score for mobile networks

The approach to determining a trust score for mobile networks in roaming that I propose in this dissertation consists of the following elements:

- **The notion of NF/PLMN trust score**, which describes a more generic longer-term trust indication, i.e., not specific to a single abnormal behavior occurrence, but to all occurred abnormal events in the past over a considered variable time period and expected (predicted) in the future.

  NF/PLMN trust score is a trust indication, represented, for example, by a scalar value within a certain range (e.g., 1-100), defined by a trust metric of the NF/PLMN, where higher values may refer for example to more trustable NF/PLMN. Of course, qualitative metrics, such as low trust, medium trust, and high trust, are also possible. The NF/PLMN trust indication can optionally contain further information, e.g.:

  - validity period, i.e., the time period in which the estimated trust score is valid.
  - fluctuation information, i.e., information on the changes and trends in the trust score over a considered period of time.
  - considered time period, i.e., information on the time window in which the relevant data has been collected, based on which the trust score is determined.
- **Deployment options**, intended to host the proposed means for determining the trust scores:

  - Option 1: The network analytics function in 5G, i.e., NWDAF, may be extended with a new capability to provide a new analytics type related to the derivation of NF/PLMN trust indication.
  - Option 2: A separate network security entity responsible for the derivation of the trust indication. This security entity may rely on NWDAF analytics capability to provide a new Analytics type related to the NF/PLMN trust indication along with additional information on the confidence of the analytics outcomes.
  - Option 3: Hosting the functionality in any existing network function; for example, for inter PLMN trust score, it can be hosted in the SEPP, for intra PLMN trust score can be hosted in UDP/PCF/… etc.

- **New analytics aspects to determine the trust score.** As mentioned above, the trust score can be calculated individually per NF and/or aggregated per VPLMN.

In order to provide the analytics outcomes, the input data is collected from multiple sources such as Core NFs, OAM systems, SEPPs, etc., and may consider different KPIs associated with failures and issues at different levels in the network.

With those inputs, the entity providing the means to determine the trust score should analyze the "exceptions" related to a particular NF/PLMN in the past, including the exception category and exception level (to be defined by the implementer), the frequency of exceptions that happened during a considered period of time in the past, and returns the trust indication information per NF/PLMN, possibly supplemented by additional information, for example a list of NF/PLMN exhibiting the same level of trust, information on the NFs interacting with the NF under evaluation with associated trusted levels, etc. The Tab. 5.2-1 presents an example of the new trust-related analytics output information for NFs. Similarly, this information can be requested and provided for other targets (NF sets, PLMNs)

Tab. 5.2-1: Example output information for trust score of NFs

Information	Description
NF trust indication (1..max)	Information on trust-related indications for a given target NF (PLMN).
Trust score	Scalar value indicating the trust measure of the NF (PLMN).
Considered time period	Time window in which the NF behavior has been monitored and based on which the output is reported.
Validity period	Time period in which the estimated trust score is valid
Fluctuation info	Information on the change/trend in trust score over considered time period. This information may capture the sudden drops in trust score (e.g., due to a single high-risk event that impacts the NF trust immediately) as well as the existence of longer low-risk events that gradually decrease the trust score.
List of NF(s) with the same trust score	One or more NFs exhibiting the same trust score

The potential consumers of the trust score might be:

- UDM or SoR AF (Application Function) can use this inter PLMN trust score to prioritize or de-prioritize the PLMN list in the UE.
- NRF can use this information to increase or decrease the priority of the discovery response.
- SEPP will use additional filtering or policy on less trusted networks.
- OAM systems, e.g., if the trust score falls under a certain minimum threshold, OAM may decide to decommission the NF.
- Federated Learning Aggregator (e.g., NWDAF) can use this information to select or unselect an NF in the training process.
- UDM will change the UE Subscription Data to include or exclude the CAG (Closed Access Group) ID based on its trust indication. This may trigger updates of the UE configurations.

The dynamic risk evaluation mechanism defined in chapter 4 of this dissertation should constitute the main baseline to build a trust indication/score per VPLMN and/or IPX provider connected to the HPLMN, although other analytics type of factors can also be taken into account to craft the final trust score. The determination of the trust score complements the response to the **Thesis 1** of this dissertation by transforming the measurement of the risk into a trust score per interconnected MNO and/or Roaming intermediary. In this chapter we have introduced the notion of trust score and several implementation options, as well some new related analytics aspects. Note that in subchapter 8.3, we provide a practical example of a possible procedure to be considered in the Network Analytics framework of future mobile generation releases for this purpose.

6 Security policies definition and profiling

This chapter introduces the concept of Security profiles in 5G Roaming, which I (together with dr. A. Jerichow) have patented in [12]. Please note that our outcomes have been already implemented in the standards specifications corresponding to 5G-Advanced (i.e., from Release 18 onwards), namely 3GPP TS 33.501 [1], TS 29.573 [59], as well as in industry Roaming guidelines such as GSMA NG.113 [2].

The introduction places the security policies topic in the generic interconnection architecture of 5G. Subchapter 6.2 provides a synthesis of the main technologies used in 5G Roaming security architecture, focused on the new application layer end-to-end security paradigm, and supported by diagrams and schemas that I depicted for better understanding of the standard procedures. Finally, subchapter 6.3 details the concept of security profiles in 5G roaming applied to that new application layer end-to-end security paradigm and the enhancement introduced by the concept in security operations.

Note that under Chapter 8, subchapter 8.4 provides the concrete implementation of the concept presented in this chapter in standard technical specifications and industry guidelines, since it was accepted to part of those in 5G-Advanced.

6.1 Introduction

The Security Framework proposed in this dissertation introduces the required dynamicity and adaptability of the SLAs between MNOs. The trust score concept described in previous chapter is intended to impact the technical security clauses of the SLAs, and accordingly the security policies in the interconnection gateways.

The Fig. 6.1-1 shows an example of the implementation of the security policies in the HPLMN and how they are applied to a request message to the home NRF API. The figure also depicts how the trust score should be considered in the continuous adaptation of those policies. I.e., the dynamically computed trust score can be used to adjust the security policies according to the risk level in each interconnection link with the peer roaming operator and/or roaming intermediary. The main target is the adaptation of security policies in the contractual Service Level Agreements and, subsequently, the enforcement of those in the signaling gateways (and/or signaling firewalls) protecting the links.

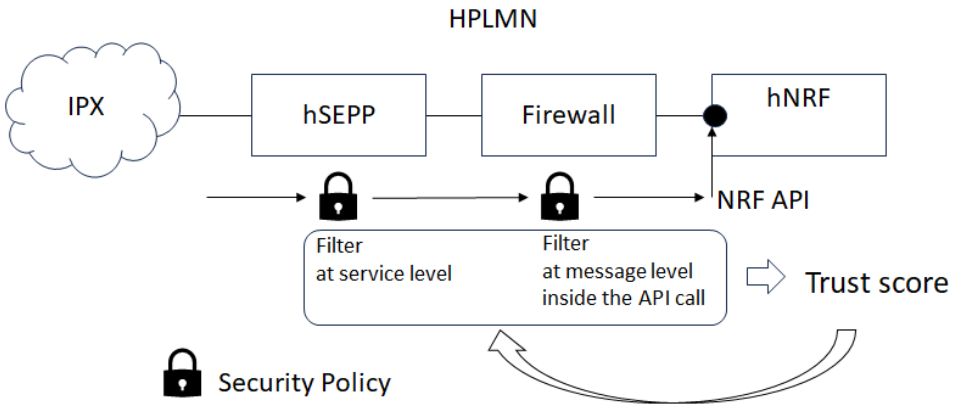

Fig. 6.1-1: Example of security policies implementation in the HPLMN

Please note that chapters 6 and 7 of the dissertation only consider 5G networks (Standalone Architecture) and future 6G networks. The reason is that we can take advantage of the new Policy control and Analytics framework specified by 3GPP in 5G, which constitutes, within the SBA architecture, a unique framework for defining any type of policies in the network and delivering those to other control plane NFs. In previous generations, the policy control functionality has been restricted to Quality of Service (QoS) and charging aspects. In contrast, the 5G system is now based on a unified policy control scheme that allows to build consistent policies covering the entire network. Of course, an implementer of the proposed methodology can build the same concepts in a proprietary manner for previous mobile generations, but this is out of the scope of this dissertation.

6.2 5G Roaming security architecture - debriefing

In 3GPP TS 33.501 [1], the clauses 13.1 and 13.2 specify a new security paradigm in Roaming, moving from hop by hop approach in previous mobile generations towards an end-to-end approach, where the actual security policies are decided between the two interconnected mobile operators.

The cornerstone of the 5G Roaming architecture is the SEPP (Security Edge Protection Proxy). The SEPP was introduced as a security entity (non-transparent proxy) in charge of the protection of the 5G Core network at N32 interface. Thus, all roaming control traffic is routed via the SEPP and the N32 interface to the SEPP of the other PLMN, where the secure interconnection between PLMNs is terminated (see Fig. 6.2-1).

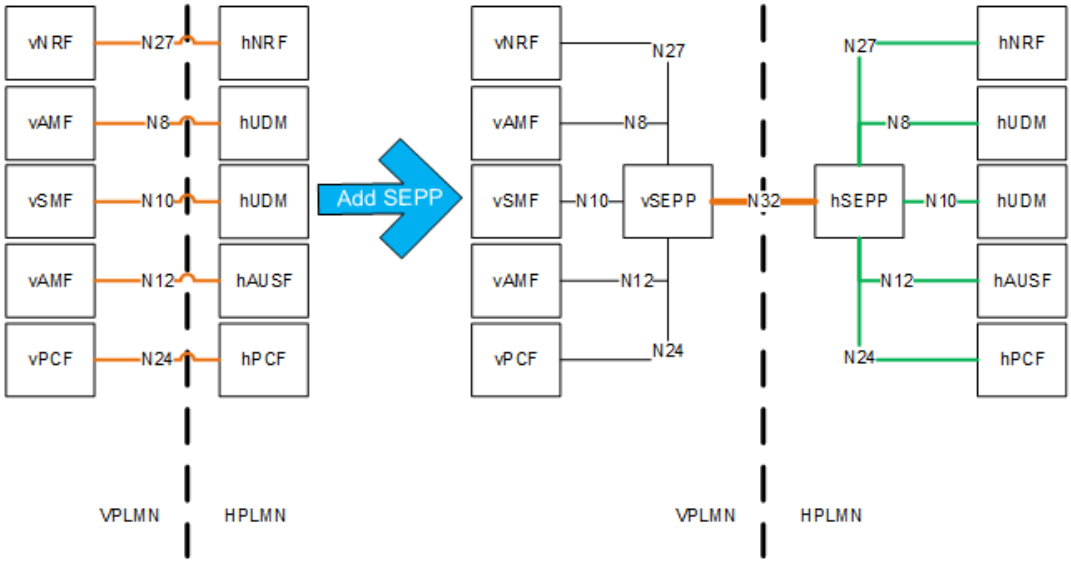

Fig. 6.2-1: SEPP introduced for securing 5G Core from VPLMN interconnection

The relevant interfaces in the 5G Roaming Architecture are listed in Tab. 6.2-1.

Tab.6.2-1: Relevant interfaces in 5G Roaming

VPLMN	HPLMN	Ref	Process Step	Description	Applicability
AMF	UDM	N8	Registration	Access and mobility data retrieval by VPLMN, SMF selection query (e.g., during	Local Breakout & Home Routed

				registration/UE latch procedure)	
SMF	UDM	N10	PDU Session Creation in LBO; in HR case, uses H-SMF to UDM	Session Management data retrieval by VPLMN (during PDP/session context for session establishment)	Local Breakout
AMF	AUSF	N12	Authentication in Registration	User authentication during registration from VPLMN (when the user latches in VPLMN)	Local Breakout & Home Routed
vSMF	hSMF	N16	PDU Session creation in HR case; in LBO case, this is handled by V-SMF itself	Create/modify/delete service mgmt. context request towards HPLMN SMF to create such context in hSMF	Home Routed
SMSF	UDM	N21	During SMS submission step	SMS subscription data retrieval for B-party subscription information	Local Breakout & Home Routed
vPCF	hPCF	N24	Registration and PDU session Creation	UE policy association (create/modify/delete) for a VPLMN. hPCF to maintain context as well	Local Breakout & Home Routed
vNRF	hNRF	N27	For all VPLMN and HPLMN SBA interfaces	For getting NF instance details in HPLMN to be contacted by VNPLMN NFs, e.g., getting the hSMF address	Local Breakout & Home Routed

vNSSF	hNSSF	N31	Registration (Network Slicing Related)	Mapping and allowance of HPLMN NSSAI to VPLMN slices	Local Breakout & Home Routed
SEPP	SEPP	N32	For all control plane signaling messages between HPLMN and VPLMN	For topology hiding and security-related data exchange	Local Breakout & Home Routed
vUPF	hUPF	N9	For Voice, data user plane in HR cases	For HR case transfer of user plane traffic to HPLMN from VPLMN. H-SMF selects H-UPF in HPLMN, and V-SMF selects V-UPF in VPLMN	Home Routed
vSMSF	UDM	N21	For SMS Services	For Enquiring User details	Not Applicable

TLS has been standardized as a security mechanism to protect the communication between SEPPs, and between SEPP and the next-hop intermediary in IPX scenarios when there is no bilateral communication between MNOs. 3GPP also specified since the very first release 15 of 5G, an additional application layer security mechanism abbreviated as PRINS (PRotocol for N32 INterconnect Security) for the JSON (Java Script Object Notation) information elements on N32.

Fig. 6.2-2 depicts a high-level schema of the 5G Roaming security architecture in control plane as specified in [1]. Each NF registers with the NRF exclusively in the same PLMN (note that registering is only required if the NF acts as a producer). An NF consumer (NFc) sends requests for both the discovery of an NF producer (NFp) in the other PLMN and token requests for this NFp to the NRF in its own PLMN (NRFc). The NRFc uses a mutually authenticated secure connection between SEPPs to forward the discovery and token requests to the NRF in the other network (NRFp), i.e., NFs in PLMN A and B can only implicitly authenticate each other via

SEPPs. The NRFp sends the responses back to the NRFc, which forwards them to the NFc. Since then, the NFc can proceed with the service requests towards the NFp, and if the communication has been authorized, the NFp can serve the NFc.

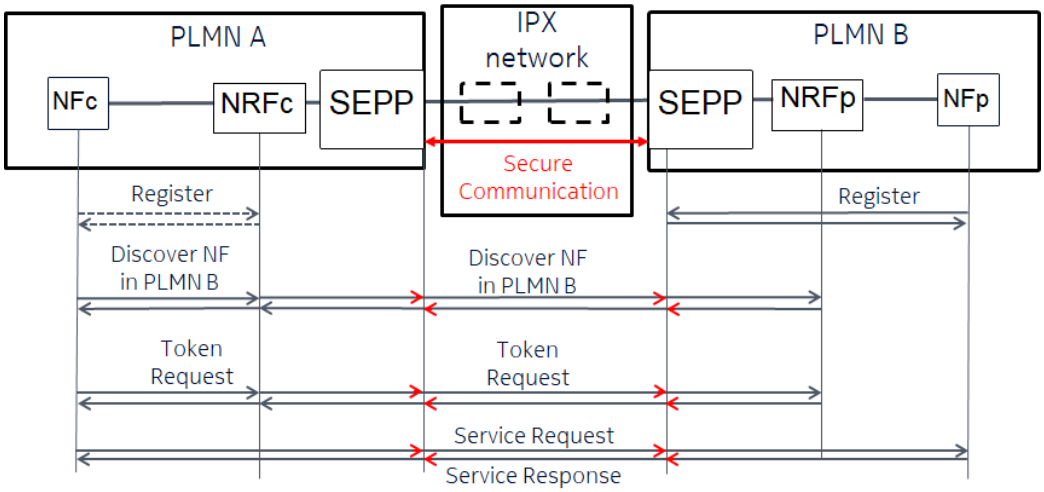

Fig. 6.2-2: Secure interconnection schema between PLMNs in 5G

N32 interface between two SEPPs consists indeed of two interfaces:

- **N32-c (control)**: It is established prior to N32-f and the control part of it. It is dedicated to negotiating the security capabilities for N32-f, error handling, and N32 termination. N32-c interface is mutually authenticated via TLS (bilateral between the two PLMNs). Thus, the roaming intermediaries (if any) are mere transport proxies for this interface. The negotiation of the security method (TLS or PRINS) for N32-f has the following industry (GSMA 5GMRR) accepted criteria:
    - **TLS** between two PLMN SEPPs in bilateral connectivity (i.e., no Roaming intermediaries, or Roaming intermediaries purely as transport proxy)
    - **PRINS** if, with the aim of providing roaming services, the Roaming intermediaries should be able to selectively read and/or modify the signaling messages in an attributable way. In this case, the negotiation includes the key agreement (shared session key) and security-related configuration parameter exchange.
- **N32-f (message forwarding):** It is established for the real signaling message exchange.
    - Either **TLS** (direct connection). I.e., HTTP/2 messages of the NF service producers and the NF service consumers in different PLMN are confidentiality and integrity protected between PLMN SEPPs (end-to-end).

- Or **PRINS** (connection via entities in the IPX), which requires:
  - Agreement of keys and cipher suites
  - Agreement of IE protection policies (encryption, modification)

In Fig. 6.2-3 I represent both N32-c and N32-f interfaces between SEPPs.

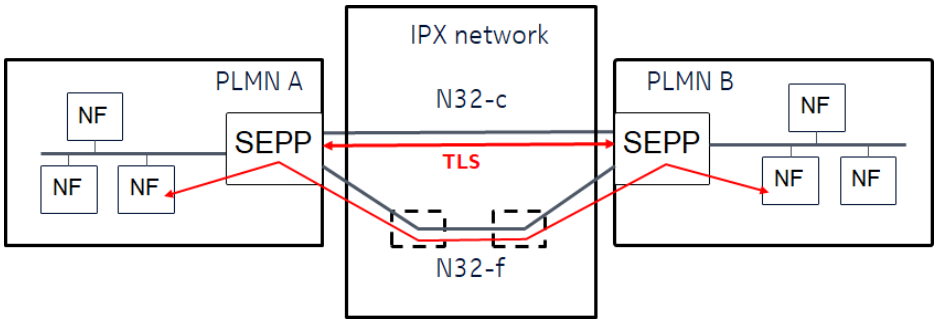

Fig. 6.2-3: N32-c and N32-f interfaces

When PRINS is negotiated HTTP/2 headers and body are transformed first into specific JSON attributes (JOSE protected messages) to allow roaming intermediaries to read and modify them in an attributable way. The links between SEPPs and Roaming intermediaries' gateways, and between those Roaming intermediaries' gateways are to be secured via VPN TLS or IPsec. The main security feature achieved by PRINS is that all messages are end-to-end integrated protected, and selected Information Elements (IEs) are confidentiality protected.

In Fig. 6.2-4 I show in more detail the PRINS procedure between two MNOs (figure adapted from Figure 13.2.1-1 of [1]).

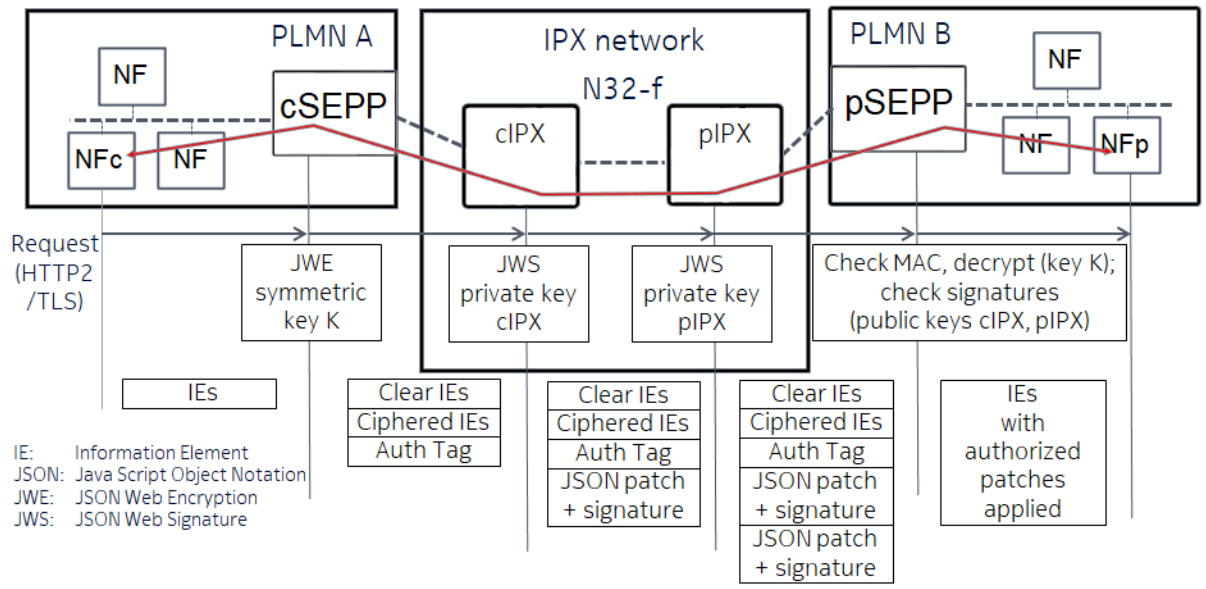

Fig. 6.2-4: Details of PRINS (figure adapted from Figure 13.2.1-1 of [1])

The PRINS protocol allows part of the signaling to be sent in cleartext to enable Roaming intermediaries (e.g., Roaming Value Add Services operators, roaming hubs, IPX carriers, etc.) to inspect and/or modify the signaling traffic in transit. Java Script Object Notation (JSON) framework is used to protect the information in the N32 message payload. More specifically, the protocol uses JSON Web Encryption (JWE), specified in IETF RFC 7516 [98], for protecting the integrity and confidentiality of certain selected IEs of the messages on the N32-f interface. Please note that the authentication tag is part of the JWE format, as it authenticates the encrypted data and additional data. The Roaming intermediaries use JSON Web Signatures (JWS), specified in IETF RFC 7515 [99], to sign the modifications needed for their mediation services. 3GPP TS 33.501 [1] refers to the security aspects provided by PRINS as Application Layer Security.

Please note that the user plane communication between PLMNs is protected via IKE/IPsec for N9 interface, as well as with the Inter-PLMN UP Security functionality (IPUPS) as described in clauses 4.2.2 and 5.9.3.4 of [1]. User plane security aspects are not part of the scope of the dissertation.

6.3 Security Profiles in 5G Roaming

Since already 3GPP Release 16 of 5G, PRINS protocol is being revisited, even challenged, by the interconnection and roaming industry represented in GSMA 5GMRR group, mainly due to business and operational requirements. The required negotiation on security configuration parameters and IEs to be protected for N32-f is considered too cumbersome and a very complex task to be accomplished per peer roaming operator. IPX providers and Roaming Hub providers have been seeking simpler and more efficient ways whilst keeping the security level.

The configuration of templates as security profiles for PRINS is intended to alleviate the operational issues foreseen by the industry. The support of predefined security profiles in 5G Roaming looks for simplifying PRINS, and particularly the complex negotiation procedures required to agree on cipher suites and the exchange of security policies.

Thanks to the security profiles, peer roaming operators do not need to negotiate anymore on particular modification policies or data_type encryption policies, even on cipher suites. Instead, a security profile will include a set of preselected cipher suites, default modification policies, and default data_type encryption policies, all that combined with a list of IEs to be protected. More specifically:

- **Cipher suites** for confidentiality and integrity protection. Even if the cipher algorithms of a cipher suite are predefined, there are still cipher suites to be negotiated. In clause 13.2.2.2 of TS 33.501 [1] it is explained how two SEPPs shall perform the cipher suite negotiation to agree on a cipher suite to use for protection of the signaling over N32-f:
    - The SEPP that initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP, including the initiating SEPP's supported cipher suites. The cipher suites shall be ordered in initiating SEPP's priority order. The SEPP shall provide an initiating SEPP's N32-f context ID for the responding SEPP.
    - The responding SEPP shall compare the received cipher suites to its own supported cipher suites and shall select, based on its local policy, a cipher suite that is supported by both the initiating SEPP and responding SEPP.
    - The responding SEPP shall send a Security Parameter Exchange Response message to the initiating SEPP, including the selected cipher suite, to protect the NF service-related signaling over N32. The responding SEPP shall provide a responding SEPP's N32-f context ID for the initiating SEPP.

3GPP profiles the security protocols TLS 1.3 and TLS 1.2 with certain available cipher suites (clauses 6.2.2 and 6.2.3 of TS 33.210, respectively), e.g., *"The requirements given in section 9.1 of TLS 1.3 RFC 8446 shall be followed, and Key exchange with secp384r1 should be supported".* Subsequently, section 9.1 of IETF RFC 8446 [100] provides several options to be negotiated, e.g., TLS_AES_128_GCM_SHA256 [GCM] cipher suite (mandatory to be implemented), TLS_AES_256_GCM_SHA384 [GCM] and TLS_CHACHA20_POLY1305_SHA256 [RFC8439] cipher suites (optional, recommended), etc.

- **Modification policies**, which IEs can be modified by the Roaming intermediaries, including removal or addition of new IEs. This would be the most tedious and complex part to build the profile, but also useful in every PRINS implementation. Out of a list of possible IEs, critical ones from security and privacy viewpoint can be marked as "non-modifiable" by the Roaming intermediaries.
- **Encryption policies.** IEs such as authentication vectors, location data and cryptographic material shall be confidentiality protected between peer roaming operators. SUPI and authorization tokens related IEs can be encrypted in one profile and be in cleartext in other profile.

A PRINS profile indicates a predefined set of one or more of the above policies. Thus, N32-f may use profiles with pre-populated parameters for cipher suites, modification policy, and data encryption policy, and that can be combined with a list of IEs to be protected and an indication of the trust level, so called in this dissertation "Trust score." The trust score should be used to select dynamically the concrete security profile.

The indication of the respective profile is to be part of the communication between SEPPs and in the eventual communication with the Roaming intermediaries. Thus, it is proposed to enhance the N32-c negotiation for PRINS with a new indicator for a PRINS (security) profile, required to be considered by the two SEPPs of the N32 communication, and also required to be propagated to the Roaming intermediaries.

If PRINS is chosen vs. end-to-end TLS, full flexibility in negotiation is certainly possible, or alternatively one of the predefined PRINS profiles may be selected. The number of different profiles may be any suitable number.

The procedure for implementing the security profiles is straightforward. There might be several standard profiles, e.g., “A”, “B”, “C”, etc., which detail by policy the IE types to be encrypted or not. For the IE types that are not encrypted, there might be an indication as to whether they are allowed to be modified. With this information, during the N32-c handshake, if the PRINS enhanced profile, e.g., “B”, is chosen, then both SEPPs in VPLMN and HPLMN know to handle the communication on the N32-f interface. I.e., at the time that the mechanism to protect N32-f is selected, there is the option to select a PRINS profile from one or more PRINS profiles. The main steps can be summarized as:

- The initiating SEPP (iSEPP) initiates a security capability negotiation procedure towards the responding SEPP (rSEPP) to agree on a security mechanism to use for protecting NF service related signaling over N32-f.
- The iSEPP provides the supported (or selected) security capability, i.e., PRINS, PRINS profile, and/or TLS. The iSEPP might provide a preference order for the list of the supported security capabilities. This may include, for example, that profile “A” is preferred, but profile “B” is also supported.
- On successful processing of the request, the rSEPP responds back and provides the selected security capability among other information. The rSEPP compares the supported security capabilities to its own supported security capabilities and selects, based on its local policy, but in priority order, the security mechanism, which is supported by both SEPPs. I.e., the rSEPP will check that it can support the requested PRINS profile.
- On failure, the rSEPP would respond with an error message.

The creation and configuration of security profiles as well as the procedures to implement them effectively in the 5G networks, described in this chapter, responds to **Thesis 2** of this dissertation.

7 Security Enforcement by 5G Policy Control framework

This chapter introduces the functionality of security enforcement within the 5G Policy Control framework, that I patented under [11], and published in [8]. It is the final chapter of the dissertation that closes the development of the overall proposed security framework, which started with the dynamic risk evaluation mechanism, followed by the definition of trust score in roaming, and the corresponding derived security policies and profiles. This chapter describes how those policies and profiles can be enforced dynamically by enhancing the actual 5G Policy Control framework.

Subchapter 7.1 (Introduction) places the chapter more specifically in the overall context of the dissertation and depicts how the functionality can be used in Interconnection. The subchapter 7.2 details the development of the functionality, which basically consists of the application of QoS policies to security use cases, the corresponding procedures to enforce security policies in the user plane through the Policy Control framework, the establishment of security policies as part of the Policy and Charging Control (PCC) rules, and the enhancement of the actual Network Analytics framework in 5G to include a new Security Analytics functionality. Please note that the user plane security aspects are provided in this chapter as a reference to show how the Policy Control framework might work in a concrete use case. As mentioned earlier, user plane security aspects are out of the scope of this dissertation and proposed as a topic for further investigation in Chapter 9.

Note that under Chapter 8, subchapter 8.5 presents the procedures for applying the described functionality in Interconnection architecture, which can be part of future standardization work.

7.1 Introduction

This chapter proposes a new approach to the dynamic enforcement of security policies in the interconnection gateways by reusing the 5G Policy Control framework.

Our patented solution [11] provides a set of techniques for dynamic security management in the mobile network. The starting point is the collection of security information (e.g., risk index, trust score, etc.) from one or various network entities. In response, the mechanism enables the dynamic enforcement of one or more security policies taking advantage of the procedures defined within the Policy Control framework in 5G specified in 3GPP TS 23.503 [56]. An enhancement in the network data analytics NF, NWDAF, specified in 3GPP TS 23.288 [4],

contributes as well to this new concept. The enhancement consists basically of providing the NWDAF with the capabilities to perform security analytics.

Although in principle the solution mainly addresses the user plane of the mobile network, the concepts are easily extended to the control plane in interconnection, i.e., N32-c/f, mainly by:

- Enabling the security analysis and management (i.e., risk assessment, trust score, policies, and profiles) in a new 'security specialized" NWDAF focused on signaling in roaming.
- Making use of the outcomes of that "security specialized" NWDAF and mapping them to concrete policies to be managed in the PCF.
- Creating an interface (and corresponding RESTful APIs) between PCF and SEPP to enable the PCF to configure and modify policies to be enforced in the SEPP.

    Note: In some implementations, another enforcer, such as a signaling firewall, could be the receptor of those policies, provided that the corresponding APIs are properly crafted to enable the communication with PCF.

The PCF is a network function that constitutes, within the SBA architecture, a unique framework for defining any type of policies in the network and delivering those to other control plane NFs. The main novel concept of the patent is the application of quality-of-service (QoS) principles to security enforcement, i.e., considering security as another quality of the network.

The NWDAF was extended in Release 16 to non-slice-specific analytics, with a few security-related use cases around denial-of-service (DoS) detection. There can be multiple NWDAFs specialized in different types of analytics, which are identified by "Analytics ID" IE. This IE is used to identify the type of supported analytics that NWDAF can generate. This research work creates new types of analytics related to security in interconnection, such as the dynamic risk evaluation and the trust score described in previous chapters. The NWDAF interacts with different entities for different purposes, such as data collection based on subscription to events provided by different NFs, retrieval of information from data repositories and NFs, and on-demand provision of analytics to different kinds of consumers. In our signaling interconnection context, the input data collection is thought to be a copy of the signaling traffic captured in the SEPP, or virtual tap part of the Containerized Virtual Function (CNF) implementing the logical SEPP, whereas the consumer is the PCF, and the enforcement point is the SEPP itself or

eventually a signaling firewall part of the infrastructure. In Fig. 7.1-1 I depict the explained overall concept.

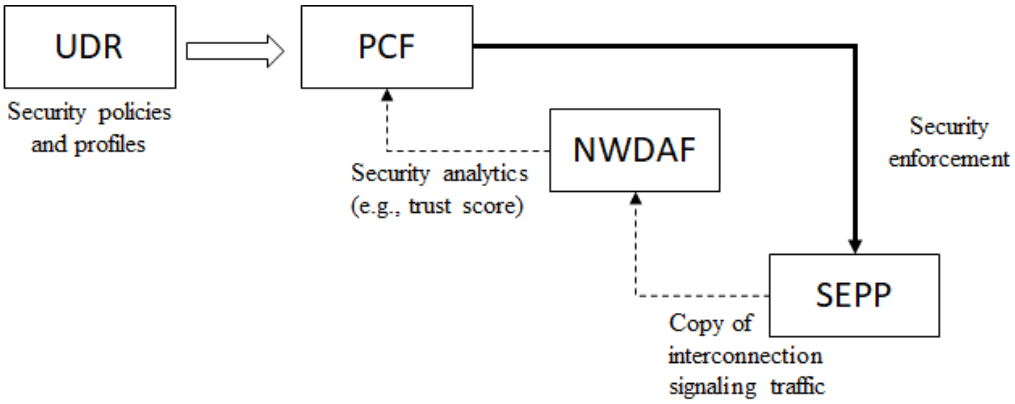

Fig. 7.1-1: Security enforcement schema for signaling interconnection

7.2 Automated security enforcement concept in mobile networks

The 5GS comprises a Policy Control Function (PCF) and Policy Enforcement Points, e.g., in the User Plane Function (UPF) in the core network, controlling in particular the usage of transmission resources (QoS), but also the access to services (gating), on a per-UE-per-session basis. Fig. 7.2-1 shows this standardized framework, which I have adapted from Figure 5.2.1-1 of 3GPP TS 23.503 [56] adding in orange the flows intended to gather information relevant to building the policies, and in red the configuration of the policies in different network elements through the standardized APIs by 3GPP.

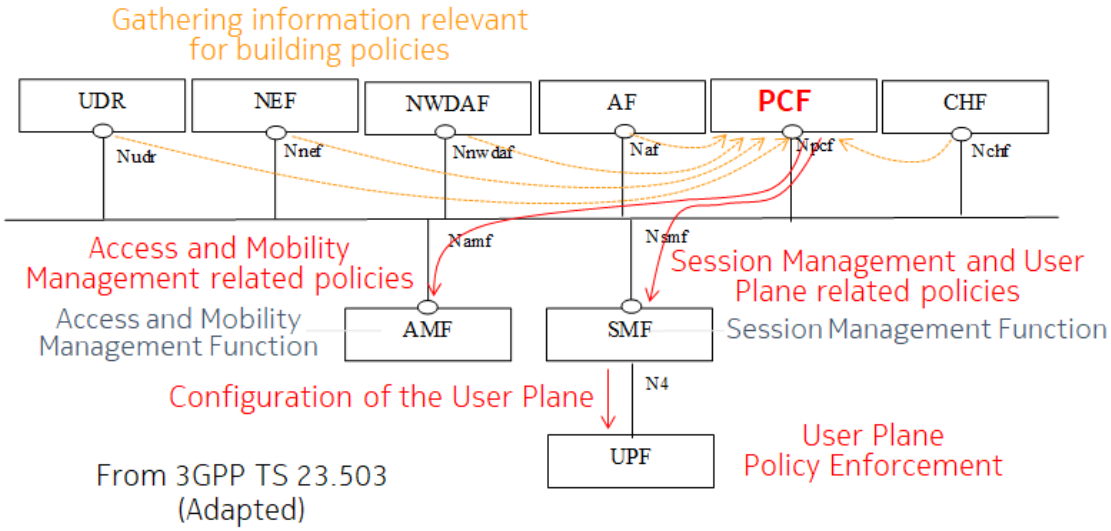

Fig. 7.2-1: 5G Policy Control architecture with flows (adapted from 3GPP TS 23.503 [56])

The concept, documented in [8] and proposed in this dissertation, to automate security enforcement in the mobile network consists of the following items:

- The application of QoS policies to security use cases
- User plane security enforcement and assurance
- Establishing security policies as part of PCC rules
- Security analytics implemented in NWDAF

The following subclauses summarize these items, and a complete description is provided in [8].

7.2.1 The application of QoS policies to security use cases

QoS policies can be applied restrictively and dynamically from the PCF into the network at the reception of security events or incidents, which might be created in NWDAF or another security analytics platform (e.g., SIEM/SOAR/xDR/… tools, IDS/IPS systems, firewalls, etc.). Based on a predetermined security indicator (e.g., trust score), different policies can be enforced from the PCF, working de facto as an efficient mitigation in the network:

- Set up a new session AMBR (Aggregated Maximum Bit Rate). The session AMBR limits the aggregate bit rate that can be expected to be provided across all Non-Guaranteed Bit Rate (GBR) QoS flows for a specific PDU session.
- Set up a new UE AMBR. Note that at UE level, each UE is associated with a per UE-AMBR. The UE-AMBR limits the aggregate bit rate expected to be provided across all Non-GBR flows of a UE. It would be a kind of quarantine for the UE, when it is for

example an active bot of a DDoS attack.

- Set up a new PDU session with more restrictive security controls in the QoS profile.

Being the PCF the policy decision point, the SMF manages QoS flows with rules, associating traffic filters with QoS policies coming from the PCF. The traffic filter set is configured in the UPF and can serve to easily manage security services, such as the security association for a particular group of UEs or slice with specific security requirements, traffic gating, etc.

Fig 7.2.1-1 represents a sample call flow of this concept.

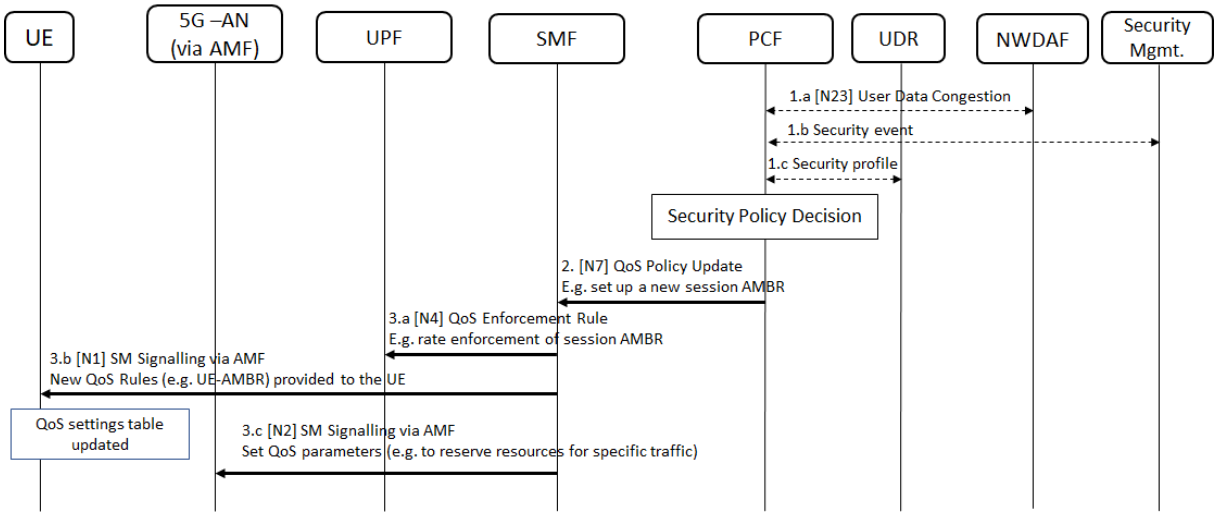

Fig. 7.2.1-1: Applying QoS rules for security

Steps 1.a, 1.b, 1.c: The PCF fetches security information (e.g., events, scores, policies, profiles, etc.) from different possible sources, such as NWDAF (N23 interface), a general security management system (e.g., customized REST API) or UDR (N-36).

Step 2: After the security policy decision is taken in PCF, the PCF determines that the SMF requires updated policy information to mitigate the security issue reported in the previous step.

Steps 4.a, 4.b, 4.c: Enforcement of the policy from the SMF towards the UPF (e.g., session AMBR), or towards the UE (e.g., UE AMBR), or towards the 5G Access Network (AN) (e.g., by reserving of resources for a specific type of traffic).

7.2.2 User plane security enforcement and assurance

Acting directly on the AMF and on the SMF control network functions, the PCF reaches the UE, Radio Access Network (RAN), and the UPF to apply security policies directly on the User Plane (UP).

There are two types of policies for access and mobility managed and enforced by the AMF, dictated by the PCF and stored in the UDR, that can support security use cases without major changes in the policies definition: policies transferred from PCF to AMF, and policies transferred from PCF to the UE via AMF. Below are a couple of examples of security policies enforced in the AMF and UE as per the indication of the PCF:

- Service area restrictions in AMF. For example, there could be sensitive geographical areas hosting critical infrastructure that may restrict the access to UEs supporting UP integrity protection in the air interface.
- UE Route Selection Policy (URSP). For example, a new PDU session could be triggered in case of a security incident, as a kind "quarantine" PDU with special policies and/or services across the data path, e.g., scrubbing center.

Certain implementations of UPF may include security-related functionalities such as firewalling, throttling, (D)DoS protection, GPRS Tunnelling Protocol (GTP) inspection, IPsec, etc. Our approach proposes that those security functionalities embedded in the UPF can be managed by security policies in the PCF by transferring them to the UPF via SMF (N4 interface). Similarly, the enablement of confidentiality and integrity protection in the air interface can be established by PCF policies based on the UE profile stored in UDR. Those policies should be part of the dynamic Policy Control and Charging (PCC) rules dedicated to UP security. Additionally, in our proposal, those policies are to be extended to other domains and UP interfaces such as N6 (UPF – Data Networks), N3 (backhauling network between RAN and Core), and N9 between two UPFs within the same operator domain or between two operators.

Based on that, the enablement of security assurance in the network requires to consider two key aspects: security data collection and closed-loop automation. The proposal consists of enriching the data collection with security-relevant data from the above-mentioned embedded security features in the UPF. The SMF would be responsible for collecting such enriched data from the UPF and transferring it to a central security management system, where this data is stored, contextualized, and correlated with security information collected from various security platforms/entities in the network, e.g., firewall logs, security telemetry, IDS logs, etc. The security management system is responsible for creating security incidents and triggering the corresponding actions on the PCF and/or directly on SMF (e.g., redirecting the traffic to a

scrubbing center, establishing a secure connection, etc.). Fig. 7.2.2-1 represents the idea of enablement of security assurance as part of the overall security enforcement concept.

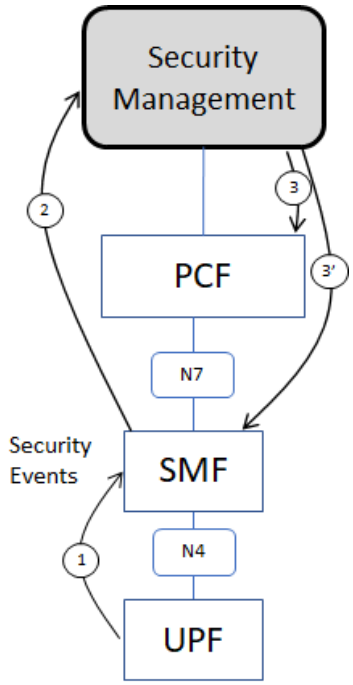

Fig. 7.2.2-1: Security assurance based on Policy Control framework

7.2.3 Establishing security policies as part of PCC rules

PCC rules connect the Service Data Flows (SDF) templates (the SDF is a set of PDUs within a PDU session identified by traffic filters) with the possible actions on the traffic, i.e., the policy enforcement. Taking the current actions proposed by 3GPP as a basis, focused on pure QoS actions, I propose to extend and apply those actions for security purposes as summarized in Tab. 7.2.3-1.

Tab. 7.2.3-1: PCC rules - Security

PCC – QoS	**PCC – Security**
Gating control (discarding traffic upon PCF Control)	Personal firewall with policies managed upon PCF control
Discard traffic not matching the SDF template of any active PCC rule	Personal firewall (last rule: 'drop any – any')
Monitoring the amount of traffic	DDoS detection
Steering the traffic towards service functions at N6 on the DN, or to different N6 interfaces of the same DN (identified as Data Network Access Identifier (DNAI))	Security functions such as firewalls, Application Layer Gateways, malware protection, content filtering, Network Address Translation, etc., shall be managed by Software Defined Networks (SDN) in a service chaining architecture. Those functions can be activated through a pre-defined subscription plan, or as a reactive action when

	facing a security incident, or as prevention/mitigation of (D)DoS attacks.
Towards 5G-AN: to apply relevant user plane security (integrity protection)	Extended to other network segments like N2 and N3 with technologies like IPSec or DTLS

7.2.4 Security analytics implemented in NWDAF

The NWDAF provides information that can contribute significantly to the PCC decision-making process performed by the PCF. Our research expands the load level information by adding security contextual information (e.g., events, attacks, vulnerabilities, etc.). It would require the feed of the security functions implemented separately or as part of the standardized network functions, such as UPF with embedded firewall capabilities, into NWDAF or an intermediate dedicated security analytics platform.

The standard TS 23.288 [4] opens the possibility to different types of NWDAFs, specialized in different types of analytics, identified by analytics ID information element. The PCF can consume this information via N23 interface. Indeed, some of the currently standardized analytics information can already provide very useful information for the security analysis and further enforcement. Table 7.1-2 of [4] shows the analytics information provided by NWDAF service. I have added a column to that table with the security information that could potentially be extracted and sent to other security analytics functions for further analysis or directly to the PCF framework for the application of specific security PCC rules. See Tab. 7.2.4-1 adapted from Tab 7.1.2 of [4].

Tab. 7.2.4-1: Security insights on the analytics information provided by NWDAF (adapted from Tab. 7.1.2 of [4])

Analytics Information	**Request Description**	**Response Description**	**Security Insights**
Slice load level information	Analytics ID: load level information	Load level of a network slice instance reported either as notification of crossing of a given threshold or as periodic notification (if no threshold is provided).	*(D)DoS specific thresholds based on volume and time*

Observed service experience information	Analytics ID: Service experience	Observed service experience statistics or predictions may be provided for a network slice instance or an application. They may be derived from an individual UE, a group of UEs or any UE. For slice service experience, they may be derived from an application, a set of applications or all applications on the network slice instance.	*Key information to be communicated to security analytics platforms. For example, an observation of a quality degradation of service experience in browsing could be a signal of a flooding attack on DNS resolvers.*
NF Load information	Analytics ID: NF load information	Load statistics or predictions information for specific NF(s).	*DoS specific thresholds based on volume and time for specific NFs (e.g., IMS AF with direct access to UEs)*
UE Abnormal behavior information	Analytics ID: Abnormal behavior	List of observed or expected exceptions, with Exception ID, Exception Level and other information, depending on the observed or expected exceptions.	*Further security analysis from the network security analytics platforms on the UE behavior.*
User Data Congestion information	Analytics ID: User data congestion	Statistics or predictions on the user data congestion for transfer over the user plane, for transfer over the control plane, or for both.	*Security issues against the availability of the service*
QoS Sustainability	Analytics ID: QoS sustainability	For statistics, the information on the location and the time for the QoS change and the threshold(s) that were crossed; or, for predictions, the information on the location and the time when a	*Due to a security attack a potential QoS change may occur, e.g. when D(DoS) volume/time thresholds have been surpassed.*

		potential QoS change may occur and what threshold(s) may be crossed.	

The PCF can subscribe to notifications of network analytics related to security with the aim of anticipating and detecting a potential security issue. Subsequently, at the reception of those security related notifications the PCF may trigger a new security policy or update an existing one.

This chapter validates **Thesis 3** of this dissertation by introducing a set of methods in the 5G Policy Control and Analytics framework, which are intended to provide an effective security enforcement schema. Those methods are to be applied in Interconnection as presented in subchapter 8.5.

8 Validation of the proposed framework

This chapter presents the validation of the proposed security framework for interconnection, to be applied in the SLAs between MNOs and in general, roaming services stakeholders.

For the first building block of the framework, i.e., the dynamic risk evaluation mechanism, described in Chapter 4, I have provided two types of results and analysis. Firstly, the mechanism is applied to a theoretical "Location tracking" use case (subchapter 8.1). Secondly, the mechanism is applied to a real Diameter trace in interconnection in 4G (subchapter 8.2). Note that at the time of writing this dissertation, there is no commercial use of 5G Roaming. In both cases, we simulated the risk computation according to the methodology CVSS, which we adapted to the context of the dissertation in chapter 4.3.

For the second building block of the framework, i.e., the determination of a trust score for Mobile Networks in Roaming, described in chapter 5, I have provided, based on one of the deployment options, a procedure for determining the trust indication of a given target, i.e., a peer roaming operator or other Roaming intermediary, that might be certainly standardized in next mobile generation releases (subchapter 8.3).

For the third building block of the framework, i.e., the security policies definition and profiling in Interconnection, described in chapter 6, I have provided the implementation of the new concepts developed and patented for PRINS in concrete standards (3GPP) and industry specialized guidelines (GSMA). This can be found in subchapter 8.4.

For the fourth building block of the framework, i.e., the security enforcement of policies by reusing the 5G Policy Control framework, described in Chapter 7, I have provided, based on the granted patent [11], developed within my PhD program, the guidelines to expand the procedures to the interconnection/roaming context (see subchapter 8.5).

8.1 Application of the risk evaluation mechanism to a theoretical Location tracking use case.

Geolocation disclosure is the most prevalent network threat type in interconnection. The attack determines the geolocation (up to Cell Id level in certain circumstances) of the targeted subscriber(s) once or repeatedly without their consent and without explicit authorization of their MNO.

Tracking the location of a subscriber can be executed from anywhere in the world connected to the IPX network. Many mobile operators have found and reported issues related to this threat within GSMA Fraud and Security Group (FASG). This type of attack in different variants has been exploited in SS7 and Diameter, and there is no reason to think that 5G will be different once 5G Standalone roaming has been massively deployed in telecom (not the case at the time of writing this dissertation).

If an attacker is able to determine the subscriber location, this information can be used as attack vector (first step) to exploit other vulnerabilities and execute other attacks like SMS interception, call interception, fraud, etc. Note that the attacks are normally performed using legitimate messages, therefore a detailed analysis as proposed in this dissertation is required.

This subchapter analyses a few messages and sequences received in an interconnection link of a MNO, which could be eventually used for a location tracking attack. The proposed methodology would support the dynamic evaluation of the risk in that link, in both scenarios 4G and 5G.

In 4G Roaming, a few messages have been classified as sensitive from security and privacy viewpoints, since they can bring a potential risk related to location tracking. Tab. 8.1-1 shows the list of those messages, extracted from annex A of [32].

Tab. 8.1-1: Diameter messages related to potential tracking attacks (extracted from Annex A of [32])

Diameter Command Code			**Interface**		**Direction**	
Command Name	*Abbr.*	*Code*	*Name*	*Application Identifier*	*Source*	*Destination*
Insert-Subscriber-Data-Request	IDR	319	S6a	16777251	HSS	MME
Insert-Subscriber-Data-Request	IDR	319	S6d	16777251	HSS	SGSN
Send-Routing-for-SM-Request	SRR	8388647	S6c	16777312	SMS-GMSC	HSS

Send-Routing-for-SM-Request	SRR	83886 47	S6c	16777312	SMS-GMSC	SMS Router
Send-Routing-for-SM-Request	SRR	83886 47	S6c	16777312	SMS Router	HSS
MO-Forward-Short-Message-Request	OFR	83886 45	SGd/Gdd	16777313	MME	SMS-IWMSC
MO-Forward-Short-Message-Request	OFR	83886 45	SGd/Gdd	16777313	SGSN	SMS-IWMSC
MO-Forward-Short-Message-Request	OFR	83886 45	SGd/Gdd	16777313	SMS-IWMSC	MTC-IWF
MT-Forward-Short-Message-Request	TFR	83886 46	SGd/Gdd	16777313	SMS-GMSC	MME
MT-Forward-Short-Message-Request	TFR	83886 46	SGd/Gdd	16777313	SMS-GMSC	SGSN
3GPP-Provide-Location-Request/Answer	PLR/PLA	83886 20	SLg	16777255		
3GPP-LCS-Routing-Info-Request/Answer	RIR/RIA	83886 22	3GPP SLh	16777291		
ProSe-Location-Update-Request	PLR/PLA	83886 73	3GPP PC6/PC7	16777340		
Reporting-Information-Request/Answer	RIR/RIA	83887 19	T6a/b, T7	16777346		

Given a data stream $x_1, x_2, \ldots, x_t, \ldots$ received in one of the interconnection links of the MNO, let's look at one single message x_t and apply the filters described in the expert knowledge analysis of the risk evaluation mechanism.

As described in the mathematical notation, x_t can be represented by certain attributes with security relevance:

$$x_t = \left(a_t^{(1)}, \ldots, a_t^{(d)}\right)$$

The following bullets describes how the proposed dynamic risk evaluation mechanism is applied stepwise to a data stream with theoretical messages and sequences that denote a location tracking use case. The ordering of the steps strictly follows the subchapters under subchapter 4.2 of the document, as well as the table 4.3-1 for the risk computation according to CVSS.

1) Origin based classification

$a_t^{(1)}: (MNC, MCC)\ data\ included\ in\ AVP\ 296$

$a_t^{(2)}: (MNC, MCC)\ data\ included\ in\ AVP\ 264$

Let's assume that the consistency check is successful: $a_t^{(1)} = a_t^{(2)}$, and that $\left\{a_t^{(1)}, a_t^{(2)}\right\} \in \{HMTO\}$

According to the criteria shown in table 4.3-1:

$CVSS_1 = 3\ (Low)$

2) Protocol conformance

Let's assume that no protocol incompliances have been found in x_t, i.e., $(p_{t,1} \dots p_{t,Q}) = (1\ 0\ \dots 0\ 0)$, Type 0.

Therefore, there is no increment of risk due to protocol conformance filtering.

$CVSS_2 = 0\ (None)$

3) Signaling application filtering

Be $a_t^{(3)}$ the attribute of x_t message that identifies the used application/interface. Let's take the following example:

$a_t^{(3)} = 16777251$ (S6a), $a_t^{(3)} \in AL$ (Allow list)

No increment of risk due to signaling application filtering.

$CVSS_3 = 0\ (None)$

4) GSMA message categorization

Be $a_t^{(4)}$ the attribute of x_t message that classify the message according to the GSMA categories (Cat 1, Cat 2, Cat 3). Let's take Insert-Subscriber-Data-Request (IDR) message as an example:

$a_t^{(4)} = (Insert - Subscriber - Data - Request\ (319), Request: Set) \rightarrow Cat\ 2$

There is no increment of risk due to GSMA message categorization, since it is a valid message in roaming-in scenarios.

$CVSS_4 = 0\ (None)$

5) Heuristics

5.1) Sensitivity information

The command mode IDR (319) contains a set of AVPs with high-sensitivity privacy information, namely:

$a_t^{(5)} = User - name\ (IMSI)$

$a_t^{(6)} = Subscription - Data$

$a_t^{(7)} = IDR - Flags$. In this example, let's assume that IDR Flag is set to 3, this implies that the location information from the subscriber is requested.

There is an increase in the risk factor due to the sensitivity of the information conveyed in the message.

$CVSS_{5.1} = 6.9\ (Medium)$

5.2) Inconsistencies

Let's assume that in the cross-checking of the MNO information (MCC, MNC) in the IMSI conveyed in the attribute $a_t^{(5)}$ (AVP: User-name) with the same information conveyed in $a_t^{(1)}$(AVP: Origin-Realm) fails, i.e., an inconsistency is found.

There is an increase in the risk factor due to the found inconsistency.

$CVSS_{5.2} = 5.5\ (Medium)$

5.3) Error messages

Not applicable in this scenario.

The second building block in the methodology is the analysis of security and privacy-sensitive (sub-) sequences. In this scenario, the focus is on those sequences related to geolocation of the subscriber. Let's assume that the analysis of sequences in the given data stream gives the following outcomes:

6.1) Valid known sequences

For sequence analysis in the data stream, as described earlier in the methodology, a preprocessing of the data is necessary. Typically, the analysis is performed over a sliding window, which we can denote as $\mathcal{W}$.

Let's take as an example a sequence corresponding to the short message mobile terminated (SM- FT) procedure as defined in 3GPP TS 29.338 [101]. Be Y a sequence pattern composed

of three messages with the following attributes identifying the Command Code of the SM-FT procedure:

$Y = (y_1, y_2, y_3)$

Where:

$y_1 = \left(a_1^{(1)}, \dots, a_1^{(d)}\right), a_1^{(4)} = (Send - Routing - for - SM - Request\ (8388647), Request: Set)$

$y_2 = \left(a_2^{(1)}, \dots, a_2^{(d)}\right), a_2^{(4)} = (Send - Routing - for - SM - Request\ (8388647), Request: Clear)$

$y_3 = \left(a_3^{(1)}, \dots, a_3^{(d)}\right), a_3^{(4)} = (MT - Forward - Short - Message - Request\ (8388646), Request: Set)$

The sequence is obviously valid but implies the fetching of the IMSI of the subscriber and the identity of the serving nodes with which the user is registered, i.e., an approximate location of the subscriber. Any of the techniques and algorithms mentioned in section 4.2.3.2 can be used to mine the sequence pattern Y over $\mathcal{W}$ across the entire data stream. When Y is found, the risk factor is modified as follows:

$CVSS_{6.1} = 3.9\ (Low)$

6.2) Rare “suspicious” known sequences

An attacker might have compromised an application server (e.g., MME) in IPX network and generated messages towards, for example, HSS over theoretically internal interfaces, which have been classified as Category 1 messages. This type of messages should be filtered accordingly to the operator roaming agreements before reaching their destination in HPLMN, but the DEA or signaling firewall may fail, and a basic message sequence of messages may disclose the subscriber location. Example: User_Data_Request/Answer (UDR/UDA) messages over Sh interface.

Be U a sequence pattern composed of two messages with the following attributes identifying the Command Code used between an IMS application server and the HSS to fetch several data such as location.

$U = (u_1, u_2)$

Where:

$u_1 = \left(a_1^{(1)}, \dots, a_1^{(d)}\right), a_1^{(4)} = (3GPP - User - Data - Request\ (306), Request: Set).$

Data-Reference AVP (703) may be considered as an attribute to evaluate in our mechanism (section 4.2.2), since when takes the value (14) it contains LocationInformation.

$a_1^{(j)} = 14\ (Data - Reference)$, where j identifies the attribute carrying Data-Reference AVP.

$u_2 = \left(a_2^{(1)}, \dots, a_2^{(d)}\right), a_2^{(4)} = (3GPP - User - Data - Request\ (306), Request: Clear)$

User-Data-Sh AVP (702) may be considered as an attribute to evaluate as well in our methodology, since it contains data requested in operations like UDR including LocationInformation (tracking area identity, cell identity, etc.).

$a_2^{(k)} = [octetstring]\ (Sh\ Data)$, where k identifies the attribute carrying User-Data-Sh AVP.

If the sequence pattern U is found in interconnection links on which there is not an explicit agreement to accept those messages, the risk posed by that sequence is critical. Any of the techniques and algorithms mentioned in section 4.2.3.2 can be used to mine the sequence pattern U over $\mathcal{W}$ across the entire data stream. When U is found, the risk factor is modified as follows:

$CVSS_{6.2} = 9.2\ (Critical)$

Other examples of sequence patterns, including Category 1 messages and related to privacy/location potential issues, include the Command Codes of Subscriber-Information-Request (SIR) and Subscriber-Information-Answer (SIA). Puzankov [25] published a sequence pattern in SS7 using silent Unstructured Supplementary Service Data (USSD) intended to track the location of a particular IMSI. In Diameter, the same use case can be easily mounted by sending a silent SMS. Thus, if in the same time window, a sequence pattern consisting of a message that pulled the location of a user, followed by a message to forward a silent SMS (returns error), and again the message to pull the location, is found, the risk factor in the signaling link posed by that sequence is critical and needs to be corrected accordingly.

7) Anomalies, outliers

As described in section 4.2.3.2, algorithms like ADWIN2 support the detection of anomalies and outliers in the normal distribution of messages.

In a more deterministic manner, based on expert knowledge, certain rules can be established that are intended to detect anomalies or suspicious activities. For example, if the number of Send-Routing-for-SM-Request (SRR) messages received in the interconnection link from a particular operator exceeds by far the number of MT-Forward-Short-Message-Request (MT-FSM) messages, it might be caused by IMSI scanning activities. The rule can be captured as follows:

$If\ |\sum_{i=1}^{N}\delta\left(a_i^{(4)}=(8388647,1)\right)-\sum_{i=1}^{N}\delta\left(a_i^{(4)}=(8388646,1)\right)|\ \gg\ \varepsilon\ ,then\ CVSS_7=2.7\ (Low)$,

where $N=|\mathcal{W}|$, i.e., the size of the window, and ε the threshold of detection of the anomaly.

8) #critical messages ≥ threshold

Count-min sketch algorithm, as described in section 4.2.3.3, can be used for example to approximate the frequency count of messages related to location data and listed in table 8.1-1. If the outcome surpasses a preestablished threshold, the risk factor in the link will be impacted as indicated in table 4.3-1.

Be $\widehat{f_y}$ the estimated frequency overall count of messages listed in Table 4.3-1,

$If\ \widehat{f_y}\ \geq threshold\ (t.b.d),then\ CVSS_8=6.9\ (Medium)$

8.2 Application of the risk evaluation mechanism using Real Data in Interconnection

In this subchapter, the proposed mechanism in Chapter 4 has been applied to an anonymized trace of real Diameter signaling traffic in 4G Roaming between two mobile operators in an Asia geographical area, each of them connected to IPX network through a different IPX provider.

The mechanism can be implemented in a Security analytics platform, assuming that the DEA of the Home PLMN sends to that platform a copy of all the messages it handles in their interfaces, namely the external interface towards its IPX provider and the internal interfaces towards the signaling firewall and DRA. DRA in HPLMN acts as a diameter routing agent for the network elements involved in the roaming interconnection. The overall end-to-end network diagram under analysis is represented in Fig. 8.2-1.

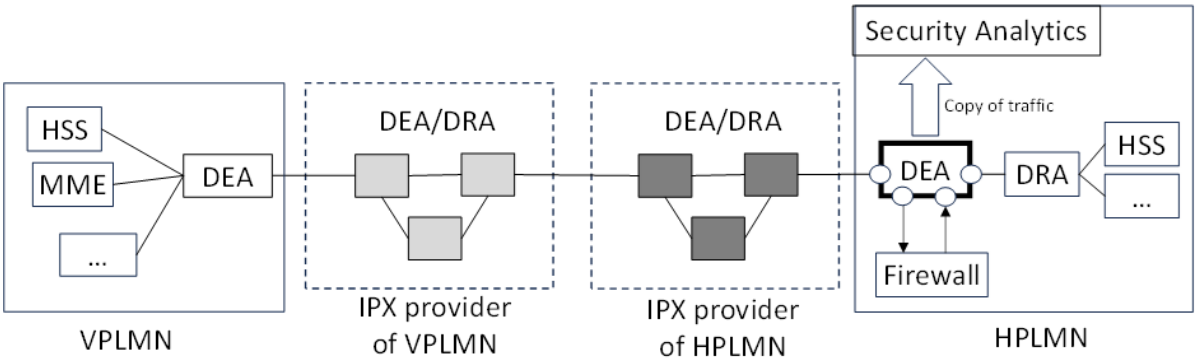

Fig. 8.2-1: Network diagram of interconnection

The following table Tab. 8.2-1 represents an extraction (.csv format) of selected fields of the diameter trace taken in a pcap file. Tshark [102] tool has been used for that purpose since it provides good capabilities for dissecting the Diameter protocol. For example, one of the commands used in my analysis was:

>> tshark -r input_file.pcap -Y diameter -T fields -e frame.time_epoch -e ip.src -e ip.dst -e diameter.cmd.code -e diameter.flags -e diameter.applicationId -e diameter.Origin-Host -e diameter.Origin-Realm -e diameter.Visited-PLMN-Id -e diameter.User-Name -e diameter.Subscription-Data -e diameter.endtoendid -E header=y -E separator=, > output.csv

Please note that all data presented in this dissertation has been conveniently anonymized.

Tab. 8.2-1: SELECTED FIELDS EXTRACTED FROM DIAMETER TRACE UNDER ANALYSIS

	Time	CC	flags	App ID	diameter.Origin-Host	diameter.Origin-Realm	VPLMN-Id	IMSI	Subs. Data	MSISDN	endtoendid	$CVSS_{5.1}$
x_1	dd/mm/yyyy hh:21:37 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x1004df99	6.9
x_2	dd/mm/yyyy hh:21:37 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x1004df99	6.9
x_3	dd/mm/yyyy hh:21:37 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x1004df99	6.9
x_4	dd/mm/yyyy hh:21:37 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x1004df99	6.9
x_5	dd/mm/yyyy hh:21:37 AM	316	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x1004df99	6.9
x_6	dd/mm/yyyy hh:21:37 AM	316	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x1004df99	6.9
x_7	dd/mm/yyyy hh:21:37 AM	316	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x1004df99	6.9
x_8	dd/mm/yyyy hh:22:43 AM	316	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456780			0x5431460e	6.9
x_9	dd/mm/yyyy hh:22:43 AM	316	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456780			0x5431460e	6.9
x_{10}	dd/mm/yyyy hh:22:43 AM	316	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456780			0x5431460e	6.9
x_{11}	dd/mm/yyyy hh:22:43 AM	316	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456780			0x5431460e	6.9
x_{12}	dd/mm/yyyy hh:22:43 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111444555	0x5431460e	6.9
x_{13}	dd/mm/yyyy hh:22:43 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111444555	0x5431460e	6.9
x_{14}	dd/mm/yyyy hh:22:43 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111444555	0x5431460e	6.9
x_{15}	dd/mm/yyyy hh:22:46 AM	323	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g		888777123456780			0x84534899	6.9
x_{16}	dd/mm/yyyy hh:22:46 AM	323	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g		888777123456780			0x84534899	6.9
x_{17}	dd/mm/yyyy hh:22:46 AM	323	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g		888777123456780			0x84534899	6.9
x_{18}	dd/mm/yyyy hh:22:46 AM	323	0xc0	16777251	mme2.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g		888777123456780			0x84534899	6.9
x_{19}	dd/mm/yyyy hh:22:47 AM	323	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g					0x84534899	0
x_{20}	dd/mm/yyyy hh:22:47 AM	323	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g					0x84534899	0
x_{21}	dd/mm/yyyy hh:22:47 AM	323	0x40	16777251	hss1.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g					0x84534899	0
x_{22}	dd/mm/yyyy hh:26:03 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x90aa8211	6.9
x_{23}	dd/mm/yyyy hh:26:03 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x90aa8211	6.9
x_{24}	dd/mm/yyyy hh:26:03 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x90aa8211	6.9
x_{25}	dd/mm/yyyy hh:26:03 AM	316	0xc0	16777251	mme1.epc.mnc333.mcc444.3	epc.mnc333.mcc444.3g	(011,111)	888777123456789			0x90aa8211	6.9
x_{26}	dd/mm/yyyy hh:26:04 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x90aa8211	6.9
x_{27}	dd/mm/yyyy hh:26:04 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x90aa8211	6.9
x_{28}	dd/mm/yyyy hh:26:04 AM	316	0x40	16777251	hss2.epc.mnc777.mcc888.3g	epc.mnc777.mcc888.3g			00000681c0	1111222333	0x90aa8211	6.9

Note that the Visited-PLMN-Id is of type OctetString, and the encoding format is specified in table 7.3.9-1 of [69]. For clarity, MCC and MNC values have been accordingly decoded for the analysis.

The entire data set X under analysis consists only of 28 messages ($x_i, i \in \{1..N\}, N = 28$). In a real scenario, as described in the introduction, N might be in the range of millions of messages per day.

For simplicity and abusing of the notation in section 4.2.1, let's assume that the data set X also represents a temporal sequence of messages, such as $X = (x_t)_{t \in N}$, where x_t arrives sequentially at the time t.

Each message is characterized by several security attributes. In our analysis of the provided data set, only a very limited set of attributes have been selected, intended to show how the mechanism works in this scenario. Each attribute corresponds to certain values included in the fields of the trace and extracted in the columns of table 8.2-1, i.e., for a message x_i:

$a_i^{(1)}$: MNC and MCC included in Origin-Realm (AVP 296).

Sample: x_1 (epc.mnc**333**.mcc**444**.3gppnetwork.org) → $a_1^{(1)} = (333,444)$

$a_i^{(2)}$: MNC and MCC included in Origin-Host (AVP 264).

Sample: x_1 (mme1.epc.mnc**333**.mcc**444**.3gppnetwork.org) → $a_1^{(2)} = (333,444)$

$a_i^{(3)}$: MNC and MCC included in Visited-PLMN-ID (AVP 1407).

Sample: x_1 → $a_1^{(3)} = (011,111)$

$a_i^{(4)}$: Interface used in Roaming, in Diameter described in ApplicationId field of the message.

Sample: x_1 → $a_1^{(4)} = (16777251)$, it corresponds in 3GPP to S6a/S6d interfaces.

$a_i^{(5)}$: Categorization of the message according to GSMA, in Diameter described in the Command Code (CC) field of the message, and 'R' bit in the Command Flags field (0xc0=Request: Set, 0x40=Request: Not set) of the Diameter header.

Sample: x_1 → $a_1^{(5)} = (316, 0xc0)$, it corresponds in 3GPP to the Update-Location-Request (ULR) message (category 3 according to GSMA classification).

$a_i^{(6)}$: Identifier of the user in MNO network (non-public), in Diameter User-Name (AVP 1), which typically contains the IMSI of the user.

Sample: x_1 → $a_1^{(6)} = (888777123456789)$, it corresponds to the IMSI of the user for whom the ULR message has been sent from VPLMN to HPLMN.

$a_i^{(7)}$: Subscription-related data of the user, in Diameter Subscription-Data (AVP 1400), which may contain a lot of information about the user, encapsulated in multiple AVPs, as specified in clause 7.3.2 of [69]. The overall subscription data can be tagged as sensitive data. Nevertheless, a more granular per embedded AVP can be done, e.g., LCS-info (AVP 1473), which provides the location of the user, MSISDN, etc.

For simplicity reasons, this attribute has not been further disaggregated or alternatively split into several attributes as per embedded AVP. The entire AVP can be taken for security analysis in hexadecimal format, and subsequently, specific values of embedded AVPs of interest can be extracted with the support of tools like Tshark or Python libraries like pycrate.

Sample: x_5 → $a_5^{(7)} = (00000681c0000010000 \ldots.)$, it corresponds to the hexadecimal value of the AVP 1400, present in the message x_5 (Update-Location Answer).

$a_i^{(8)}$: Public identifier of the user, i.e., MSISDN (AVP 701).

Sample: x_5 → $a_5^{(8)} = (1111222333)$, it corresponds to the MSISDN of the user present in the message x_5 (Update-Location Answer).

$a_i^{(9)}$: Diameter End-to-End Identifier. It is used by the diameter protocol to detect multiple messages. It must not be modified by Diameter agents, so it remains the same in the entire sequence of messages from the original request to the final provided answer.

Sample: $x_1 \rightarrow a_1^{(9)} = (1004df99)$

Other multiple attributes can be defined to characterize the message, even at other layers as IP (e.g., source/destination IP addresses).

The mechanism for dynamic evaluation of the risk relies on two threads running in parallel:

- Thread 1: Message analysis supported by expert knowledge.
- Thread 2: Online sequences security analysis on data streams

The Thread 1 consists of the following tasks:

1) Origin based classification

The consistency checks on PLMN Ids values in Origin-Realm and Origin-Host AVPs are positive, i.e., $\forall i, i \in \{1..N\}, N = no.of\ messages\ in\ data\ set, a_i^{(1)} = a_i^{(2)}$.

However, certain messages (in our sample ULR messages) include a different PLMN Id in the Visited-PLMN-Id AVP, i.e., $for\ x_i \mid a_i^{(5)} = (316, 0xc0), a_i^{(1)} = a_i^{(2)} \neq a_i^{(3)}$. I.e., the signaling messages arriving at the home network come from an IPX intermediary (MNC 333, MCC 444) and not from the original source of the message (MNC 011, MCC 111), which in the case of ULR is the VPLMN hosting the MME node (requestor of location update).

The interest in the origin of the message obviously comes from the messages coming from outside of the HPLMN, where the security analytics is performed. It is assumed that, while the IPX provider, identified by $a^{(1)}$ and $a^{(2)}$ attributes, corresponds indeed to an IPX provider with whom the HPLMN has a contract of interconnection (SLA); $a^{(3)} \in \{HMTO\}$, i.e., there is a roaming agreement between HPLMN and VPLMN through IPX provider(s).

According to the proposed risk evaluation mechanism described in Chapter 4, the associated risk for the messages exchanged in this link due to origin-based classification criteria is:

$CVSS_1 = 3\ (Low)$

2) Protocol Conformance

No protocol incompliances have been found in the provided data set.

$CVSS_2 = 0\ (None)$

3) Signaling application filtering

$\forall i \in \{1..N\}, a_i^{(4)} = 16777251$ (S6a/S6d) $\Rightarrow\ a_i^{(4)} \in\ AL$ (Allow List)

S6a/S6d interface is generally used for roaming purposes according to specifications. Thus, there is no increment of risk due to that filtering.

$CVSS_3 = 0\ (None)$

4) GSMA message categorization

There are only two different types of messages in the data set:

- Update Location ($a_i^{(5)} = (316, 0\text{xc0}\ or\ 0\text{x40})$)
- Notify ($a_i^{(5)} = (323, 0\text{xc0}\ or\ 0\text{x40})$)

Both messages belong to Category 3 of GSMA, i.e., messages corresponding to the signaling exchanged between HPLMN and VPLMN for outbound roamers, thus no impact on the risk due to the categorization.

$CVSS_4 = 0\ (None)$

5) Heuristics

5.1) Sensitive Information Elements

Three types of sensitivity information are evaluated:

- MNO user identifier (IMSI) ($a_i^{(6)}$)
- Subscriber data ($a_i^{(7)}$)
- Public use identifier (MSISDN) ($a_i^{(8)}$)

Accordingly, the CVSS score has been added per message in the last column of Tab. 8.2-1, taken from Tab. 4.3-1 as a baseline.

5.2) Inconsistencies

No inconsistencies were found in the messages of the provided data set.

$CVSS_{5.2} = 0\ (None)$

5.3) Error messages

Not applicable in this 4G scenario.

The Thread 2 consists of the following tasks:

1) Streaming data preprocessing

Examining the architecture in detail, as I depict in Fig. 8.2-2, we observe that every "Request" type of message (e.g., ULR) would typically generate six messages to be managed in the DEA before an "Answer" can be sent to the roaming partner operator. Fig. 8.2-2 shows the example of an Update-Location-Request (ULR) for an IMSI denoted as $IMSI - A$.

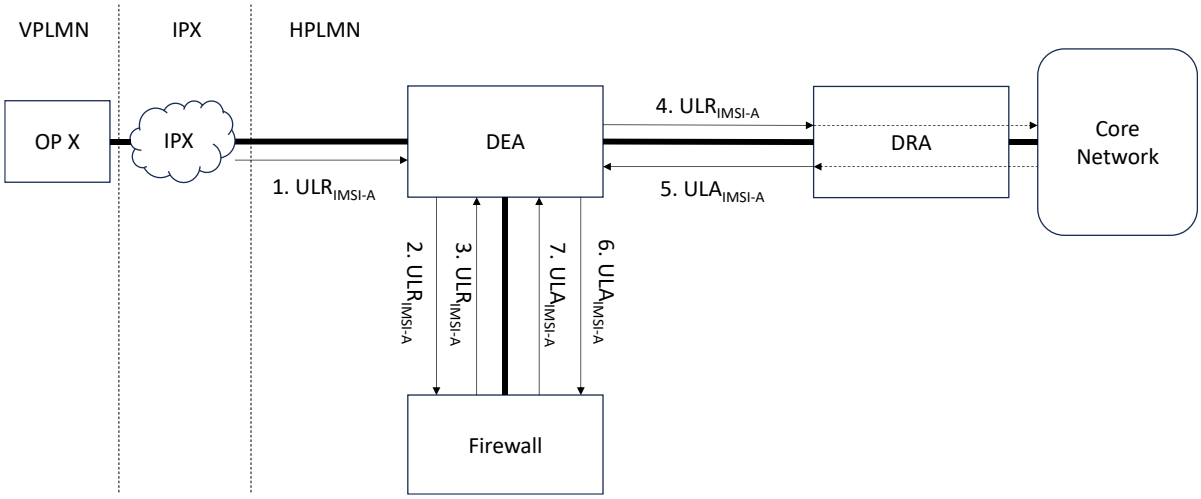

Fig. 8.2-2: Architecture and example of generated messages as per one incoming ULR

Without applying any pre-processing technique (e.g., data reduction, sliding windows…) in the received data for security analytics, subsequences of 7 messages can be easily discovered, corresponding to the same command code ($a_i^{(5)}(1)$) and the same user identifier ($a_i^{(6)}, a_i^{(8)}$). Alike a sequence pattern of signaling messages per command code can be defined as a tuple of seven items. For example, a sequence pattern $U(\subset X)$ of Update-Location (category 3) messages:

$$U = (u_1 \dots u_n), n = 7, \forall i \in \{1,2, \dots, n\}, a_{u_i}^{(5)} = 316$$

It is straightforward to select a sequence-based sliding window model, defined in terms of the number of observations with a fixed size, i.e., $|\mathcal{W}| = 7, or\ |\mathcal{W}| = 7n$.

If the signaling firewall lets the message pass through, i.e., the message is not blocked or modified by any policy after being processed, the subsequence of messages provides redundant information intended to calculate the risk. A custom sampling conditional algorithm can be easily applied, which, for example, discards the messages sent and received to/from the firewall in the DEA if there is not a security log generated by the firewall alerting of a security event. Thus, the subsequences could be optimized to two or three messages for further processing.

2) Data mining

As explained in subchapter 4.2.3.2, the application of data mining techniques is intended to:

- Detect known security-sensitive sequences.
- Detect rare non-predetermined sequences.
- Make a statistical analysis of messages.

The next sub-clauses show a simple implementation of the proposed mechanism, limited to the very short amount of data available for the experiment.

2.1) Detect known security-sensitive sequences

There are multiple security-sensitive sequences exchanged in roaming, for example, the sequence of two messages to update location information in the HSS, i.e., ULR (Update-Location-Request) and ULA (Update-Location-Answer).

An Update-Location-Request coming into the roaming interface from the MME in the VPLMN, if not blocked by the firewall, will be followed by an Update-Location-Answer from the HPLMN HSS. The sequence pattern that we want to find in the data stream can be reduced to two messages:

$$update\_location\_sequence = (u_1, u_2)$$

The following specific attribute values characterize the messages of the $update\ location$ sequence pattern, to be mined in the data stream and corresponding to the signaling with a specific VPLMN:

$$u_1 = \begin{Bmatrix} a_1^{(3)}: \text{Identity of the VPLMN, i. e., } (011{,}111) \\ a_1^{(4)}: \text{Interface in roaming. S6a } (16777251) \\ a_1^{(5)}: \text{Command Code. For ULR: } (316, 0\text{xc0}) \\ others\ e.g., source\ IP\ address \end{Bmatrix}$$

$$u_2 = \left\{ \begin{matrix} a_1^{(1)}\text{: Origin Realm, i. e. , identifier of HPLMN (777,888)} \\ a_1^{(4)}\text{: Interface in roaming. S6a (16777251)} \\ a_1^{(5)}\text{: Command Code. For ULA: (316, 0x40)} \\ others\ e.g.,source\ IP\ address \end{matrix} \right\}$$

Pre-condition: The End-to-End identifier diameter attribute correlates the two messages of the sequence for a given user identifier (e.g., IMSI), i.e., $a_1^{(9)} = a_2^{(9)}$.

Using a sliding window (e.g., $|\mathcal{W}| = 7$), and applying a sequence pattern mining algorithm, we can efficiently scan the data stream and match the messages attributes against the predefined sequence pattern, i.e., by comparing the specific attributes defined for each message in the pattern with the corresponding attributes in the data stream messages, in this case corresponding to Update Location use case.

Note that typically, in the context of sliding window pattern matching, the length of the sliding window is set to the same length as the sequence pattern, basically looking to match the entire sequence of messages. However, in our scenario, we aim to find the pattern in subsets of the stream where additional information is present but not relevant to the pattern matching, e.g., the messages exchanged with the firewall.

The above-defined sequence pattern ($update\_location\_sequence$) has been found three times in the following subsequences extracted from the given dataset:

$(x_1, x_5), (x_8, x_{12}), (x_{22}, x_{26})$

The subsequences are valid, and the risk factor is modified per found subsequence as indicated in subchapter 3.3:

$CVSS_{6.1} = 3.9\ (Low)$

2.2) Detect rare non-predetermined sequences

The short amount of data under analysis in this experiment is obviously insufficient to obtain meaningful results by applying any type of anomaly detector or similar algorithm.

Nevertheless, the very first glance at the messages of the data stream reveals that in less than 5 minutes there are two Location-Update-Request messages on the same IMSI. Depending on the thresholds pre-established or discovered to determine rare sequences, a repetitive security-

sensitive message like ULR in certain interval might be considered a suspicious behavior of the VPLMN aiming to track the user.

2.3) Statistical analysis of messages

The **count-min sketch** algorithm, as described in section 4.2.3.3, can be used to approximate the frequency of items in a stream of data, in this case, the count of sensitive messages (e.g., Update-Location-Requests) or messages containing privacy user information like IMSI. If the outcomes surpass certain preestablished thresholds, the risk factor in the link will be impacted accordingly, as described in Tab. 4.3-1.

The short amount of data under analysis in this experiment makes the statistical analysis trivial. Nevertheless, it is still possible to run the algorithm using the available data. There are multiple available implementations of the algorithm in Python libraries, specifically designed for Count-Min Sketch operations. The only design parameters to be set are the width and depth to control the accuracy and memory usage (given the short amount of data, those parameters won't influence the results).

Be $\widehat{f_{ULR}}$ the estimated frequency overall count of ULR messages; and be $\widehat{f_{IMSI}}$ the estimated frequency overall count of messages that includes the IMSI parameter as an information element, the risk can be impacted as follows:

$If\ \widehat{f_{ULR}}\ \geq threshold\ (to\ be\ defined), then\ CVSS_8 = 6.9\ (Medium).$

$If\ \widehat{f_{IMSI}}\ \geq threshold\ (to\ be\ defined), then\ CVSS_8 = 6.9\ (Medium).$

8.3 Enhancing standardized 5G Analytics framework for determining the trust indication

In the Fig. 8.3-1 I present the enhancement proposal for the 5G 3GPP standardized Analytics framework with the target of determining the trust indication of a given target entity and illustrates the deployment option 1 described in subchapter 5.2 (similarly options 2 and 3 are applicable). The example relies on the NWDAF capabilities for data collection and analytics derivation, and it is extended further to accommodate the trust indication derivation.

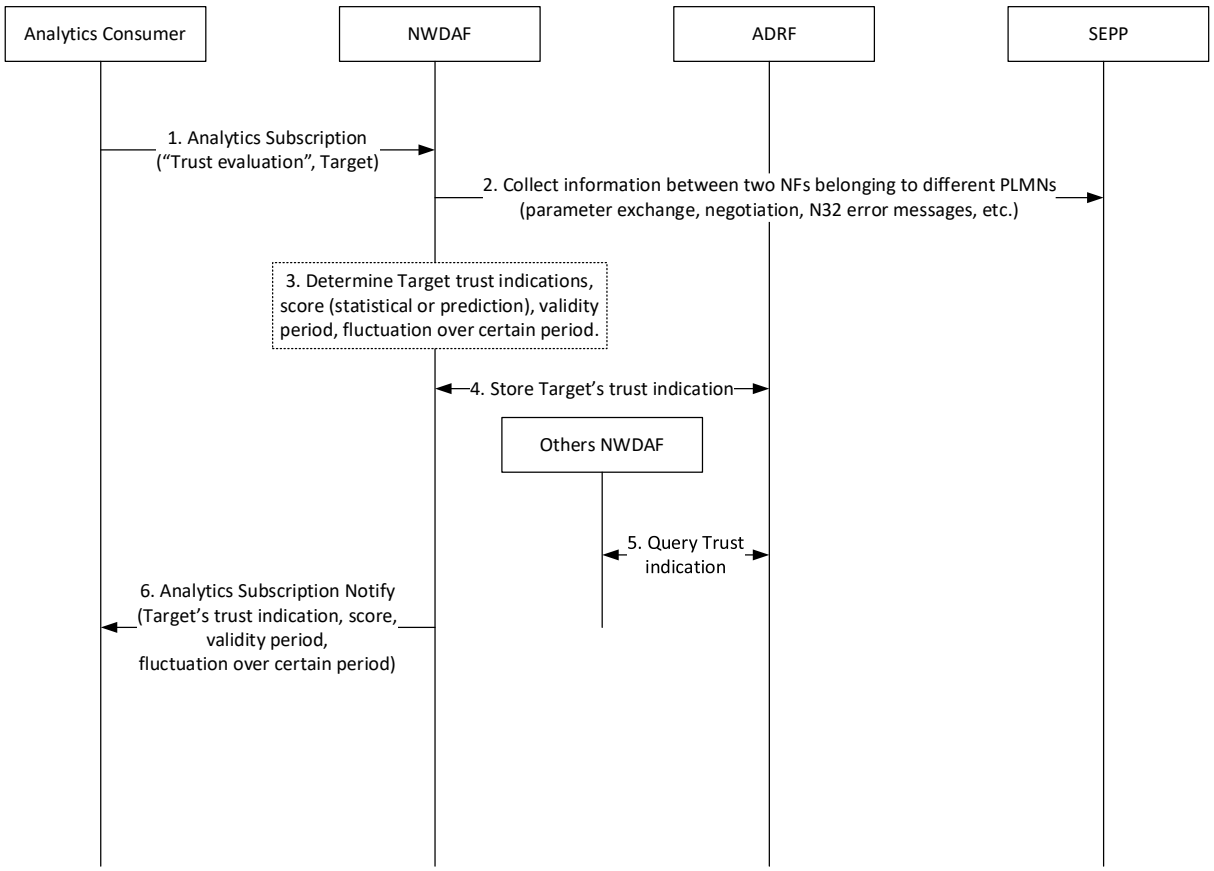

Fig. 8.3-1: Procedure for determining the trust indication of a given target, e.g., PLMN

Step 1: An Analytics Consumer, e.g., OAM entity, may subscribe to a novel analytic type, defined for example by an analytics identifier "Trust evaluation", by providing the information of the desired target of the analytics, in this context of Roaming it could be the V-PLMN ID.

Step 2: The NWDAF collects the data needed for performing the requested analytics. In the case of VPLMN trust evaluation, the NWDAF will collect the relevant data from SEPP. Such data may comprise full copy of the signaling traffic, or extracted preprocessed information by

the SEPP on discarded malformed N32 messages, messages mismatches (e.g., Category 1 non allowed by SLA messages), etc.

Step 3: The NWDAF determines the trust score, and further complementary information related to the trust indication, e.g., validity period, trust fluctuation, etc. The Security Analytics building block of the overall schema represented in Fig. 3.2-1 can be implemented in the NWDAF. It would be also possible in a particular implementation to dedicate a NWDAF entity just for security purposes in signaling interconnection.

Step 4: The outcome of NWDAF analytics, i.e., the trust indication of a target entity in this case is stored in ADRF (Analytical Data Repository Function). The ADRF offers services that enable a consumer to store and retrieve data and analytics.

Step 5: Other NWDAF can directly query the ADRF in order to retrieve the trust indication of the target entity (in this case VPLMN).

Step 6: The NWDAF notifies the Analytics Consumer, e.g., OAM or PCF, about the derived trust indication of the target entity.

The trust indication of a given target (e.g., VPLMN) can be utilized by multiple consumers. In Chapter 7, it is proposed that the Policy Control Function (PCF) be that consumer, and acts as Policy Decision Point to establish security policies to be enforced in this environment in the interconnection gateways such as the SEPP or signaling firewalls.

8.4 Implementation of 5G security profiles in standards

The concept introduced in patent US 12,192,208 B2 [12] has been accepted in standardization and implemented in the following specifications: 3GPP TS 33.501 (stage 2) and 3GPP TS 29.573 (stage 3). Basically, 3GPP has enabled the option to announce and communicate the profiles, whereas the definition of the profiles itself is being done by the industry in GSMA (NG.113 [2]).

In the following paragraphs, the text introduced in the corresponding standards, based on the concept developed as part of this dissertation, has been highlighted by highlighting it in grey.

3GPP TS 33.501 [1]:

The following clause was enhanced:

clause 13.2.2.2 "Procedure for Key agreement and Parameter exchange"

"…2. The two SEPPs may perform the following exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store protection policies sent by the peer SEPP.
2a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP's Data-type encryption policies, as described in clause 13.2.3.2, and Modification policies, as described in clause 13.2.3.4.
2b. The responding SEPP shall store the policies if sent by the initiating SEPP.
2c. The responding SEPP shall send a Security Parameter Negotiation Response message to the initiating SEPP with the responding SEPP's suite of protection policies.
2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP.
Alternatively to exchanging complete policies in steps 2a and 2c, the SEPPs may indicate a security profile.
NOTE: A security profile can for example include default modification policies and default data_type encryption policies and/or a list of IEs to be protected, during the N32-c negotiation process. PRINS security profile specification is out of scope in 3GPP…"

3GPP TS 29.573 [59]:

The following clauses were enhanced:

- clause 5.2.3.3 “Parameter Exchange Procedure for Protection Policy Exchange”

- clause 6.1.5.2.4 “Type: SecParamExchReqData”

- clause 6.1.5.2.5 “Type: SecParamExchRspData”

- clause 6.1.7 “Feature Negotiation”

The relevant text of those clauses is hereby attached for the purpose of highlighting the feature in the stage 3 specification of 3GPP:

“…The procedure is described in Figure 5.2.3.3-1 below.

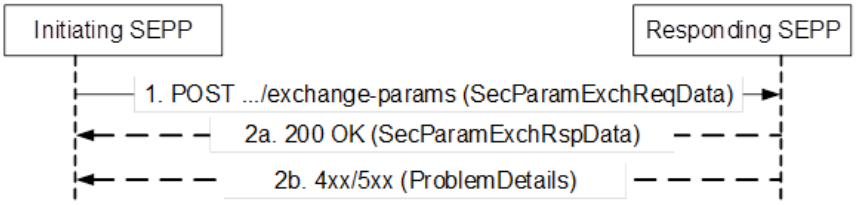

Figure 5.2.3.3-1: Parameter Exchange Procedure for Protection Policy Exchange

… Alternatively, if both the initiating SEPP and the responding SEPP support the PSEPRO feature (PRINS Security Profiles Support, see clause 6.1.7), the initiating SEPP may include a candidate list of security profiles instead of Protection policy information in the parameter exchange request message towards the responding SEPP.

NOTE 1: The definition of security profiles is out of scope of 3GPP….”

“…

Table 6.1.5.2.4-1: Definition of type SecParamExchReqData

Attribute name	Data type	P	Cardinality	Description	Applicability
secProfiles	array(string)	C	1..N	Either this IE or the protectionPolicyInfo IE shall be present during the parameter exchange procedure for protection policy exchange(see clause 5.2.3.3). When present, this IE shall indicate the candidate list of security profiles that the initiating SEPP is supporting for PRINS. The list may contain up to 256 profiles.	PSEPRO

…”

“…

Table 6.1.5.2.5-1: Definition of type SecParamExchRspData

Attribute name	Data type	P	Cardinality	Description	Applicability
selSecProfiles	*array(string)*	*C*	*1..N*	*This IE shall indicate the list of selected security profiles applicable for messages forwarding over N32-f if the initiating SEPP sent a candidate list of security profiles in the exchange parameter request message to the responding SEPP. The list may contain up to 256 profiles.*	*PSEPRO*

…"

"…

Table 6.1.7-1: Features of supportedFeatures attribute used by N32 Handshake service

Feature Number	Feature	M/O	Description
2	*PSEPRO*	*O*	*PRINS Security Profiles Support* *A SEPP that supports this feature shall support the negotiation of security profiles as specified in clause 5.2.3.3.*

…"

GSMA NG.113 [2]:

Annex F of NG.113 [2] was recently introduced to provide some guidelines on the implementation of security profiles. It starts with the motivation of the mechanism intended to make the task of negotiating security policies (encryption and modification) at IE granular level operationally manageable, noting that there are a few thousands of IEs being used in the RESTful APIs used in the mentioned 5G roaming interfaces.

The task of GSMA is to provide a set of IE security policy templates, i.e., security profiles, that support the implementation of PRINS in MNOs. I.e., with a standardized (and limited) set of IE protection policy templates defined by GSMA, MNO and its roaming partners would only need to negotiate which template to use instead of each individual IE policy.

Nevertheless, those templates are just possible implementations. MNOs could certainly decide on creating their own templates according to their security policies, provided that they are well communicated and supported by the roaming peers and eventually Roaming intermediaries. Each security profile implemented by a predefined security templates contains a list of IEs to be encrypted, and a list of IEs that can be modified by Roaming intermediaries by adding the signed patches as explained above.

As mentioned in section 4.2.2.5.1, 3GPP in TS 29.573 (clause 6.1.5.3.5) [59] lists seven IE data types for "Protection" policy: UEID, LOCATION, KEY_MATERIAL,

AUTHENTICATION_MATERIAL, AUTHORIZATION_TOKEN, OTHER, NONSENSITIVE. Even if defined in the ALS context, they can easily be generalized as "security data types". LOCATION may further be divided into deeper levels of granularities, e.g., country / state / operator level; city / TAC / LAC level; cell / gNodeB level; longitude / latitude. Annex F of [2] includes a reference table with 5 different profiles based on the 3GPP security data type classification, added here in Tab. 8.4-1 for illustration of the work generated by the industry out of our security profile concept.

Tab. 8.4-1: GSMA Security profiles (extracted from [2])

Security profile	Profile A	Profile B	Profile C	Profile D	Profile E
UEID (Data of the type 'SUPI')	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
LOCATION (location data)	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
KEY_MATERIAL (cryptographic material)	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
AUTHENTICATION_MATERIAL (authentication vector)	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
AUTHORISATION_TOKEN	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
OTHER	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
NONSENSITIVE	clear non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable

From the security profiles the SEPP knows the IE data types that need encryption, and which are modifiable. Since the same IE may appear in several categories, there could be conflicting policies, e.g.:

- 'supi' is in UEID with policy 'clear'
- 'supi' is also in 'authz' (AUTHENTICATION_MATERIAL) with policy 'encrypted'

For that reason, the SEPP needs to identify (per API) the IEs, in which the IE Data Type is used.

8.5 Automated security enforcement applied to interconnection

The concept of security enforcement by using the 5G Policy Control framework explained in Chapter 7, is perfectly applicable to interconnection at control (N32) and user planes (N9).

Certainly, there should be consistency in UE-level security policies when the user moves from one MNO to another, although it is also highly possible that security services are not updated frequently on a per UE basis. Hence, MNOs would need to share upfront security policies and some level of subscriber information [103]. Currently, the security policies established between peers are configured statically and locally based on contractual SLAs, whereas the new 5G services create a very dynamic and unpredictable environment that requires a new security framework.

Fig. 8.5-1 depicts (in blue) the proposal of expansion of the standardized Policy Control framework illustrated in Fig. 7.2-1 in chapter 7 to cover the proposal for *security enforcement in the interconnection*.

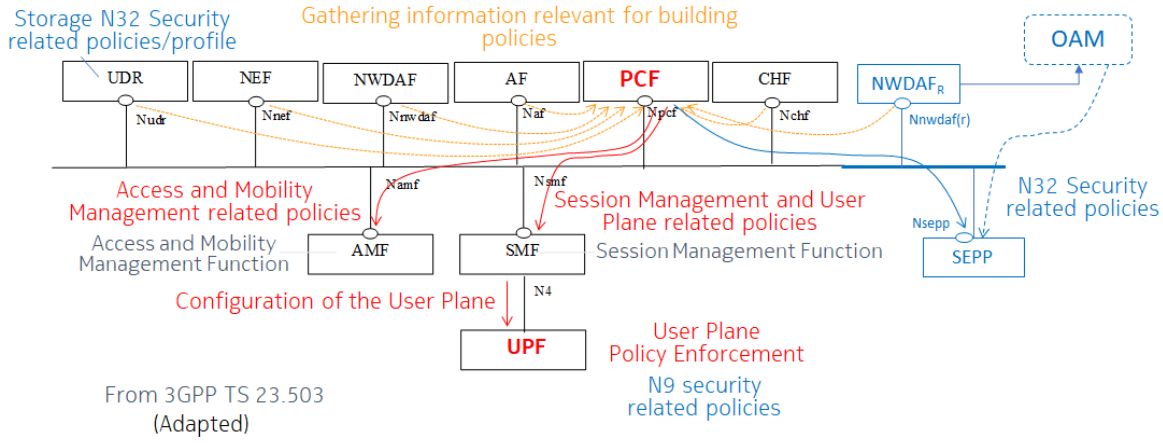

Fig. 8.5-1: Expansion of Policy Control framework to Security in interconnection (adapted from 3GPP TS 23.503 [56])

The expansion of the Policy Control framework consists of:

- Specialized security analytics for signaling traffic in interconnection/roaming. It is proposed that this functionality be implemented in a dedicated analytics network entity, represented in the schema as NWDAF$_R$. This new entity could perform the functionalities described in previous chapters of the dissertation, i.e., the dynamic computation of the risk per MNO, as well as the trust score. This new entity would communicate with PCF as any other NWDAF via N23 interface.

- New interface (N#) between PCF and SEPP. The implementation of a new interface might be done in two ways:
    - Via a SBI control plane interface. This approach would require the definition of new SBA services in SEPP, through which the PCF would configure the security policies to be applied in the N32 interface.
    - Via OAM (Operations, Administration, and Maintenance) interface or configuration in the SEPP.

  The SBI approach would require the definition of the API by standardization (3GPP). Even though OAM approach would be a less dynamic approach than the previous one based on SBI, it could be a good enough for certain scenarios.

- Definition and storage of N32 security policies/profiles. Fig. 8.5-1 shows that those security policies can be stored, and consequently fetched by the PCF, in UDR as well as in OAM system. Both approaches are valid.

The same concept is applicable to the security mechanisms applied to N9 for certain use cases such as the UP interconnection with another operator. In this context GTP inspection or IPSec [22] are already standardized, but not the enforcement via PCF as part of a 'Security' SLA. The enforcement could create a new IPSec tunnel or allocate the PDU to an existing IPSec tunnel.

Note that the use of cryptographic solutions in N9 interface is an operator's decision. These types of solutions in the near future could be selectively deployed based on the security level offered to a group of users, slices and/or tenants, depending on the requirements and criticality of the service or infrastructure.

9 Limitations and future research

This chapter summarizes the inherent limitations of the conducted research and outlines the potential directions for future investigation. While the study has contributed significantly to the development of a comprehensive security framework intended to support a risk-based approach and dynamic establishment of policies based on trust in interconnection, certain constraints were found that influenced the results and scope of the dissertation. Additionally, I would like to propose future research directions in this field, which should help in the horizon of reaching the most secure communication networks in the upcoming 6G era.

Adding an Offline analysis by the implementation of AI/ML techniques in the proposed Security framework

The proposed security framework in the dissertation is intended to guide an online evaluation of risk in the interconnection links of a telecommunication network used to provide roaming services. It addresses the analysis of signaling streaming data in an online manner, i.e., considering online pipelines. Assuming an average of around 600-1000 signaling messages per second as an input data stream[6], it is highly recommended, as pointed out in subchapter 4.2.3.1 of the dissertation, to apply simplification techniques like sampling, reduction, sketching, synopsis, etc. Consequently, certain relevant information can be missed or "skipped" in the risk computation. In addition, another type of threats like Advanced Persistent Threats (APT), causing, for example, fraud, can be easily overlooked by an online analysis typically made in limited time windows. Those types of threats would require forensics and, in general, an offline analysis of batch data collected in corresponding storage platforms where different techniques, for example, based on AI/ML, can be applied. Therefore, the framework can certainly be expanded with an offline analysis of batch data, where we would need, from one side, the storage of all data exchanged in interconnection, and not only samples or sketches as in our recommended data mining approach for data streams. Subsequently, we would need to preprocess all data in batches to finally be capable of using it in anomaly detection systems, based typically on clustering Machine Learning algorithms to ultimately detect fraud and feed accordingly the trust score established with a particular peer operator or roaming intermediary.

[6] The approximate volumetric information comes from statistics in real networks to which I could have access due to my professional career.

Fig. 9-1 shows (in red) the expansion of our model (represented in Fig. 4.2-1) considering an offline security analysis of batch data.

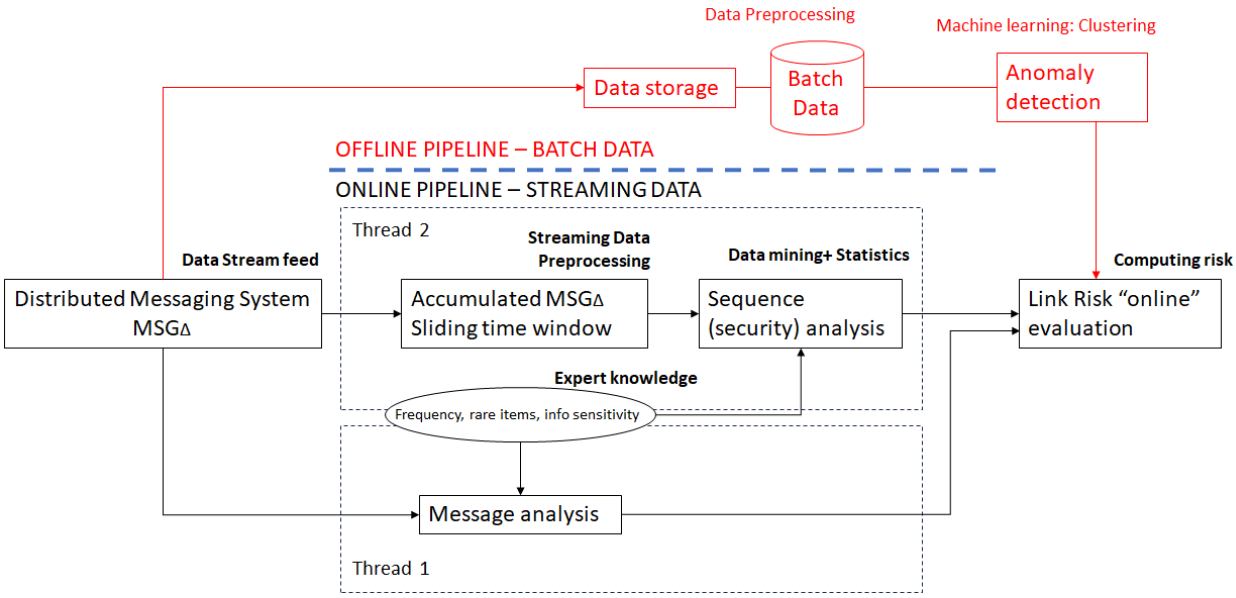

Fig. 9-2: Adding Offline Security analysis to the Security framework of the dissertation

The offline analysis of the data collected in signaling links is left for further discussion and investigation, as well as how both the online and offline analyses can be combined and serve the purpose of computing the risk in the interconnection links.

The use of machine learning for security detection functionality in telecom networks is already in use in some environments, specifically in roaming for the detection of fraud in most cases. There are some works published in recent years addressing how big data techniques and machine learning address the protection of SS7 networks, e.g., Jensen et al. in [104] presented a proof of concept of an SS7 protection system based on big data techniques and machine learning (Seasonal Hybrid ESD algorithm), Ullah et al. in [105] also provides a machine learning based framework to detect anomalies in the SS7 network, etc.

We have identified at least two key limitations in the current approaches to using AI/ML for the purpose of security analysis in interconnection/roaming that should be considered as opportunities for further investigation in the near future:

1) *The expansion of the proposed ML techniques for SS7 (2G/3G) to 4G (Diameter) and 5G (HTTP/2)*. All three schemas will coexist for a certain period of time, so the offline analysis needs to consider all of them and the impact of the specific vulnerabilities in one generation into another generation, especially from SS7 (the least secure) towards 4G and 5G networks.

Attacks on Diameter were described as an evolution of SS7-based attacks in [106], mainly in theoretical scenarios. In addition, there is no commercial service of 5G Standalone roaming at the time of writing this dissertation, and the potential attack vectors in roaming are described by GSMA in [51]. It is expected that the activation of the roaming services in 5G SA will be accompanied by new sophisticated attack vectors and vulnerabilities supported by AI/ML techniques, probably with the same targets, i.e., location tracking, fraud, DoS, etc., that will require efforts in security and AI/ML research community to find the adequate mitigations.

2) *Access to real data for academic use due to privacy concerns*. Signaling data exchanged in interconnection contains a significant amount of Personal Identifiable Information (PII) and, in general, data-sensitive information of the subscribers that shall be protected according to legislations like GDPR [36] in most parts of the world. Just a few authors have analyzed in detail the impact of GDPR on mobile networks [107], their infrastructure [108], as well as the derived privacy policies' compliance with the regulation [109], but unfortunately there are not comprehensive studies treating the impact of the recent privacy related regulations in interconnection/roaming context, and how the security frameworks, primarily intended to protect the availability of the services provided by MNOs, can cope with the constraints imposed by those regulations.

   Privacy and security concerns regarding accessing the signaling data in interconnection hinder academic experimentation with different algorithms and techniques that are exposed in this dissertation. The simulation of signaling according to standard formats may help to obtain some practical results, but without knowledge of the distributions of the multiple messages coming from the different stakeholders, those results would be quite unrealistic. Consequently, we encourage mobile operators and/or IPX providers to study how the data can be shared in privacy-preserving formats and compliant with the regulations in order to facilitate the security research and analytics that are critical in those interfaces already at present.

Interconnection/Roaming Security aspects in private networks (example: Military services)

3GPP standards for 5G have introduced a new security paradigm in interconnection/roaming, which brings significant enhancements to the schemas developed in the past for 2G/3G/4G, reducing some of the vulnerabilities on roaming subscribers. Two main concepts have been part

of that paradigm already since the first release of 5G (release 15), firstly moving the authentication procedure to the home network (HPLMN), and secondly the introduction of a new interconnection gateway called Secure Edge Protection Proxy (SEPP). Those improvements are also attractive in the case of private networks, especially in very critical networks. Note that the current 5G architecture, as defined by 3GPP, does not provide support for roaming between NPNs. Recent publications such as References [110] and [111] intend to build a framework that expands the current public network roaming architecture to adapt it to Private Networks. In 2024, the Idaho National Laboratory and the Cooperative Cyber Defence Center of Excellence (CCDCOE) demonstrated for first time a secure 5G Roaming interconnection for military communications [112]. Alternatively, Dzogovic and Holtmanns proposed in [113] the use of 5G slicing for military applications, aiming to facilitate cooperation among partners across countries and regions.

Security is a non-negotiable and paramount pillar in private networks, especially in the case of military and defense services. The standardization of 5G networks for use in Military and Defence sector have started in 2024 with 6G in the horizon, becoming Roaming a key use case due to geopolitical reasons. The adaption of existing security framework and/or the development of new ones for those Private Networks environments will be definitely required.

Interconnection/Roaming Security aspects in Slicing

Although Network Slicing support for roaming is defined in 5.15.6 of [48] and some guidance is provided by GSMA, Roaming slicing is a feature not commercially available for multiple factors, being one of them security in its widest meaning. Dhanasekaran et al. in [9] analyze the gaps in network slicing standardization with respect to security, inviting for further investigation on specific topics like isolation in end-to-end services, security for slices across multiple operators, SLA monitoring and closed-loop security assurance, etc.

The use of Distributed Ledger Technologies in Interconnection/Roaming

For a few years, telecommunication and security researchers have been looking at the potential use of Distributed Ledger Technologies (DLT), such as blockchain in different parts of the network, claiming that the new decentralized trust model introduced by those technologies will increase the trust level and transparency. Recently, Dimou et al. [114] presented a blockchain-based roaming subscriber authentication and registration system for MNOs that use smart contracts to deliver roaming services. Earlier, Harris [115] presented another use of blockchain

in roaming basically by incorporating the legal roaming agreements negotiated between roaming partners for billing into smart contracts (Chaincode). Other works related to blockchain use cases in telecom, including roaming, have been done on the topic, such as [115], [116], or [117], among others. However, all intents of introducing DLT in Mobile Networks standardization have failed so far, in my own experience, not due to the technology itself but due to the drastic in the actual trust models. Note that schemas of cross-certification based on traditional PKI (Public Key Infrastructure), even if standardized since 4G times more than a decade ago, were never implemented in the telecom market. In our view, the research in this area should continue, focused on demonstrating the benefits of adopting the technology in environments like Roaming, but considering as well very seriously business and trust type of constraints. The adoption of DLT in roaming, the impact of DLT on the trust model and how it would impact the proposed security framework in this dissertation are, in our view, interesting topics for further investigation.

Security considerations in the User plane in interconnection/roaming

The protection of the interface N9 in the 5G architecture (home routed scenario) was addressed in 3GPP standards [1] [48] already since Release 16. The main reasoning behind is that N9 interface can transport in addition to the actual payload data, user data, subscription data or other sensitive information such as security keys.

The exchange of N9 traffic in a secure tunnel (e.g., IPsec) and the introduction of Inter-PLMN UP Security (IPUPS) functionality at the perimeter of the PLMN, but controlled by the SMF, that basically enforces GTP-U security (confidentiality, integrity and replay protection) at the N9 interface. IPUPS functionality in UPFs ensures that only GTP-U packets belonging to an active PDU session that are not malformed will be forwarded between VPLMN and HPLMN. MNOs can also implement IPUPS functionality as a separate NF. IPUPS would act as a GTP firewall, which has been an existing technology for many years in the market.

Obviously, the security insights coming from IPUPS on the user plane traffic exchanged between MNOs are relevant for the evaluation of risk in interconnection, the trust score, corresponding security policies, and further enforcement in the UPF or separate NF hosting the functionality. However, the nature of the traffic and protocols are different than in the signaling plane, e.g., user payload is mostly end-to-end encrypted at application level and several orders of magnitude bigger than the signaling traffic. A thorough study is required to expand the proposed framework to cover the user plane.

10 Summary

The fifth generation of mobile networks (5G) standardization has designed a network architecture with built-in strong security concepts, that include a substantial improvement in the interconnection environment with other networks by the introduction of a new end-to-end security paradigm. Nevertheless, the interconnection through previous mobile generations (2G/3G/4G) will coexist with this new 5G paradigm (not yet deployed at the time of writing this dissertation) still for several years. The Mobile Network Operators interconnect their networks to provide roaming services supported by Service Level Agreements (SLAs). SLAs include security clauses intended to further determine the corresponding protection mechanisms that guarantee the privacy and security level required by the business and applicable regulation.

The dissertation presents a new risk-based security framework that addresses the current static security posture in interconnection across the three schemas of interconnection, which rely on manually provisioned security policies and neglect the continuously changing threat landscape in IPX networks. To address these challenges, the building blocks of the security framework propose:

- A novel approach/mechanism to evaluate dynamically the risk in interconnection. The signaling messages and corresponding data streams have been mathematically modeled, and the model has been used as a baseline to apply expert knowledge in the measuring of the risk per message and data mining techniques to proceed with sequences. In addition, the Common Vulnerability Scoring System has been adapted to quantify the risk in each case. This mechanism has been applied theoretically to a flagship use case, such as location tracking, as well as practically to a real 4G roaming anonymized trace.
- Several methods that leverage the existing standardized Network Analytics and Policy Control frameworks in 5G to enable:
    - A trust score for Mobile Networks in Roaming.
    - Security profiles to negotiate between Mobile Networks when Application Layer Security is activated in interconnection.
    - Security enforcement of security policies in the interconnection gateways.

These methods have been designed on the basis of 5G architecture, taking advantage of the work made by 3GPP in the standardization of 5G. Accordingly, new procedures are proposed in both Network Analytics and Policy Control frameworks, prone to be standardized in 5G-Advanced or even future 6G releases. In previous mobile generations, the network analytics

framework did not exist, and only in 4G a Policy Control function was developed with a very limited scope in functionalities. The adaptation of the proposed methods in 5G to previous mobile generations (2G/3G/4G) is certainly feasible from implementation viewpoint, although it would require ad-hoc type of solutions due to the lack of standardization in network analytics and policy control.

The proposed mechanism to evaluate dynamically the risk in interconnection and the procedure to determine a trust score for mobile networks in Roaming respond to the requirement of continuous evaluation and measurement of the security posture in this environment, as defined in **Thesis 1** of the dissertation. The definition of security profiles responds to the challenge of reducing the operational complexity introduced by the new end-to-end security paradigm in 5G as defined in **Thesis 2** of the dissertation. Finally, the design of the methods to be implemented in the existing Network Analytics and Policy Control frameworks in 5G respond to requirement about the automated security enforcement of policies defined in **Thesis 3** of the dissertation.

11 References

[1] 3GPP TS 33.501: “Security architecture and procedures for 5G system”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[2] GSMA Official Document “NG.113 5GS Roaming Guidelines v11.0”. Available: https://www.gsma.com/newsroom/wp-content/uploads/NG.113.v.11.0.pdf

[3] “ISO/IEC 27005:2022,” ISO. Accessed: Jan. 03, 2025. [Online]. Available: https://www.iso.org/standard/80585.html

[4] 3GPP TS 23.288: “Architecture enhancements for 5G System (5GS) to support network data analytics services”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579

[5] Silke Holtmanns, Ian Oliver, Yoan Miche, Aapo Kalliola, Gabriela Limonta, and German Peinado Gomez, “5G Security – Complex Challenges,” in *Wiley 5G Ref*, John Wiley & Sons, Ltd, 2019, pp. 1–15. doi: 10.1002/9781119471509.w5GRef161.

[6] Jordi Mongay Batalla, Luis J. de la Cruz Llopis, Germán Peinado Gómez, Elzbieta Andrukiewicz, Piotr Krawiec, Constandinos X. Mavromoustakis and Houbing Herbert Song, “Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 5, pp. 3496–3512, May 2024, doi: 10.1109/TITS.2023.3325908.

[7] Jordi Mongay Batalla, Elżbieta Andrukiewicz, German Peinado Gomez, Piotr Sapiecha, Constandinos X. Mavromoustakis, George Mastorakis, Jerzy Żurek, and Muhammad Imran, “Security Risk Assessment for 5G Networks: National Perspective,” *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 16–22, Aug. 2020, doi: 10.1109/MWC.001.1900524.

[8] German Peinado Gomez, Jordi Mongay Batalla, Yoan Miche, Silke Holtmanns, Constandinos X. Mavromoustakis, George Mastorakis, Noman Haider, “Security policies definition and enforcement utilizing policy control function framework in 5G,” *Comput. Commun.*, vol. 172, pp. 226–237, Apr. 2021, doi: 10.1016/j.comcom.2021.03.024.

[9] R. M. Dhanasekaran, Jing Ping, and German Peinado Gomez, “End-to-End Network Slicing Security Across Standards Organizations,” *IEEE Commun. Stand. Mag.*, vol. 7, no. 1, pp. 40–47, Mar. 2023, doi: 10.1109/MCOMSTD.0005.2200055.

[10] Andreas Andreou, Constandinos X. Mavromoustakis, Houbing Herbert Song, German Peinado Gomez, and Jordi Mongay Batalla, “Transforming ageing in the metaverse: embracing virtual communities for enhanced well-being and empowerment,” *Adv. Metaverse Wirel. Commun. Syst.*, pp. 457–494, doi: 10.1049/PBTE112E_ch16.

[11] German Peinado Gomez, Anja Jerichow, and Chaitanya Aggarwal, “Security enforcement and assurance utilizing policy control framework and security enhancement of analytics function in communication network,” Patent No. (Granted): US12126658B2. Date of Patent: Oct. 22, 2024. Available: https://patents.google.com/patent/US12126658B2/en?inventor=German+PEINADO+GOMEZ

[12] Anja Jerichow and German Peinado Gomez, “Apparatus, method, and computer program of protecting communications between networks using predefined security profiles.” Patent No. (Granted): US 12,192,208 B2. Date of Patent: Jan. 7, 2025. Available: https://ppubs.uspto.gov/dirsearch-public/print/downloadBasicPdf/12192208?requestToken=eyJzdWIiOiIxZmYyOGU1YS1iMjViLTQ1YzQtYWI1ZC1iYTZmMjdjZTIyODIiLCJ2ZXIiOiI2NjEwMDNhZi02MDZhLTRlYjYtOTMxZi1jMDQzN2M5ZGViZjkiLCJleHAiOjB9

[13] Borislava Gajic, German Peinado Gomez, Saurabh Khare, and Tejas Subramanya, “Method and apparatus for determining and utilizing a trust indication in mobile networks,” US20230413029A1, Dec. 21, 2023. [Online]. Available: https://patents.google.com/patent/US20230413029A1/en?oq=US20230413029A1

[14] 3GPP TS 29.002: “Mobile Application Part (MAP) specification”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1585

[15] 3GPP TS 29.078: “Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase X; CAMEL Application Part (CAP) specification”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1597

[16] IETF RFC 2719: “Framework Architecture for Signaling Transport”

[17] IETF RFC 3788: “Security Considerations for Signaling Transport (SIGTRAN) Protocols,”

[18] A. S. and B. Gellman *et al.*, “New documents show how the NSA infers relationships based on mobile location data,” *Washington Post*, Dec. 12, 2013. Available: https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/

[19] E. Биволъ, “Bulgarian company – Global Innovator in Wiretapping,” Bivol!. Available: https://bivol.bg/en/bulgarian-company-global-innovator-in-wiretapping.html

[20] J. Cox, “You Can Spy Like the NSA for a Few Thousand Bucks,” *The Daily Beast*, Nov. 03, 2017. Available: https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks

[21] S. Alfonsi, “Hacking Your Phone - CBS News”. Available: https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

[22] M. J. S. May 5 and 2017, “Bank Account Hackers Used SS7 to Intercept Security Codes.” Available: https://www.bankinfosecurity.com/bank-account-hackers-used-ss7-to-intercept-security-codes-a-9893

[23] T. Engel, “SS7: Locate. Track. Manipulate.,” Available: https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

[24] “The Fall of SS7 - How Can the Critical Security Controls Help? | SANS Institute.” Available: https://www.sans.org/white-papers/36225/

[25] S. Puzankov and Positive Technologies, Russia, “Stealthy SS7 Attacks,” *J. ICT Stand.*, vol. 5, no. 1, pp. 39–52, 2017, doi: 10.13052/jicts2245-800X.512.

[26] “Attacking SS7 - P1 Security (Hackito Ergo Sum 2010) - Philippe Langlois,” SlideShare. Available: https://www.slideshare.net/slideshow/hes2010-philippe-langlois-attacking-ss7/18618014

[27] GSMA Official Document “FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines,” Available: https://www.gsma.com/security/resources/fs-11-ss7-interconnect-security-monitoring-and-firewall-guidelines-v6-0/

[28] IETF RFC 3588: “Diameter Base Protocol”

[29] IETF RFC 6733: “Diameter Base Protocol”

[30] 3GPP TS 23.401: “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access” Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849

[31] IETF RFC 9260: “Stream Control Transmission Protocol”

[32] GSMA Official Document “FS.19 Diameter Interconnect Security” GSMA Members: https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/Doc.aspx?sourcedoc=%7BE1BBAC17-0747-4EFE-8D04-05E13F787D17%7D&file=FS.19%20v9.1.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[33] GSMA Official Document “IR.88 EPS Roaming Guidelines Version 28.0,” Newsroom. Available: https://www.gsma.com/newsroom/gsma_resources/ir-88-eps-roaming-guidelines-version-27-1/

[34] GSMA Official Document “FS.21 Interconnect Signalling Security Recommendations,” Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-21-interconnect-signalling-security-recommendations-v6-0/

[35] https://globalcarrier.telekom.com/newsroom/news/news-pages/deutsche-telekom-global-carrier-disrupts-roaming-industry-with-launch-of-magenta-security-roaming

[36] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, vol. 119. 2016. Available: http://data.europa.eu/eli/reg/2016/679/oj/eng

[37] “Regulation - 2019/881 - EN - EUR-Lex.” Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[38] “5G-ENSURE publishes initial study on risk assessment, mitigation and requirements.” Available: https://5g-ppp.eu/5g-ensure-publishes-initial-study-on-risk-assessment-mitigation-and-requirements/

[39] J. T. F. T. Initiative, “Guide for Conducting Risk Assessments,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-30 Rev. 1, Sep. 2012. doi: 10.6028/NIST.SP.800-30r1.

[40] “IP_19_6049_EN.pdf.” Available: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_19_6049/IP_19_6049_EN.pdf

[41] “ENISA - 5G Standards.pdf.” Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20-%205G%20Standards.pdf

[42] “EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex.” Available: https://eur-lex.europa.eu/eli/dir/2022/2555

[43] National Cyber Security Centre “Summary of the NCSC’s security analysis for the UK telecoms sector”. https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector

[44] ETSI GR NFV-SEC 003: “Networks Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance” Available: https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/003/01.03.01_60/gr_NFV-SEC003v010301p.pdf

[45] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[46] 3GPP TR 33.894: “Study on applicability of the zero trust security principles in mobile networks” Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4086

[47] 3GPP TR 33.794: “Study on enablers for Zero Trust Security” Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4235

[48] 3GPP TS 23.501: “System architecture for the 5G System (5GS)” Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[49] 3GPP TR 33.866: “Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2” Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3823

[50] 3GPP TR 33.738: “Study on security aspects of enablers for network automation for the 5G system phase 3”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4049

[51] GSMA Official Document “FS.36 5G Interconnect Security”. GSMA Members: https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/Doc.aspx?sourcedoc=%7BB4F98886-6B9E-4C6B-A62C-AA0DB4588505%7D&file=FS.36%20v2.4.docx&action=default&mobileredirect=true

[52] 3GPP TS 33.210: “Network Domain Security (NDS); IP network layer security”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279

[53] GSMA Official Document “AA.12 Standard Template for International Roaming Agreement”. GSMA Members: https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/Doc.aspx?sourcedoc=%7BC7B586B0-F49B-4FBF-A412-ABF99305C94D%7D&file=AA.12%20v16.7%20(1).docx&action=default&mobileredirect=true&DefaultItemOpen=1

[54] GSMA Official Document “AA.13 International Roaming Agreement - Common Annexes”. GSMA Members:

https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/Doc.aspx?sourcedoc=%7B27A259B8-B218-404C-BB9B-EE7C6398671D%7D&file=AA.13%20v26.1.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[55] GSMA Official Document "BA.51 Roaming Service Level Agreement Guidelines". GSMA Members: https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/doc2.aspx?sourcedoc=%7B8A33B4AC-A4D3-4FAA-BB15-B3ADFBF32C12%7D&file=BA.51%20v7.0.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[56] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2". Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3334

[57] "Spy companies using Channel Islands to track phones around the world," The Bureau of Investigative Journalism (en-GB). Available: https://www.thebureauinvestigates.com/stories/2020-12-16/spy-companies-using-channel-islands-to-track-phones-around-the-world

[58] "Common Vulnerability Scoring System SIG," FIRST — Forum of Incident Response and Security Teams. Available: https://www.first.org/cvss

[59] 3GPP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3". Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3530

[60] "Fraud and Security Group #19," Working Groups. Available: https://www.gsma.com/get-involved/working-groups/gsma_events/fraud-and-security-group-19

[61] S. Wares, J. Isaacs, and E. Elyan, "Data stream mining: methods and challenges for handling concept drift," *SN Appl. Sci.*, vol. 1, no. 11, p. 1412, Nov. 2019, doi: 10.1007/s42452-019-1433-0.

[62] A. Margara and T. Rabl, “Definition of Data Streams,” in *Encyclopedia of Big Data Technologies*, S. Sakr and A. Y. Zomaya, Eds., Cham: Springer International Publishing, 2019, pp. 648–652. doi: 10.1007/978-3-319-77525-8_188.

[63] S. Muthukrishnan, “Data Streams: Algorithms and Applications”.

[64] ITU “E.212: The international identification plan for public networks and subscriptions.” Available: https://www.itu.int/rec/T-REC-E.212/en

[65] GSMA Official Document “IR.21 GSM Association Roaming Database, Structure and Updating Procedures”. GSMA Members: https://membergateway.sharepoint.com/:w:/r/sites/OfficialDocuments/_layouts/15/Doc.aspx?sourcedoc=%7BD09252A8-643E-4C85-9C7C-74B25F7A72DD%7D&file=IR.21%20v17.0.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[66] 3GPP TS 23.003: “Numbering, addressing and identification”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729

[67] 3GPP TS 29.230: “Diameter applications; 3GPP specific codes and identifiers”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1683

[68] “All Groups / 5G APIs · GitLab,” GitLab. Available: https://forge.3gpp.org/rep/all/5G_APIs

[69] 3GPP TS 29.572: “5G System; Location Management Services; Stage 3”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1690

[70] M. Thomson and C. Benfield, “HTTP/2,” Internet Engineering Task Force, Request for Comments RFC 9113, Jun. 2022. doi: 10.17487/RFC9113.

[71] 3GPP TS 29.500: “5G System; Technical Realization of Service Based Architecture; Stage 3”. Available:

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3338

[72] A. C. Gilbert, Y. Kotidis, S. Muthukrishnan, and M. J. Strauss, “Surfing Wavelets on Streams: One-Pass Summaries for Approximate Aggregate Queries”. https://dl.acm.org/doi/10.5555/645927.672174.

[73] P. B. Gibbons, “Distinct Sampling for Highly-Accurate Answers to Distinct Values Queries and Event Reports”. https://dl.acm.org/doi/abs/10.5555/645927.672351

[74] J. S. Vitter, “Random sampling with a reservoir,” *ACM Trans. Math. Softw.*, vol. 11, no. 1, pp. 37–57, Mar. 1985, doi: 10.1145/3147.3165.

[75] B. Babcock, S. Babu, M. Datar, R. Motwani, and J. Widom, “Models and issues in data stream systems,” in *Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, in PODS ’02. New York, NY, USA: Association for Computing Machinery, Jun. 2002, pp. 1–16. doi: 10.1145/543613.543615.

[76] Y. Matias and M. Wang, “Dynamic Maintenance of Wavelet-Based Histograms”. https://dl.acm.org/doi/10.5555/645926.672011

[77] A. C. Gilbert, S. Guha, P. Indyk, Y. Kotidis, S. Muthukrishnan, and M. J. Strauss, “Fast, small-space algorithms for approximate histogram maintenance,” in *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, Montreal Quebec Canada: ACM, May 2002, pp. 389–398. doi: 10.1145/509907.509966.

[78] S. Tsang, Y. S. Koh, and G. Dobbie, “RP-Tree: Rare Pattern Tree Mining,” in *Data Warehousing and Knowledge Discovery*, vol. 6862, A. Cuzzocrea and U. Dayal, Eds., in Lecture Notes in Computer Science, vol. 6862. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 277–288. doi: 10.1007/978-3-642-23544-3_21.

[79] R. Agrawal and R. Srikant, “Mining sequential patterns,” in *Proceedings of the Eleventh International Conference on Data Engineering*, Taipei, Taiwan: IEEE Comput. Soc. Press, 1995, pp. 3–14. doi: 10.1109/ICDE.1995.380415.

[80] R. Srikant and R. Agrawal, “Mining sequential patterns: Generalizations and performance improvements,” in *Advances in Database Technology — EDBT ’96*, vol. 1057, P. Apers, M. Bouzeghoub, and G. Gardarin, Eds., in Lecture Notes in Computer Science, vol.

1057. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 1–17. doi: 10.1007/BFb0014140.

[81] Jian Pei, Jiawei Han, Behzad Mortazavi-Asl, Helen Pinto, Qiming Chen, Umeshwar Dayal, Mei-Chun Hsu, “PrefixSpan,: mining sequential patterns efficiently by prefix-projected pattern growth,” in *Proceedings 17th International Conference on Data Engineering*, Heidelberg, Germany: IEEE Comput. Soc, 2001, pp. 215–224. doi: 10.1109/ICDE.2001.914830.

[82] M. J. Zaki, “SPADE: An Efficient Algorithm for Mining Frequent Sequences”. https://link.springer.com/article/10.1023/A:1007652502315

[83] J. Han, J. Pei, B. Mortazavi-Asl, Q. Chen, U. Dayal, and M.-C. Hsu, “FreeSpan: frequent pattern-projected sequential pattern mining,” in *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, Boston Massachusetts USA: ACM, Aug. 2000, pp. 355–359. doi: 10.1145/347090.347167.

[84] G. S. Manku and R. Motwani, “Approximate Frequency Counts over Data Streams”. https://doi.org/10.1016/B978-155860869-6/50038-X

[85] R. M. Karp, S. Shenker, and C. H. Papadimitriou, “A simple algorithm for finding frequent elements in streams and bags,” *ACM Trans. Database Syst.*, vol. 28, no. 1, pp. 51–55, Mar. 2003, doi: 10.1145/762471.762473.

[86] A. Metwally, D. Agrawal, and A. E. Abbadi, “An integrated efficient solution for computing frequent and top- *k* elements in data streams,” *ACM Trans. Database Syst.*, vol. 31, no. 3, pp. 1095–1133, Sep. 2006, doi: 10.1145/1166074.1166084.

[87] C. Raıssi, P. Poncelet, and M. Teisseire, “Need for SPEED: Mining Sequential Patterns in Data Streams”. https://www.lirmm.fr/~poncelet/publications/papers/FinalBDA05CPT.pdf

[88] V. E. Lee, R. Jin, and G. Agrawal, “Frequent Pattern Mining in Data Streams,” in *Frequent Pattern Mining*, C. C. Aggarwal and J. Han, Eds., Cham: Springer International Publishing, 2014, pp. 199–224. doi: 10.1007/978-3-319-07821-2_9.

[89] P. Kumar and P. Rao, “Frequent Pattern Retrieval on Data Streams by using Sliding Window,” *EAI Endorsed Trans. Energy Web*, p. 168091, Jul. 2018, doi: 10.4108/eai.13-1-2021.168091.

[90] M. Krishnamoorthy and R. Karthikeyan, “Pattern mining algorithms for data streams using itemset,” *Meas. Sens.*, vol. 24, p. 100421, Dec. 2022, doi: 10.1016/j.measen.2022.100421.

[91] “Learning from Time-Changing Data with Adaptive Windowing.” Accessed: May 31, 2024. [Online]. Available: https://epubs.siam.org/doi/epdf/10.1137/1.9781611972771.42

[92] “Maintaining Stream Statistics over Sliding Windows.” Accessed: May 31, 2024. [Online]. Available: https://epubs.siam.org/doi/epdf/10.1137/S0097539701398363

[93] G. Cormode and S. Muthukrishnan, “An improved data stream summary: the count-min sketch and its applications,” *J. Algorithms*, vol. 55, no. 1, pp. 58–75, Apr. 2005, doi: 10.1016/j.jalgor.2003.12.001.

[94] O. Papapetrou, M. Garofalakis, and A. Deligiannakis, “Sketch-based Querying of Distributed Sliding-Window Data Streams,” Jun. 30, 2012, *arXiv*: arXiv:1207.0139. Available: http://arxiv.org/abs/1207.0139

[95] “Common Vulnerability Scoring System Version 4.0 Calculator,” FIRST — Forum of Incident Response and Security Teams. Available: https://www.first.org/cvss/calculator/4.0

[96] “GSMA Coordinated Vulnerability Disclosure programme,” Security. Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma-coordinated-vulnerability-disclosure-programme/

[97] “5G zero trust – a zero-trust architecture for telecom”. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g

[98] IETF RFC 7516: “JSON Web Encryption (JWE)”

[99] IETF RFC 7515: “JSON Web Signature (JWS)”

[100] IETF RFC 8446: “The Transport Layer Security (TLS) Protocol Version 1.3”

[101] 3GPP TS 29.338: “Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)”. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1714

[102] “tshark” Available: https://www.wireshark.org/docs/man-pages/tshark.html

[103] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5G and Beyond,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3682–3722, 2019, doi: 10.1109/COMST.2019.2916180.

[104] K. Jensen, H. T. Nguyen, T. V. Do, and A. Årnes, “A big data analytics approach to combat telecommunication vulnerabilities,” *Clust. Comput.*, vol. 20, no. 3, pp. 2363–2374, Sep. 2017, doi: 10.1007/s10586-017-0811-x.

[105] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash, and H. Abbas, “SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1337–1371, 2020, doi: 10.1109/COMST.2020.2971757.

[106] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, “We know where you are!,” in *2016 8th International Conference on Cyber Conflict (CyCon)*, May 2016, pp. 277–293. doi: 10.1109/CYCON.2016.7529440.

[107] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, “GDPR Interference With Next Generation 5G and IoT Networks,” *IEEE Access*, vol. 8, pp. 108052–108061, 2020, doi: 10.1109/ACCESS.2020.3000662.

[108] E. Rios *et al.*, “Service level agreement-based GDPR compliance and security assurance in(multi)Cloud-based systems,” *IET Softw.*, vol. 13, no. 3, pp. 213–222, 2019, doi: 10.1049/iet-sen.2018.5293.

[109] L. Zhang, N. Moukafih, H. Alamri, G. Epiphaniou, and C. Maple, “A BERT-based Empirical Study of Privacy Policies’ Compliance with GDPR,” in *2023 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2023, pp. 1–6. doi: 10.1109/CNS59707.2023.10288797.

[110] M. Corici, P. Chakraborty, T. Magedanz, A. S. Gomes, L. Cordeiro, and K. Mahmood, "5G Non-Public-Networks (NPN) Roaming Architecture," in *2021 12th International Conference on Network of the Future (NoF)*, Oct. 2021, pp. 1–5. doi: 10.1109/NoF52522.2021.9609936.

[111] P. Chakraborty *et al.*, "A Framework for Roaming between 5G Non-Public-Networks (NPNs)," in *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*, Nov. 2023, pp. 247–253. doi: 10.1109/CSCN60443.2023.10453146.

[112] A. Bhuyan and M. Gheorghevici, "Real-world Demonstration of Secure 5G Roaming for Military Communications," in *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, Oct. 2024, pp. 639–640. doi: 10.1109/MILCOM61039.2024.10773651.

[113] B. Dzogovic and S. Holtmanns, "Securing 5G Communication in Joint Operations Between NATO Partners," in *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, May 2024, pp. 29–46. doi: 10.23919/CyCon62501.2024.10685610.

[114] S. Dimou, K. Choumas, and T. Korakis, "On using Blockchain in beyond 5G: Roaming Improvements," in *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Oct. 2024, pp. 1–2. doi: 10.1109/BRAINS63024.2024.10732174.

[115] C. Harris, "Improving Telecom Industry Processes Using Ordered Transactions in Hyperledger Fabric," in *2019 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6. doi: 10.1109/GCWkshps45667.2019.9024541.

List of Abbreviations

3GPP	3rd Generation Partnership Project
5G	Fifth Generation of Mobile Networks
5GMRR	5G Mobile Roaming Revisited
AC	Attack Complexity
ADRF	Analytical Data Repository Function
ADWIN	ADaptive sliding WINdow
AF	Application Function
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AKMA	Authentication and Key Management for Applications
AL	Allow List
ALS	Application Layer Security
AMBR	Aggregated Maximum Bit Rate
AMF	Access and Mobility Management Function
API	Application Programming Interface
APT	Advanced Persistent Threats
ASN.1	Abstract Syntax Notation One
AT	Attack Requirement
AUTH	Authentication_Material
AUTHZ	Authorization_Material
AV	Attack Vector
AVP	Attribute Value Pair
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CAP	CAMEL Application Part
CC	Command Code
CCA	Client Credentials Assertions, Credit-Control-Answer
CM	Count-min
CP	Control Plane
CSA	Cyber Security Act
CVD	Coordinated Vulnerability Disclosure
CVSS	Common Vulnerability Scoring System
CVSS-BT	CVSS-Based on Threat metrics

DEA	Diameter Edge Agent
DESS	Diameter End-to-End Signaling Security
DLT	Distributed Ledger Technologies
DNS	Domain Name System
DoS	Denial of Service
DRA	Diameter Routing Agent
DS	Data Sensitivity
DSR	Delete-Subscriber-Data-Request
DTLS	Data Transport Layer Security
EAP-AKA’	Extensible Authentication Protocol for AKA
ECM	Exponential Count-Min
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FreeSpan	FREquEnt pattern-projected Sequential PAtterN mining
FTO	Fully Trusted Operators
GBR	Guaranteed Bit Rate
GDPR	General Data Protection Regulation
gNB	Next Generation NodeB
GPRS	General Packet Radio Service
GSMA	Global System for Mobile Communications Association
GSP	Generalized Sequential Patterns
GTP	GPRS Tunnelling Protocol
GTP-C	GTP Control Plane
GTP-U	GTP User Plane
GUTI	Globally Unique Temporary Identifier
HLR	Home Location Register
HMTO	High-Medium Trusted Operators
HPLMN	Home PLMN
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTP/2	HTTP version 2
IANA	Internet Assigned Numbers Authority
IDR	Insert-Subscriber-Data-Request
IDS	Intrusion Detection System

IE	Information Element
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPUPS	Inter-PLMN UP Security
IPX	Internet Protocol Exchange
JOSE	JSON Object Signing and Encryption
JSON	Java Script Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signatures
KPI	Key Performance Indicator
LAN	Local Area Network
LMTO	Low-Medium trusted operators
MAP	Mobile Application Part
ML	Machine Learning
MME	Mobile Management Entity
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station Integrated Services Digital Network
NF	Network Function
NFc	NF consumer
NFp	NF producer
NFV	Network Functions Virtualization
NG-RAN	Next Generation Radio Access Network
NIS2	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
NOR	Notify-Request
NRF	Network Repository Function
NTO	Non-trusted operators

NWDAF	Network Data Analytics Function
OAM	Operations, Administration, and Maintenance
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDU	Protocol Data Unit
PE	Policy Engine
PEP	Policy Enforcement Point
PII	Personal Identifiable Information
PIV	Potential Impacts of the Vulnerability
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PR	Privileges Required
PrefixSpan	Prefix Projected Sequential pattern Mining
PRINS	PRotocol for N32 INterconnect Security
PSTN	Public Switched Telephone Network
RAN	Radio Access Network
RAR	Re-Auth-Request
RFC	Request for Comments
QoS	Quality of Service
SBA	Service Based Architecture
SBI	Service Based Interface
SCP	Service Communication Proxy
SCTP	Stream Control Transmission Protocol
SDF	Service Data Flows
SDIF	Subscription Identity De-Concealing Function
SEPP	Security Edge Protection Proxy
SIEM	Security Information and Event Management
SIGTRAN	Signaling Transport (SS7 over IP)
SLA	Service Level Agreement
SMF	Session Management Function
SMS	Short Message Service
SOAR	Security Operations, Automation and Response

SoR	Steering of Roaming
SPADE	Sequential PAttern Discovery using Equivalence classes
SPAM	Sequential PAttern Mining
SPEED	Sequential Patterns Efficient Extraction in Data streams
SS7	Signaling System No. 7
SSLA	Security in the SLA
STP	Signaling Transfer Point
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TDM	Time Division Multiplexer
TLS	Transport Layer Security
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UI	User Interaction
ULR	Update Location Request
UP	User Plane
UPF	User Plane Function
URI	Uniform Resource Identifier
VA	Availability Impact
VC	Confidentiality Impact
VI	Integrity Impact
VLR	Visitor Location Register
VPLMN	Visited PLMN
VPN	Virtual Private Network
XDR	Extended Detection and Response
ZTA	Zero Trust Architecture

List of Figures

List of Tables