Deliverable D2.6
Risk Assessment, Mitigation and Requirements (final)

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	V2.5: 2017-11-15	
Lead beneficiary	ALBLF[1]	Linas Maknavicius <linas.maknavicius@nokia-bell-labs.com>
Authors	EAB: Mats Näslund IT Innovation: Mike Surridge, Toby Wilkinson NEC: Mihai Moraru NIXU: Seppo Heikkinen, Tommi Pernila Nokia: Linas Maknavicius Orange: Ghada Arfaoui, José Manuel Sanchez Vilchez, Jean-Philippe Wary OXF: Piers O'Hanlon TASE: Ana Jalon Valero, Gorka Lendrino, Carla Salas TIM[2]: Madalina Baltatu, Luciana Costa, Pier Luigi Zaccone, Paolo De Lutiis TS: Edith Felix, Olivier Bettan, Pascal Bisson VTT: Jani Suomalainen, Pekka Ruuska	

[1] NOKIA Bell Labs since Jan 14, 2016
[2] The merger of TIIT in TIM occurred on December 31, 2016

European Commission

5G PPP

Executive summary

Risk Assessment, Mitigation and Requirements deliverable proposes a risk assessment and mitigation approach for the full set of 5G- ENSURE security use cases. This document is also investigating some intrinsic risks of new 5G infrastructure and network (which is not yet fully defined in standard bodies).

Firstly we discuss and define terminology. This is essential, as common speech terminology can be quite inexact but in risk management we must be precise. We then review the state of the art in risk assessment and mitigation, understanding what existing methodology, or combination of, suits the evaluation of 5G-ENSURE proposed use cases.

To understand 5G networks we must understand the proposed architectural framework and its differences when compared to the previous 4G networks. We therefore introduce the conceptual 5G security framework proposed within the 5G-ENSURE project.

The Risk Management Context is then defined, looking first at the 5G assets and actors, which is followed by the identification of threats. The 5G-ENSURE risk evaluation methodology for use case analysis is also introduced with some possible approaches to risk likelihood & impact estimation.

The core chapter provides threat analysis of representative use cases defined by the 5G ENSURE project, after the threat description formalism (template) is introduced. As agreed by the 5G-ENSURE partners, the focus is made on the 'internal' threats in this document, i.e. those derived from 5G-ENSURE specific use cases are analyzed, as they capture the very essence of security and privacy aspects of 5G networks as seen by the project.

We then provide a summary table of threat mitigation strategies, with quantification of associated risk levels.

To complement this analysis, we propose a 'hollistic' approach to define additional ('external') risks of 5G system infrastructure.

Finally, the chapter 8 gives some security design recommendations with respect to the analyzed 5G threats, as well as corresponding security requirements, both high-level and 5G PPP specific ones.

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G-PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement, standardisation and vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and testbed with 5G security enablers) to market validation and stakeholders engagement - spanning various application domains.

The document has been written in cooperation with the D2.2 'Trust model (draft)' contributors (as for the common terminology and analysis of use cases). This study is primarily nourished by D2.1 'Use cases' deliverable for the derivation of major 5G threats as seen by the consortium and, along with the trust model, feeds into the work on 5G security architecture reported in D2.7. Of course, the risk assessment, mitigation and especially requirements also contributed to the work in WP3 in all tasks for security enabler definitions.

Disclaimer

The information in this document is provided 'as is', and no guarantee or warranty is given that the information is fit for any particular purpose.

The EC flag in this deliverable is owned by the European Commission and the 5G PPP logo is owned by the 5G PPP initiative. The use of the flag and the 5G PPP logo reflects that 5G-ENSURE receives funding from the European Commission, integrated in its 5G PPP initiative. Apart from this, the European Commission or the 5G PPP initiative have no responsibility for the content.

Copyright notice

© 2015-2017 5G-ENSURE Consortium

Contents

1 Introduction 8
2 Terminology 9
3 Methodology/related work 10
4 Risk Management Context – Threats in 5G-ENSURE Use Cases 15
4.1 The reference 5G security framework 16
4.2 Risk Identification 18
4.2.1 5G-ENSURE Assets Identification 18
4.2.2 5G-ENSURE Threat Identification and categorization 23
4.3 Risk Evaluation methodology 30
5 'Internal' threat description/analysis (from Use Cases) 32
5.1 Threat descriptions Use Cases cluster 1 - Identity Management 32
5.2 Threat descriptions Use Cases cluster 2 - Enhanced Identity Protection and Authentication 39
5.3 Threat descriptions Use Cases cluster 3 - IoT Device Authentication and Key Management 44
5.4 Threat descriptions Use Cases cluster 4 - Authorization of Device-to-Device Interactions 49
5.5 Threat descriptions Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitoring 51
5.6 Threat descriptions Use Cases cluster 6 - Radio Interface Protection 68
5.7 Threat descriptions Use Cases cluster 7 - Mobility Management Protection 69
5.8 Threat descriptions Use Cases cluster 8 - Ultra-Reliable and Standalone Operations 71
5.9 Threat descriptions in Use Cases of Cluster 9 - Trusted Core Network and Interconnect 74
5.10 Threat descriptions in Use Cases of Cluster 10 - 5G Enhanced Security Services 84
5.11 Threat descriptions in Use Cases of Cluster 11 - Lawful Interception 87
5.12 Risk mitigation proposals from Use Case analysis 91
6 Holistic approach to risk analysis of 5G system infrastructure 94
6.1 5G PPP major security risks 94
6.2 Holistic view on 5G 'System of systems' risks 94
7 Analysis: Functional design recommendations & security requirements 99
7.1 5G system design options 99
7.2 5G security requirements 99
7.2.1 High-level 5G security requirements 99
7.2.2 Specific 5G PPP security requirements 100
8 Conclusions 103
9 References 104

A Annex A: Use cases threats Identification 105
B Annex B: COMMON D2.5+D2.6 ANNEX: Use Case Analysis 106
B.1 Factory Device Identity Management for 5G Access (UC 1.1) 106
B.1.1 Use case description with architectural components 106
B.1.2 Identified threats 107
B.2 Using Enterprise Identity Management for Bootstrapping 5G Access (UC 1.2) 108
B.2.1 Use case description with architectural components 108
B.2.2 Identified threats 109
B.3 Satellite Identity Management for 5G Access (UC 1.3) 111
B.3.1 Use case description 111
B.3.2 Identified threats 111
B.4 MNO Identity Management Service (UC 1.4) 115
B.4.1 Use case description 115
B.4.2 Identified threats 115
B.5 Device Identity Privacy (UC 2.1) 118
B.5.1 Use case description with architectural components 118
B.5.2 Identified threats 119
B.6 Subscriber Identity Privacy (UC 2.2) 121
B.6.1 Use case description with architectural components 121
B.6.2 Identified threats 122
B.7 Enhanced Communication Privacy (UC 2.3) 126
B.7.1 Use case description 126
B.7.2 Identified threats 126
B.8 Authentication of IoT Devices in 5G (UC 3.1) 128
B.8.1 Use case description with architectural components 128
B.8.2 Identified threats 131
B.9 Network-Based Key Management for End-to-End Security (UC 3.2) 134
B.9.1 Use case description with architectural components 134
B.9.2 Identified threats 135
B.10 Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1) 136
B.10.1 Use case description with architectural components 136
B.10.2 Sunny day scenario 136
B.10.3 Identified threats 137
B.11 Virtualized Core Networks and Network Slicing (UC 5.1) 139

B.11.1 Use case description with architectural components 139
B.11.2 Identified threats 140
B.12 Adding a 5G node to a virtualized core network (UC 5.2) 141
B.12.1 Use case description with architectural components 141
B.12.2 Identified threats 141
B.13 Reactive Traffic Routing in a Virtualized Core Network (UC 5.3) 145
B.13.1 Use case description with architectural components 145
B.13.2 Identified threats 145
B.14 Verification of the Virtualised Node and the Virtualisation Platform (UC 5.4) 147
B.14.1 Use case description with architectural components 147
B.14.2 Identified threats 148
B.15 Control and monitoring of slice by service provider (UC 5.5) 151
B.15.1 Use case description with architectural components 151
B.15.2 Identified threats 152
B.16 Integrated Satellite and Terrestrial Systems Monitor (UC 5.6) 159
B.16.1 Use case description 159
B.17 Attach Request During Overload (UC 6.1) 161
B.17.1 Use case description with architectural components 161
B.17.2 Identified threats 162
B.18 Unprotected User Plane on Radio Interface (UC 6.2) 163
B.18.1 Use case description with architectural components 163
B.18.2 Identified threats 164
B.19 Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1) 165
B.19.1 Use case description with architectural components 165
B.19.2 Identified threats 166
B.20 Satellite Network Monitoring (UC 8.1) 167
B.20.1 Use case description with architectural components 167
B.20.2 Identified threats 167
B.21 Standalone EPC (UC 8.2) 169
B.21.1 Use case description with architectural components 169
B.21.2 Identified threats 170
B.22 Alternative Roaming in 5G (UC 9.1) 171
B.22.1 Use case description with architectural components 171
B.22.2 Identified threats 172

B.23 Privacy in Context-Aware Services (UC 9.2) 175
B.23.1 Use case description with architectural components 175
B.23.2 Identified threats 176
B.24 Authentication of new network elements (UC 9.3) 177
B.24.1 Use case description with architectural elements 177
B.24.2 Identified threats 178
B.25 Botnet mitigation (UC 10.1) 181
B.25.1 Use case description with architectural components 181
B.25.2 Identified threats 182
B.26 Privacy Violation Mitigation (UC 10.2) 184
B.26.1 Use case description with architectural components 184
B.26.2 Identified threats 184
B.27 SIM-based and/or Device-based Anonymization (UC 10.3) 186
B.27.1 Use case description with architectural components 186
B.27.2 Identified threats 187
B.28 Lawful Interception in a Dynamic 5G Network (UC 11.1) 190
B.28.1 Use case description 190
B.28.2 Identified threats 191
B.29 End to end encryption in a LI aware network (UC 11.2) 192
B.29.1 Use case description with architectural components 192
B.29.2 Identified threats 192
C Annex C: Positioning wrt 3GPP SA3 195
C.1 Analysis of 3GPP TR 33.899 195
C.2 5G-ENSURE security areas versus 3GPP SA3 TR 33.899 197
D Annex D: Abbreviations 204

1 Introduction

5G network architecture is significantly different from the architectures of any previous generation network, where new network technologies are proposed both for the access and core network infrastructures, new actors (stakeholders) arise and novel business models are made possible.

The biggest difference between 4G and 5G design requirements is the diversity of use-cases that 5G networks must support as compared to 4G networks that were primarily designed for the single use-case of delivering high speed mobile broadband.

5G is the new generation of radio systems and network architecture delivering **extreme broadband** and **ultra robust**, **low latency** connectivity and **massive networking** for the Internet of Things to enable the programmable world, which will transform our individual lives, economy and society.

What 5G will be good for and what technical requirements that imposes on the network have become quite clear. 5G will be about people and things as per the following three use case categories:

1. ***Massive broadband*** that delivers gigabytes of bandwidth on demand

2. ***Critical machine-type communication*** that allows for the immediate, synchronous eye-hand feedback that enables remote control over robots

3. ***Massive machine-type communication*** that connects billions of sensors and machines

A key design principle for 5G networks is **flexibility**, to cater to unknown use-cases of the future. And related to flexibility is another key design principle of **'reliability'**. With the flexible integration of different technology components, we will see a step away from best effort mobile broadband towards truly reliable communication. Reliability is not only about equipment up-time, it also relates to the perception of infinite capacity and coverage that future mobile networks need to deliver anytime anywhere. Furthermore, reliability is becoming more critical as we start to rely on mobile communications for control and safety.

The attack surface in 5G is much bigger because of massive number of connected devices, the virtualization techniques, the support for open networks, etc. We foresee that 5G systems design and deployment will raise **numerous security challenges and resulting risks**, like:

- related to network virtualization (specific mobile and multi-tenant VNFs, sensitive data isolation etc.);
- risks induced by wireless network topology: multi-RAT, HetNets, multi-hop, D2D, unlicensed spectrum as alternative access…;
- new services (plain "old" communication services, utilities, mission-critical applications, M2M/IOT/sensors, V2X…) will co-exist and thus will necessitate devising particular end-to-end 5G security architecture allying optimization and complexity of the system.

Therefore the Risk assessment for 5G must be carefully studied and defined by examining the current methodologies and coming with a comprehensive model that will best adapt to the new network architecture, stakeholders and business models. Our approach is to perform a risk assessment and mitigation evaluation related to multi-stakeholder 5G system and NFV, comprising new risks and modifying existing ones.

2 Terminology

Risk assessment and mitigation is of interest in many different research IT disciplines, but also in military and civil industry, economics, etc. To avoid the problems of 'jargonised' terminology, we propose to follow a common definition alongside the whole 5G-ENSURE project, therefore a terminology which is also shared with the project's deliverable D2.5 'Trust model' [2].

Risk: exposure (of someone or something valued) to danger, harm or loss

In classical risk analysis, including information system risk management based on ISO 27001, a risk exists where there are potential threats, i.e. a threat is a source of risk. Here we need to move away from the strict English definition, which encompasses the notion that a threat is a statement of intent to cause harm or loss. In the context of 5G-ENSURE, it does not matter whether or not intent to cause harm exists or is communicated. The definitions from RFC 4949 are actually more useful:

Threat: a potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

RFC 4949 makes it clear that threats could be 'intentional' (involving attack by a malicious and intelligent entity), or 'accidental' (arising from an unintended error or natural disaster). It goes on to define further terms describing the structure of a threat:

Threat action: a realization of a threat, i.e. an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act.

Threat consequence: a security violation that results from a threat action.

Threat agent: a system entity that performs a threat action, or an event that results in a threat action.

Finally, we can add two more definitions that are important in risk analysis:

Threat likelihood: the probability that a threat is realised, i.e. that the threat action will occur.

Threat impact: the level of harm caused by the threat consequence.

In conventional risk analysis based on [ISO 27005] or (more generally) [ISO 31010], the level of risk is determined from a combination of threat likelihood and impact. The correct treatment depends on the level of risk, the main options being to:

- accept the risk (i.e. trust that it won't arise);
- avoid the risk (by disengaging with the untrusted entity);
- transfer the risk (e.g. by insuring against the risk or reaching an agreement with someone else making them responsible); or
- reduce the risk (by using security measures to reduce the threat likelihood or to mitigate its consequences).

3 Methodology/related work

Without an understanding of the threats posed to a system it is impossible to select or devise appropriate measures to counter these threats. The **ETSI Threat, Vulnerability and Risk Analysis (TVRA)** [16] is used to identify risks to a system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system. The method described in ETSI TS 102 165-1 can be used to determine risk factors based upon the likelihood of a particular attack being successful and the impact that a successful attack would have on the system. The TVRA method involves the following seven steps:

1) Identify security objectives.
2) Identify security requirements.
3) Produce an inventory of system assets.
4) Classify system vulnerabilities and threats.
5) Quantify the likelihood and impact of attack.
6) Determine the risks involved.
7) Specify detailed security requirements (countermeasures).

There are a number of documents from different standardization bodies addressing the issues of threat and risk assessment and mitigation in computer or telecommunication networks. In this document we provide a brief description of the standard well consolidated methodologies which have been taken into account by the 5G-ENSURE project.

ITU-T Recommendation X.805 “Security architecture for systems providing end-to-end communications” [3] has been developed by ITU-T SG 17 (ITU-T Lead Study Group on Telecommunication Security) and was published in October 2003. This architecture provides a structured framework that forces the consideration of all possible threats and attacks to provide comprehensive end-to-end network security. It is based on the concepts of:

- Security Layers (Infrastructure Security Layer, Services Security Layer, Applications Security Layer): they represent a hierarchical approach to securing a network. Each Security Layer has unique vulnerabilities, and specific threats. For this reason each of these layers must be addressed when creating an end-to-end security solution because at each point the network may be exposed to a new risk, threat or attack.
- Security Planes (End-User Security Plane, Management Security Plane, Control/Signaling Security Plane): they represent the types of activities that occur on a network. Different security vulnerabilities may exist in each of these planes and each plane along with the three layers must be secured in order to provide an effective security plan.
- Security dimensions (access control, authentication, Non-Repudiation, Data Confidentiality, Communication Security, data integrity, availability, privacy): they represent the classes of actions that can be taken or technologies that can be deployed in order to counteract threats or potential attacks present at each security layer and plane.

The **ITU-T X.805 Security Architecture** is illustrated in the following figure (Figure 1). In the ITU X.805 standard the definition of threats makes reference to another document (X.801) [4], which, in turn, does not contain any further useful threat description, at least as far as telecommunication networks are concerned.

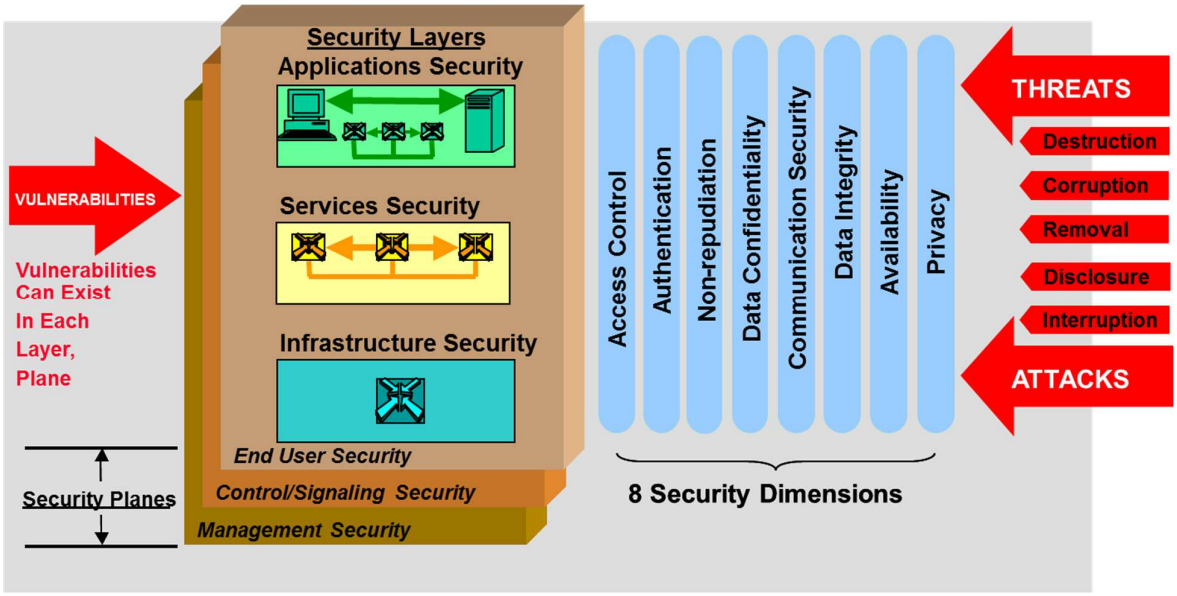

Figure 1. ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications

A further document, NIST SP800-30, "Risk Management Guide for Information Technology Systems" delivered by NIST (National Institute of Standards and Technology) [5], presents a guide for risk assessment, evaluation and mitigation more specifically related to IT systems (networks included). The risk assessment process in SP 800-30 takes inputs from a preparatory step that establishes the context, scope, assumptions, and key information sources for the process, and then uses identified threats and vulnerabilities to determine their likelihood impact on assets and risk. Figure 2 gives an overview of the key steps required in order to complete a comprehensive risk assessment program as outlined in NIST SP 800-3.

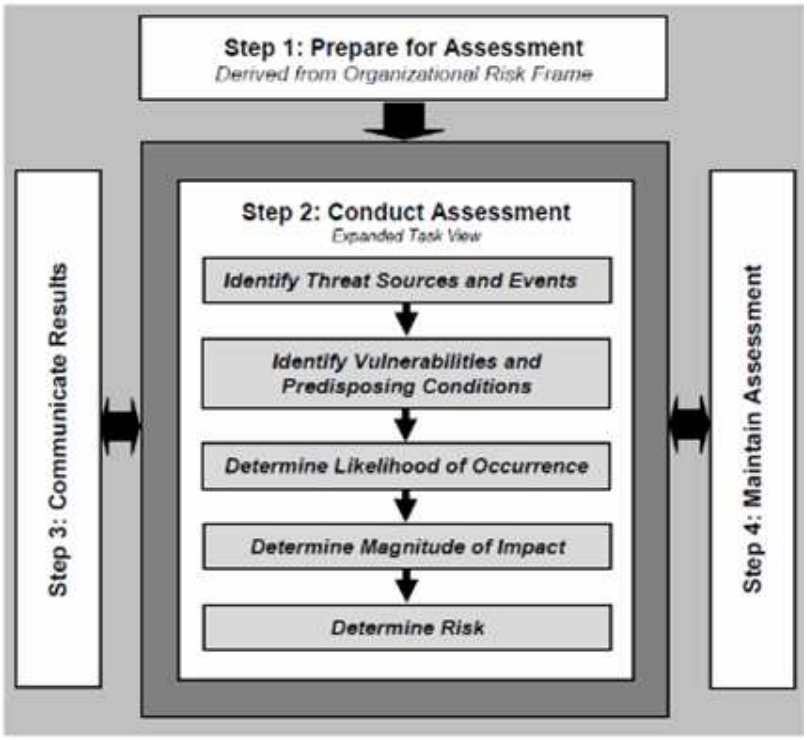

Figure 2. NIST SP800 -30 is "Risk Management Guide for Information Technology Systems"

Yet another standard, the ISO/IEC 27005:2011 'Information technology - Security techniques - Information security risk management' [6] contains the description of the information security risk management process and its activities, which include context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

The context establishment consists of:

- Setting the basic criteria such as the risk management approach, the risk evaluation criteria, the impact criteria and the risk acceptance criteria;
- Defining the scope and boundaries of the risk management;
- Defining the organisation and the responsibilities for information security risk management.

The risk assessment consists of:

- Identifying the risk by considering the assets within the defined scope, the threats, the vulnerabilities that can be abused by threats having a negative impact on the assets
- Estimating the risk by selecting the risk analysis methodology (which can be qualitative, quantitative or mixture of both) by defining the likelihood and determining the risk level for all relevant incident scenarios.
- Evaluating the risk evaluation by comparing the level of risk against the risk evaluation criteria and the risk acceptance criteria (defined in the context establishment).

The risk treatment consists of:

- Selecting four different options (risk removing, retention, avoidance, sharing) by considering the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options.

The purpose of ISO 27005 is to provide guidelines for information security risk management. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analysing risks to creating the risk treatment plan. For this reason the terminology and concepts used in ISO 27005 are widely accepted.

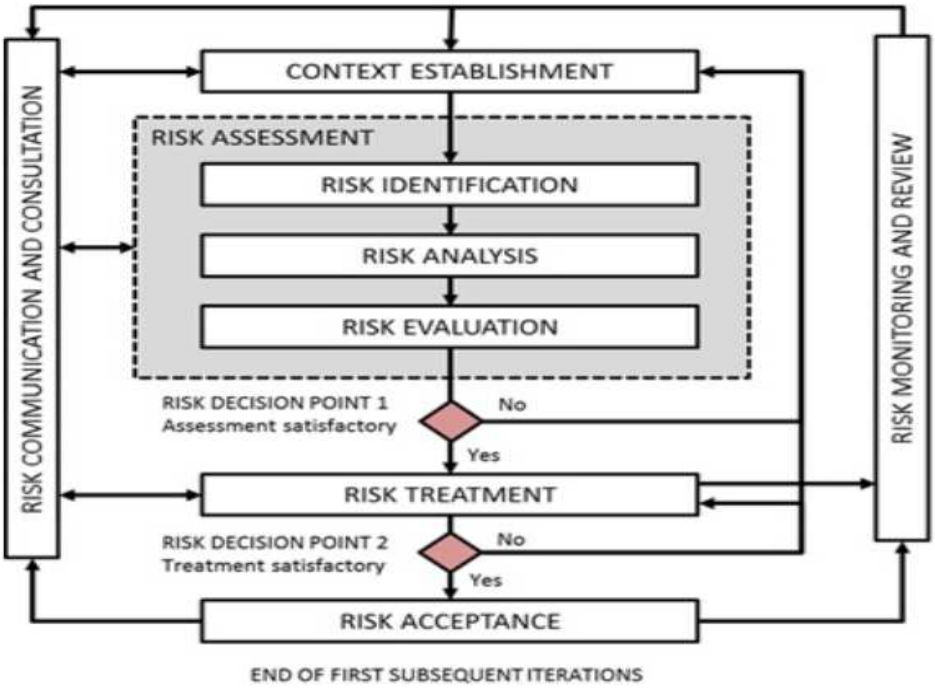

Figure 3. ISO/IEC 27005:2011 Information security risk management process

As a global remark on the methodologies, we want to outline that we have also considered the literature addressing the limits of the traditional well consolidated risk assessment methodologies we have considered herein [7]. It turns out that the traditional approaches, where assets are persistent items or properties of value and have owners, would work at their best in situations where the evaluated IT systems run in closed environment within an organization and therefore have unique owners, which is not always the case for 5G systems. For example, all roaming scenarios, and VMNOs which do not actually own the equipment (even though we can subdivide assets into the "service" of the operator and the actual hardware of the infrastructure owner). Nonetheless 5G-ENSURE adopts a traditional approach as the alternatives would require a larger consensus. For simplification the proposed methodology application will have to be reiterated for each security layer, and by each asset owner at the infrastructure layer. The higher services and application layers will have to take into consideration an inherent risk posed by threats/attacks at the infrastructure layer.

As a final remark, a bridge could be made to model driven approaches. Architecting and Engineering frameworks such as Arcadia enable to capture business and system's needs, requirements and functionalities and architecture by means of models. The benefit of these models is that they can be shared by different specialty stakeholders and can be used to confront different aspects of the model by means of specialty viewpoints. Risk management is one of the specialties which can be modeled this way [13].

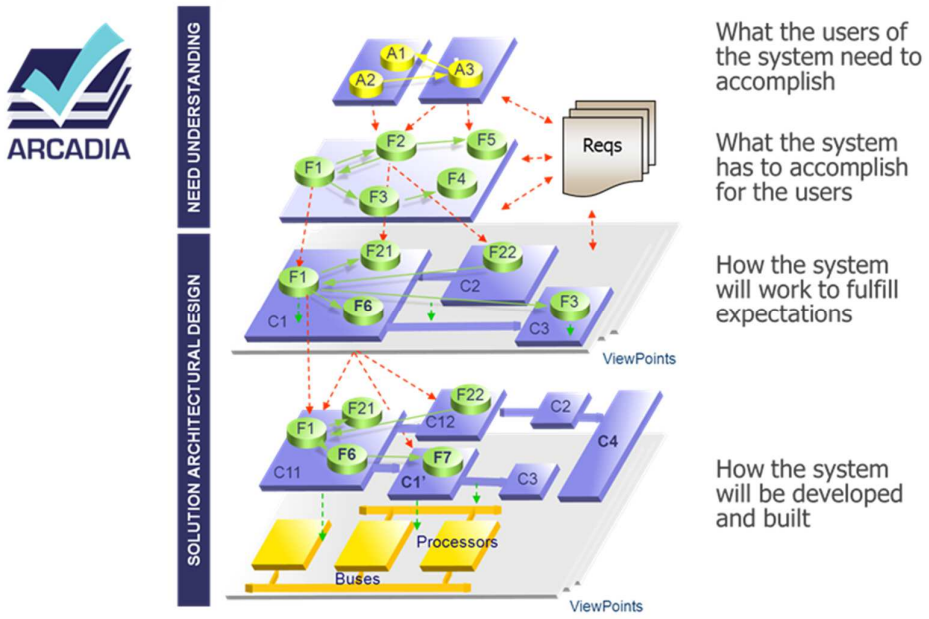

Figure 4. Arcadia methodology phases

The methodology decomposes the architecting and engineering work into a five layered model including User need or Operational analysis, System need analysis, Logical architecture, Physical architecture, and Product Breakdown Structure. It builds on a well-balanced consideration of three main part of the work: need analysis and modeling, requirements engineering and architecture building. The traceability between the three parts is determinant for change and evolution management.

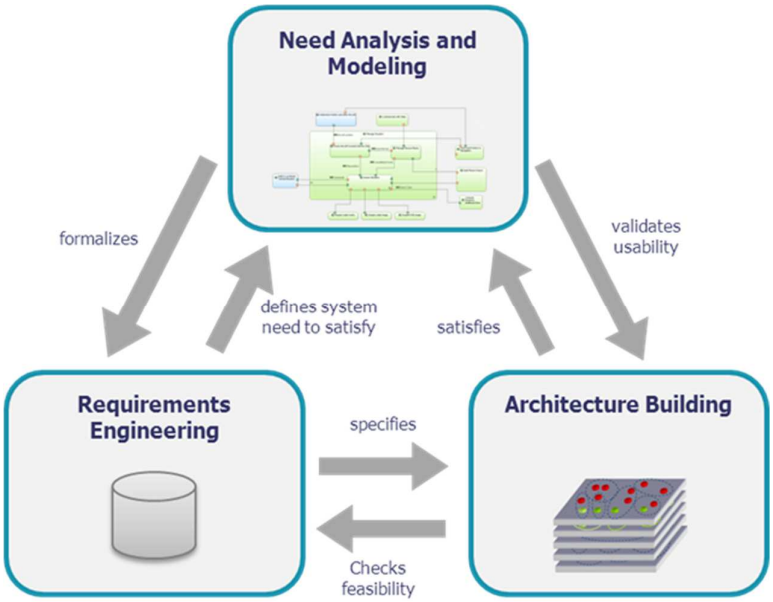

Figure 5. Arcadia methodology principles

4 Risk Management Context – Threats in 5G-ENSURE Use Cases

The methodology which will be used within the 5G-ENSURE project for the risk assessment is based on the Risk Management Process (ISO 27005) and, especially, on its simplification represented by NIST SP-800-30. We have based the process on this standard mainly for its wide-spread acceptance and usage in the IT industry and because it provides a complete well-defined and consistent terminology and methodology for risk management.

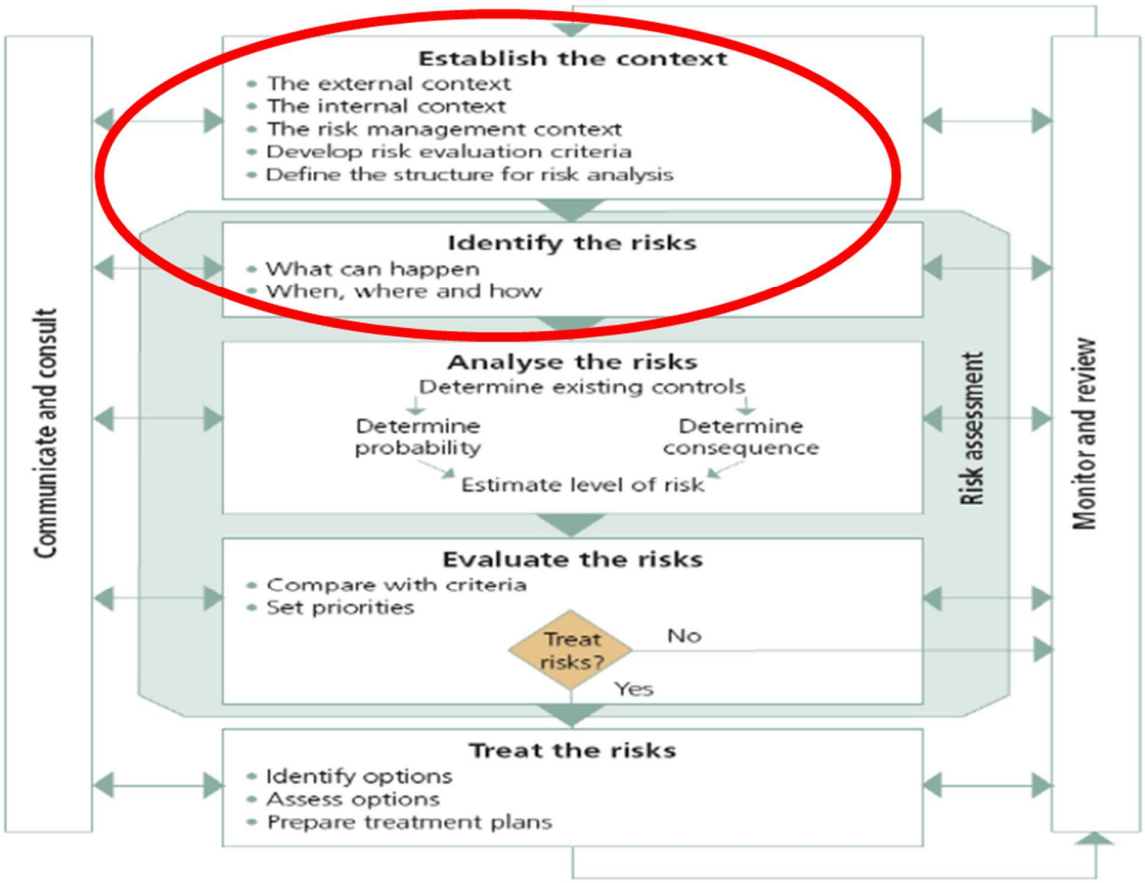

Figure 6. Complete Risk Assessment Procedure

According to the ISO 27005 standard, the Risk assessment process has 3 main parts, which will be detailed in the rest of the document:

- Risk identification
- Risk analysis
- Risk evaluation

Before going further, a reference 5G security architecture will be illustrated.

4.1 The reference 5G security framework

The reference 5G security architectural framework, where these risk assessment processes will be applied, is still under definition within the project's task 2.4. We can consider herein a high level architectural considerations proposed by the 5G-ENSURE project for 5G [14].

In particular, the concept of domain in 5G network and system has to be defined. A domain is traditionally (3G and 4G networks) the highest-level group of physical entities. Reference points are defined between domains.

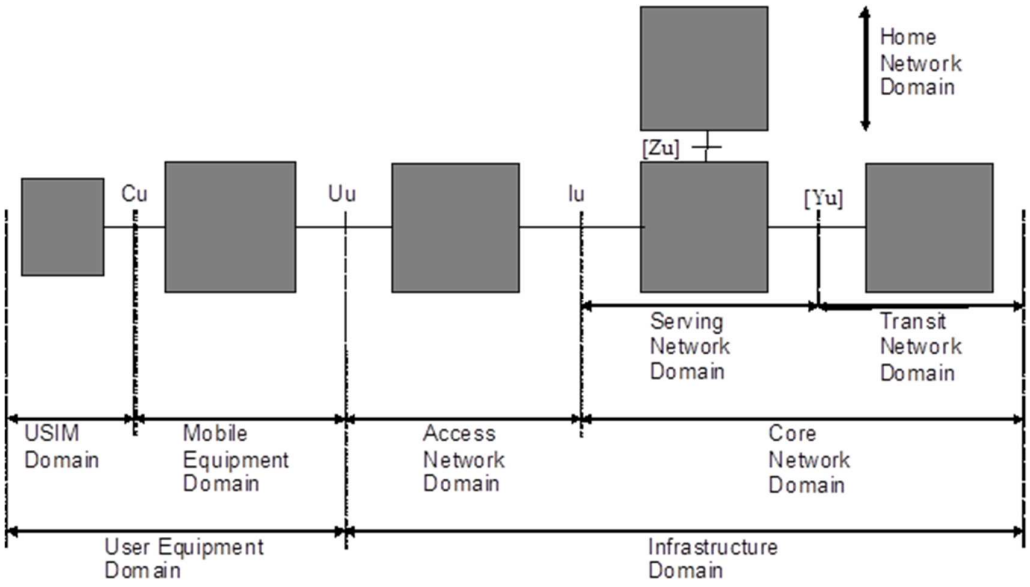

Figure 7. Domains defined in TS 23.101

This 4G domain structure may remain valid in 5G with the following considerations requiring adaptations and associated risk impact:

- in 5G we may have 3rd party ID providers (that may affect the home network domain)
- in 5G in the User Equipment domain we may have direct connections between UEs
- in 5G we may have several Infrastructure domains from different providers (owners), such as access/core/transit network or cloud infrastructure providers
- User Equipment and Infrastructure domain will remain as physical grouping
- the USIM, Mobile Equipment, Access Network and Core Network domains may to some degree remain as physical entities and will certainly remain valid as "trust domains".

The main concept not illustrated in the current domain's definition is the slicing concept introduced in 5G.

A draft security domains proposal for 5G which considers subdivision of domains and slicing is presented in Figure 8 (acronyms: "SN" = Serving Network, "AN" = Access network, "IM" = Identity Management, "ID" = Infrastructure providers e.g. ID2 could be Amazon EC2, "Rn" = Resource 1,2..n, etc.).

Specifically we use the following definition of **5G domain**:

- "A grouping of network entities according to physical *or logical* aspects, *relevant for 5G networks*."

Physical grouping is similar to 23.101. Logical groupings can be according to similarity in functionality (e.g. "RAN vs CN") or administrative/ownership related (e.g. "home vs serving", "operator vs 3rd party vertical" or "infrastructure provider vs tenant").

We propose to also add the concept of compound domains. **Slices**, as special services offered to 5G users seem to be an example of this since they may be "transversal" (e2e) to other domains. Slicing is indeed a major concern, on which strong security risk analysis has to be done.

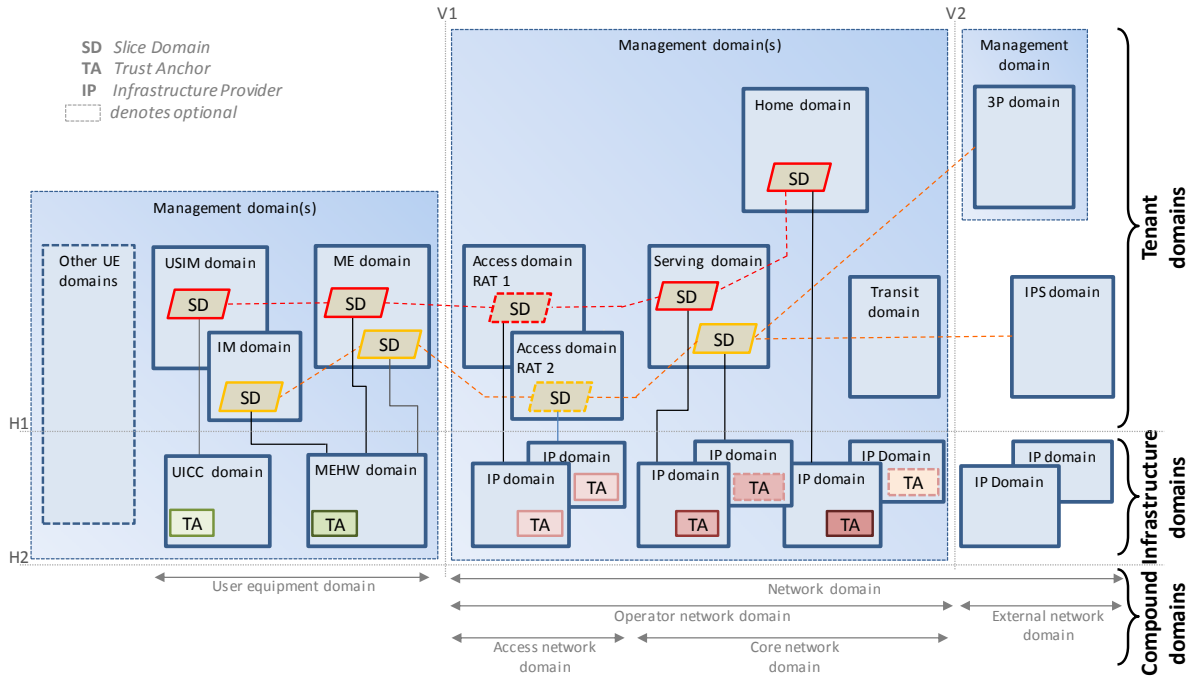

Figure 8. Domains of the 5G-ENSURE Security Architecture [14]

The functionality and communication protocols used in this domain structure maps to the **functional/logical strata** shown in Figure 9, taken from [14]. **A stratum** (in 23.101 parlance) is defined as "Grouping of protocols, *data and functions* related to one aspect of the services provided by one or several domains" (e.g. home stratum contains the protocols and functions related to the handling and storage of subscription data: functions related to subscription data management, customer care, including billing and charging, mobility management and authentication are located in this stratum).

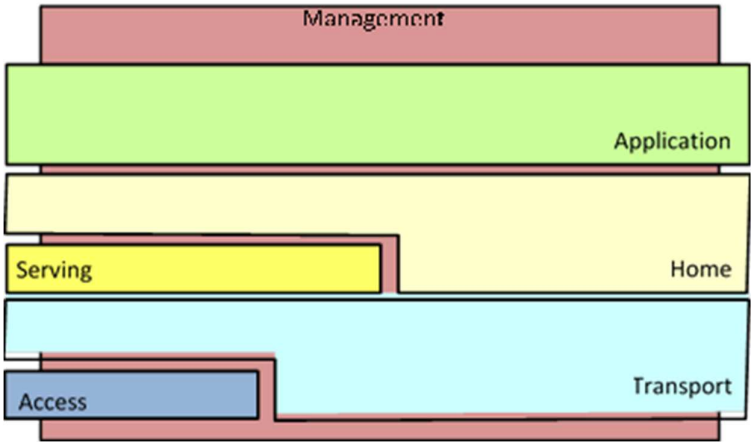

Figure 9. Strata of the 5G security architecture [14]

The application, home, serving and transport strata have been already identified within UMTS and remain the same in 5G, while the management stratum was not included before. **Management stratum** contains the protocols and functions related to network configuration: this includes the functions of creating and deleting virtualized networks and network slices. It also contains SDN specific protocols like OpenFlow and northbound APIs for network applications. Furthermore, network monitoring functionalities are also contained in the management stratum. Several issues are still to be addressed, e.g. if there is a need for a sub-stratum for security management or for monitoring (for detecting security anomalies, intrusion detection, lawful interception in a dynamic 5G network)? How to reflect multi-party trust issues? These are being discussed in ongoing D2.4 (5G-ENSURE security architecture) work.

For risk assessment purposes we note that these logical architectural views present a one to one mapping to the security planes defined in ITU-T X.805, which makes us more confident that the right approach is being followed in the initial steps of context establishment.

4.2 Risk Identification

The purpose of risk identification is to determine what factors can cause a potential loss/damage, and where and how it might happen (ISO, 2011). In order to manage the risks, it is necessary to identify the assets, consider the threats that could compromise those assets, and estimate the damage that the realization of any threat could pose to them.

4.2.1 5G-ENSURE Assets Identification

The first step is the identification of all the assets, within the 5G scope, that need to be protected, with special attention to those that are considered most critical because they cause most damage if compromised.

As a first step towards the assets identification we looked at the available taxonomies and we found a very simplified but still useful one from ENISA [12], where the main assets of a mobile network are grouped into the following 7 categories:

- Data Plane Assets:
  - *Network Elements*
  - *Communication medium*
- Control Plane Assets:
  - *Software*
  - *Hardware*
  - *Data*
- Application Plane Assets:
  - *Software*
  - *Hardware*
- Service provider IT Infrastructure:
  - *IT Infrastructure*
  - *Billing systems*
  - *Operator data*
  - *End user data*
- Network service provider physical infrastructure:
  - *Facilities*
  - *Energy Power*
- SDN users:
  - *End user data*
  - *SLAs and regulations*
- Human agents:
  - *SDN Administrators*
  - *SDN Application Developers*
  - *Network Service Operators*
  - *End User Application Developers*
  - *End User Application Administrators*
  - *End User Service Providers*
  - *End Users.*

The approach adopted within the 5G-ENSURE project was to start with this high level set of assets and try to come with more specific assets by focusing on a generic 5G mobile network vision. This list has been extended to contain the assets related to SDN and NFV technologies, since they will be largely used to implement the 5G mobile network.

In the rest of this section, we provide an enriched 5G assets list with a focus on mobile network vision. Though, we also propose a list of assets related to SDN and NFV technologies which can be used to implement the 5G mobile network.

We distinguish three types of assets: “Primary assets” which are functions and components related to a mobile network, “Secondary assets” which are associated to the technologies used to implement the mobile network (i.e., SDN and NFV technologies), and “actors” which are users and organizations participating to the 5G security use cases mainly described in D2.1.

Note that in the threat description tables from Chapter 5 we will indicate the ENISA high level asset categories in order to keep the tables simple and legible. More detailed 5G-ENSURE asset specification can be provided by each use case by filling in the appropriate field in the "Other" category.

4.2.1.1 Primary assets

We consider the following primary assets [9], [10]:

- **Components:** these are physical machines and servers used to provide mobile network functions.
  - **User equipment:**
    - **Secure Element:** This is a tamper resistant platform, e.g. certified at EAL4+.
    - **Mobile Equipment**
  - **Access Network**
    - **Base Station:** This is the antenna and hardware running functions related to radio transmission and reception such as Radio resources management, Mobility management and Security (i.e., confidentiality and integrity protection).
  - **Core Network:** This includes hardware servers used to run core network functions (home or serving).
- **Functions**
  - **Radio Resources Management:** allocation and maintenance of radio resources
  - **Mobility Management:** handover and inter-working management
  - **Session Management**
  - **Accounting and Charging**
  - **Security Management**
    - **Authentication and Authorization**
      - The authentication of mobile users
      - Authentication of "admin" personnel, network management , inter-network node authentication etc
    - **Confidentiality Protection**
      - core network encryption
      - air interface encryption
    - **Integrity Protection**
    - **Cryptographic Key Management**
      - Key Derivation: derivation of session and hierarchical keys
      - Key distribution: e.g. TLS keys for encryption of authentication protocols
      - Key Agreement
- **Services**
  - **IP connection:** Allocation and maintenance of IP addresses, naming resolution and, flow forwarding definition.
  - **Basics:** Voice / SMS
  - **Slice-specific service:** e.g. for critical MTC

4.2.1.2 Secondary assets

We consider the following secondary assets [11]:

- **SDN assets**
  - **Control Plane**
    - **Entities:** an entity has a given role(s) and performs one or several functions.
      - **SDN Controller**
    - **Functions** (realized by the entities)
      - **Network Topology discovery**
      - **Forwarding installation:** pushing forwarding rules from SDN controller to switches
    - **Components:** these are physical machines and servers over which an SDN controller can run.
  - **Data Plane**
    - **Components**
      - **Switches**
      - **Hosts**
    - **Functions**
      - **Forwarding execution**
- **NFV assets**
  - **Entities:** an entity has a given role(s) and performs one or several functions.
    - **NFV Orchestrator:** resource management of the NFV infrastructure and, lifecycle management of network services (e.g., instantiation, scale-out/in, performance measurement results, event collection and correlation, termination).
    - **VNF Manager:** life cycle management of VNF instances.
    - **VIM:** controlling and managing the NFV infrastructure compute, storage and network resources and, collection and forwarding of performance measurement results and faults/events information relative to virtualized resources.
  - **Functions** (realized by the entities)
    - **Resource management**
      - **Storage management**
        - **Isolation**
      - **Resource allocation**
        - **Virtual link allocation**
        - **VNF allocation**
      - **Post deployment VNF operations**
        - **VNF creation**
        - **VNF deletion**
        - **VNF scaling-out**
        - **VNF scaling-in**
        - **VNF scaling-up**
        - **VNF scaling-down**
        - **VNF updating**
    - **Security management**
      - **Confidentiality protection**
      - **Integrity protection**
      - **Trust boot (root of trust)**
  - **Components**

4.2.1.3 Actors

The actors are organizations and users that participate in use cases described in D2.1. They have been fully listed in the proposed 5G Trust model described in deliverable D2.5 [2]. We can summarize the 5G actors in the following succinct list and in Figure 10:

- Mobile/Satellite Network Operator (MNO) (taking the role of "home" or "serving" operator); commonly also the infrastructure provider
    - Virtual mobile network operator (VMNO) who purchases bulk capacity from MNOs and may (or may not) have their own HSS
    - Virtual mobile network operator (VMNO) who purchases SDN slices from an Infrastructure Provider
    - Factory or enterprise owner operating a AAA in a network linked to a (V)MNO
    - *Note that all (V)MNO entities submit to telecom regulation framework*
- Infrastructure Provider, including Virtual infrastructure provider (VIP), and satellite/HAPS provider
    - *those actors do not submit to telecom regulation framework, as they deliver technical services, as subcontractors, to operators (in the scope of their regulation framework)*
- Interconnect network provider
- Network access provider
- Service Provider including OTT/3rd Party service provider; commonly also the (V)MNO
- Network software provider, including VNF provider; commonly also the network equipment manufacturer
- Network equipment manufacturer
- User equipment manufacturer, including phone, USIM, sensor and robot
- User equipment software developer/provider, including OS, app and app store
- End user, including phone users, WSN owner/operator and enterprise employee
- Regulators, law enforcement agencies

An overall summary of 5G assets and actors is provided in Figure 10 below.

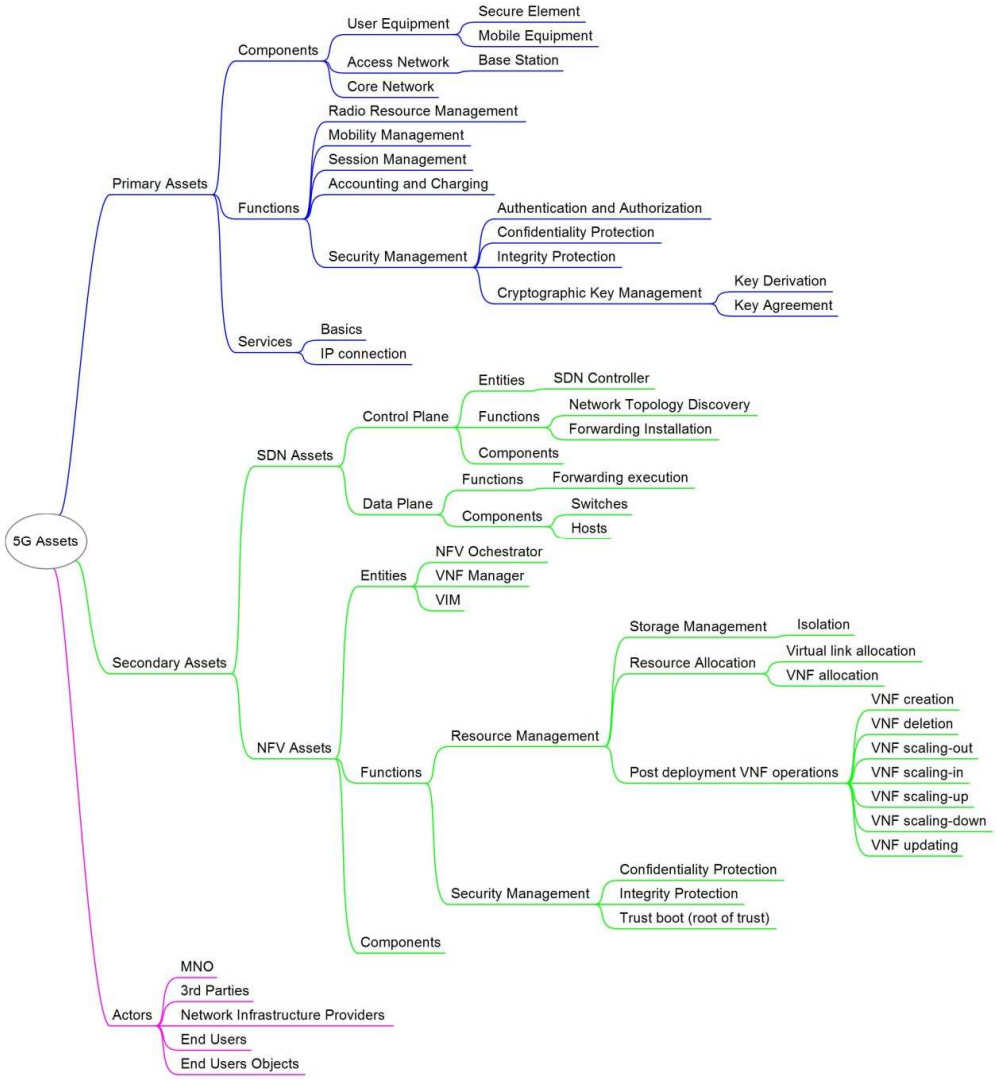

Figure 10. Summary of 5G Assets

4.2.2 5G-ENSURE Threat Identification and categorization

A threat analysis must start with a thorough threat taxonomy and identification in each specific context. A threat has a potential to exploit vulnerabilities and harm assets. Threat identification can be made based on history of previous incidents (if it exists) or an external threat catalogue. The approach adopted in this document has been to perform the identification of relevant threats through an assessment of a subset of use cases reported in the first technical deliverable of the project, D2.1. All use cases are evaluated regarding the possible threats to the list of asset reported in section 2.1.1. The advantage of this approach if compared to the one based on a predefined list of threats is that it can allow one to address the 'known unknown' or the 'unknown unknown' threats and therefore it allows for identification of individual threats depending on the specific context.

For this reason a set of the 5G use cases defined in D2.1 has been used to drive the threat analysis. The use cases have been analysed to gain an understanding of:

- the main threat/s the use case is exposed to
- the vulnerability exploited by the threat (threat's description)
- the category the threat belongs to
- the impact caused by the threats
- the assets the attacker would be interested in
- the entry point where a potential attacker could interact with the service and/or business-model described in the use case
- possible mitigation that is the set of controls or measures that could prevent the threat from causing impacts

The threat analysis based on 5G-ENSURE use cases is carried out using a clearly defined structure, to ensure that the correct information has been collected. For this purpose a specific template has been defined to derive threat descriptions from 5G-ENSURE use cases and facilitate the risk analysis associated with each threat. The template is illustrated in the following Figure 11.

ID: Unique ID # of the threat	*Numbering scheme: <T_UC-number_associated-threat-number>,* *e.g.* T_UC1.3_1, T_UC1.3_2, T_UC5.3_1, …
Name: Brief name of the threat	
Description: Detailed description of threat and its importance	
Category: ITU-T X.805 security dimension(s) – tick the appropriate box(es)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	
Assets impacted: What assets could be damaged? – from ENISA 5G/SDN asset categories, and/or others	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware*

	☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

Figure 11. Threat description template

There are various ways to classify the threats to a given system. A threat classification identified to be useful for the purpose of the 5G-ENSURE project is the one provided by ENISA in the *Threat Landscape for SDN/5G* [12]. The threat taxonomies in the form of a mind map is shown in the following figure.

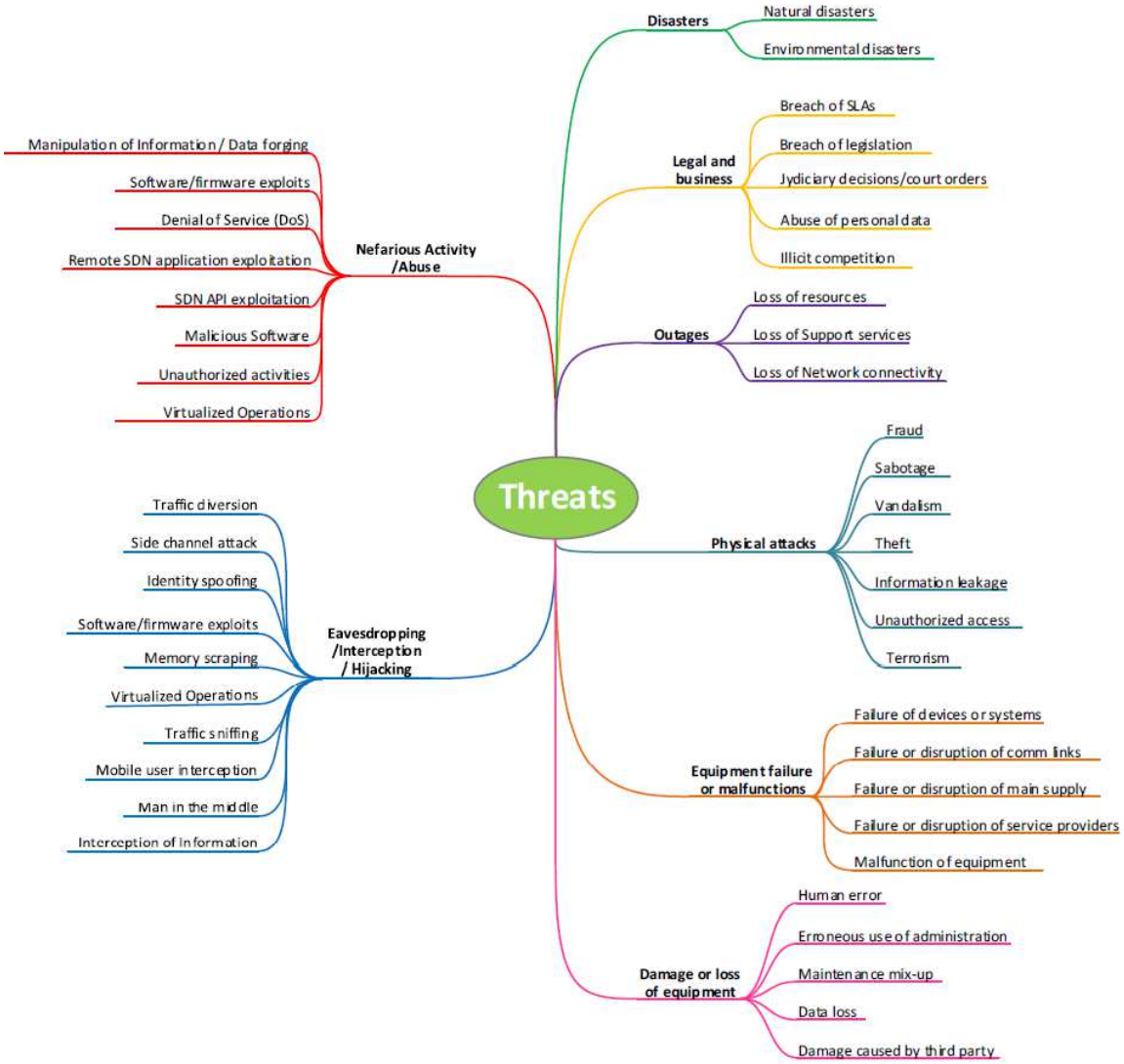

Figure 12. Lists of SDN/NFV/5G and Generic Network Threats (source ENISA)

The left side of the map lists the *threats specific to SDN/NFV/5G* referring to the categories:

- Nefarious Activity/Abuse
- Eavesdropping/Interception/ Hijacking.

The right side of the map lists the *generic network threats* referring to the categories:

- Disasters
- Legal and business
- Physical Attacks
- Outages
- Equipment Failure or malfunctions
- Damage or loss of equipment

The threat taxonomy from ENISA that is considered useful for the scope of the project is the one related to SDN/NFV/5G threats. Since having only two categories was considered too restrictive for the inclusion of the threats identified with the use cases analysis, it was decided to categorize the threats based on the ITU-T X.805 "security dimensions" herein reported:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

The list of threats derived from the analysis of the subset of 5G-ENSURE use cases (see full threat description in Chapter 5) and categorized based on the ITU-T X.805 security dimensions is reported in the following table.

Threat Category	**Threats derived from 5G-ENSURE use cases in D2.1**
Access Control	• *Unauthorised activities related to satellite devices or (satellite) network resources* • *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Compromised authentication gateway* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Hardening or patching of systems is not done* • *Unauthentic device installed into the system*
Authentication	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages*
Non-repudiation	• *Compromised authentication gateway* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Service failure over satellite capable eNB* • *Spoofed signalling messages* • *Disputes in charging* • *Compromised / malicious LI (Lawful Interception) function*

Data confidentiality	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Mobile user interception and information interception* • *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Forwarding logic leakage* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages* • *Disclose of sensitive data* • *Nefarious activities (malicious software, unauthorized activities, interception of information): privacy violations* • *Nefarious activities (manipulation of information, interception of information): personal information disclosure* • *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Communication security	• *Mobile user interception and information interception* • *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Forwarding logic leakage* • *Manipulation of forwarding logic* • *Misuse of open control and monitoring interfaces* • *Unauthorized access to a network slice* • *Bogus monitoring data* • *No control of Cyber-attacks by the Service providers* • *Compromise the availability and integrity of the radio interface* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Hardening or patching of systems is not done* • *Unauthentic device installed into the system* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Data integrity	• *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access*

	• *Misbehaving control plane* • *Add malicious nodes into core network* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages* • *Disclose of sensitive data* • *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Availability	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Authentication traffic spikes* • *Compromised authentication gateway* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Manipulation of forwarding logic* • *Fingerprinting attack* • *Misuse of open control and monitoring interfaces* • *Unauthorized access to a network slice* • *Bogus monitoring data* • *Security threats in a satellite network* • *Compromise the availability and integrity of the radio interface* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Service failure over satellite capable eNB* • *Spoofed signalling messages*
Privacy	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *User's privacy attack* • *Mobile user interception and information interception* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Misuse of open control and monitoring interfaces* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *User privacy policies are not respected* • *Nefarious activities (manipulation of information, interception of information): privacy violations* • *Nefarious activities (manipulation of information, interception of information): personal information disclosure*

	• *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*

The analysis of each specific 5G use cases is reported in Section 5, while the use cases themselves are briefly summarized in the Appendix 1.

4.3 Risk Evaluation methodology

The risk evaluation procedure is usually based on the identification of risk criteria and the definition of metrics for risk quantification based on likelihood and impact.

- **Risk criteria**: Decide on the acceptable level of risk for each activity / use case / asset
  - One can define a threshold of 'acceptable' risks (after their quantification as product of likelihood and impact), stating that only risks above value e.g. {4} should be treated...
- Define risk **Likelihood** & **Impact** metrics:
  - An even number of range of values is recommended, e.g. { *low, medium, high, extreme/critical* }, so as to avoid classical pitfall to evaluate likelihood and impact to the 'middle' value;
  - A likelihood range of values could be based on the periodicity of possible risk occurrence;
  - There is currently a debate within risk management community about the very concept of categorizing likelihoods, consequences (impact), risks and acceptability *vs.* simply ranking them on continuous scales…

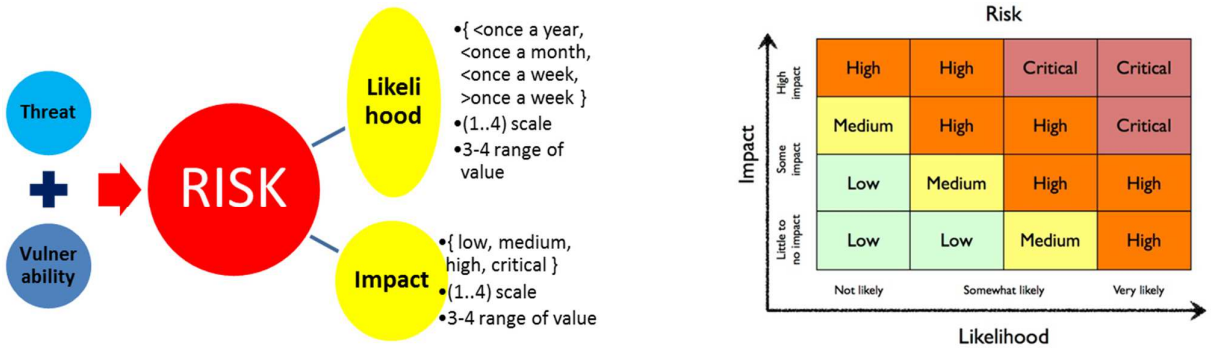

Figure 13. Risk Evaluation Procedure

Computing risk likelihood and impact for 5G assets is quite a challenge, since the system is not actually active and used yet. Three main approaches can be used:

1. Based on our evaluation on estimations performed for 4G systems.
2. Provide a theoretical value based on existing literature (again for 4G networks).
3. Based on our evaluation of values provided by the experts present in the 5G PPP projects.

The ETSI TVRA method [16] evaluates and calculates factors that are associated with the risks posed by the threats, which are time, expertise, knowledge, opportunity, equipment, asset, impact and intensity. The likelihood is calculated based on the attack potential value, which is calculated using the factors of time, expertise, knowledge, opportunity, and equipment. The impact is calculated from the asset impact value and the attack intensity value. The TVRA method usually defines three or four levels of risk: *Low*, *Medium*, *High* and *Critical*, which are derived from a qualitative combination of likelihood and impact. The *Low* risk level is the only one considered to be acceptable and, therefore, countermeasures should be introduced in order to reduce all *Medium/High* or *Critical* risks to *Minor*. There are two countermeasure strategies defined in the TVRA method, as follows:

i) asset redesign:

- removal of identified problem areas and weaknesses through fundamental design changes specifying the architecture, protocols and communications processes;
- can reduce both the likelihood and the overall impact of a successful attack.

ii) asset hardening:

- specification of additions to the system that will mask the effects of a problem area rather than remove it completely;
- likely to be used in cases where:
    - the cost of asset redesign is unacceptable;
    - the change itself is unnecessarily complex; or
    - redesign does not reduce the risk level to *Low (Minor)*.
- can only affect the likelihood of a successful attack, not the impact.

5 'Internal' threat description/analysis (from Use Cases)

The 5G-ENSURE project has proposed and analyzed use cases covering a wide variety of 5G deployment scenarios including Internet of Things, Software Defined Networks and virtualization, ultra-reliable and standalone operations. The analysis has produced 31 security relevant use cases grouped in 11 security clusters described in detail in the project's deliverable 2.1 [1], which highlight security issues inherited from current generation networks, as well as security and privacy functionality needed to support the new scenarios introduced in 5G. Most of the clusters focus on the availability, reliability and integrity of the network and the supported services. An initial threat analysis of the major use cases is provided as the basis. A more detailed analysis and risk mitigation recommendations are provided in the Annex B of this deliverable.

The reader is invited to refer to [1] for use case settings from which the threats are derived. Use case descriptions are not reproduced here.

Note that in the threat description tables we indicate the high level asset categories in order to keep the tables simple and legible. More detailed asset specification can be provided by each use case by filling in the appropriate field in the "Other" category.

5.1 Threat descriptions Use Cases cluster 1 - Identity Management

ID: Unique ID # of the threat	**T_UC1.3_1**
Name: Brief name of the threat	Unauthorised activities related to satellite devices or (satellite) network resources
Description: Detailed description of threat and its importance	Network Operators (e.g. SatNO) and M2M communications (e.g. updated satellite device SW) require fine-grained access to network resources (e.g. satellite device, eNB…). Also, satellite devices shall be authenticated to access satellite services (e.g. broadband access, direct-to-home services…). These network components and devices are distributed in a wide-area large enough that other wired or wireless network connectivity is not feasible. In this scenario, main threats are related to Unauthorised activities: • Unauthorised access • Unauthorised administration of devices and systems • Falsifications of configurations
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Information integrity. Information destruction. Service availability.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen):	Fine-grained access control focusing on the application level. In case of resource constrain devices (e.g. satellite devices), the fine-grained access control can be based on tokens evaluated directly in the device.

How can we protect against the threat?	
Entry Points (optional, if known): What possible means does an adversary have?	Non updated network components or satellite devices compromise system security/functionality. Wide-area distributed network composed of resource constrained devices (i.e. satellite devices) with high latency.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Fine-grained Authorization enabler.

ID: Unique ID # of the threat	**T_UC1.3_2**
Name: Brief name of the threat	Fake roaming from terrestrial network into satellite network (and vice versa)
Description: Detailed description of threat and its importance	Due to the fact that 5G is of multi-operator nature, 5G devices shall be connected to different networks. These 5G devices could be identified in either the satellite network or the terrestrial network with a set of credentials that allows access to both networks. Then due to coverage issues the 5G device performs a roaming to the other network. Non-repudiation of SLAs between integrated satellite and terrestrial networks and different operators should be considered. In this scenario, main threats are related to Legal and business category: • Breach of SLAs • Abuse of personal data from not honestly operators • Identity theft: a customer of MNO A (authenticated by A), present an identity of MNO B inside MNO B network thank to the roaming agreement (SIP fraud over VoIP interconnect) Thread agents could be dishonest external operators.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☒ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Service availability. Information confidentiality.

Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Integrating the envisaged 5G AAA system mechanisms with satellite authentication function using standard interfaces.
Entry Points (optional, if known): What possible means does an adversary have?	Heterogeneous security levels between network operators may allow fraudulent behaviours and permits customers to gain unauthorised access to content, services and resources.

5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Fine-grained Authorization enabler R2.

ID: Unique ID # of the threat	**T_UC1.4_1**
Name: Brief name of the threat	Compromised data
Description: Detailed description of threat and its importance	In this use case, the MNO needs to collect data about a user from the mobile network (step (c) in Figure 5 of Deliverable D2.1). If the user device or any network component is compromised, this can tamper with the integrity and confidentiality of the collected data. As the metrics provided to the service provider are cryptographically computed based on the collected data, collecting fake data may compromise the metrics, hence, the provided service.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☒ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	In order to provide this enhanced service, the MNO needs to have an assurance about the validity of the collected data. This may imply the use of attestation protocols between the collect points (in the network) and the MNO.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems*

	☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	In order to protect against this threat, the MNO needs to perform validity checks on the collected data. The solution may include remote attestation protocols and investigation in statistics data processing.
Entry Points (optional, if known): What possible means does an adversary have?	An adversary can have one or all the following means: Communication channels, user equipment and a network component
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Generic collector interface enabler can be part of the solution.

ID: Unique ID # of the threat	**T_UC1.4_2**
Name: Brief name of the threat	User's privacy attack
Description: Detailed description of threat and its importance	The MNO performs cryptographic computations on the collected data to obtain metrics. These metrics are going to be shared with the service provider (Step (d) in Figure 5 of the deliverable D2.1). If the computed metric do not properly anonymize user's data, this can break the user's privacy.

Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The MNO must carefully choose the cryptographic mechanisms used to compute the shared metrics.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users*

	☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	A solution can consider the state of the art about secure attribute sharing mechanisms and perhaps enhancements or adaptations of these mechanisms to the mobile network context.
Entry Points (optional, if known): What possible means does an adversary have?	In order to get the shared metrics between the MNO and the service provider, an adversary can control the communication channel or compromise the service provider.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

5.2 Threat descriptions Use Cases cluster 2 - Enhanced Identity Protection and Authentication

ID: Unique ID # of the threat	**T_UC2.1_1**
Name: Brief name of the threat	Mobile user interception and information interception
Description: Detailed description of threat and its importance	In some situations in current mobile networks (GSM and UMTS and in all networks during an emergency call setup) the IMEI is sent to the network in plain text. This opens the door to device identity disclosure and unauthorized device tracking attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, end users, end devices …) or e2e effect…	User privacy violation through IMEI (International Mobile Equipment Identity) interception and tracking.

Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	The solution space includes exploration of protocol enhancements and investigation into state-of-the art end-to-end encryption/anonymization techniques, offering protection against device identity disclosure and unauthorized device tracking. Therefore 5G should ensure that the IMEI is sent only in a confidentiality protected message (e.g., through encryption). In addition the enhancement should aim to also address the emergency call case where the IMEI is sent over the network unprotected. This may imply the implementation of additional possibly public key-based cryptographic techniques

Entry Points (optional, if known): What possible means does an adversary have?	Communication channel (IMEI sniffing over the air)
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The Enhanced Identity Protection Enabler and Device Identifier(s) Protection may be employed to provide IMEI encryption as well.

ID: Unique ID # of the threat	**T_UC2.2_1**
Name: Brief name of the threat	Tracking of device's (user's) location
Description: Detailed description of threat and its importance	Terminals' (and users owning them) location can be tracked by eavesdropping identifiers transmitted between a base station and user terminal. [1, 2] The location can be tracked using either permanent identifiers, which may be transmitted when device joins the network, or using temporary identifiers (pseudonyms like GUTI or TMSI). Such identifiers are broadcasted in clear text so that devices identify which communication is targeted for whom. If such identifiers are not changed (re-pseudonymized) before an adversary is able determine which identifier belongs to a victim, so the victim's location can be tracked. Broadcasting a temporary identifier, which is known or suspected to belong to Alice, is an indication that Alice is close to the broadcasting base station. By analysing signal directions, Mallory may be able to determine UE's location more accurately.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☐ Communication security; ☐ Data integrity; ☐ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	5G network is not able to protect end-user's privacy and will be considered less trustworthy by the end-users.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data*

	☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Using of encrypted identifiers when possible. However, devices need to be aware that the communication is targeted for them, so encrypted identifier will become a pseudo-identifier that can be mapped to the device. Frequent changing of temporary identifiers. This solution may add complexity or signalling.
Entry Points (if known): What possible means does an adversary have?	Adversaries must link terminals identifiers to the users' identity. This can be achieved by triggering the mobile network into initiating the generation of paging messages to the victim (and thus to victim's terminal). For instance, adversaries may connect users with using social media application to initiate unobtrusive communications. Location tracking can be done at the granularity of base station's coverage or in more detail if the adversary has capabilities to analyse signal directions. Also, detailed location tracking is possible by eavesdropping plaintext signal measurement reports.

ID: Unique ID # of the threat	**T_UC2.2_2**
Name:	Mobile user interception and information interception.

Brief name of the threat	
Description: Detailed description of threat and its importance	In some situations in all current mobile networks the IMSI is sent to the network in clear text. This opens the door to subscriber's identity interception/disclosure and unauthorized user tracking attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	User privacy violation through IMSI (International Mobile Subscriber Identity) interception and tracking.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐*Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers*

	☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Potential solutions to provide for subscriber privacy include encryption of the IMSI and/or use of improved pseudo-identifiers. Anonymisation systems may be investigated to provide for unlinkability of subscriber and device identities.
Entry Points (optional, if known): What possible means does an adversary have?	Communication channel (IMSI sniffing over the air, rogue eNBs)
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The Enhanced Identity Protection Enabler may be employed to provide IMSI protection through encryption and improved anonymization to temporary identifiers.

5.3 Threat descriptions Use Cases cluster 3 - IoT Device Authentication and Key Management

ID: Unique ID # of the threat	**T_UC3.1_1**
Name: Brief name of the threat	Authentication traffic spikes
Description: Detailed description of threat and its importance	Simultaneous or periodic authentication events may cause excessive amount of traffic for network. Adversaries – aiming to perform a denial-of-service attack - may try to initiate traffic spikes or emphasize the effects of natural traffic spikes with IoT application specific means. As a consequence, the network will experience more signalling and authentication functions needs to perform more processing. Potentially, the authentication of devices may fail and devices may lose connectivity.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☐ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The 5G network must be over-resourced in order to handle large short-term traffic amounts.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☒ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Different means may be utilized to mitigate traffic spikes. Methods include relying gateway or one group member to perform authentication on the behalf of individual devices. For instance, using group authentication schemes such as [3]. Monitoring and filtering approaches can be used to mitigate effects.
Entry Points (if known):	The traffic spikes may emerge naturally in the IoT network as devices may be programmed e.g. to join the network at the same time. However, an adversary

What possible means does an adversary have?	may try to guide this behaviour with different means, for instance, by tampering network time or causing power outages to get large amount devices to authenticate at the same time.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC3.1_2**
Name: Brief name of the threat	Compromised authentication gateway
Description: Detailed description of threat and its importance	Compromised and maliciously acting node providing authentication on the behalf of a group – an IoT gateway or a mobile phone - may endanger IoT devices' security. Authenticating node may act as a man-in-the-middle – tamper or eavesdrop communication – or provide tampered security configurations. As a result, data collected from IoT devices may leak from to wrong parties and IoT devices may receive commands from malicious party.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☒ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	5G network will have more potentially misbehaving end-points. Application services cannot rely on strong authentication of individual nodes.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data*

	☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	
Entry Points (if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC3.2_1**
Name: Brief name of the threat	Leaking keys
Description: Detailed description of threat and its importance	End-to-end keys may be stolen or leak from the centralized key servers. The key server may also become tampered. As a consequence, the end-to-end secured communication is vulnerable for different attacks and adversaries gain an access to the end-points. The may e.g. provide false information to application services or send malicious commands to IoT devices.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality;

	☒ Communication security; ☒ Data integrity; ☐ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The leaking keys will compromise the security (confidentiality and integrity) of those applications that are end-to-end secured.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☒ *End User Application Developers* ☒ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known):	The key server could be used only for authentication purposes and not for delivering the sessions keys. This would make attacks more difficult as the

How can we protect against the threat?	attacker would be required to compromise the server to provide wrong (asymmetric) authentication keys and then mount an interception attack on the end-to-end communication. However, all IoT devices may not be computationally capable to asymmetric key operations. The key server should be hardened to withstand attacks. The server cannot be isolated from the open internet as it needs to be available for the clients. However, some isolation techniques – e.g. micro-segmentation – may be utilized to control which applications may access the server.
Entry Points (if known): What possible means does an adversary have?	Attacker may compromise the key server in various ways. For instance, the attacker may utilize vulnerabilities in server interfaces to gain an access to the service. Lawful interception mechanisms may be vulnerable and leak keys for third-party attackers or authorities that are misusing their privileges.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

5.4 Threat descriptions Use Cases cluster 4 - Authorization of Device-to-Device Interactions

ID: Unique ID # of the threat	**T_UC4.1_1**
Name: Brief name of the threat	Unauthorized data access
Description: Detailed description of threat and its importance	The main threats are due to a malicious user who may want to access the sensors' data without authorization. Such a malicious user may either try to generate a fake token or try to modify the security policy to get access to the sensors. Moreover, the AAA server may introduce several vulnerabilities in the 5G network infrastructure, which have to be carefully investigated. In any case, an investigation of liabilities between parties will have to be performed (AAA owner, sensor owner and 5G operator).
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The sensors become vulnerable to information leakage and tampering as well as denial-of-service attacks.

Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☒ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Use of authorization mechanisms, for example based on tokens. The generation of the authorization token should be based both on the security policy, as defined by the sensor owner, and on the 5G credentials which provides the overall trust. The AAA server activities should not affect the security of the 5G Network to which it is connected (for example not contribute to other attacks such as cloning, eavesdrop of communication, network element compromise, etc.).
Entry Points (if known): What possible means does an adversary have?	To compromise a sensor: • Adversaries may send malicious commands / policies to the sensor or sensor controller/gw, can install malicious software. • Alternatively, adversaries may compromise sensor's traffic.

5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.5 Threat descriptions Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitoring

ID: Unique ID # of the threat	**T_UC5.1_1**
Name: Brief name of the threat	Misbehaving control plane
Description: Detailed description of threat and its importance	Malicious or compromised control plane may jeopardize the network and the data plane. For instance, a compromised SDN controller or virtualization orchestrator may prevent data flows or direct them to a man-in-the-middle switch for eavesdropping or tampering. Centralized network controllers are an alluring targets for attacks as adversaries are not required to compromise switches or network functions it is enough that they steer data flows to their own malicious components.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The network and applications become vulnerable to eavesdropping and tampering as well as denial-of-service attacks.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure:

	☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☐ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Strong protection should be provided for control plane components. They should authenticate and authorize commands and support up-to-date trusted interfaces.
Entry Points (if known): What possible means does an adversary have?	To compromise control plane: • Adversaries may send malicious commands / policies to the controller, if controller does not strongly authenticate and authorize the source of the policies. As a consequence, a legitimate controller will behave maliciously according to adversaries' policies. • Alternatively, adversaries may compromise legitimate control plane component, for instance, by utilizing weaknesses in the controller and its interfaces. • Adversaries may also get credentials to provide the controller policies using e.g. social engineering attacks against the operator. A data plane may be misconfigured so that it accepts control commands also from other slices or external parties. If data plane does not authenticate commands from the controllers, an adversary may masquerade as legitimate control plane component and send malicious southbound control messages.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.2_1**
Name: Brief name of the threat	Add malicious nodes into core network
Description: Detailed description of threat and its importance	Malicious nodes may e.g. eavesdrop, tamper, and prevent data flows.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☐ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Confidentiality, integrity and availability of e2e communication are compromised.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☐ *SDN Application Developers*

	☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Applying security verification procedures – technical and organisational - for assuring that the added nodes are trustworthy. Only authenticated and authorized entities should be allowed to add nodes. Security monitoring of behaviour of added nodes as well as communication over the network.
Entry Points (if known): What possible means does an adversary have?	Software, image used for deploying new nodes may be compromised. Forwarding logic may be misconfigured so that illegitimate node, switch is able to get access to data flows. In this case, the malicious node is unintentionally added to the core network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.2_2**
Name: Brief name of the threat	Forwarding logic leakage
Description: Detailed description of threat and its importance	A network application running on the controller is able to see the forwarding logic of another application (i.e.: the OpenFlow rules installed in the switches). The applications can belong to different virtual network operators who do not want to leaking sensitive information about how their virtual nodes are located or migrated. The leakage can happen in two directions. Controller-to-switch contains rules that have been installed in the switches. A malicious application can not only intercept the OpenFlow messages as they are sent, it can also request information from the switch about installed rules and related statistics belonging to other applications. Eavesdropping on switch-to-controller (e.g.: OFPT_PACKET_IN) messages can also leak information not only about the forwarding logic, but about application data that might be confidential.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability

	☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Information about forwarding logic is leaked: positioning of network elements like DNS or other services provided through VNFs and how they are migrated which can be used to infer user population, reliability information etc.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen):	Insert a reference monitor at the southbound interface.

How can we protect against the threat?	
Entry Points (optional, if known): What possible means does an adversary have?	Deploy an application on the controller in a multi-tenant virtualized network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Enabler 6.2 “Access Control Mechanisms”

ID: Unique ID # of the threat	**T_UC5.2_3**
Name: Brief name of the threat	Manipulation of forwarding logic
Description: Detailed description of threat and its importance	The setting is the same as T_UC5.2_2, however this time the attacker decides to become active. Instead of simply gleaning information about the forwarding logic of a competing application running on top of the same controller, it modifies the flow entries.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☒ Data confidentiality ☒ Communication security ☒ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	In order of increasing attacker power and severity: • Overflow the switch table causing the switch to act much slower (due to limited TCAM), causing degraded performance • Evict or delete rules, causing denial of service • Modify rules to redirect data plane traffic through attacker’s listening point, causing all data to be intercepted (instead of just the initial PACKET_IN from the passive case) • Modify rules to intercept and tamper data.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware*

	☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	See T_UC5.2_2
Entry Points (optional, if known): What possible means does an adversary have?	See T_UC5.2_2
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	See T_UC5.2_2

ID:	**T_UC5.3_1**

Unique ID # of the threat	
Name: Brief name of the threat	Fingerprinting attack
Description: Detailed description of threat and its importance	Unlike T_UC5.2_2, the attacker is external to the controller. The attacker can measure the time of reconfiguring the physical network. This way, the attacker can gain information about which and when a network packet triggers a reconfiguration of network components.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The attacker can exploit the obtained information to mount DoS attacks by overloading the controller with packets that will most likely trigger a reconfiguration of the network. Furthermore, installing flow rules in current SDN switches is a costly operation. This means that even the performance of the physical network can be impacted.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations*

	☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Enabler 6.1 “Anti-fingerprinting”

ID: Unique ID # of the threat	**T_UC5.5_1**
Name: Brief name of the threat	Misuse of open control and monitoring interfaces
Description: Detailed description of threat and its importance	Third-party service providers may misuse the access to control and monitoring interfaces and cause service disruptions for the operator or attack against data flows. For instance, monitoring information on flowing data may be captured in order to profile end-users. While interfaces are opened for service providers they may also become available for other adversaries.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☒ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Resources and user data become available for larger amount of parties. More trusted parties means that there may be parties that do not provide good enough security and follow good security practises.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Service providers should be required to protect the monitoring data they acquire. Service providers should protect their own resources sufficiently, so that adversary cannot access slices through service providers' systems. Strong isolation is needed to prevent service providers from accessing resource outside a slice. Service providers should be allowed to access only

	those control interfaces that are required to minimize service providers potential to escape
Entry Points (if known): What possible means does an adversary have?	Control interfaces can be enable access to operator's functions either directly (if not sufficient fine-grained protection is available) or the interfaces may contain vulnerabilities that may be utilized to gain additional privileges. A service provider itself may be untrustworthy. Alternatively, an adversary may compromise service providers systems in order to gain access to the slice.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_2**
Name: Brief name of the threat	Unauthorized access to a network slice
Description: Detailed description of threat and its importance	Isolation of the slice may fail allowing a service provider to gain an access to resources belonging to the operator or other slices. This may jeopardize availability and security of the operators and other services providers' network services.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Availability and security of operators' resources and service provider's resources jeopardized. This may prevent opportunities that are gained by opening operator's network to third-party service providers.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure:

	☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☒ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Strong isolation between slices is needed. Authentication and authorization over the access to control and data plane. Security monitoring is needed to detect ongoing incidents.
Entry Points (if known): What possible means does an adversary have?	Failing or misconfigured authentication and authorization both in the control or data plane may enable access to slices.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_3**
Name: Brief name of the threat	Bogus monitoring data
Description: Detailed description of threat and its importance	False monitoring data / measurements may cause monitoring / control plane to perform wrong control actions. For instance, adversary may impair the availability of the system by getting nodes (which will appear malicious) to be dropped from the topology. The adversary may also change forwarding policies in order to affect availability or to direct data flows into nodes that are e.g. under the control of the adversary and may thus perform eavesdropping or tampering.

Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The threat in impairs availability of the network services and may ease eavesdropping and tampering attacks against the data flows. The threat also makes security monitoring (or security countermeasures that are based on monitoring) less effective.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☒ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐

Possible Mitigation Hints (if known): How can we protect against the threat?	Sources of monitoring data should be authenticated and the source identity information should be available for the information user. In cases where monitored data is processed, e.g. aggregated, and then made available for other parties, the original sources of data could be available to enable information users to make sufficient estimates on the reliability of the data. The sources of bogus measurements may be detected by monitoring the measurements streams and analysing the data e.g. against correlated data sources.
Entry Points (if known): What possible means does an adversary have?	Adversaries may produce bogus information easily if the measurement sources are not authenticated. If sources are authenticated, an adversary may try to invade and compromise an authentic measurement source.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_4**
Name: Brief name of the threat	No control of Cyber-attacks by the Service providers
Description: Detailed description of threat and its importance	The use case features a Service Provider (SP) offering its Massively Multiplayer Online Game service to gamers. The Service Provider buys its network service to Virtual Mobile Network Operator (VMNO) which itself relies on an Infrastructure Provider. The VMNO supplies a sub-slice to the SP with the required QoS. The service of the SP is subject to cyber-attacks. The SP wants to manage the cyber-security of its service. It signs a contract with a third party Security Service Operator (SSO) to monitor and remediate to cyber-security attacks. Thanks to the terms of the contract between the SP and the VMNO, the SSO can benefit from network topology information and routing tables from the slice controller. Nevertheless, since it has not the information about the configuration of the NVF and their vulnerabilities, it cannot build a classical attack graph to monitor the cyber-attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☐ Availability; ☐ Privacy
Potential effect: What effect it will have on 5G system (network, hosts, applications…)	The Service Provider has no control over the cyber-attacks on its slice.
Assets impacted:	

What assets could be damaged?	☒ Data Plane Assets: ☒ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☒ *Software* ☒ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☒ *Billing systems* ☒ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	A possible mitigation hint would be to enable the SSO to get access to the information from the infrastructure domain, especially the type of software used for NVF in order to establish the vulnerabilities of it. Another way to mitigate this is to separate the responsibilities by contract between the infrastructure domain and the VMNO. The SP will have to rely on the VMNO interface and will only control its cyber-threats at application level.
Entry Points (if known): What possible means does an adversary have?	An adversary could attack the VNFs, hypervisor or orchestrator of the Infrastructure Provider to compromise the Service Provider's service.

ID: Unique ID # of the threat	**T_UC5.6_1**
Name: Brief name of the threat	Security threats in a satellite network
Description: Detailed description of threat and its importance	Security client-side agents are deployed over the satellite network components in order to periodically collect information related to the security dimensions. Once registered, these components deliver to the security monitoring (server-side) the compiled information. This information is supervised in the security monitor that carry out a security analysis to detect attacks and malicious behaviour. The origin of most fraudulent accesses or security breaches can be summarized as either technical identity alteration (after an illegal or illegitimate privilege augmentation) or signalling messages received outside of the normal sequences. These systems are exposed to new threats in 5G that must be mitigated. …). Some of the threats identified are: • Attack on network components: RF interference, power or communications lines… • Attack on the network management system: intruding the system by hijacking, blackmailing, placing or impersonating the operator, to obtain credentials or/and gain control of the system… • Denial of service: flood the network with dummy indicators to make the network unusable, preventing any useful communications with the network management system.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☒ Authentication ☒ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☒ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The security properties that this threat can compromise are: • Service availability • Outages • Information confidentiality
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data*

	☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	System can be protected against these threats acting on three levels: • Client-side: Generic secure interface to provide indicators from a heterogeneous network. • Server-side: Data analytics and intelligence-driven security to detect threats based on security metrics. • Network-side: Partitioning the satellite network into virtual private networks.
Entry Points (optional, if known): What possible means does an adversary have?	Heterogeneous networks (satellite and terrestrial) which components are geographically widespread distributed. Some of these network components (e.g. eNBs) are outside the MNO facilities and even on the customer's premises (e.g. satellite device).
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Satellite Network Monitoring

5.6 Threat descriptions Use Cases cluster 6 - Radio Interface Protection

ID: Unique ID # of the threat	**T_UC6.1_1**
Name: Brief name of the threat	Compromise the availability and integrity of the radio interface
Description: Detailed description of threat and its importance	A critical communication device D, e.g. serving critical infrastructure or used by user Bob in an emergency situation, is trying to attach to the MNO's network. The network is busy serving many other attach requests so D does not get immediate access to the network. Even devices which are attached but lose radio synchronization are required to perform the random access procedure and may become locked out of the network in these situations.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Potential consequences include: • Disrupted availability of critical communications network. Deceptive illegitimate requests may cause disruption in network access • Emergency and critical communication requests cannot get higher priority than non-urgent attachment requests
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power*

	☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	• A secure method for priority of access requests • Save resources by rejecting illegitimate or non-prioritized request at early stage, i.e. enable integrity protection at a low layer in the radio network stack • Give priority for re-attachment to devices losing radio synchronization • Threats of cyber-attacks directly targeting 5G networks needs to be dealt with in the 5G design
Entry Points (if known): What possible means does an adversary have?	Access to the radio interface is required, for example by means of a fake BTS.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.7 Threat descriptions Use Cases cluster 7 - Mobility Management Protection

ID: Unique ID # of the threat	**T_UC7.1_1**
Name: Brief name of the threat	Denial of service due to Unprotected Mobility Management Exposes Network
Description: Detailed description of threat and its importance	User powers on his phone, as part of the LTE specification [TS33.401] the phone will initiate an "*Attach request*" to the base station (eNB). Once connected to the MNO, the user equipment (UE) will send periodic tracking area update (TAU) request messages intended for the MNO's Mobility Management Entity (MME).

	1. Attacker intercepts the TAU request and responds with a TAU Reject with EMM cause number 7 "*LTE Services not allowed"* or cause number 8 "*LTE and non-LTE services not allowed".* 2. User's phone accepts the TAU Reject message and acts accordingly a. If EMM cause number 7, user's phone will consider itself invalid for LTE services. If supported the phone will connect to available 3G or 2G networks b. If EMM cause number 8, user's phone will consider itself invalid for all services and enter the state EMM-DEREGISTERED.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	• The TAU Request is sent without confidentiality protection, hence the attacker can decode it. • The TAU Reject message is accepted by the UE without integrity protection and without an established security context between the UE and network. • The "*Attach request"* is sent unprotected, hence the list of the network capabilities can be altered by the attacker. • The "*Forbidden PLMN*" are accepted by the UE without integrity protection and without an established security context between the UE and network. These vulnerabilities can be used to perform a denial of service or downgrade attacks, which persists until the user reinserts the USIM, reboots the UE, or in one case, physically moves the UE to a new tracking area.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data*

	☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Security monitoring could be one solution to capture those attacks where UE is denied service or forced to use weaker services. UE that previously has been able to use full services, typically does not downgrade its own capabilities. If the TAU Reject messages were digitally signed, which are verified by the UE, an adversary's messages would be rejected by the UE. This would require the introduction of MNO specific public keys. A mitigation that makes it more difficult to implement a persistent denial of service attack would be to introduce a mechanism based on a timer or counter value, to allow the UE to re-attach itself to the network after a certain time. To mitigate the man-in-the-middle attack on the *Attach* request, the 5G network could require an identical integrity protected reconfirmation of the network capabilities as is required for the security capabilities in LTE.
Entry Points (if known): What possible means does an adversary have?	Access to the radio interface is required, for example by means of a fake BTS.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.8 Threat descriptions Use Cases cluster 8 - Ultra-Reliable and Standalone Operations

ID: Unique ID # of the threat	**T_UC8.1_1**

Name: Brief name of the threat	Service failure over satellite capable eNB

Description:
Detailed description of threat and its importance
	Main threats that may cause a service failure are related to the following activities:
	• Failures or malfunctions:
	  ○ Failure or disruption of communication links
	  ○ Failure or disruption of main supply
	  ○ Failure or disruption of service providers
	  ○ Malfunction of equipment
	• Outages:
	  ○ Network connectivity
	  ○ Loss of physical resources
	  ○ Support services (Internet provider or Electricity provider)
	• Disasters:
	  ○ Natural disasters
	  ○ Environmental disaster
	• Physical attacks:
	  ○ Sabotage
	  ○ Vandalism
	  ○ Terrorists attack
	
	A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity with some QoS guarantees to be used by its customers. Therefore, the Service Provider has to ensure that the SatNO is providing what is required by the contract (SLA).
	This threat is particularly acute in ultra-reliable services (i.e. e-health, lifeline communications, military scenarios…).

Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Service availability or traffic congestion

Assets impacted:
What assets could be damaged?
	☐ Data Plane Assets:
	  ☐ *Network Elements*
	  ☐ *Communication medium*
	
	☐ Control Plane Assets:
	  ☐ *Software*
	  ☐ *Hardware*

	☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Allowing the Service Provider to have some degree of control over their micro-slice or sub network enabling dynamic allocations and network reconfigurations on the fly. Evolving the Transport Network Architecture (TNA) by combining both satellite and terrestrial transport architectures. Once a link failure has been detected, new topology is forwarded to base stations with satellite links and smart antennas, enabling topology reconfiguration according to traffic failures and traffic demands.
Entry Points (optional, if known): What possible means does an adversary have?	4G backhaul networks are fixed topologies, therefore the network barely manages accidental/deliberate link failures or traffic congestion. An exhaustive radio planning is needed before base station deployment and new backhaul nodes cannot be easily added.
5G-ENSURE enablers (optional, if covered for given threat):	Once a link failure/congestion is detected, Satellite Network Monitoring provides a Topology algorithm to reconfigure the network components.

What possible means does an adversary have?	

5.9 Threat descriptions in Use Cases of Cluster 9 - Trusted Core Network and Interconnect

ID: Unique ID # of the threat	**T_UC9.1_1**
Name: Brief name of the threat	Spoofed signalling messages
Description: Detailed description of threat and its importance	If the authenticity of the messages related to the user cannot be verified, the integrity of the actions cannot be ensured. The actions can cause effects, which lead to further compromises or have other unwanted consequences. This applies to other signalling messages as well, e.g., management related.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☒ Authentication ☒ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Network could take actions that were not really authorized by the user. This could relate to billing (customer gets extra charges that were not caused by them) or it could cause messages (such as SMS) redirected to somewhere else (potentially leaking information). Also, if management messages are spoofed, this could change the infrastructure, potentially in a devastating way.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure:

	☐ *IT Infrastructure* ☒ *Billing systems* ☒ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	All signalling messages should be integrity protected and bound to correct entities. Cryptographic identities is one possible approach.
Entry Points (optional, if known): What possible means does an adversary have?	Adversary can try to inject signalling traffic into the core by either subverting a node inside the core or bypassing the filtering of ingress traffic.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.1_2**
Name: Brief name of the threat	Disputes in charging

Description: Detailed description of threat and its importance	The user could dispute charges or operator could place unfounded charging on the user actions. Basically, the operator can produce billing records, but the customer has no way of proving whether they are correct or not.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Decrease of trust into the system and loss of revenue.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☒ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☒ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators*

	☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	The charging related messages should have non-repudiation properties. Cryptographic identities could be one possible approach of creating records that are always strongly bound to the entity and cannot be disputed afterwards.
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.1_3**
Name: Brief name of the threat	Disclose of sensitive data
Description: Detailed description of threat and its importance	If visited network is not well-established operator, e.g., this could be a mall network, then there is an amount of certainty regarding the trust level of the interconnect party for the home network. In order to provide service to the end user, the visited network needs to obtain, e.g., authentication vectors from the home network. In general, the requests for such sensitive information should come only from verified source (and not necessary just relying on network topology).
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☐ Availability ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Obtaining sensitive information in unauthorized fashion could lead to further compromise of the network and possibly make it easier to spoof other entities.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Interconnect networks need to be authenticated and authorized. One should not rely on requests coming from a certain network address (e.g., coming through an established IPsec tunnel).

Entry Points (optional, if known): What possible means does an adversary have?	Potentially malicious interconnect partner or other malicious entity within operator network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.2_1**
Name: Brief name of the threat	User privacy policies are not respected
Description: Detailed description of threat and its importance	If the system provides the possibility for the user to dictate user specific privacy policy to be handed over to the visited or home network, nothing prevents the operator from not honouring this policy. This could lead to the breach of user privacy.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	User trust to the system is decreased.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software*

	☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☒ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Regulatory sanctions and oversight could decrease the incentives to engage in disclosing user information to third parties. Audit programs could be used to monitor compliance.
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.3_1**
Name:	Hardening or patching of systems is not done

Brief name of the threat	
Description: Detailed description of threat and its importance	If the systems are not hardened correctly or if the patching processes do not keep the systems up-to-date, the systems could be compromised through the vulnerabilities existing in the systems.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Systems can be compromised through the vulnerabilities and elevated privileges gained. Thus, total control of a node can be achieved.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☒ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☒ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators*

	☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Monitoring of systems can help in detecting breaches. This can potentially be cooperative actions between different operators, so that indicators of compromise are reported to the operator of the source traffic. Proper segmentation of systems can isolate the breach to only one system. Thus, other systems should be considered potentially hostile.
Entry Points (optional, if known): What possible means does an adversary have?	Abuse of software vulnerabilities in the software
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Proactive security analysis and remediation Microsegmentation

ID: Unique ID # of the threat	**T_UC9.3_2**
Name: Brief name of the threat	Unauthentic device installed into the system
Description: Detailed description of threat and its importance	Breach of physical security could result in an unauthentic device to be installed into the network.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Unauthentic device could send traffic to the network and pose to be an authentic entity. This could lead to various man-in-the-middle or spoofing attacks.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☒ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☒ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☒ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Proper physical security measures are needed to prevent access to the communication equipment. Logical access control also needs to be in place to ensure that no unauthorized device can be just plugged into any open port. Hence, devices need to be authenticated before allowed to access the network. Monitoring can be used to detect unauthentic devices or traffic that does not match the typical usage pattern of the network.

Entry Points (optional, if known): What possible means does an adversary have?	Physical plugging in of the device
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Proactive security analysis and remediation Microsegmentation

5.10 Threat descriptions in Use Cases of Cluster 10 - 5G Enhanced Security Services

ID: Unique ID # of the threat	**T_UC10.2_1**
Name: Brief name of the threat	Nefarious activities (malicious software, unauthorized activities, interception of information): privacy violations
Description: Detailed description of threat and its importance	Mobile devices and the installed applications disclose a large amount of private information both personal and device related information mostly through misbehaving apps, PUAs (Potentially Unwanted Applications), adware and ransomware.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, end users, end devices, e2e effect…)	Threat effect: information leakage, disclosure of sensitive info, privacy violation in general.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware*

	☐ *Data* ☐ Application Plane Assets: ☒ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☒ *End User Application Developers* ☒ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Potential solutions include means to protect the user's privacy at the application layer. The 5G network adopts a privacy policy containing various privacy parameters (related to device and apps activity on user data) that can be controlled on user's demand or upon some anomalous event detection. The 5G network offers to subscribers a service that checks the privacy risk of devices and their installed apps. A useful tool for this service is to require the mobile applications and servers to declare a human readable privacy policy and to offer a tool to the user's device to verify it. 5G should support an application level service that provides privacy policy analysis.
Entry Points (optional, if known): What possible means does an adversary have?	Compromised devices by malicious app.

5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The enabler is Policy Privacy Analysis

ID: Unique ID # of the threat	**T_UC10.3_1**
Name: Brief name of the threat	Nefarious activities (manipulation of information, interception of information): personal information disclosure
Description: Detailed description of threat and its importance	Mobile devices and/or the installed applications (malware/spyware, misbehaving applications and also common applications) disclose a large amount of personal and device identifying information (e.g., IMSI, phone number, location data, IMEI etc.).
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Threat effect: information leakage, disclosure of sensitive identifying info, privacy violation in general.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data*

	☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☒ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Potential solutions include an anonymization service that can be subscribed by 5G users needing it (5G users that have privacy concerns regarding their data). Network offers to subscribers a SIM (or a device) that implements anonymization algorithms like for example lightweight format preserving algorithms that can be implemented with little computational resources. Network offers to subscribers a means to configure their anonymization preferences.
Entry Points (optional, if known): What possible means does an adversary have?	Mobile Device
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The enabler is SIM or device-based Anonymization.

5.11 Threat descriptions in Use Cases of Cluster 11 - Lawful Interception

ID: Unique ID # of the threat	**T_UC11.1_1**
Name: Brief name of the threat	Compromised / malicious LI (Lawful Interception) function
Description:	Attacking the LI function may result in to various issues: unauthorized disclosure of user's data / communications, a disruption or degradation of the

Detailed description of threat and its importance	service used by the user, and reporting fake or compromised information about the suspected data.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	A solution may encompass mechanisms to check the validity of the reported data and mechanism to check the validity of the LI function.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers*

	☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	We can consider the state of the art about remote attestation mechanism and perhaps investigate enhancements of these mechanisms.
Entry Points (optional, if known): What possible means does an adversary have?	An adversary may attack the LI function.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC11.2_1**
Name: Brief name of the threat	Nefarious activities (manipulation of information, interception of information) over LI-aware network
Description: Detailed description of threat and its importance	The user data traffic can be eavesdropped and manipulated on some possible paths if there is no end-to-end protection. In this way the user data privacy is not guaranteed completely from its source to the final destination.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☒ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Data disclosure, data manipulation with e2e effect
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium*

	☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	5G should provide an optional end to end encryption service Potential solutions include an end-to-end encryption service applicable on IP or higher layer independently by the type of UE using an application which is installed as part of the service. The encryption key may be part of an escrow system provided by the 5G operator to enable secure communication and at the same time enable lawful interception.
Entry Points (optional, if known): What possible means does an adversary have?	Communication medium using a fake access node or a compromised mobile device.
5G-ENSURE enablers (optional, if covered for given threat):	The enabler is end to end encryption.

What possible means does an adversary have?	

5.12 Risk mitigation proposals from Use Case analysis

Initial threat descriptions resulting from an analysis of a subset of 5G-Ensure use cases were performed in Chapter 5. Later we completed a full use case analysis, describing 'Sunny day' vs 'Rainy day' scenario and locating involved 5G processes, resources and stakeholders within 5G-Ensure architecture. This analysis is provided in the Annex B: COMMON D2.5+D2.6 ANNEX: Use Case Analysis and describes related trust implications and threat mitigation strategies.

For each of the threats identified in our threat & risk analysis it is necessary to consider what measures could be implemented to reduce the risk of an attack being successfully mounted in 'Rainy day' scenario. The following table specifies a range of options evaluated as potential countermeasures / threat mitigations, together with risk quantification, which is expressed in scale {*Low/Medium/High/Critical*}.

Countermeasure / mitigation strategy	Threat (ID)	Risk
Charging solution; factory owner's network resource isolation	Freeride devices authenticated by factory owner (T_UC1.1_1)	High
IMEI transport layer encryption	Leaked AAA/IMEI credentials (T_UC1.2_1)	High
Real time data gathering; traffic trend analysis	Unauthorised activities related to satellite devices or (satellite) network resources (T_UC1.3_1)	Medium
Monitoring probes	Fake roaming from terrestrial network into satellite network (T_UC1.3_2)	Medium
Validity checks on the collected data; remote attestation	Compromised data from user device (T_UC1.4_1)	High
Collected data anonymization such as k-anonymity algorithm	User's privacy attack (T_UC1.4_2)	Critical
IMEI protection/encryption during transport	Mobile user interception and information interception (T_UC2.1_1, T_UC2.2_2)	High
Privacy enhanced identity protection	Tracking of device's/user's location (T_UC2.1_2, T_UC2.2_1)	Medium
Data plane encryption	Passive communication interception (T_UC2.3_1)	High
Group-based authentication, monitoring & filtering	Authentication traffic spikes (T_UC3.1_1)	Critical
Certified software / hardware	Compromised authentication gateway (T_UC3.1_2)	High
Service and device discovery	Leaking e2e keys (T_UC3.2_1)	Critical
AAA at the token level	Unauthorized data access on sensors (T_UC4.1_1)	Medium
Micro-segmentation to split network slices into smaller parts	Misbehaving control plane (T_UC5.1_1)	Critical
Advanced software verification; node behaviour monitoring	Add malicious nodes into core network (T_UC5.2_1)	Critical
	Forwarding logic leakage (T_UC5.2_2)	High

Reference monitor at the southbound interface	Manipulation of forwarding logic (T_UC5.2_3)	Critical
Slice load monitoring & capacity adjustment	Fingerprinting attack on a virtualised network (T_UC5.3_1)	Critical
	Misuse of slice control and monitoring interfaces (T_UC5.5_1)	Critical
	Unauthorized access to a network slice (T_UC5.5_2)	Critical
Physical hardware location imprinting; TPM/HSM binding; packet delay analysis	Generic VNF Location hacking (T_UC5.4_1)	High
Software / image authenticity & integrity verification	Manipulation of data stored in VNF repository (T_UC5.4_2)	Critical
Strong checksum of the content	Compromised software signing key (T_UC5.4_3)	Critical
Full system audit	Integrity of the testing machine compromised (T_UC5.4_4)	High
Monitoring data source authentication	Bogus monitoring slice data (T_UC5.5_3)	High
SSO-VMNO-VIP interface (data access) assurance	No control of cyber-attacks by the Service Providers (T_UC5.5_4)	High
Satellite network monitoring for RT events & alarms; Integrating Satellite and Terrestrial systems for topology reallocation	Security threats in a satellite network (T_UC5.6_1)	High
	Service failure over satellite capable eNB (T_UC8.1_1)	High
Access request prioritization	Unable to attach radio interface when Overloaded (T_UC6.1_1)	High
Integrity checking on packets in eNB or ePC edge	Unprotected User Plane on Radio Interface (T_UC6.2_1)	High
Integrity protection reconfirmation	Denial of service due to Unprotected Mobility Management (T_UC7.1_1)	Medium
	Spoofed signalling messages (T_UC9.1_1)	High
Roaming connection / capacity monitoring	Standalone EPC loses connection to the Home Network (T_UC8.2_1)	Medium
Cryptographic identities on Interconnect	Spoofed signalling messages (T_UC9.1_1)	High
	Disputes in charging on Interconnect (T_UC9.1_2)	High
	Disclose of sensitive data on Interconnect (T_UC9.1_3)	High
Regulatory schemes, audits; Privacy policy analysis on Interconnect	User privacy policies not respected (T_UC9.2_1)	Medium
VNF Certification; Proactive Security Monitoring	Hardening or patching of systems not done (T_UC9.3_1)	High
	Unauthentic device installed into the system (T_UC9.3_2)	High
Anomaly-based network intrusion detection	Botnet subverted user equipment (T_UC10.1_1)	High
App-level privacy policy analysis	Nefarious activities on privacy violation (T_UC10.2_1)	High
SIM/Device-based Anonymization	Nefarious activities on personal information disclosure (T_UC10.3_1)	High
Remote attestation; software integrity verification	Compromised / malicious Lawful Interception (T_UC11.1_1)	High
Configurable e2e encryption on IP or higher layer	Nefarious activities over LI-aware network (T_UC11.2_1)	High

6 Holistic approach to risk analysis of 5G system infrastructure

6.1 5G PPP major security risks

5G PPP security White Paper [15], as the result of a joint effort across the various 5G PPP Phase 1 projects, lists the following major 5G security risks:

- Unauthorized access or usage of assets, e.g. 5G Identity thefts or cloning, opportunistic and fraudulent usages of shared resources, unauthorized access and/or modification of 5G connected devices critical data, etc.;
- Weak slices isolation and connectivity, e.g. sensitive data, managed inside a slice, could be exposed to applications running in other slices services, through side channel attacks;
- Traffic embezzlement due to recursive/additive virtualization;
- Insufficient technology level readiness (TRL);
- Difficulties to manage vertical SLA and regulation compliance, e.g. difficulties to address, manage and deliver, from an E2E perspective, the verticals' SLA and to comply with actual present regulations and known evolutions of the regulatory framework;
- Slicing VS Neutrality risks, i.e. slicing concept seems not to be fully compatible with network neutrality concept, while both, however, are regulated by the EU Regulation;
- Trust Management Complexity and liabilities between parties in complex 5G infrastructures;
- Provisions to facilitate change of service provider Domain Lock-in, i.e. lack of common security standards and guarantees across multiple domains could lead to provider lock-ins, a slice owner being unable to easily and flexibly migrate all or parts of its virtual service infrastructure from one provider to the other, without affecting or degrading the security requirements and the expected levels of security SLAs.

6.2 Holistic view on 5G 'System of systems' risks

In this section we present a method to identify outer threats, which were not captured by 5G-ENSURE use case analysis, by applying a prospective approach over 5G 'system of systems'.

Indeed, 5G may be defined as a 'System of Systems': a programmable multi-service network called upon to support a vast array of uses with diverse performance needs. E.g. connecting huge numbers of consumer health sensors is a very different proposition (mission-critical) to delivering high quality UHD video to TV sets (massive broadband). Clearly, 5G networks will need to offer a greater range of capabilities than 4G technologies, by meeting all these requirements invisibly from the user's perspective into a single 'System of systems'.

This means that 5G is a multi-RAT and programmable networking system, which natively combines LTE and new 5G technologies, in addition to other access types like Wi-Fi or fixed (optical), in addition to massive virtualisation and software-defined technologies, including private/public clouds, mobile edge data centers, converged control functions, shared data layer, OSS systems etc. (Figure 14). The new 5G 'System of Systems' will be built upon a strong foundation with an adaptive and programmable multi-service architecture.

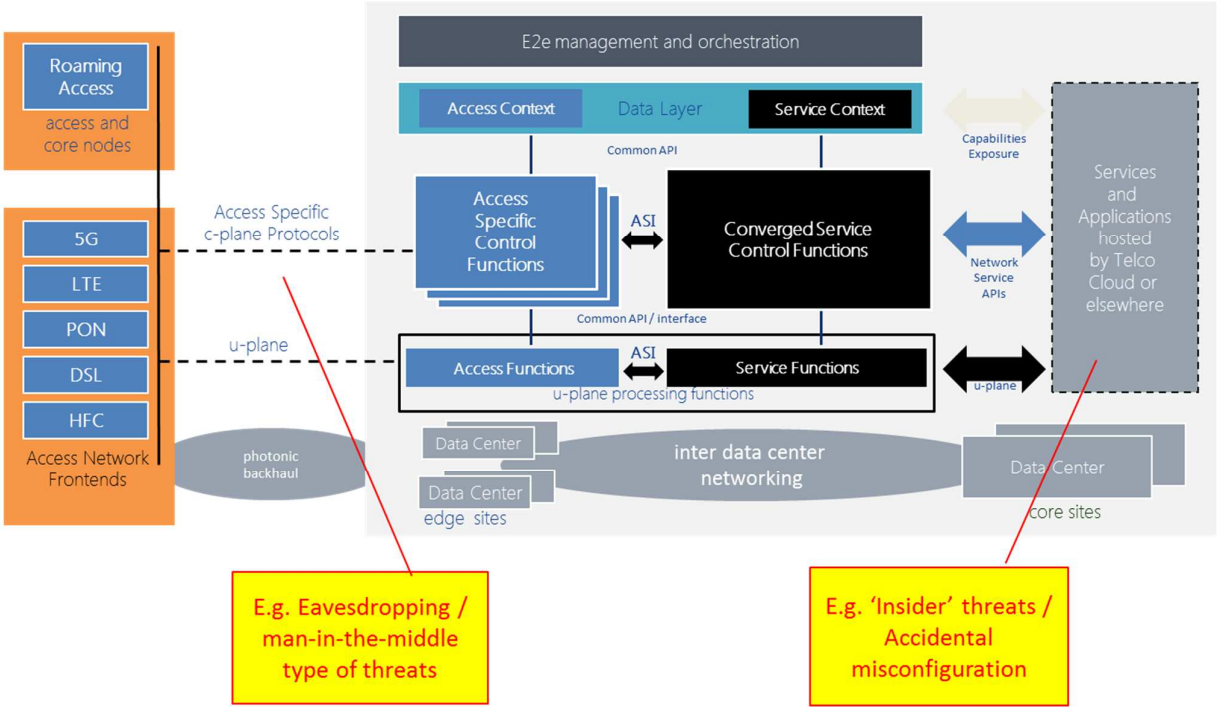

Figure 14. Example of holistic analysis of 5G 'system of systems' threats

If we apply a holistic attack vector / risk analysis from technology point of view over the 5G 'System of systems' multi-service architecture, we will be able to identify additional threats which were not apprehended during 5G-ENSURE use case analysis. For instance, additional threat types can be captured (Figure 14, non-exhaustive list):

- man-in-the-middle type of threat over control- or user-planes,
- overload/congestion attacks (DDOS type) over signalling- or user-planes,
- frequency jamming attacks over different frequency bands for e.g. IoT devices / PLMN,
- accidental misconfiguration of e.g. services hosted in the telco cloud or incorrect SDN / backhaul MPLS configurations,
- unappropriated QoS policy settings / QoS class mappings,
- perimeter protection breaches (e.g. interdomain interfaces, roaming, DNS, SS7…),
- etc.

In the remainder of this section, we will strive to identify new attack vectors, and then possible additional threat types. These are given for illustration purposes, with no ambition to be totally comprehensive, as 5G systems are still under definition. Two technological areas impacted by 5G are explored – mobile access and virtualization related threat types.

To start securing a mobile operator network one must first identify the specific attack vectors, as shown in the following diagram:

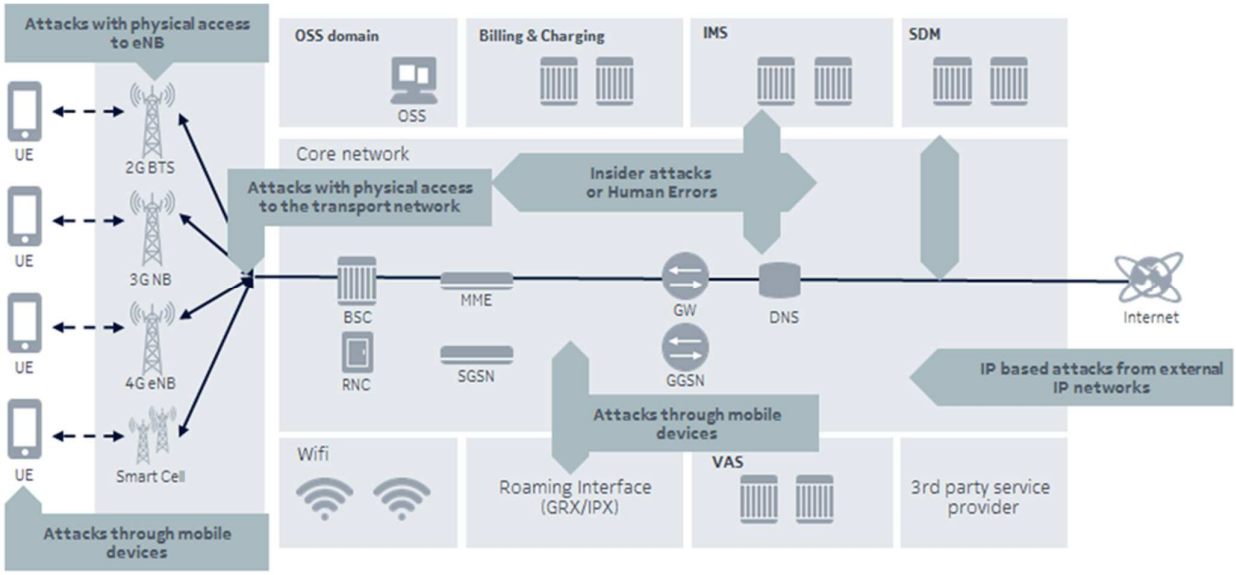

Figure 15. Attack vectors in a mobile operator network

The main attack vectors for mobile networks (relevant to both 4G and 5G) are:

- Attacks coming from the Internet (external network).
- Attacks coming from the roaming interface (both data and signaling interfaces).
- Attacks coming from the transport network, using or targeting the transmission lines or communication channels connecting the base stations to the core network.
- Attacks targeting the base stations themselves as the most exposed network elements regardless of the radio technology (4G/5G) or type (macro, micro or Femto).
- Insider attacks, originating from the internal domains.
- Growing threats coming from the devices connected to the network i.e.:
  - targeting the mobile operator infrastructure directly,
  - directed towards targets outside the operator network but using the operator infrastructure directly or indirectly (such as DNS amplification attacks).

Cloud computing and virtualization promise lower costs and greater business agility to allow operators to adapt to fast-changing user demands and creating new services models. With cloud-based model evolution, inherent security threats from the virtualization layers are becoming critical threats also endangering privacy. Attributes like VNF, hypervisors, elasticity of resources, distributed, heterogeneous and shared infrastructure bring a set of challenges, which were not present in traditional non-cloud deployments.

Figure 16. Threat vectors pertinent to cloud-based models

NFV transformation is bringing a new paradigm for security. Even a private cloud requires telco-cloud-specific security features to provide a comparable grade of security as in traditional telco networks. Key security challenges and threats are:

- Virtualization technologies increase the attack surface:

The Hypervisor itself is a new software layer which introduces new weaknesses regarding isolation of processing, memory, storage and networking. The Hypervisor can be directly exploited from the Network or through a compromised Virtual Machine (elevation of privileges). Once a VM or the Hypervisor is compromised, all other VM and underlying resources can be directly attacked resulting in total loss of the Cloud system integrity.

- The isolation principle weakens by the Cloud dynamic and distributed architecture:

Virtual Network Function (VNF) or new forms of virtualized Telco network elements can be created or withdrawn dynamically from multiple Cloud Data Centers. Dynamicity and Site distribution drive the demand for reliable and constantly updated Security Safeguards. As an example, policies that allow legitimate traffic to a virtualized NE shall be automatically blocking all such traffic when the virtualized NE is no longer available in the Cloud.

- Cloud management Integrity and confidentiality - Unsecured API interfaces could allow compromising the whole cloud system:

Many new management interfaces are required to orchestrate and automate the Telco Cloud operations and any single vulnerability on such protocols would expose the overall Telco Cloud to high-security risks.

- Intellectual property threats:

A copy of proprietary vNF remains a target for reverse engineering and side channel attacks. Since NE now consist of a set of Virtual Machines both the internal SW architecture and the proprietary Virtual Machines SW are susceptible to be copied, replicated and moved across geographical sites. The attacker's objective is to ex-filtrate patented technologies for making cheap SW replica as a copycat.

- SDN security exposure:

Attacks towards SDN switches and controller could cause DoS and even allow compromising the entire network. Traffic redirection, eavesdropping, malicious traffic injection, surveillance are all threats amplified and facilitated by network virtualization technologies such as SDN.

- Data security and privacy:

Finally yet importantly, the weakened processing, memory, networking and storage isolation principles of the Cloud technologies could allow attackers to gain access to subscriber critical data such as subscriptions, profiles, locations.

7 Analysis: Functional design recommendations & security requirements

7.1 5G system design options

We can observe some interesting 5G usage patterns from the descriptions previously outlined in Chapter 5 "'Internal' threat description/analysis (from Use Cases)". They imply the following non-exhaustive recommendations for 5G system security design.

The first one comes from the very essence of multi-stakeholder setting of 5G, e.g. how to ensure integrity and confidentiality of data collected/exchanged between infrastructure providers, MNOs, service providers or even third-party operators such as SSO (threats T_UC1.4_1, T_UC1.4_2, T_UC5.5_4). Also, liabilities between involved parties can be performed (as for the threat T_UC4.1_1) or multi-tenant interfaces can be hardened (as between different VNO network applications and controllers to avoid leakage or manipulation of the forwarding logic as in threats T_UC5.2_2 and T_UC5.2_3).

Also, complex 5G network and system topology needs careful design of technical interfaces between and inside the domains, e.g. how to avoid data leakage through vulnerable or misbehaving end-points (threats T_UC3.1_2, T_UC1.4_1) or how to protect SDN control plane components through trusted interfaces (threat T_UC5.1_1). Indeed, while control and monitoring interfaces are opened for third- party service providers they may also become available for other adversaries (threat T_UC5.5_1).

Also, specific 5G radio interface protection schemes need to be devised so as to ensure availability of critical communication network, e.g. by prioritizing attach requests (threat T_UC6.1_1).

End-to-end encryption techniques emerge several times, e.g. to avoid user data eavesdropping but at the same time to enable lawful interception (threat T_UC11.2_1) or against device identity disclosure (threat T_UC2.1_1).

Moreover, appropriate security monitoring measures appear to be important in 5G networks (threats T_UC5.5_2, T_UC5.5_3, T_UC7.1_1, T_UC9.3_1) in order to detect security incidents/attacks and to perform corrective actions.

These observations have been captured to feed 5G security architecture work in D2.7 [14], especially when defining security objectives.

7.2 5G security requirements

7.2.1 High-level 5G security requirements

From what has been discussed earlier, both relevant to 5G-ENSURE specific security use case analysis and 5G 'system of systems' holistic risk analysis, we can derive the following **high-level 5G security requirements**:

A) Security mechanisms with highest robustness

- Increased robustness against cyber attacks, e.g. in protocol design, consider more intensely the possibility of misbehavior or attacks of communication peers like user devices or network nodes in roaming networks etc.
- Enhanced privacy; an example could be protection against IMSI catching – the decision not to provide such protection in LTE should be reconsidered for 5G.
- Security Assurance: Methods to ensure security properties of entities (or even systems, e.g. network slices). Some care is required here, as such methods may put a heavy burden on vendors.

B) Security mechanisms with highest flexibility

- Alternative identification and authentication procedures: In LTE, user identification and authentication is based on credentials on a removable UICC (universal integrated circuit card). The GSMA has also specified an embedded UICC (not removable from the device) and mechanisms how to provision the required information to such an eUICC. For simple devices like sensors, one may consider cheaper solutions with no dedicated hardware to hold the credentials. The security implications must be balanced against factors such as manufacturing and provisioning costs.
- User plane encryption and integrity protection optional to use: In LTE, there is only publicity protection (encryption) for the user plane, and the network decides whether to use it. For 5G, we consider both encryption and integrity protection, where the user decides what to apply. The idea is not to forego security, but to avoid for example double encryption if the application uses end-to-end security mechanisms anyway.
- Adjust security mechanisms per network slice.

C) Security mechanisms with highest automation

- Holistic security orchestration and management: Goal is to highly automate the management of security functions, virtual functions as well as physical boxes, with a holistic view over the complete network and all deployed security functions.
- Self-adaptive, intelligent security controls: More futuristic measures to protect the network against yet unknown attacks. Could involve anomaly detection, self learning, artificial intelligence, big data processing, global intelligence gathering etc. Obviously, these functions contribute also to (A).

7.2.2 Specific 5G PPP security requirements

Additional to the previous analysis, 5G PPP security working group defines more specific requirements in its Security White Paper [15]:

A) 5G Security and Privacy level above 4G level

5G must provide a security and privacy level higher or at least equal to the security and privacy level in 4G. That is, 5G must be able to deliver and maintain SLA to verticals in terms of: availability, security, resilience, latency, bandwidth, access control from an end to end perspective. Furthermore, 5G systems and components must provide strong mutual authentication and authorization and should not be negatively affected by the security of legacy systems with which it interworks.

B) Security Automation

5G infrastructures' heterogeneity and complexity require security to be dealt at multiple levels and across domains. Therefore, automation of 5G security is vital to successful functioning and adaptation of 5G technologies. This is also in favour of 5G security to be composed and dynamically adapted upon context at hands, as a service (5G Security As A Service: SecaaS).

C) Security Monitoring

5G systems must support security monitoring capable of detecting advanced cyber security threats and support coordinated monitoring between different domains and systems (e.g. mobile and satellite). New innovative approaches to predict, detect and counter these challenges may need to be considered. For example we may think of relying on analytics for enhanced security operations (based, for instance, on Machine Learning or Artificial Intelligence approaches) to develop intelligence driven security capabilities able to gain a more accurate understanding of the risks and exposures of SDN infrastructures.

One of future solution could be to collect and analyse in real time events and logs within each slice (from RAN to vertical services) and among slices (this approach is identified as FAST Data technologies, due to its reactivity time and the very short storage duration to achieve massive collect of information).

D) Security Management

End to End security management and orchestration should be put in place taking into account correlation and coherence / consistency between data exchanged/shared at Security Architecture Inter-domain interfaces. For example, an appropriate use of Big Data technologies may allow consistency evaluation between RAT to Verticals in term of customer 5G security context (i.e. notification of country localization during service delivery).

Customers, slice owners and vertical services should be aware of their technical 5G contextualization, particularly to asses and address their security needs. For example, security KPI and proofs should be available and collected at 5G infrastructure. 5G systems and components must provide functionality to mutually assess the trustworthiness before, and during interactions. Furthermore, if required by local regulation, 5G infrastructure operator must have means to demonstrate their provided level of security.

E) Security liability Schemes

New responsibility schemes should be proposed, in coherence with existing Regulation, regarding the distribution and allocation of responsibilities and obligations in a multi-tenant softwarized telecom infrastructure, and in particular for potential delegation of regulation obligation to non-regulated third parties (today Licence obligations are *intuitae personae* and may not be subdelegated).

F) Inter-tenant/Slice Isolation

Infrastructure sharing by multiple network operators will require strict isolation at multiple levels to ensure the expected security level. Various aspects of control-plane, data-plane and resource isolation must be guaranteed to ensure zero correlation among different slices/tenant operations. Tenant/slice isolation is important to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality.

Therefore, inter-tenant/slice isolation security of sensitive data, should at least be equal that of physically separated networks. Moreover, this strong slice/tenant isolation should be demonstrable and evidence should be collected and computed over the entire infrastructure.

G) 5G Liability

The chain of Trust and liability of multi-tenants should be managed and auditable for each service, component supplier, operator and customer. 5G Liability schemes will have to be defined and applied, particularly to address breach of Trust/Security (backdoor, Quality impact, regulation impacts, data leakage etc.) between parties.

5G Liability could be reinforced by VNF certification or labelization, SDN Controller or Orchestrator evaluation, or proper orchestration of virtualized security functions. For instance, it is important to address the security of the VNF itself as an element, e.g., VNF hardening, VNF verification/certification/attestation and corresponding industrial processes, VNF code robustness, etc.

H) Enabling Value Added Services with end to end encryption

Enabling value-added security services in the context of encrypted traffic. In order to comply with privacy regulations and protection of user data, traffic encryption is expected to be generalized across 5G networks. End-to-end encryption may hamper the use of multiple value-added security services such as attack detection, QoS monitoring, fine-grained access control, among others. In this respect, high-level privacy guarantees may have the adverse effect of lowering security guarantees. Therefore, the development and wide adoption of 5G should happen alongside new technologies and capabilities that enable value-added security services in the context of encrypted traffic, thus conciliating between security requirements and privacy guarantees.

I) 5G regulation conformity

5G technology should be developed in compliance with legislation/regulation that apply or could anticipate be anticipated (for instance Lawful Interception and Data Retention Regulations appeared as difficult to comply with and mist be taken into account in the case of Slicing implementation).

8 Conclusions

This document provides 5G Threat and Asset descriptions, Mitigation recommendations and Requirements definition, by addressing risk assessment approach for 5G-ENSURE specific security use cases.

As observed today, 5G networks will need complex security requirements at different layers within the system. Moreover, with standardization at an early stage, innovative security solutions proportionate to the threats will have to be built into the network from the very start. This approach will protect subscribers, devices and their communications, as well as the integrity of the network itself — whatever the use case.

Investing in 5G security now is also a wise insurance policy to avoid unexpected costs that might arise later from countering attacks or from suffering the consequences of insufficiently protected high-value data and processes. The wrong decision about security today will only prove to be false economy in the future.

Note that potential mitigation/security solutions are provided by usable and efficient 5G-ENSURE enablers developed in WP3.

9 References

[1] 5G-ENSURE Deliverable D2.1 “Use Cases”, Febr 1, 2016, http://www.5gensure.eu/deliverables

[2] 5G-ENSURE Deliverable D2.5 “Trust model (final)”, Nov 15, 2017, http://www.5gensure.eu/deliverables

[3] ITU-T Recommendation X.805 “Security architecture for systems providing end-to-end communications”

[4] ITU-T Recommendation X.801

[5] NIST SP800-30, “Risk Management Guide for Information Technology Systems”, NIST (National Institute of Standards and Technology)

[6] ISO/IEC 27005:2011 “Information technology - Security techniques - Information security risk management”

[7] A. Roller, S. Turpe, K. Kinder-Kurlanda, “An Asset to Security Modeling? Analyzing Stakeholder Collaborations Instead of Threats to Assets”

[8] ETSI TS 123 101 V3.1.0 (2000-12), http://www.etsi.org/deliver/etsi_ts/123100_123199/123101/03.01.00_60/ts_123101v030100p.pdf

[9] ASMONIA Project, http://www.asmonia.de/index.php?page=20

[10] ETSI TS 133 401 V10.3.0 (2012-07), http://www.etsi.org/deliver/etsi_ts/133400_133499/133401/10.03.00_60/ts_133401v100300p.pdf

[11] ETSI NFV, http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf

[12] “Threat Landscape and Good Practice Guide for Software Defined Networks/5G”, ENISA, December 2015, https://www.enisa.europa.eu/publications/sdn-threat-landscape

[13] V. Normand, E. Félix, Toward model-based security engineering: developing a security analysis DSML, ECMDA-FA, 2009

[14] 5G-ENSURE Deliverable D2.7: Security Architecture (Final), Oct 31, 2017, http://www.5gensure.eu/deliverables

[15] 5G PPP Phase1 Security Landscape (White Paper), https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[16] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis" (TVRA).

A Annex A: Use cases threats Identification

The following set of use cases in D2.1 [1] are used to derive threats description for 5G networks:

Cluster no.	Cluster name/topic	Use case no.	Use case name
1	Identity Management	1.1	Factory Device Identity Management for 5G Access
		1.2	Using Enterprise Identity Management for Bootstrapping 5G Access
		1.3	Satellite Identity Management for 5G Access
		1.4	MNO Identity Management Service
2	Enhanced Identity Protection and Authentication	2.1	Device Identity Privacy
		2.2	Subscriber Identity Privacy
		2.3	Enhanced Communication Privacy
3	IoT Device Authentication and Key Management	3.1	Authentication of IoT Devices in 5G
		3.2	Network-based Key Management for End-to-End Security
4	Authorization of Device-to-Device Interactions	4.1	Authorization in Resource-Constrained Devices Supported by 5G Network
		4.2	Authorization for End-to-End IP Connections
		4.3	Vehicle-to-Everything (V2X)
5	Software-Defined Networks, Virtualization and Monitoring	5.1	Virtualized Core Networks, and Network Slicing
		5.2	Adding a 5G Node to a Virtualized Core Network
		5.3	Reactive Traffic Routing in a Virtualized Core Network
		5.4	Verification of the Virtualized Node and the Virtualization Platform
		5.5	Control and Monitoring of Slice by a Service Provider
		5.6	Integrated Satellite and Terrestrial Systems Security Monitor
6	Radio Interface Protection	6.1	Attach Request During Overload
		6.2	Unprotected User Plane on Radio Interface
7	Mobility Management Protection	7.1	Unprotected Mobility Management Exposes Network for Denial-of-Service
8	Ultra-Reliable and Standalone Operations	8.1	Satellite-Capable eNB
		8.2	Standalone EPC
9	Trusted Core Network and Interconnect	9.1	Alternative Roaming in 5G
		9.2	Privacy in Context-Aware Services
		9.3	Authentication of New Network Elements
10	5G Enhanced Security Services	10.1	Botnet Mitigation
		10.2	Privacy Violation Mitigation
		10.3	SIM-based and/or Device-based Anonymization
11	Lawful Interception	11.1	Lawful Interception in a Dynamic 5G Network
		11.2	End-to-End Encryption for Device-to-Device Communications

B Annex B: COMMON D2.5+D2.6 ANNEX: Use Case Analysis

This section forms a Common Annex for Deliverables D2.5 and D2.6. It contains detailed analysis of the use cases from D2.1 and the corresponding threats identified in D2.6. The Common Annex provides the common starting point for the analysis of trust relationships in D2.5 and the analysis of risk mitigation measures in D2.6.

For each use case an overview is presented mapping the use case to the Security Architecture defined in D2.4. This is the "sunny day" scenario. Then each of the corresponding threats identified in D2.6 is analyzed in terms of trust implications and proposed mitigation strategies. These are the "rainy day" scenarios.

B.1 Factory Device Identity Management for 5G Access (UC 1.1)

B.1.1 Use case description with architectural components

In this use case, we consider factory robots accessing a factory network over 5G connectivity but using credentials and AAA managed by a Factory Owner. The factory owner installs 5G base stations in the factory but will rely on an MNO to perform services such as IP connectivity and mobility.

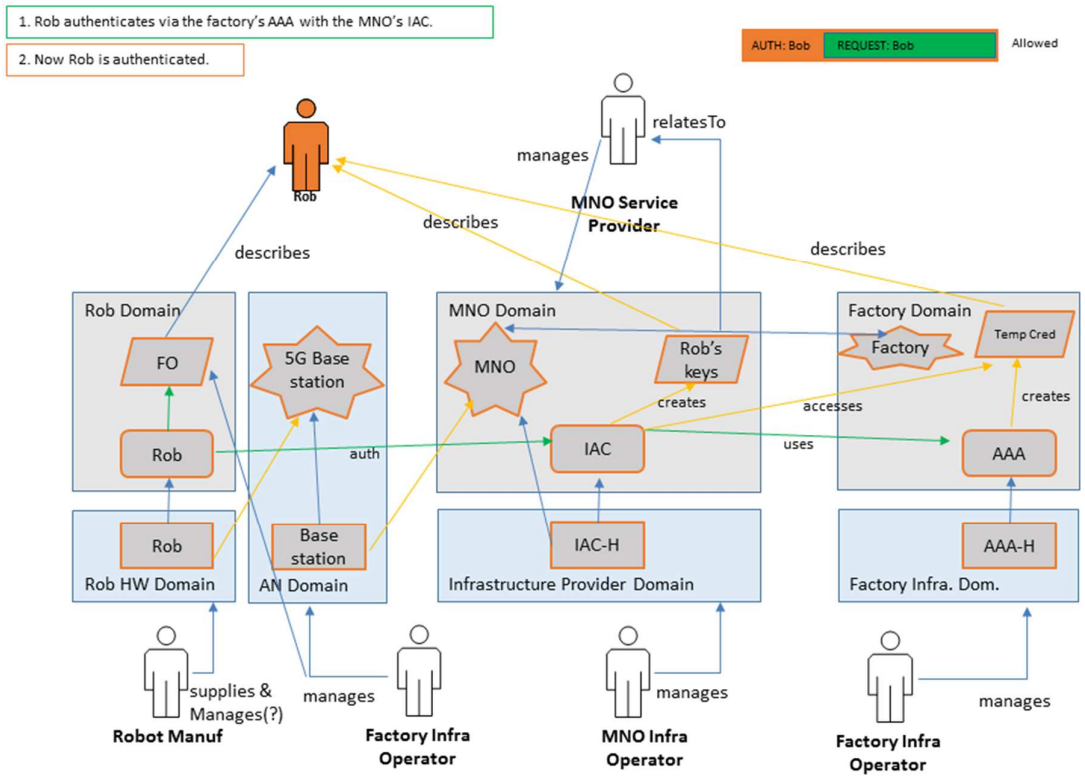

Figure 17. Factory Device Identity Management for 5G Access (UC 1.1): sunny day scenario

Figure 17 describes the use case in relation to the architecture, in the absence of any threat (sunny day scenario). When the robot establishes a connection to the base station the base station will ask the IAC for authentication. The IAC forwards the robot's identity in the factory owner identity space to the AAA of the factory owner. After the AAA of the factory owner and the robot have successfully authenticated each other (or IAC and the robot have successfully authenticated each other with support of the factory owner AAA), the MNO starts to provide connectivity services to the robot.

B.1.2 Identified threats

B.1.2.1 Attacker tries to freeride devices authenticated by factory owner (T_UC1.1_1)

The attacker's motive is to freeride devices. When the robot establishes a connection to the base station the base station will ask the IAC for authentication. The attacker could be the factory owner manipulating the AAA for its own advantage, by bringing own devices on network which should not (according to contract), or offering a connection service to third parties. The attacker could also be a third party which has hacked the factory owner's AAA to get own devices onto the network for free.

In Figure 18, the threat is explained in relation to the architecture. Alice authenticates via the factory's AAA with the MNO's IAC. The attacker Mallory has manipulated the factory owner's AAA server to issue temporary credentials, although service for Alice is not included in the service agreement between MNO and the Factory owner.

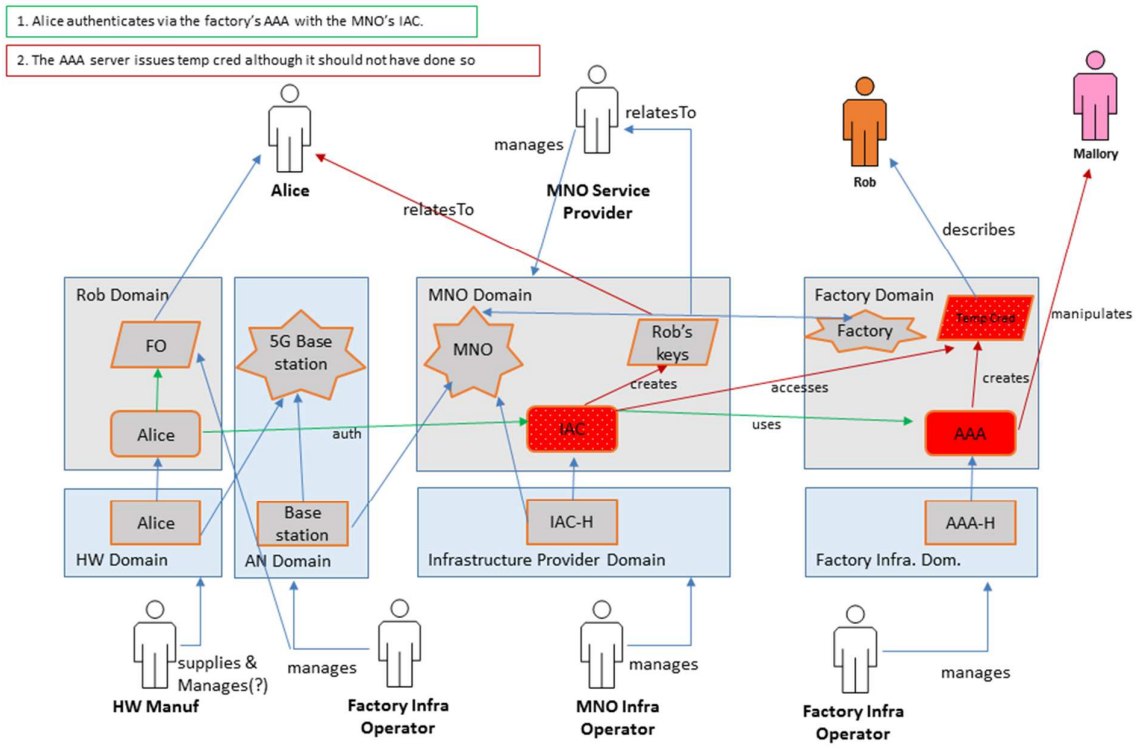

Figure 18. Attacker tries to freeride devices authenticated by factory owner (T_UC1.1_1) – 'rainy day'

This threat affects particularly the relation between MNO and factory owner. If the factory owner either purposely freerides devices or has not secured its AAA server properly to prevent attackers from doing so, the MNO may be fooled to provide service to the factory owner or external attacker without being paid for the service. Furthermore, general network quality may be affected if a large number of devices freeride the MNO service. In consequence, network quality for legitimate users of the MNO services (the factory owner itself or possibly other users) may be degraded.

Trust implications

This threat affects primarily the MNO:

- The MNO may lose income due to freeriding devices that use the MNO's service without payment.

- The MNO may also lose trust from legitimate users if the network quality degrades due to a large number of illegitimate devices using the MNO's network.

However, the threat also affects legitimate customers of the MNO. The legitimate customers could be the factory owner, but also other customers of the MNO:

- Network quality could degrade due to a large number of illegitimate devices using the MNO's network.

The factory owner may also be affected specifically:

- If the attack was performed by an external attacker to a legitimate factory owner and the attack is finally discovered, the factory owner may lose trust from the MNO.

Threat mitigation strategy

The threat should be addressed both at the MNO domain and the factory domain.

At the MNO domain, the MNO should deploy charging and network management solutions that are designed to ensure both payment for provided services and adequate network quality. In detail:

- The charging solution towards the factory owner should be load-dependent. In this way, the factory owner will not be able to freeride devices without paying for them. Such a charging solution will also give incentive to the factory owner to secure its AAA server properly against external attacks.
- The network management solution should make it possible to isolate the factory owner's network resources, so that other users of the network are not influenced by possible attacks in the factory owner domain. Technically, this could be solved by QoS or slicing, or simply by providing a separate network infrastructure to the factor owner that is not shared with other customers.

At the factory domain, the factory owner should secure its AAA server against external attacks.

B.2 Using Enterprise Identity Management for Bootstrapping 5G Access (UC 1.2)

B.2.1 Use case description with architectural components

This use case describes a situation where an enterprise wants to provide its employees with devices that are 5G enabled. It is wishes to use its existing collection of credentials to authenticate with the MNO operator, however the enterprise does not wish to operate its own HSS. So the MNO operator is willing to allow provisioning of 5G credentials to the enterprise.

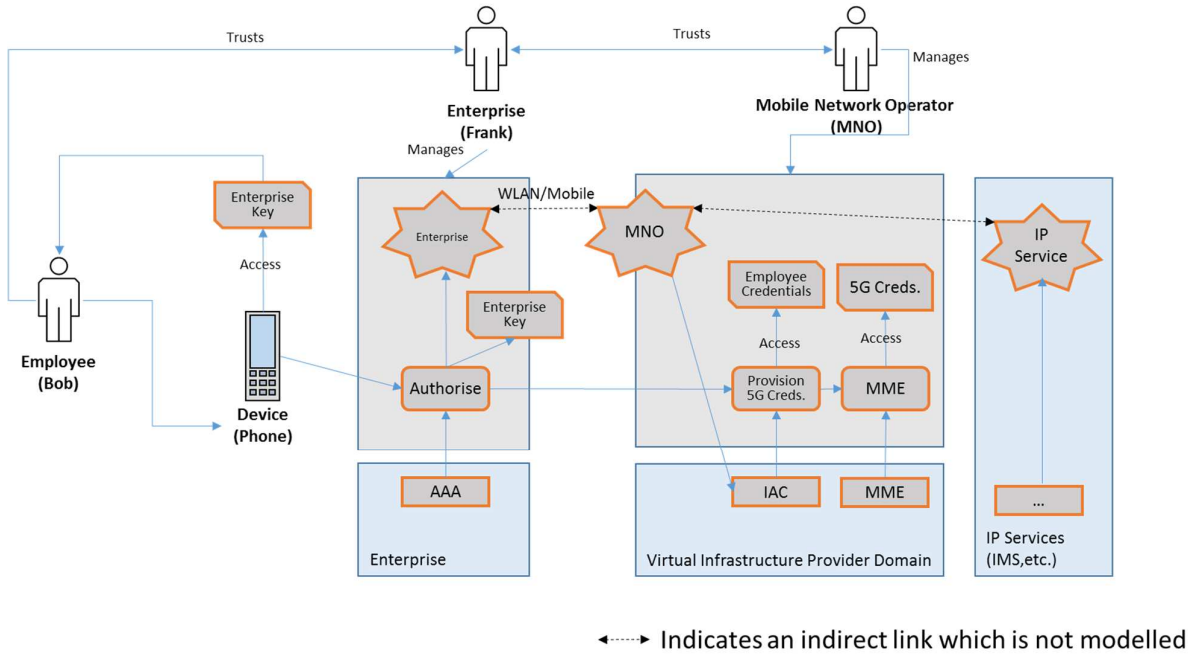

Figure 19. Using Enterprise Identity Management for bootstrapping 5G Access (UC 1.2): sunny day scenario

Starting from left to right of Figure 19, we have the enterprise's device, which is used by the employee. The device will use the enterprise key, which is maintained by the enterprise's AAA server, to request access to the MNO's 5G service. The MNO will authenticate the device based on the employee's credentials, and provision access to the 5G network to the device. The MNO trusts the enterprise to maintain control over who has access to the devices and credentials. The enterprise trusts that the MNO does provide its devices with adequate service and does so in a secure fashion.

B.2.2 Identified threats

B.2.1.1 Leaked AAA credentials (T_UC1.2_1)

The root cause is the leaking of AAA credentials from the employee network, allowing unauthorised actors to authenticate with the MNO. The MNO may provide them with access to 5G connectivity, at the expense of the enterprise. The credential data leak could be from a malicious insider, or phishing attack on the enterprise, or even on the employee.

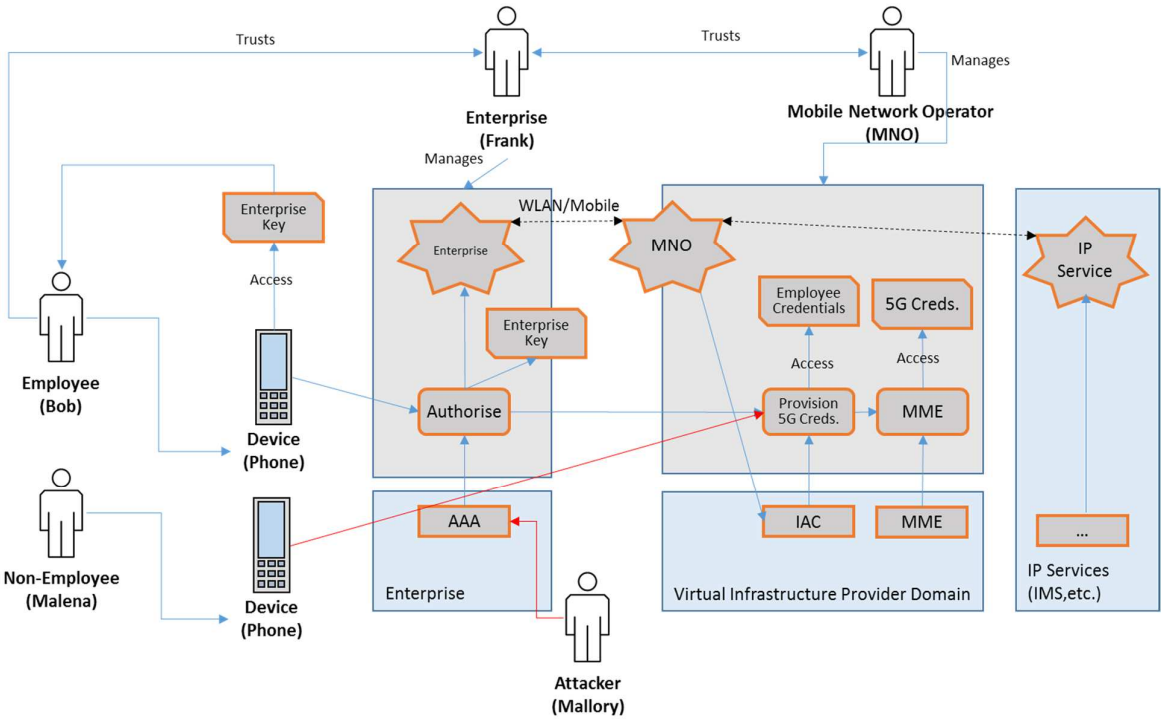

Figure 20. Leaked AAA credentials T_UC1.2_1 – 'rainy day'

Once credentials are leaked from the AAA server, as shown by the attacker 'Mallory', it would then be possible for malicious users to connect to the MNO using the enterprise details. Once an unauthorised user is able to connect to the MNO as an employee they will have access rights which match the compromised credentials. This could allow for further lateral movement with the enterprise. It also means that what usage costs occur will be charged to the enterprise, Frank.

Secondary effects of this could be the loss of access for employee's who have had their details compromised. It could also result in a loss of availability between the enterprise and the MNO if a large quantity of the malicious users were to access the MNO at once.

Trust implications

The MNO trusts that the enterprise will secure their AAA server and employee devices enough to prevent such data leakage and abuse of the system. The enterprise also trusts that the MNO would alert the enterprise to any anomalous access to their network, which could be the result of unauthorised activity from. One other such trust issue to consider here is that the employee might use the enterprise credentials for personal use of the MNO's network. This again might be something the enterprise would want the MNO to prevent, such as only provisioning access to 5G networks from certain locations.

Threat mitigation strategy

Once such mitigation strategy would be to limit credentials to device and user, this would mean that even if an attacker is able to compromise the AAA server and steal the certificates/hashes. They can only be used on a specific device. This mitigation would be completed by the enterprise who manage the credentials. Another mitigation method would be to enable EAP based authentication to the AAA server. Again, this would have to be completed by the enterprise, but would provide a more secure authentication method.

B.3 Satellite Identity Management for 5G Access (UC 1.3)

B.3.1 Use case description

This use case is focus on represent the scenario where a Service Provider needs to warranty the authenticity of the satellite network devices across the network to avoid the appearance of unauthorized or fake satellite devices that can be enable the access to the network resources to end users with not trustable goals. The next figure represents the start scenario and the elements involved, in this case the satellite network domain will have a special focus.

The SNO systems is collecting information about all the Satellite eNodeB and GW Satellite across the system offering real time information to the operator about the devices status.

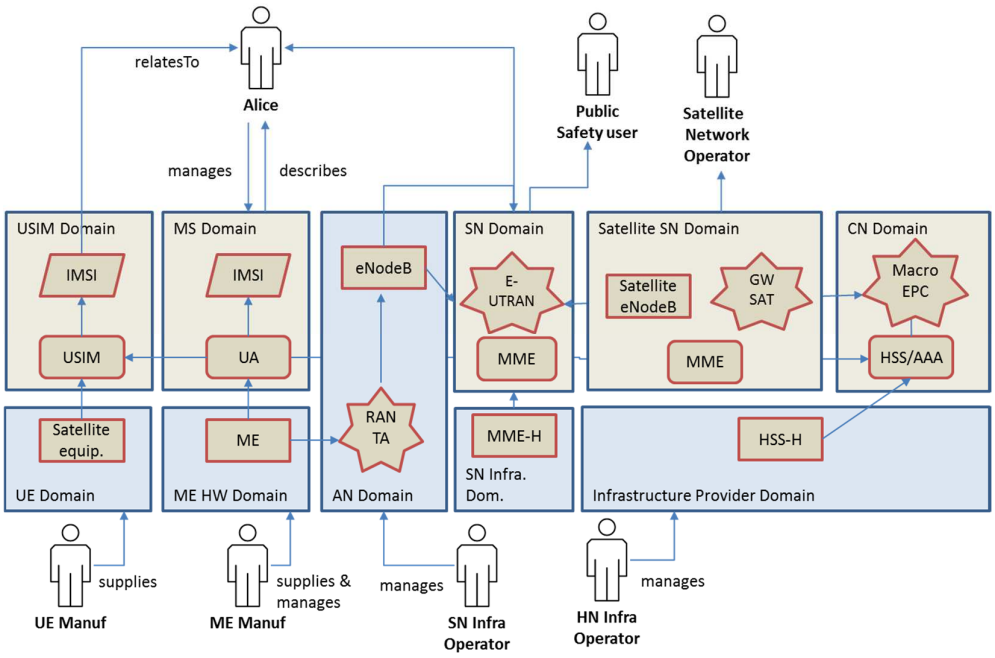

Figure 21. Satellite Identity Management (UC 1.3): sunny day scenario

B.3.2 Identified threats

B.3.2.1 Unauthorised activities related to satellite devices or (satellite) network resources (T_UC1.3_1)

A Service Provider (i.e. a telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable satellite system capacity to be assigned to the customer in a dynamic way. However this capacity use is limited and should be strictly controlled/monitored to warranty the correct use and avoid extra-charges for satellite capacity extra consumption or generate possible interference or unreal work load over the network that can limit the resources assignation across the users.

This threat can impact on a wide amount of services present over the network.

In this case, Alice detect a decrease in the network performance accessing to different applications, in parallel the SNO detects an increase in the satellite capacity resources uses from one or multiple Satellite eNodeB, the SNO after analyse the traffic consumption statistics from previous days can determine that an unauthorized application is requesting a huge amount of satellite resources, regarding to warranty the resources for the rest of the users, the application is blocked at Satellite eNodeB level to avoid service

degradation. As a result the threat have been neutralized and the service impact for the users have been minimized.

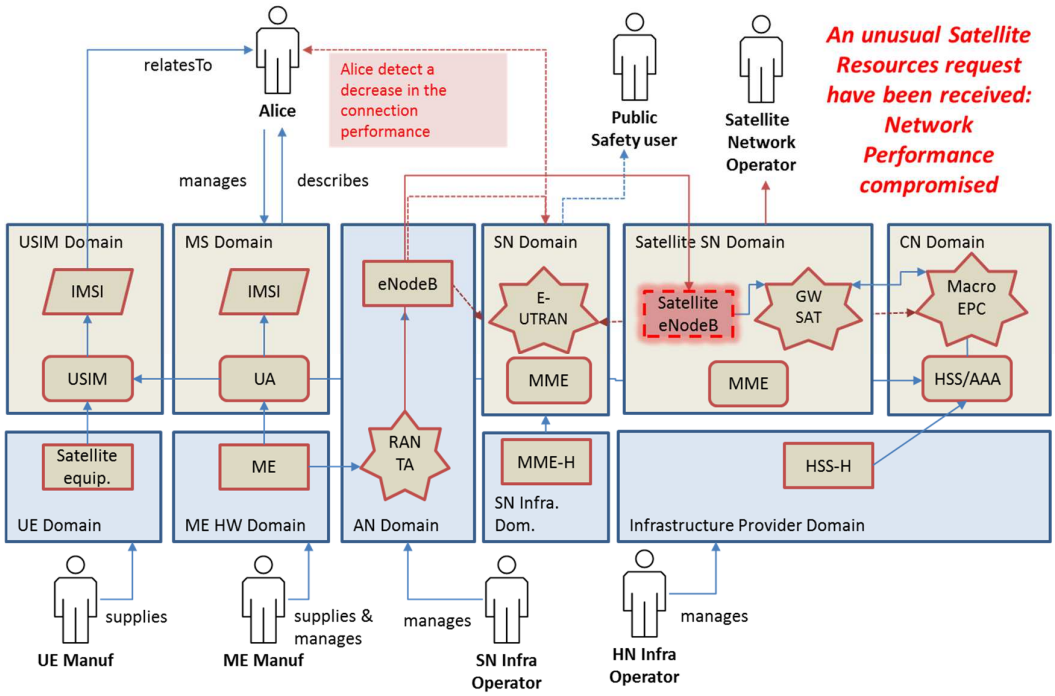

Figure 22. Unauthorised activities related to satellite devices or (satellite) network resources (T_UC1.3_1) – 'rainy day'

Main domains involved in this action are shown in Figure 22, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite resources allocation into the network.

Without the mechanisms present, reliability of the system is in risk, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a lack of trust based on the network performance and the capabilities for the VMNO to guarantee their service level agreements.
- The VMNO needs to demonstrate a trustable recovery actions regarding to guarantee the control over the VNO, offering detailed action plans that cover typical operations issues in sensible highly exposed locations.
- In this use case, the threat is specially focus in an insider attack that can be try to access to collapse the network affecting a huge amount of customers.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Real time data gathering about network status and trends analysis can supply the foundations to accurate network performance and generate patterns consumptions at Satellite eNodeB level.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.
- Generate pre-emptive configuration policies across the Satellite eNodeB can decrease the reaction time and automatize the network recovery process, decreasing the SNO / VMNO actions and dependencies.

B.3.2.2 Fake roaming from terrestrial network into satellite network (and vice versa) (T_UC1.3_2)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity associate to an specific number of Satellite eNodeB, this satellite eNodeB are responsible to provide services access to the end users in a determinate coverage area, the Satellite Network Operator needs to warranty the end users connectivity across the satellite eNodeB resources for the scenarios identified, any attend of access to these resources can generate extra charges for capacity use, decrease the network performance or generate potential security breaches.

This threat can be impact in the performance of several services when service lost scenarios or service recovery appears and satellite resources are incorrectly allocated or the satellite capacity cost is increased in a non-justifiable way.

In this case a natural disaster occurs and connection between Alice and eNodeB is lost, the network manager detects the failure event and proceed to performs topology calculation to guarantee ultra-reliable services. The new topology is configuration is populate across the network elements and the satellite-capable eNB activates the alternative route to Macro EPC via the satellite link. As a result the service lost is minimized and service restore is achieved, the issue appears when the network connection across the eNodeB is recovered and connection needs to be re-established using the old path, during all the time that the calls have been routed using the Satellite eNodeB a Fake Roaming scenarios is on-going, network operator needs to minimize the time and the traffic involved.

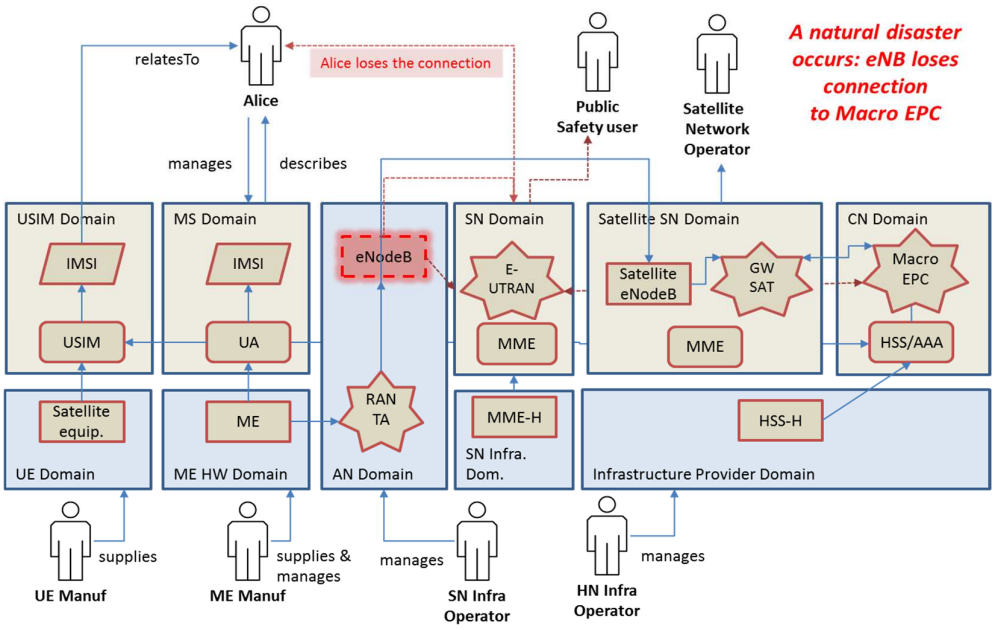

Figure 23. Fake roaming from terrestrial network into satellite network (and vice versa) (T_UC1.3_2) – 'rainy day'

Main domains involved in this actions are shown in Figure 23, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite connections capabilities to the network increasing the recovery time and decreasing the service lost, but adding the possibilities to generate fake roaming scenarios for the calls involved between both systems under different scenarios.

Without the mechanisms present, service lost time will be increasing, reliability of the system is decrease and mitigations actions are limited, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a decrease of the network performance due to use satellite resources while terrestrial network resources are still available. Additionally in the opposite way customer can perceived that network is unavailable when they are incorrect assign to resources over the terrestrial network when this is not fully available.
- In this use case, the threat the issue specially focus in the service recovery and service lost operation scenarios, where availability in the eNodeB or satellite eNodeB can be the root case, and service level agreement can be compromised.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Establish monitoring Probes focus in not just verify the status of the access at lowest layers and check the service status in the highest layers before balance the traffic between satellite and terrestrial networks.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.
- Generate ad-hoc mechanism to control the switch over process to identify the elements involved and the traffic flows across them.

B.4 MNO Identity Management Service (UC 1.4)

B.4.1 Use case description

This use case describes an MNO which provides an advanced management service to a 3rd party service provider on behalf of a user. When the user Bob, connects to the MNO with his device the MNO assigns a 'Network ID' to him. This network ID allows the service provider to gain detailed information about Bob which is provided by the MNO. Note that the MNO can share the user data only if the user has already agreed on that. The service provider may use this information to determine the level authentication methods needed to access the service.

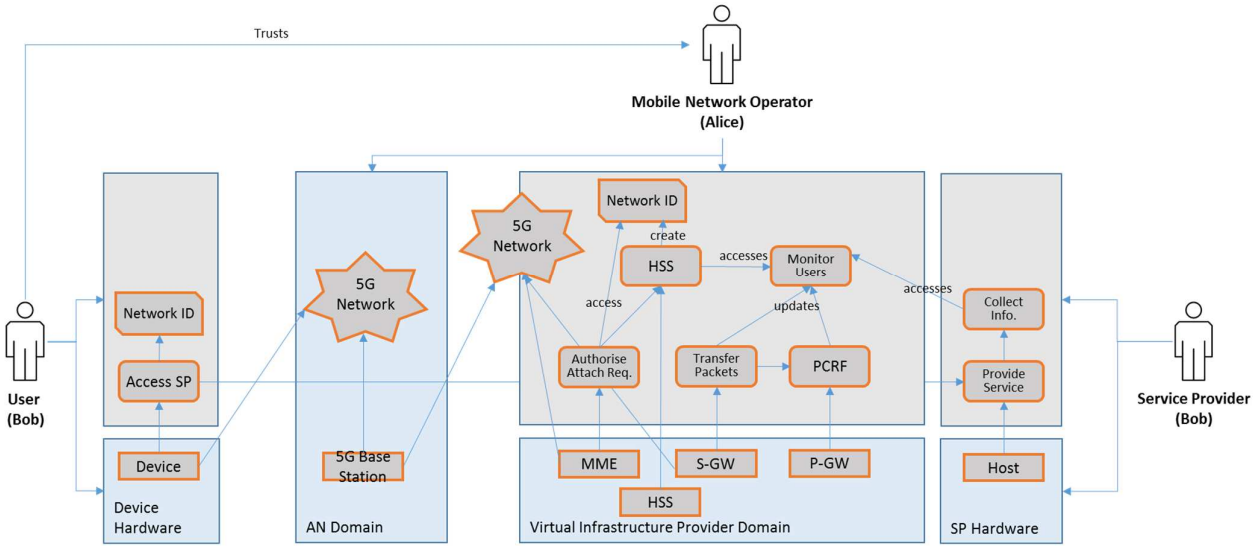

Figure 24. MNO Identity Management Service (UC 1.4): sunny day scenario

The key stakeholders in this instance are the MNO and Service Provider. The MNO agrees to provide the service provider with details on the user's device, such as the location it is in, software and hardware version and so on. This allows for the service provider to determine what types of authentication to challenge the user. This allows the service provider to better secure their infrastructure from attacks. This means that the user will have to trust both the MNO and SP with more personally identifiable information.

B.4.2 Identified threats

B.4.2.1 Compromised data (T_UC1.4_1)

The root cause of this attack is an attacker compromising a network component, in this case the device. Then forcing the device to use a weaker protocol which is susceptible to decryption attacks. This will allow the

attacker to effect the integrity and confidentiality of the data which is collected by the MNO then sent to the SP. Resulting in a secondary effect of the service provider being feed misinformation. In certain cases this may prevent the user from accessing the service.

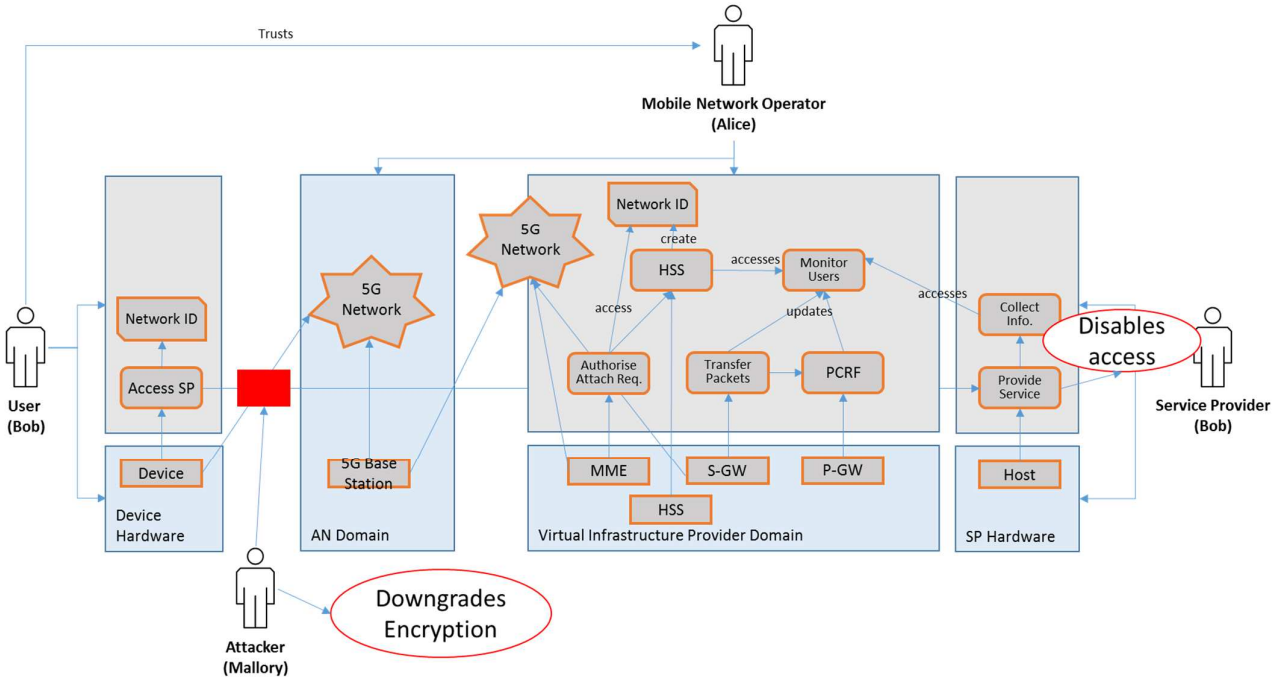

Figure 25. Compromised data (T_UC1.4_1)

The key components for this threat are the user's device and the service provider which relies on the metrics provided by the MNO. This threat exploits the fact that the device is unable to prevent the downgrade attack, and that the MNO accepts the invalid data fed to it by the attacker, Mallory.

Secondary effects arising from this threat would be other attacks which Mallory is capable of accomplishing other than the bypassing the service providers extra authentication. Such as manipulating data from the user to the MNO and vice versa. This could have a catastrophic effect on the network if Mallory is able to perform a DoS to one or more of the MNO services.

Trust implications

The service provider trusts the data received from the MNO is accurate. Indeed, the MNO should apply mechanisms to verify that the reported network information is not compromised. If this data is incorrect or falsified then the actions which the service provider takes do not match the real world scenario and result in a loss of trust between the MNO and the service provider. The MNO may try to transfer this trust over to the user or device manufacturer which allows for the downgrade attack to succeed.

Threat mitigation strategy

In order to protect against this threat, the MNO needs to perform validity checks on the collected data. This might include remote attestation protocols such as Direct Anonymous Attestation (DAA), which enables remote authentication of a trusted computer whilst preserving privacy of the platforms user. This would be placed in the MNO network when data is collected about the device. This would be expected to be completed

by the MNO since they are the stakeholders which will be collecting the data. It would be performed each time the user's device connects to the network. Another mitigation, again expected to be completed by the MNO, would be to roll out new encryption protocols which prevent encryption downgrade attacks. This would be placed on either the device or the access network.

B.4.2.2 User's privacy attack (T_UC1.4_2)

In this threat, we can distinguish two types of attackers: an external attacker and an internal attacker. In the first case, an external attacker can try to intercept exchanges between the MNO and the service provider to get the metrics about the user. In the second case, the service provider is considered as malicious. The service provider may try to get information about the user more than what is really needed to enhance the security of the service. The goal of the service provider can be to construct profiles of user and use it to other purposes than the security of the service such as oriented publicity. Normally, the MNO collects data about user (after user's agreement), performs cryptographic computations on the collected data to obtain metrics. These metrics are going to be shared with the service provider (Step (d) in Figure 5 of the deliverable D2.1). If the computed metrics do not properly anonymize user's data, this can break the user's privacy. These are the main sources of the threat.

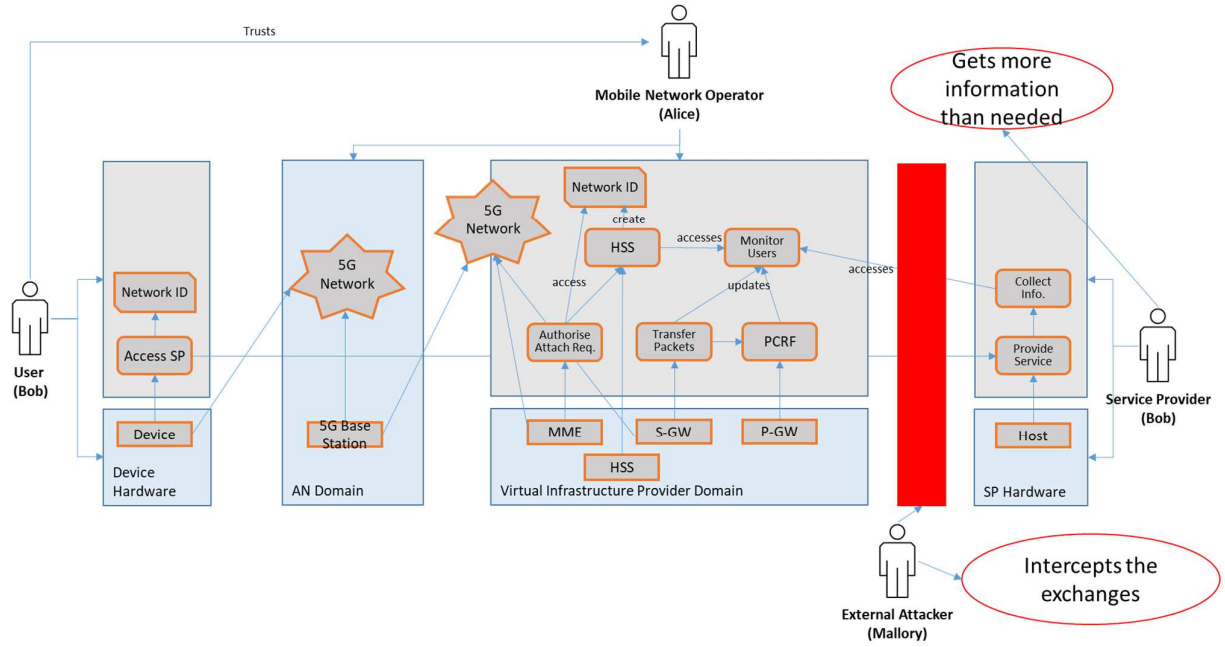

Figure 26. User privacy attack (T_UC1.4_2)

Trust implication

In the first case, the user trusts the MNO and service provider that the exchanges are secured.

In the second case, the user trusts the MNO that he collects only data agreed on previously when adhering to this service. The user also trusts the MNO that he properly anonymizes the collected data and share only metric with the service provider.

Threat Mitigation strategy

In order to protect against this threat, the MNO and the service provider need to use approved security protocols to secure their exchanges, such as IPsec. The MNO should also use securely approved algorithms to anonymize the collected data such as k-anonymity algorithm. The MNO can also provide the user the ability to check and modify the shared metrics and the level of anonymization.

B.5 Device Identity Privacy (UC 2.1)

B.5.1 Use case description with architectural components

The use case relates to a user attaching to a 5G network. The description of this procedure and its related function blocks are illustrated in Figure 27, which illustrates the scenario with respect to the architecture, in the absence of any threat (the sunny day scenario).

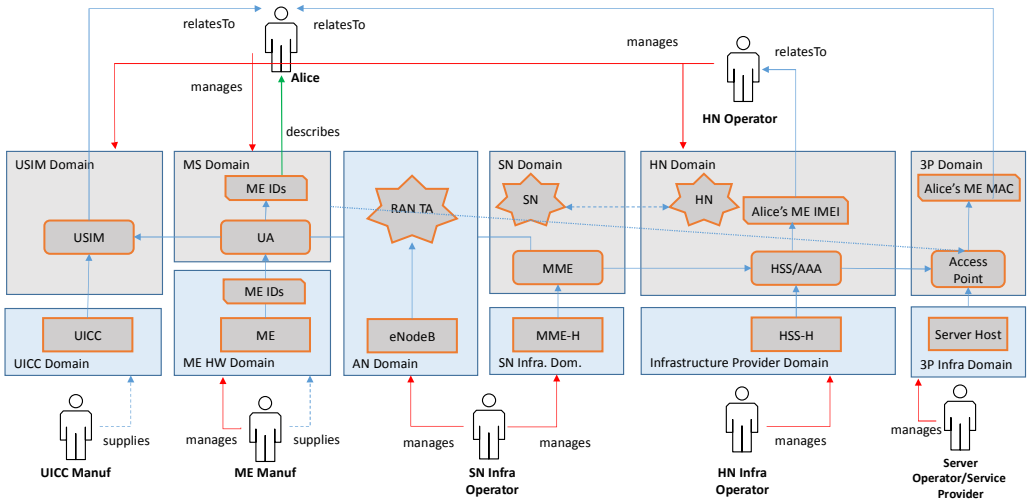

Figure 27. Device Identity Privacy (UC 2.1): sunny day scenario

Alice has a subscription with a Mobile Network Operator (MNO) and she has been provisioned with USIM credentials in her UE which has certain fixed identifiers (ME IDs) associated with her Mobile Equipment (ME) device such as her International Mobile Equipment Identifier (IMEI) and WiFi MAC address.

When Alice's UE is switched on, the ME connects to the mobile serving network (SN) using the NAS-level Security Mode Command procedure which attempts to establish a security context. Provided Allice's ME has supplied an authorized identity to the SN a security context will be instantiated, after which Alice's ME will respond to request for its International Mobile Equipment Identifier (IMEI).

Alice's UE may also establish a non-3GPP connection via a 3P domain which may be authenticated through the use of Alice's USIM credentials. In the case where Alice's UE utilizes 'WLAN direct IP access' (3GPP TS33.234) to attach to an MNO controlled Access Point (AP) in a 3P domain, or any other AP, it will expose it's WiFi MAC address to the AP and if using the DNA protocol (IETF RFC4436) it can also leak MAC addresses of previously visited APs and the order in which they were visited.

B.5.2 Identified threats

B.5.2.1 Mobile user interception and information interception (T_UC2.1_1)

The attacker, Mallory, wants to gather the ME device identifiers (e.g. IMEIs) of users which are active in a geographic area.

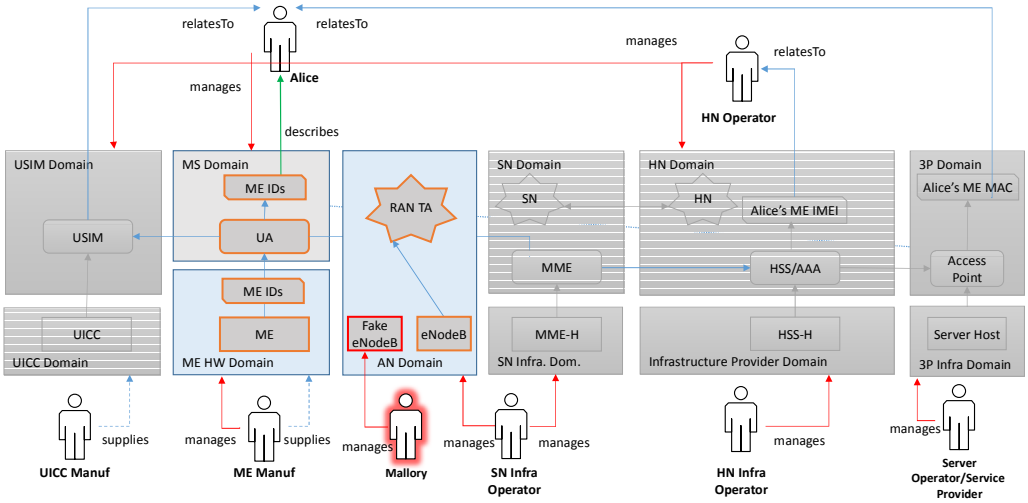

Figure 28. Mobile user interception and information interception (UC 2.1) – 'rainy day'.

In Figure 28, Mallory can achieve this by setting up a fake eNodeB which can passively monitor the radio spectrum in the AN domain to obtain IMEIs from emergency calls.

The consequence of this attack is that the private device identity can be obtained by an unauthorised party. When the IMEI is obtained then the attacker also knows the device's Type Allocation Code (TAC) is the initial eight-digit portion of the IMEI, which uniquely identifies the device and indicates the GSMA-approved organization that registered the device.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- The ME trusts its HMNO as part of the direct service agreement.
- The HMNO trusts the SMNO as part of the roaming agreement contract. The IMEI is exchanged to ensure it is not on a blacklist of devices.

The implication related to the trust model are:

- The user/ME has no way to detect the trustworthiness of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- Since the IMEI is not encrypted when initiating an emergency call the fake eNodeB can capture the IMEI.

Threat mitigation strategy

Mitigation of this threat may be achieved through protection of the device identifier during transport. Such an approach might protect the transfer of the IMEI between the UE and AN using transport layer encryption. Another approach might be to use a mobile Operator supplied key to just encrypt the IMEI in transit. These solutions should ensure that the user's IMEI is not sent in clear text during network attachment. Whilst these approaches would make passive interception significantly harder, these solutions may not prevent the UE from attaching to a rogue eNodeB, but they would raise the bar in making it more difficult for an attacker to obtain the IMEI.

B.5.2.2 Tracking of device's (user's) location (T_UC2.1_2)

The attacker, Mallory, wants to track the UE, based upon its ME device identifiers, in this case WiFi MAC address and associated protocols. Mallory can achieve this by setting up a WiFi monitor near the AP(s) in the location of interest and observing the protocol interactions.

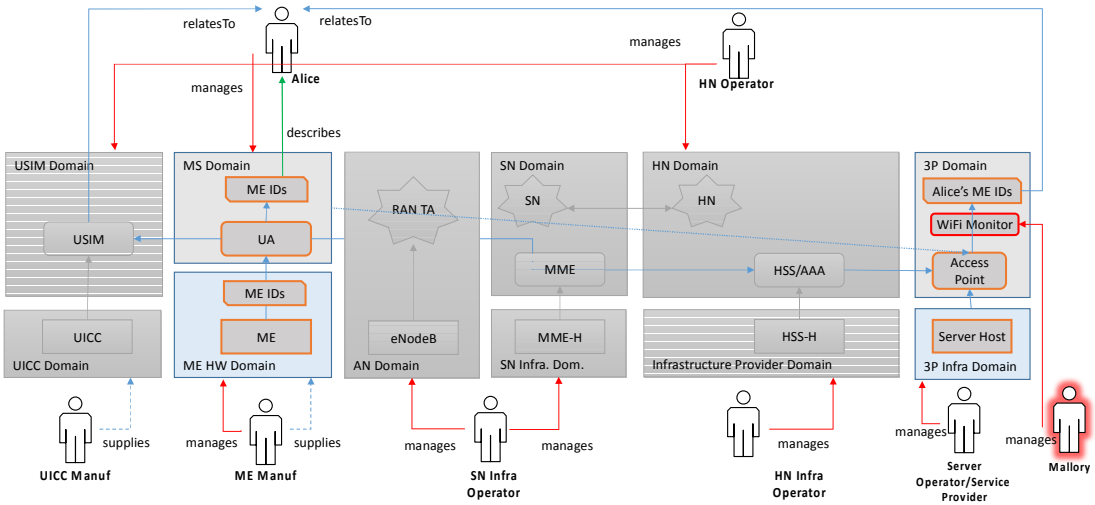

Figure 29. Mobile user interception and information interception (UC 2.1) – 'rainy day'.

Based on Figure 29, Mallory sets up a rogue WiFi monitor near the Access Point(s) of interest so can passively observe the MAC address of the device. Also, provided the device uses RFC4436, Mallory can also potentially monitor the MAC addresses of previously visited APs and the order in which they were visited.

The consequence of this attack is that the presence of the device in that location may be revealed and also potentially the previous points of attachment and the order of their visitation. Once Mallory knows the MAC addresses, due to their format he also knows the manufacturer of the user's device and potentially those to which the user has previously attached. The subscriber's previous location may also be linked to the user's previously visited MAC addresses using Geolocation lookup APIs such as those offered by Google and others.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships:

- The ME trusts its HMNO as part of the direct service agreement
- The HMNO trusts the 3P domain to host their Access Points (AP)
- Both HMNO and 3P domain trust their interconnection provider

The implications related to the trust model are:

- The user/ME has no way to detect the trustworthiness of the AP.
- The user/ME connects to an AP and it is unaware that it may be monitored by a third party since the user/ME trusts it unconditionally.

Threat mitigation strategy

The threats may be mitigated in this case through the deployment of privacy enhanced functionality into the UE. One approach to limit tracking is to provide for randomisation of the device's MAC addresses. Whilst a number of mobile Operating Systems do now provide for randomisation of the device's MAC addresses these are typically limited in their privacy protection as the randomisation only occurs in a limited set of protocol interactions.

Other solutions can ensure that MAC addresses associated with sensitive locations may be not be reused and that noise may be added to the information an attacker may obtain through randomisation of the ordering of emitted MAC addresses and by dummy MAC address injection. The 'Device Identity Privacy' enabler provides such features to enhance the location privacy afforded to the UE.

B.6 Subscriber Identity Privacy (UC 2.2)

B.6.1 Use case description with architectural components

The use case relates to a user attaching to a 5G network for the first time (e.g. in a roaming situation or after the user's ME is switched on). The description of this procedure and its related function blocks is illustrated in Figure 30.

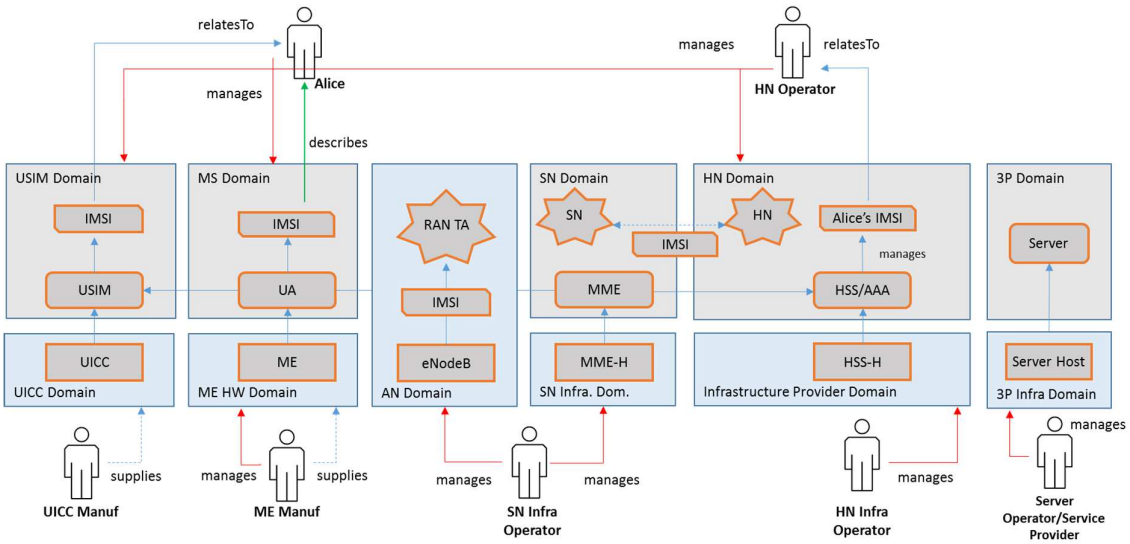

Figure 30. Subscriber Identity Privacy (UC 2.2): sunny day scenario

Figure 30 shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

Alice has a subscription with a Mobile Network Operator (MNO) and she has been provisioned with credentials (the IMSI and the secret key Ki). The secret key Ki has been stored on the UICC domain. When Alice's ME is switched on, the ME attempts to attach to the mobile serving network (SN) by sending an **Attach**

Request message. Alice's ME does not have a short or temporary subscriber identifier (i.e. the GUTI in LTE) because this is the first attach to the network. Alice's ME sends the permanent or long-term subscription identifiers (i.e. IMSI) over the access network (AN) domain towards the serving network (SN) domain. Alice's IMSI is sent in clear text because no cryptographic material has yet been negotiated between the ME and the AN/SN. The SN uses Alice's IMSI to route the request towards the HN domain. The HN uses the IMSI to identify Alice's subscription and to start the authentication procedure by providing the SN with an authentication vector. After Alice's successful authenticate, the ME and the SN have negotiated a security context used to protect Alice's traffic over the AN domain.

B.6.2 Identified threats

B.6.2.1 Tracking of device's (user's) location (T_UC2.2_1)

Mallory wants to track a target user Alice in Figure 31.

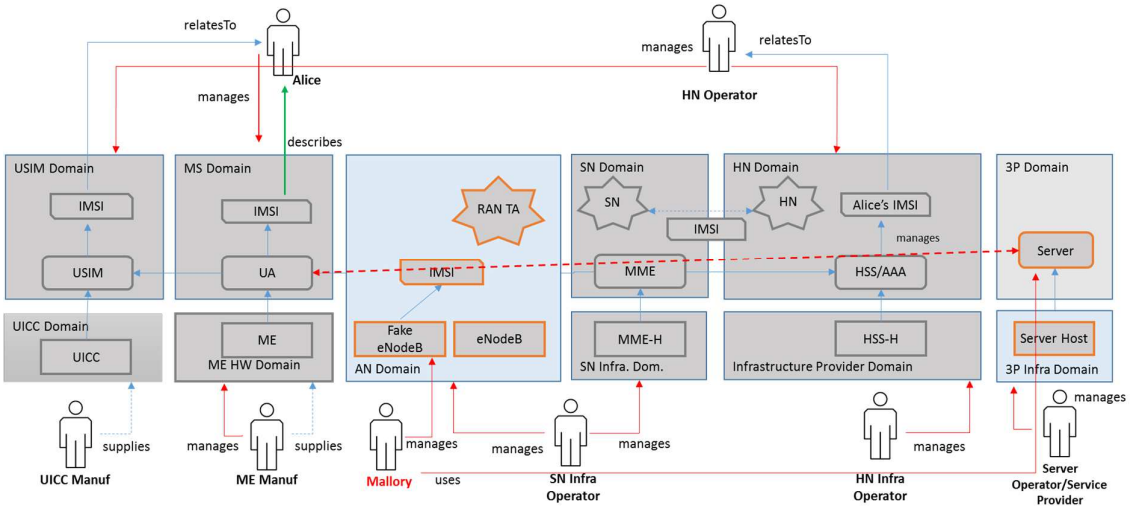

Figure 31. Tracking of device's (user's) location (UC 2.2) – 'rainy day'.

In a first phase Mallory operates in passive mode. Mallory's objective is to collect a set of users' identities, permanent (IMSIs) and temporary (GUTIs), which can be used for two purposes. One is to link subscriber's presence to a certain area, and other is to reveal his past and future movements in that area. To achieve this, Mallory sniffs over the AN (Figure 31) and decode broadcast paging channels to extract IMSIs and GUTIs.

Mallory then needs to map IMSI or GUTI associated with a particular subscriber (e.g. Alice) to reveal his/her presence in that area. The mapping between GUTI and IMSI is possible using semi-passive attacks.

The objective of the semi-passive attack is to determine the presence of a subscriber in a Tracking Area (TA) and further, to find the cell in which the subscriber is physically located in. In particular, Mallory tracks Alice's current location by triggering the mobile network into initiating the generation of paging messages to Alice's ME (e.g. by using social media application hosted on a 3P server to initiate unobtrusive communications)

Mallory observes the paging messages sent and can potentially correlate the contained GUTI with Alice's social network identity.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- the ME trusts its HMNO as part of the direct service agreement.
- The HMNO trusts the SMNO as part of the roaming agreement contract and it confers full trust in the SMNO with regards to the IMSI of a subscriber. For authentication, authorisation and billing purposes, the IMSI is exchanged unabated between the serving network (SN) and the home network (HN).
- Both HMNO and SMNO trust their interconnection provider.

The implication related to the trust model are:

- The user/ME has no way to detect the trustworthy of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- The user/ME answers to the rogue AN/SN request asking the transmission of the user's permanent identity (IMSI).

Threat mitigation strategy

Subscriber identities are transmitted unprotected over the AN enabling tracking of MEs.

To protect IMSI transmission over AN during the first network attach solutions based on the use of a public key encryption can be used like the *Encryption of Long Term Identifiers* feature and the *Home Network-centric IMSI protection* feature. Those features also limit the possibility for Mallory to locate a user.

A second mitigation strategy is to ensure temporary subscriber identities are reallocated often enough to avoid tracking. Today the reallocation of temporary user's identity depends entirely on the operator network's configuration with the risk that they tend to remain the same even if a ME is moving. Hence temporary identities are not really temporary. This allows an attacker to perform passive attacks. In addition the generation mechanism for the temporary identities is vendor dependent and not defined. Often the newly assigned temporary identity differed from the old one by only one hexadecimal digit. This implies that temporary identities were not chosen randomly.

The *"Privacy Enhanced Identity Protection"* enabler provides the *IMSI pseudonymization feature* to mitigate the user's location tracking. The feature provides:

- A generation function for temporary or short term identifier having the following properties:
  - it ensures that the temporary subscriber identifier are univocal random numbers (Random Temporary Mobile Subscriber Identity - RTMSI) over the entire Tracking Area
  - it ensures that the probability of collisions between the RTMSI allocated to different MEs over the entire Tracking Area is sufficiently small.
- A mechanism for triggering the RTMSI refreshing and it's periodically update to avoid dependence on the operator's network configuration. The new RMTSI is triggered after each usage (one-time).

The solution impacts the SN that needs to support the *IMSI pseudonymization feature.* The SN can trigger the use of a new one-time pseudonym (after each usage) according to the "push model".

The solution can impact also the user's ME in the case where a "synchronized" model is adopted. In this case also MEs have to implement the *IMSI pseudonymization feature* to generate and update the new RTMSI in a synchronized way, after each usage.

B.6.2.2 Mobile user interception and information interception (T_UC2.2_2)

The attacker, Mallory, wants to gather the IMSIs of all users which are active in a geographic area.

Mallory can achieve this in two different ways: passive and active. Mallory opts for the more effective active attack allowing at any time to retrieve users IMSIs, instead of waiting for users MEs to send out their IMSIs as in the passive attack.

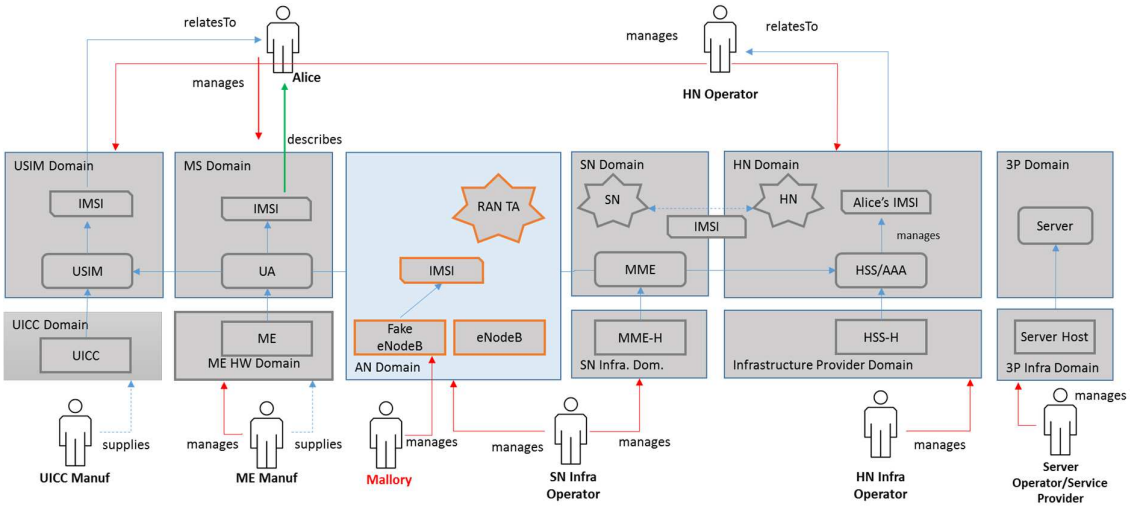

Figure 32. Mobile user interception and information interception (UC 2.2) – 'rainy day'.

Based on Figure 32, Mallory sets up a rogue 5G Base Station (known as an IMSI catcher), operating with higher power than the legitimate one, to which MEs in the neighbourhood will attempt to connect. Mallory's IMSI catcher acts between the target ME and the SN's real towers. As such it is considered a Man-in-The-Middle (MiTM) attack and usually is undetectable for the users MEs.

Alice's ME, as part of its scanning activity for 5G Base Station with the best signal power around it, camps on the rogue 5G Base Station (Mallory). The fake base station then simply commands Alice's ME to identify itself. Alice's ME returns in response Alice's IMSI. Mallory is able to retrieve Alice's user identity since it is transmitted in clear text over the AN.

The consequence effects of users' identifiers exposure over-the-air signalling messages mostly relate to the issue that the subscription identifier is disclosed or made inferable to an unauthorized party. Once the Mallory knows the IMSI, due to its format she also knows the home country where subscriber resides and the home mobile network operator. Also the subscriber's location might be linked to the user's identifier as the transmission of the IMSI reveals the user approximate location.

The information gained exploiting the lack of IMSI protection during the initial attach opens the door to other attacks like the sending of fake signalling messages (e.g. SS7) towards the HN having impact on the HSS (e.g. fake Authentication Request to retrieve user's authentication vector or fake Location Update Request to redirect the target user in another location under Mallory's control or to create a user's DoS).

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- The ME trusts its HMNO as part of the direct service agreement.
- The HMNO trusts the SMNO as part of the roaming agreement contract and it confers full trust in the SMNO with regards to the IMSI of a subscriber. For authentication, authorisation and billing purposes, the IMSI is exchanged unabated between the serving network (SN) and the home network (HN).
- Both HMNO and SMNO trust their interconnection provider.

The implication related to the trust model are:

- The user/ME has no way to detect the trustworthy of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- The user/ME answers to the rogue AN/SN request asking the transmission of the user's permanent identity (IMSI).

Threat mitigation strategy

The types of trust required in this use case can be ensured/guaranteed through technical solutions in addition to agreements between partners. These solutions should ensure that the user's IMSI is not sent in clear text during the first attack to the network (Attach Request) or in case of explicitly Identity Request. From the technical point of view this can be achieved, for example, by the use of encryption schemes based on public key cryptography that can provide the necessary root of trust and the key material in situations where no keys are yet negotiated between the ME and the network.

These solution do not prevent to a ME to attach to a rogue AN, but they significantly make ineffective the attack since Mallory can't be able to retrieve the user's IMSI.

The "Privacy Enhanced Identity Protection" enabler provides two alternative features to counteract this threat based on different approaches.

The *Home Network-centric IMSI protection* feature demands to the user's HN the responsibility for performing the decryption of user's IMSI and the sharing afterwards of the clear-text IMSI to the rest of the network elements on the system that may need it (i.e. the SN for LI purpose). The feature needs to be implemented on the ME and on the HN. The ME uses the HN's public-key to encrypt only part of the user's IMSI. The Mobile Country Code (MCC) and the Mobile Network Code (MNC) of the IMSI are left in clear-text, to allow the SN to route the encrypted IMSI to the user's HN.

The *Encryption of Long Term Identifiers* feature demands to the SN the responsibility for performing the decryption of user's IMSI. In this case the entire IMSI is encrypted by the ME using a global public key generated according to the KP-ABE scheme combined with an attribute that identifies the SN to which the user's ME is connected to. This means that the same public key is used also when the user is in roaming. Only the attribute changes since it is the one that identify the current trusted SN.

B.7 Enhanced Communication Privacy (UC 2.3)

B.7.1 Use case description

This use case details the user Bob communicating securely via a device over the eNodeB and into the MNO network. Bob wants his communications to be resistant to passive interception. The use case discusses ways which this might be by passed, and Bob's communications are compromised via a passive attacker.

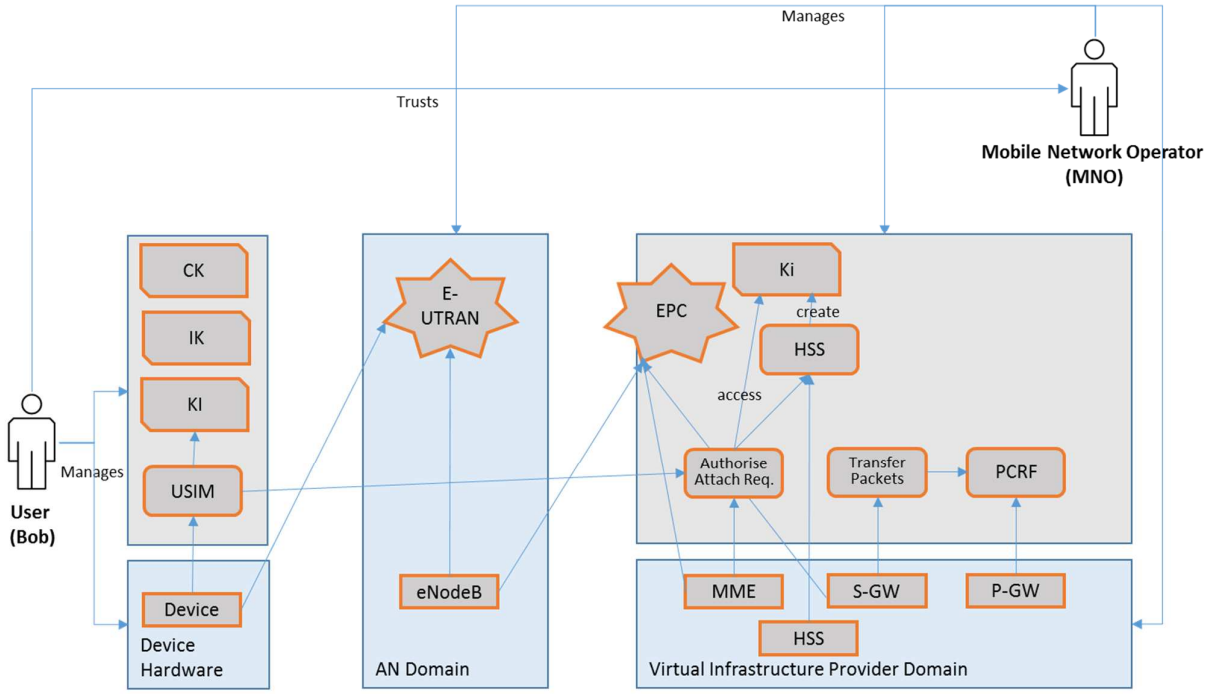

Figure 33. Enhanced Communication Privacy (UC 2.3): sunny day

User Bob manages a device which connects to the MNO's network via the access network. The AN and MNO network is both managed by the mobile network operator, the hard for the MNO network can be managed by the MNO, for this scenario there is no difference. Bob, the user, trusts the network is correctly managed by the MNO. And when his device authenticates with the USIM with the network it will be accepted and his communications are to be secured from any and all adversaries.

B.7.2 Identified threats

B.7.2.1 Passive communication interception (T_UC2.3_1)

The attacker has compromised bob's user-specific Ki, 'Ki'. This gives Malory to ability to decrypt data which Bob transfers to the MNO, which is authenticated using the Ki. Malory is able to perform this attack without any activing influence on the either the user or operator, because of this there is no way which either can detect the attack.

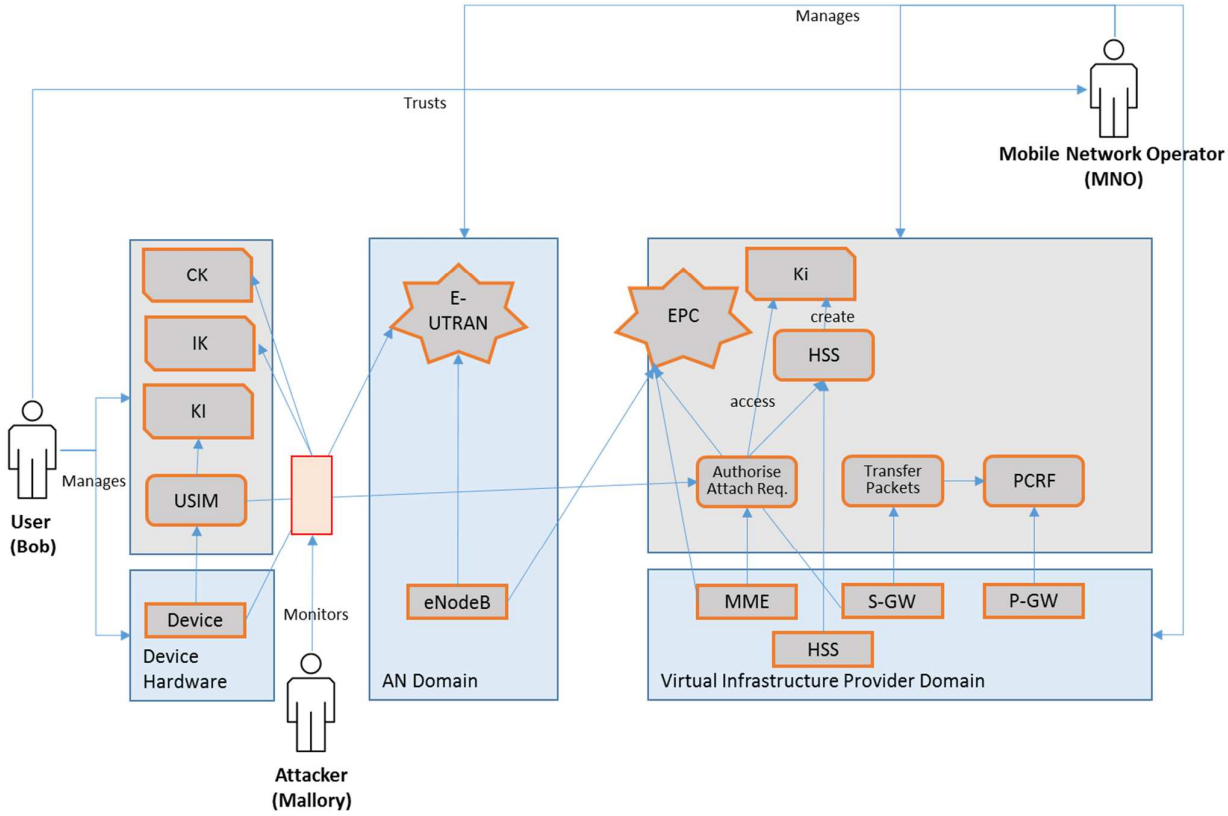

Figure 34. Passive communication interception (T_UC2.3_1) – 'rainy day'

When Mallory performs this attack any and all communication between the users can be intercepted. Because this is a passive attack Mallory is limited in what he can do. This can cause leaking of secure information from users of the network. Since a user has more trust in the phone network than they would a traditional computer network. They might feel they can talk more freely over the telephone network resulting in a larger personal or commercial impact when private information is leaked from this attack. If the device compromised is used to administer other devices on the 5G network then they could also become compromised as well as Bob's device.

Trust implications

Bob who manages the device connecting to the network, trusts the MNO will not allow passive attacks like this to happen. The MNO may transfer responsibility of trust from them to the receiver of the communications i.e. whomever bob is talking to. Because the MNO is not required to encrypt user plane data, and this is the responsibility of the user. Bob may choose to use end to end encryption to protect his communication. To a certain degree the MNO has to take responsibility, this depends on the severity of data being compromised on their network otherwise their customers will lose faith in their abilities.

Threat mitigation strategy

Aside from what was discussed with end to end encryption for the users. A better solution for the 5G network would be to force data plane encryption which support perfect forward secrecy. This would force the attack from passive to an active attack, which would increase the complexity of the attack required. This mitigation technique would be implemented on the user's device and within the MNO's network. Stakeholders who

would be expected to enforce and implement this would be the MNO and maybe the device/USIM manufacturer.

B.8 Authentication of IoT Devices in 5G (UC 3.1)

B.8.1 Use case description with architectural components

The use case relates to IoT authentication following different ways depending on their capabilities. The figure below describes the different possible scenarios for using 5G resources.

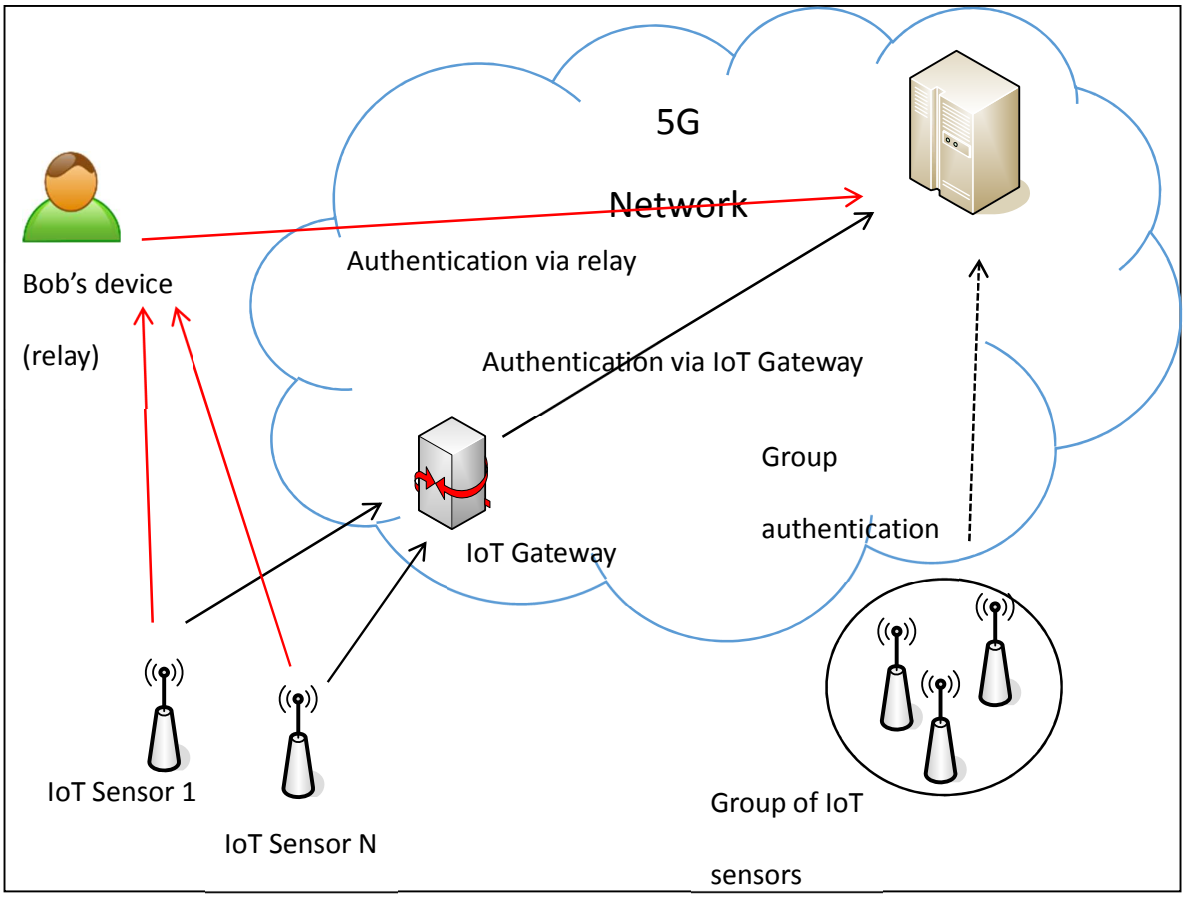

Figure 35: Authentication of IoT Devices in 5G (UC 3.1)

The description of different scenarios and their related function blocks are illustrated in the next three figures, which illustrates the different scenarios with respect to the architecture, in the absence of any threat (the sunny day scenario). On the different architecture diagram, the scenario is the storage of a sensor data in a cloud infrastructure offered by a cloud provider.

B.8.1.1 Basic IoT Authentication by 5G UE

The more simple way to allow a sensor to call services hosted by a cloud provider is to re-use an existing authorized access, which can be offered by a user's UE or a specific IoT gateway. For the architectural description, we simplify by using only a user's ME (Bob's ME) because the IoT gateway could be seen as a specific user's UE. For this basic IoT authentication, all operations are performed at the user's UE without impact on the rest of the architecture. The sunny day described in Figure 36 is very simple.

For the targeted scenario:

1. Bob defines all authorized equipment for using his UE.
2. The sensor is authenticated to Bob's UE (or IoT gateway)
3. The sensor call a storage service hosted by the cloud provider and use Bob's account to store its data.

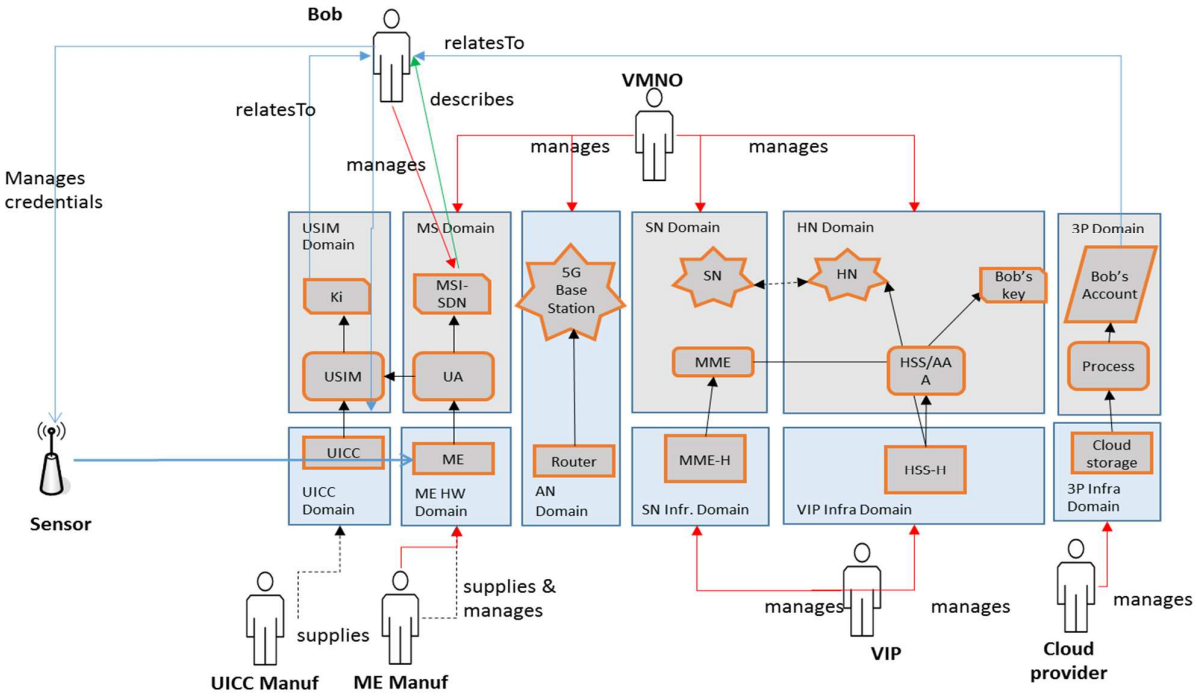

Figure 36: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for basic IoT authentication by 5G ME

B.8.1.2 IoT Authentication relayed by 5G ME

Another way for a device to call services hosted by a cloud provider is to have its own credential but by using the ME to communicate with the HSS/AAA. This case is relevant when the device is not using the standard 5G interfaces. In this specific case, the ME has to implement the specific interface before being able to relay the authentication information. In our scenario, the sensor owner is associated with Bob for using the cloud storage service. The following Figure 37 describes this scenario.

For the targeted scenario:

1. The sensor owner has registered his sensors and their credential in the HSS.
2. Bob's ME (or IoT gateway) is configured to relay specific sensors authentication.
3. The sensor call a storage service hosted by the cloud provider and use Bob's ME to perform its authentication and then, to store its data.

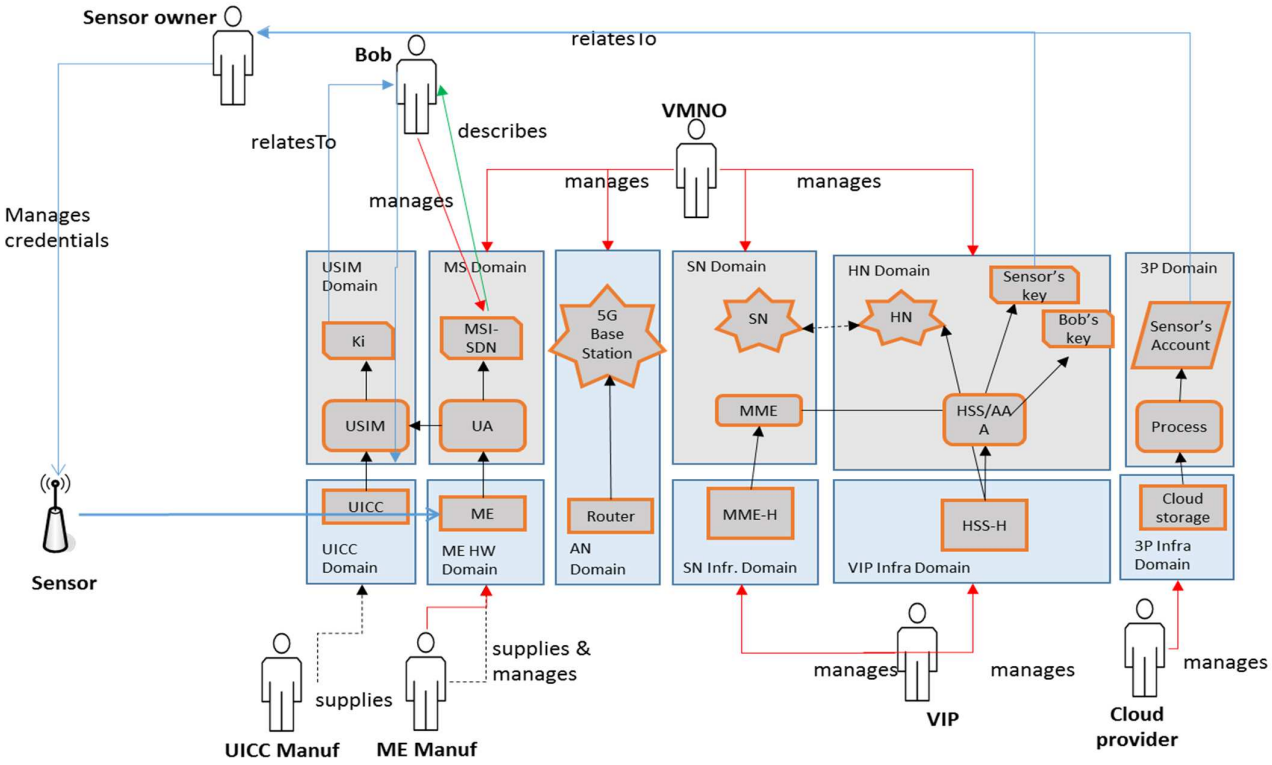

Figure 37: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for IoT Authentication relayed by 5G ME

B.8.1.3 IoT Group based authentication

For this kind of authentication, we use the open specifications of "Internet-of-things" enabler described in D3.6. With this enabler, the authentication is performed, for the first MTC, with the HSS but, for the other MTC (Machine-Type Communication) belonging to the same group, the authentication is performed by the MME. The Group-based authentication involves MTC(s), MME and HSS configuration.

For the targeted scenario:

1. The MTC(s) owner (group of sensors) has registered his group and their credential in the HSS. Each MTC USIM stores the group ID.
2. The MME is configured to perform group-based authentication
3. One of the MTC call a storage service hosted by the cloud provider and use its own credentials to perform its authentication and then, to store its data.

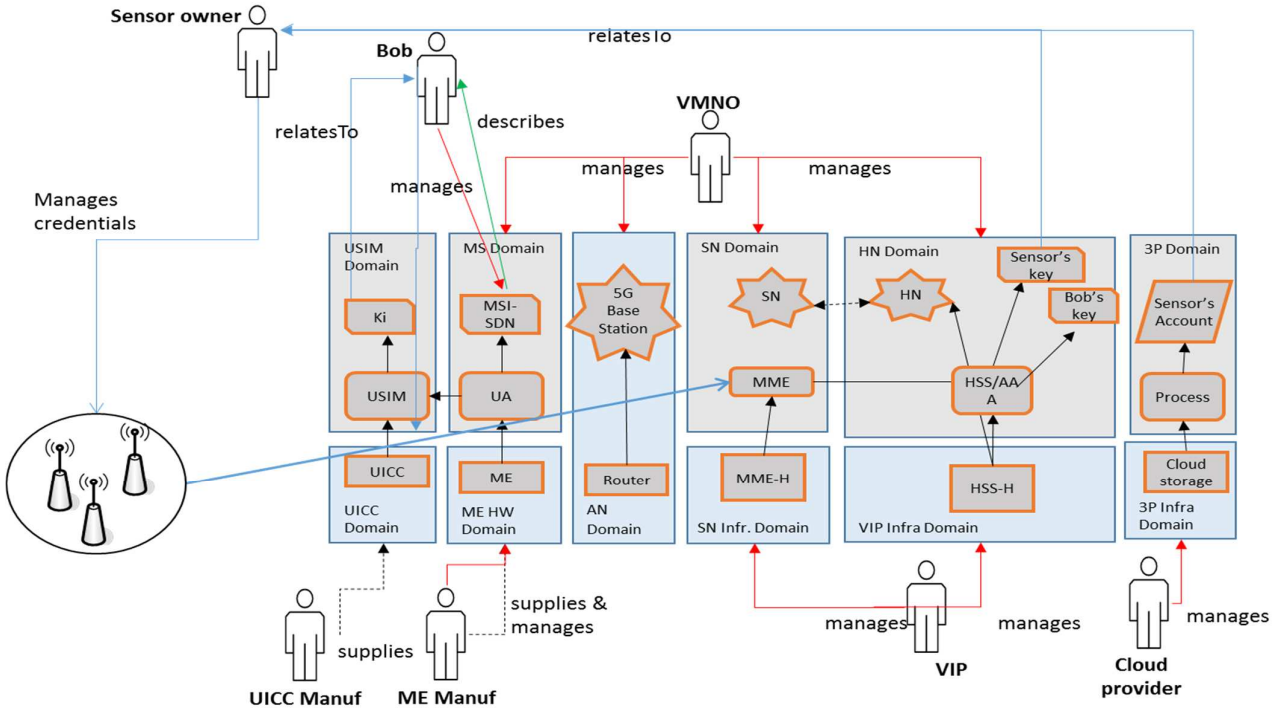

Figure 38: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for IoT Group based authentication

B.8.2 Identified threats

B.8.2.1 Authentication traffic spikes (T_UC3.1_1)

The attacker, Mallory, wants to perform a denial-of-service attack. For that, she initiates traffic spikes or emphasize the effects of natural traffic spikes with IoT aiming to be connected. As a consequence, the network will experience more signaling and authentication functions needs to perform more processing. Potentially, the authentication of authorized devices may fail and these devices may lose connectivity.

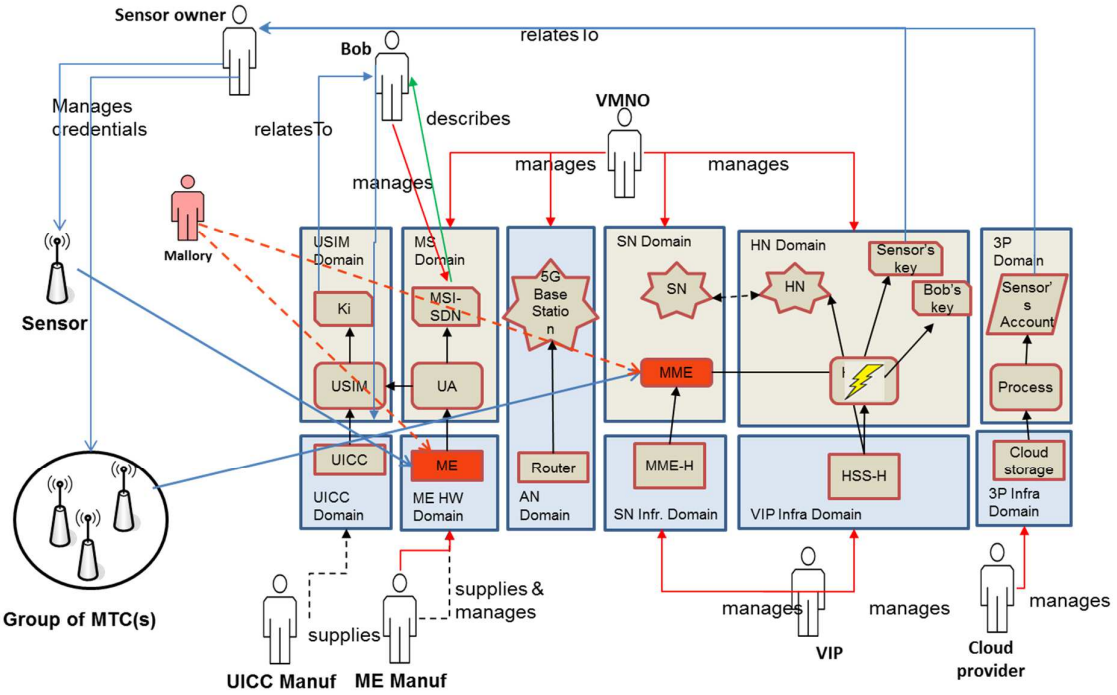

Figure 39: Authentication traffic spikes (T_UC3.1_1) – 'rainy day'

Based on Figure 39, Mallory has two options for that. She can increase the number of connections at the MME level (3rd scenario) or she can increase the number of connections at the UE level (2nd scenario). This threat didn't affect the first scenario because the authentication lacks are more the problem than the number of connections (all connections will be performed by the same user or IoT Gateway owner). For the 2 last scenarios, each time a connected device is attached to the network, an authentication is performed between the device and the MME but also between the MME and the HSS. If the HSS is overload, other connection of legitimate devices could be rejected.

Trust implications

This use case involves several actors: the sensors, the relay (Bob's UE or IoT gateway), the sensors owner, the relay owner and the VMNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships.

- The VMNO is secured and its HSS is protected against identity theft (specifically for the 2nd and 3rd scenarios).
- The sensor owner never discloses the sensors information (and especially their identity)
- The VMNO trusts the User equipment software developer/provider delivering the specific application on ME (specifically for the last 2 scenarios) and on the HSS.

The implications related to the trust model are:

- The MME are not able to detect that unauthorized device try to be connected.

Threat mitigation strategy

The threats may be mitigated in this case at the MME level to avoid traffic spikes regarding the signalisation (authentication mechanisms). For example the Group-based authentication mechanism is a good way to limit the number of complete authentications involving MTC, MME and HSS.

B.8.2.2 Compromised authentication gateway (T_UC3.1_2)

The attacker, Mallory, wants to intercept data exchange between sensors and the services provided by the cloud provider (a storage service for example). For that, she compromises specifically an IoT gateway or a mobile phone. In this case, she could act as a man-in-the-middle. As a result, data collected from IoT devices may leak from to wrong parties and IoT devices may receive commands from malicious party. The group-based authentication is not impacted due to the usage only of signalization mechanisms without gateways.

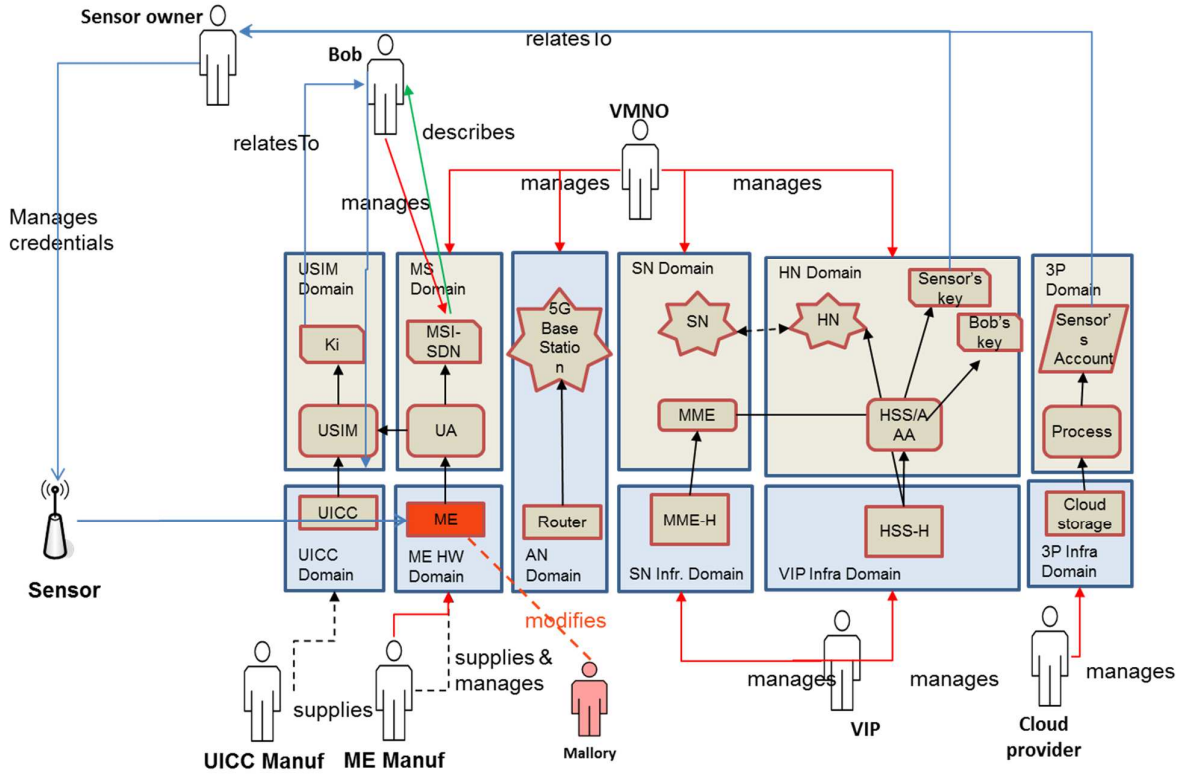

Figure 40: Compromised authentication gateway (T_UC3.1_2) – 'rainy day'.

In Figure 40, Mallory can achieve this by modifying the user's ME or the IoT gateway. In this case, Mallory is able to have all the traffic exchanged between the sensors and the services provider. Another way to perform this attack would be to have an exact copy of the ME (including UICC card).

Trust implications

The use case involves several actors: the sensors, the relay (Bob's UE or IoT gateway), the sensors owner, the relay owner and the VMNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships:

- The sensor owner never discloses the sensors information (and especially their identity)
- The VMNO trusts the User equipment software developer/provider delivering the specific application on ME (specifically for the 2 first scenarios).
- The relay owner (user's mobile phone or the IoT gateway owner) trust the User equipment software developer/provider.

The implication related to the trust model are:

- The sensor owner has no way to detect an abnormal behaviour of the relay (user's mobile phone or the IoT gateway owner)

Threat mitigation strategy

Mitigation of this threat may be achieved by using certified software and/or certified hardware. Another way is to guarantee the confidentiality between the sensor and the service using these data by cipher mechanisms. In this last case, all man in the middle attacks won't be able to interpret the data.

B.9 Network-Based Key Management for End-to-End Security (UC 3.2)

B.9.1 Use case description with architectural components

An IoT device is connected to a 5G network and authenticated to use the network. The communication should be end-to-end secured (encrypted and authenticated) but the endpoints have no means to connect each other securely (e.g., they do not share secret keys). The IoT device needs to communicate with an IoT backend service (operated by Alice) which utilizes 5G systems' network-enabled key management service. The key management service provides keys and the connected IoT device achieves secure end-to-end communication to the IoT backend service located, e.g., in the cloud. Figure 41 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

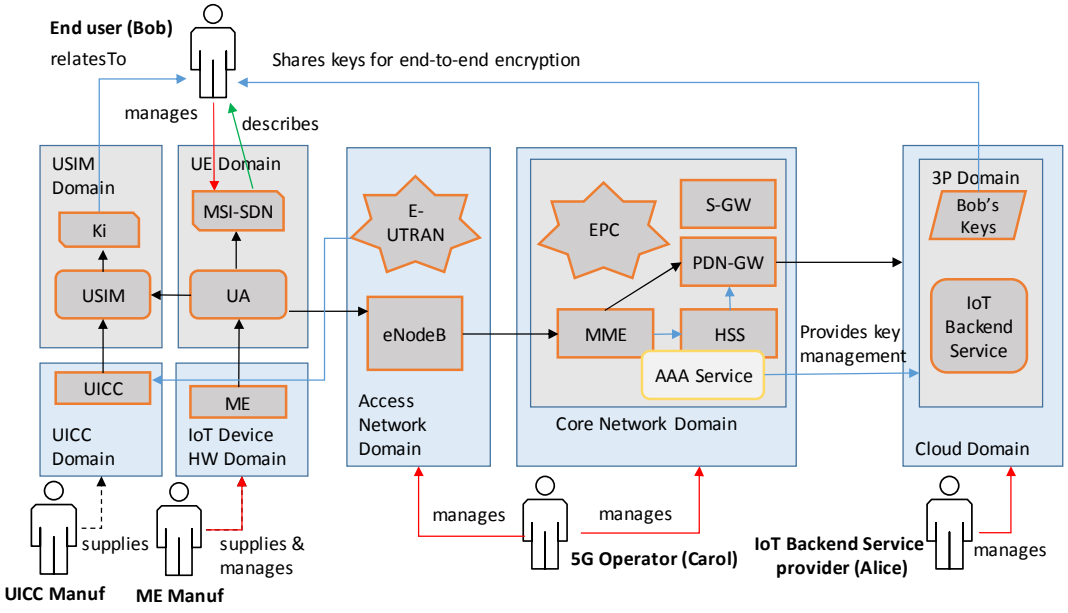

Figure 41. Network-Based Key Management for End-to-End Security (UC 3.2): sunny day scenario

B.9.2 Identified threats

B.9.2.1 Leaking keys (T_UC3.2_1)

End-to-end keys may be stolen or leak from the centralized key servers. The key server may also become tampered. As a consequence, the end-to-end secured communication is vulnerable for different attacks and adversaries can gain an access to the end-points. They may e.g. provide false information to application services or send malicious commands to IoT devices. The VNFs which may get involved are indicated in Figure 42.

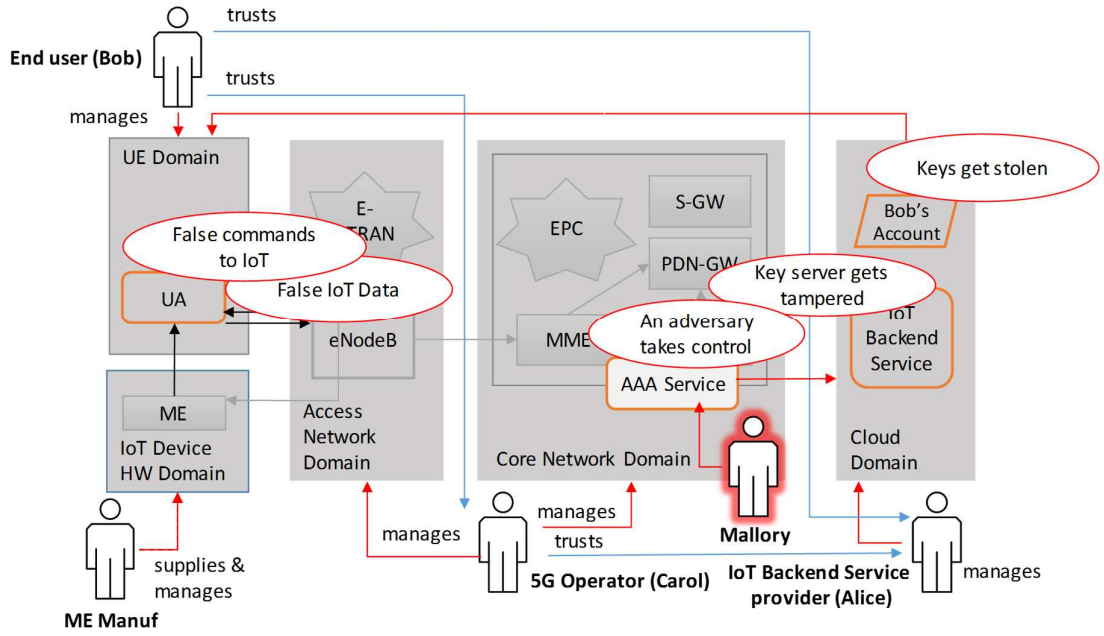

Figure 42. Leaking keys (T_UC3.2_1) – 'rainy day'

Trust implications

Potential trust implications are the following:

- Bob loses trust to both the 5G system operator (Carol) and the IoT Backend Service Operator (Alice) since his system does not work properly or its data leaks to outsiders
- Alice probably loses trust to Carol although the adversary may actually tamper only the IoT Backend System which should be under Alice's own control.
- Carol, the MNO may lose trust to Alice as it is possible that the real adversary never gets identified. It is also possible that Bob's system look malicious and Carol loses trust to Bob.

Threat mitigation strategy

Potential ways to mitigate this risk:

- If lawful interception is not required (it is always required in some countries) implementing a key management server to a 5G system is not quite necessary
- Service and device discovery can be controlled to limit utilization of leaked keys. IoT service can be configured without providing any address of remote IoT service. In that case the 5G mobile

operator may fully control the IoT devices and Alice may not need the device addresses, while all communication is encrypted.

B.10 Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1)

B.10.1 Use case description with architectural components

The use case relates to authorization management performed at the sensor level. As the sensor could be considered as a resource-constrained device, the authorization should be delegated to an AAA server. The following figure describes the different actors involved in the use case.

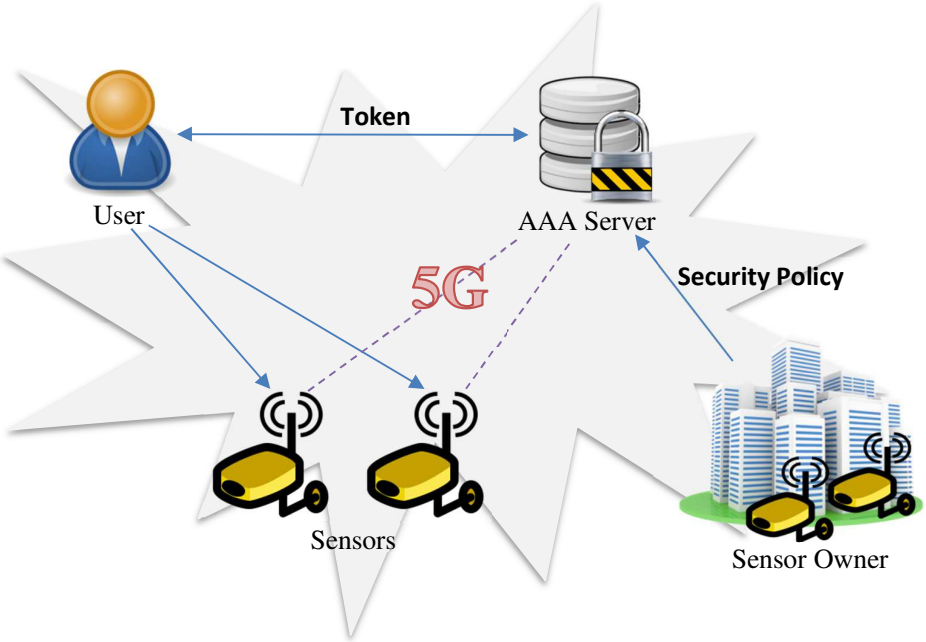

Figure 43: Setting for Authorization in Resource-Constrained Devices

The main components of the architecture involved are specifically the HSS (the AAA server) and the different components used in standard authentication of a ME.

B.10.2 Sunny day scenario

For this scenario, the different actors are:

- Alice: she wants to use one sensor
- Sensor's owner: he manages the sensors and has defined the access control rights for using them.

The prerequisites are:

- The sensors and Alice use their 5G credentials to be authenticated in 5G context.
- The AAA server was modified to accept to check an authorization token for a specific token.
- The HSS was modified to manage security policy for sensors and especially to use token access control for specific sensors. The security policies are provided by the sensor's owner.

- 5G operator trusts the sensor's owner and allows him to define the security policies at AAA server level

The standard scenario is the following:

- The sensors' owner issues security policies to the AAA Server concerning access to its sensors to the AAA Server.
- The sensors have used their 5G credential to be connected.
- Alice uses her 5G credential to be connected.
- Alice authenticates to the AAA Server and requires access to the sensors.
- The AAA Server issues an authorization token based on 5G credentials of Alice according to the security policies.
- Alice uses this token for accessing the sensors
- The sensors contact the AAA server to check the token
- If the token is valid and authorizes Alice, she has access to the sensor(s)

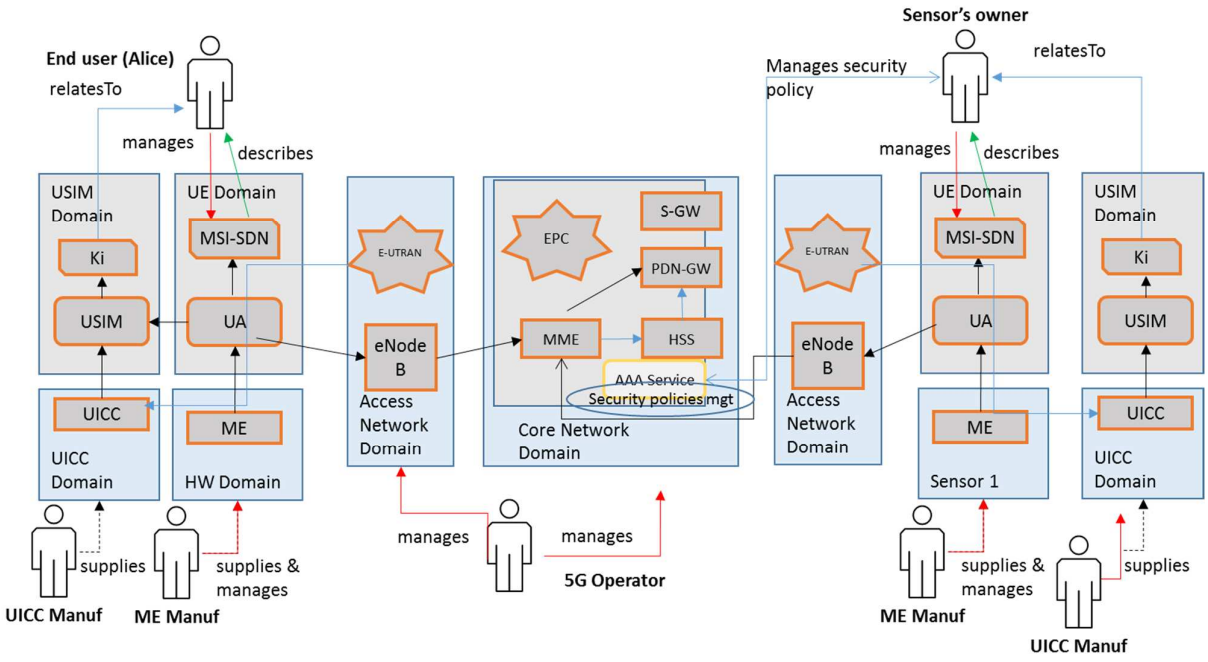

Figure 44: Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1): sunny day scenario

B.10.3 Identified threats

The way to obtain tokens, to validate tokens or to generate tokens are not standardized for now and so this analyse doesn't take into account the threats of this detailed interfaces.

B.10.3.1 Unauthorized data access (T_UC4.1_1)

The attacker, Mallory, wants to access the sensors' data without authorization. She can exploit the two main vulnerabilities by trying to generate a fake token or by trying to modify the security policy to get access to the sensors. The new vulnerabilities, due to the AAA server modifications are not in the scope of this use case.

Generation of a fake token or replay of an existing token: Two specific attacks could be performed by Mallory regarding the token. The first one is to build a new token giving all the right to use sensor data. The second one is to capture an existing token and to replay it in another context. To avoid this vulnerability, a specific attention should be given to the design of the token. The token will be injected at UA level (see Figure 45).

Modification of security policies: The token generation and the associated security policy are not standardized for now and so, different modifications should be performed. The main one is to develop an interface with AAA server to configure the security policy. This interface must guarantee that only the sensor's owner can modify the security policy and only for his sensors (see Figure 45).

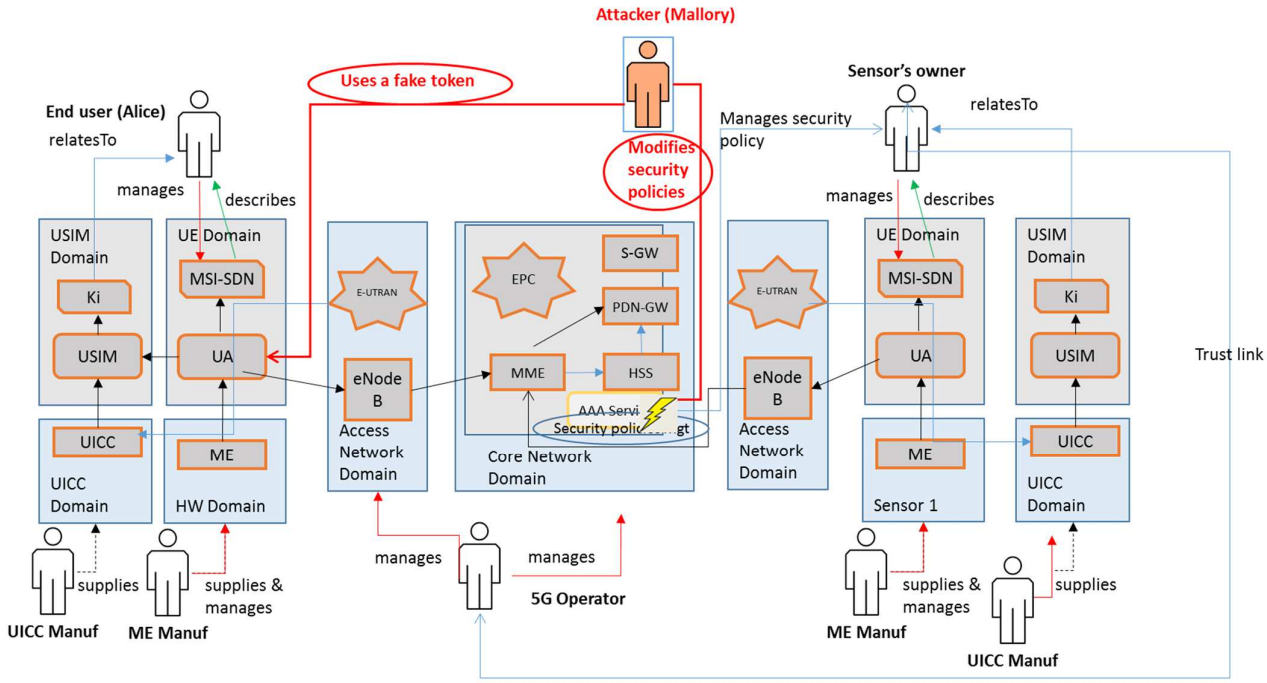

Figure 45: Unauthorized data access (T_UC4.1_1) – 'rainy day'

The different parts of the architecture involved in the attacks are displayed in Figure 45. The two main components involved are the user's UA and the AAA server (especially the modifications).

Trust implications

This use case involves several actors: the sensors, Alice's UE, the sensors owner, the 5G Operator to which the user and the sensor's owner have a subscription. The current trust model is based on the following relationships.

- The agreement between the 5G Operator (VMNO) and the sensor's owner. If this agreement is not clear and if the liability of the two parties is not well established, the sensor's owner could, for example, gives to anyone the credentials to modify a security policy. This weakness could be used by Mallory.
- The sensor's owner trust Alice

Threat mitigation strategy

The main action to mitigate the threats is at the token level. A specific attention should be given to the design of the token with, for example, a timestamp to avoid the token replay and crypto mechanisms (signature) to limit the possibility to build a new fake token.

B.11 Virtualized Core Networks and Network Slicing (UC 5.1)

B.11.1 Use case description with architectural components

This use case concerns micro-segmentation as a good way to ensure isolation of end-users' specific needs to manage their own sensors through the 5G infrastructure. Network slicing (and further sub-slicing) could be used to create portions of the underlying network which can be further used to provide network services with particular properties. Micro-segmentation could provide a more fine-grained approach than traditional network slicing and with micro-segmentation it may be possible to create secure segments where more granular access controls and stricter security policies can be enforced.

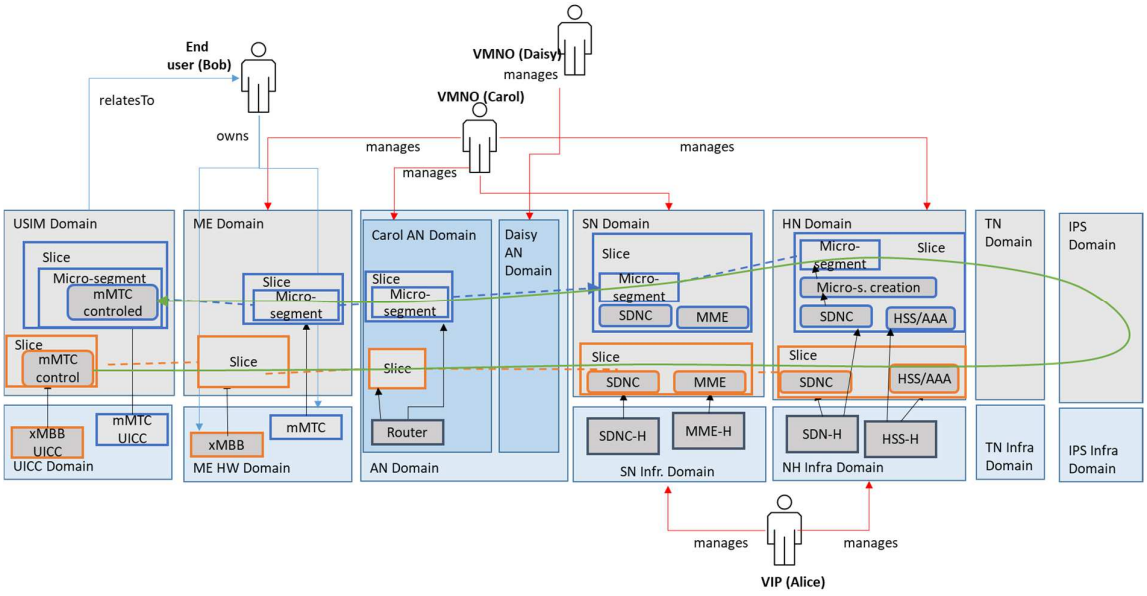

Figure 46. Virtualized Core Networks and Network Slicing (UC 5.1): sunny day scenario

Figure 46 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). The subscriber (Bob) has two different devices and has a subscription to the virtualised network provided by the VMNO (Carol) for both devices, a 5G xMBB device and also a sensor that is a 5G mMTC device. VMNO (Carol) is providing an Internet accessible API for 5G mMTC device subscribers to control the behaviour of the mMTC devices.

Bob turns on the power in his 5G xMBB device and 5G mMTC sensor, and the attach requests are routed via the 5G radio network (AN). The base station (AN) contacts the MMEs in the VMNO network slices for xMBB and mMTC. The devices are authenticated towards the HSS/AAA of their slice after attachment. The VMNO decides to create a micro-segment for Bob's mMTC communications. This micro-segment is extended to include this 5G base station if not already included. The micro-segments are allocated for the devices that are authorized for it. The micro-segment has a security mechanism of its own.

The Network Slices are configured in such way that one slice does not accept commands from another slice. Nevertheless, through VMNO's Internet accessible API for 5G mMTC device subscribers, Bob can command his mMTC sensor by means of his xMBB device (Green flow).

B.11.2 Identified threats

B.11.2.1 Misbehaving control plane (T_UC5.1_1)

Malicious or compromised control plane may jeopardize the network and the data plane.

For instance, a compromised SDN controller or virtualization orchestrator may prevent data flows or direct them to a man-in-the-middle switch for eavesdropping or tampering. Centralized network controllers are an alluring targets for attacks as adversaries are not required to compromise switches or network functions it is enough that they steer data flows to their own malicious components.

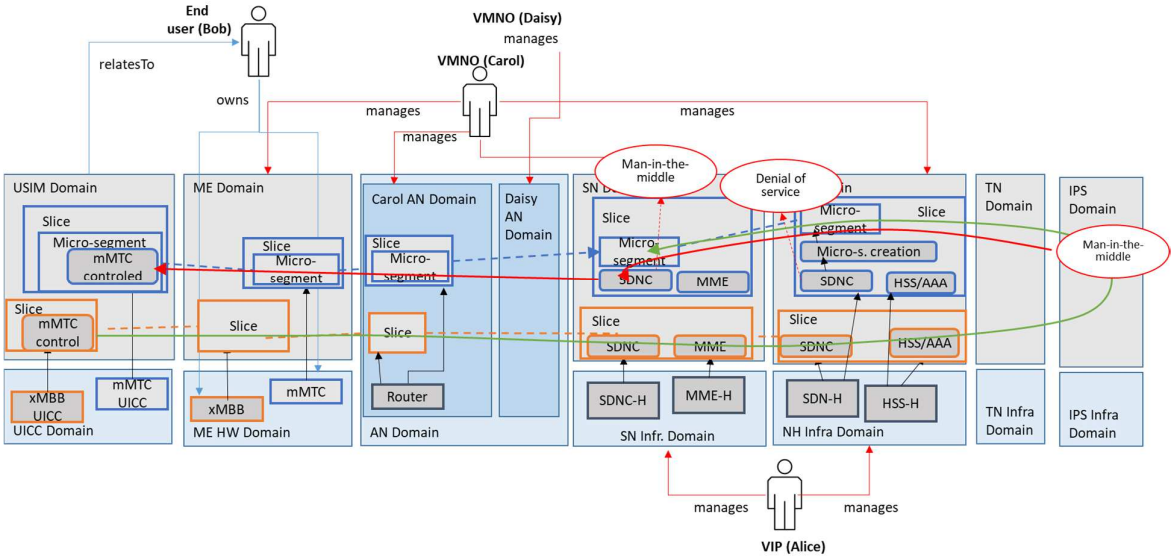

Figure 47. Misbehaving control plane (T_UC5.1_1) – 'rainy day'

Figure 47 shows the primary threat by which this attack is carried out, and the architectural components involved in the attack.

Since SN Domain micro-segment serving the mMTC sensor is accessible from the Internet through the an Internet accessible API for 5G mMTC, and if the micro-segment controller has a vulnerability, this could be a way for attackers to send fake commands to the mMTC device, or to compromise the SN SDN controller of the related mMTC slice in order to reach the mMTC device with fake commands (the red flows).

Also if compromised the SN SDN controller could deny the service to command the mMTC device.

Trust implications

The trust implications of this are as follows:

- The Subscriber (Bob) cannot manage his own mMTC sensor if his VMNO is compromised. Therefore, Bob has to trust his VMNO.
- The VMNO (Carol) suffers because her network is degraded and her customers (like Bob) will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on

behalf of her customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.

Threat mitigation strategy

To mitigate this risk, the following option is possible:

- Micro-segmentation should split network slices into smaller parts with more restricted and controlled security policies dedicated for specific application services or users. By combining micro-segments similar guaranteed security levels can be provided even over multiple network domains and multiple network operators.

B.12 Adding a 5G node to a virtualized core network (UC 5.2)

B.12.1 Use case description with architectural components

In this use case, we assume that each UE is associated with a network slice before they have been authenticated. A new network slice requires configuring a new virtual MME which is done with software provided by a 5G Node Provider (5GNP). The control plane of SDN should not and cannot modify the physical network resources reserved to another Virtualized Core Network. Figure 48 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

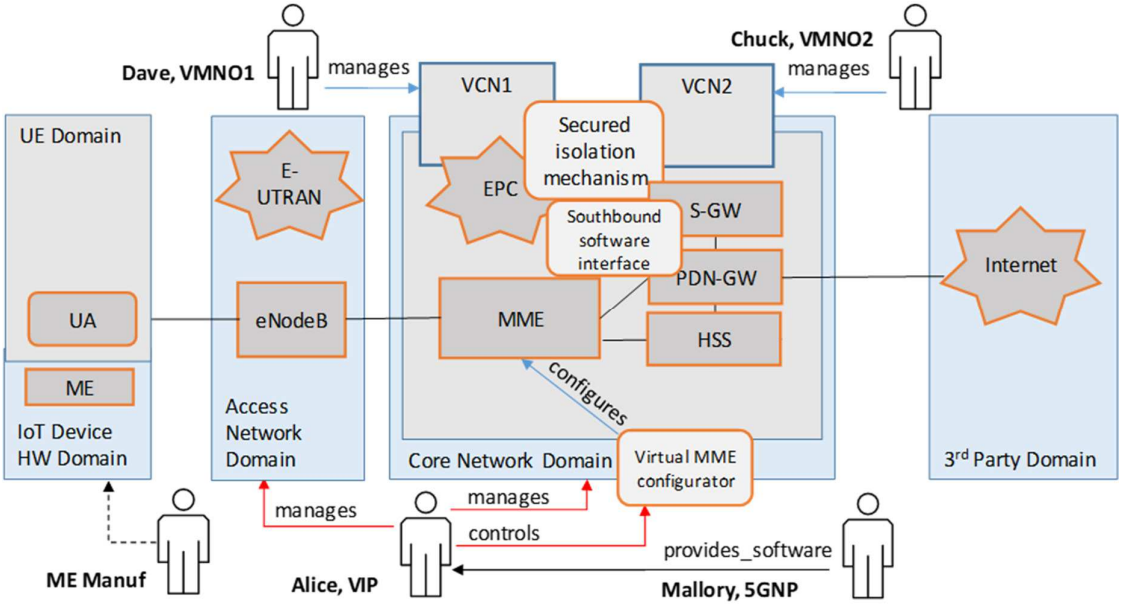

Figure 48. Adding a 5G node to a virtualized core network (UC 5.2): sunny day scenario

B.12.2 Identified threats

B.12.2.1 Add malicious nodes into core network (T_UC5.2_1)

Software tools which are used to create a new MME or a new network slice can be corrupted, if they were obtained from a precarious vendor (Mallory). In such case, a new network node, which Alice carefully installs, may eavesdrop, tamper or even prevent data flows. Confidentiality, integrity and availability of communication gets severely compromised. Meanwhile, Alice can be completely unaware of this. Figure 49 depicts the VNFs involved in the occurrence.

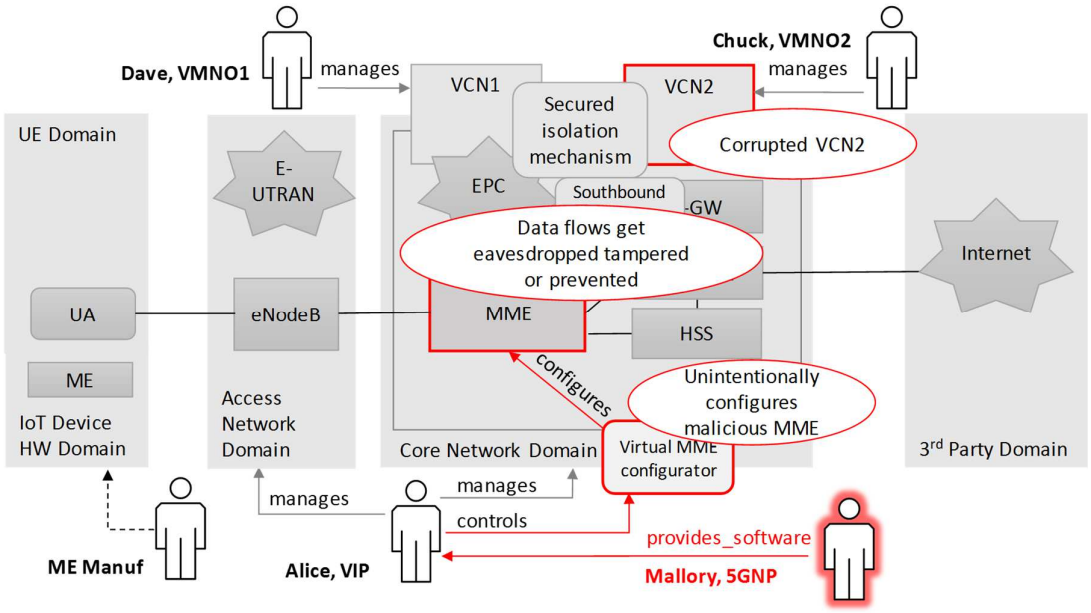

Figure 49. Add malicious nodes into core network (T_UC5.2_1) – 'rainy day'

Trust implications

Potential trust implications are the following:

- Both VMNOs, Dave and Chuck, lose their trust to Alice since they may not be aware of Mallory's real role in the occurrence.
- Dave's and Chuck's customers, which are the end users of 5G network services, may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.
- Alice may lose her trust to Mallory for a reason, but also to some other software vendors although they have not done anything undesirable or malicious on purpose.
- Alice may think that either Chuck or Dave have ignored some important security measures either on purpose or accidentally

Threat mitigation strategy

Potential ways to mitigate this risk:

- All stakeholders, Alice, Chuck and Dave should apply advanced security verification procedures, both technical and organisational, to all software which they acquire
- Only authenticated and authorized entities should be allowed to add nodes to SDN
- Specific verification procedures should be utilized to assure that all added nodes are trustworthy
- Strict security monitoring of behaviour of added nodes as well as to communication over the network.

B.12.2.2 Forwarding logic leakage (T_UC5.2_2)

A network application (serving VCN2) at the southbound interface may be able to see the forwarding logic installed in the physical switches which are supporting another virtual network operator's domain (VCN1). Such information leak can be malicious and it can enable intercepting messages, gathering statistic

information and analysing installed forwarding rules of another competing VCN. Even confidential application data could be captured. Among potential effects is serious loss of confidentiality, outsiders may get to know positioning of virtual network components or critical service elements. This information can be used to infer end users or to disrupt reliability of a VMNO's system.

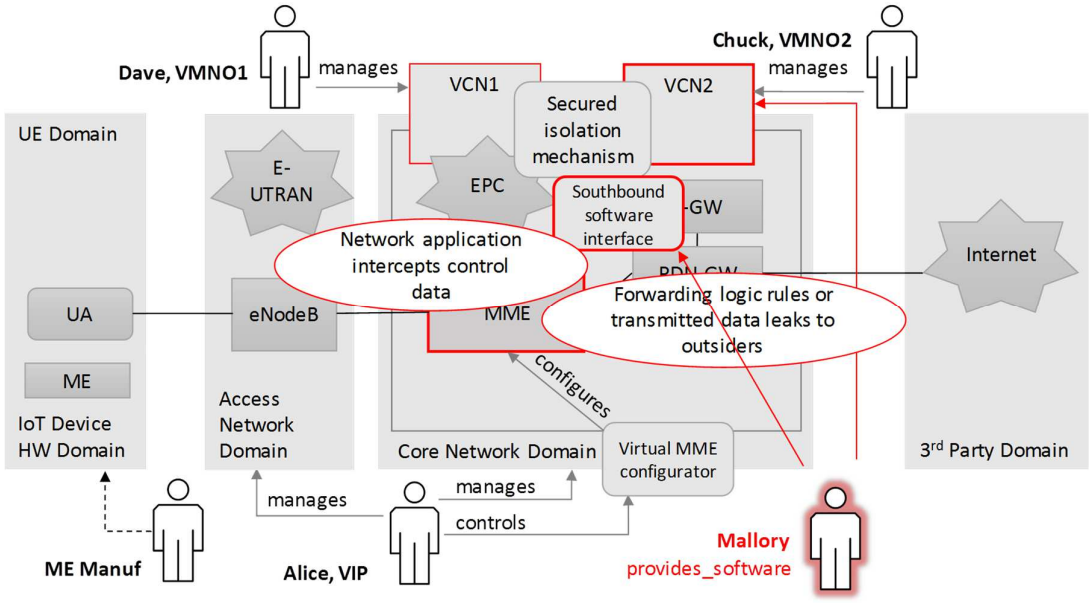

Figure 50. Forwarding logic leakage (T_UC5.2_2) - 'another rainy day'

Trust implications

Potential trust implications are the following:

- Dave may lose trust to Alice, although Chuck or Mallory can be the real threat
- Chuck may not be aware of Mallory's malicious actions and his trust may not change at all
- If Chuck utilizes the leakage, he will lose some trust to Alice, if Alice does not notice the leak or if she cannot stop it
- Chuck can hardly trust Mallory, even if Mallory lets him use the leaked information
- Alice may lose trust to Chuck, even when Mallory is the only guilty stakeholder
- The end users of 5G network services may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Inserting a reference monitor at the southbound interface

B.12.2.3 Manipulation of forwarding logic (T_UC5.2_3)

The basic setting is the same as in T_UC5.2_2 except that in this case the intruder acts more aggressively. In addition to collecting confidential information of the competitor, malicious actions that change data flows are executed. Potential effects are: overflow of switch tables which causes slower and degraded performance, manipulating forwarding rules to trigger denial of service, modifying the rules to redirect traffic to allow intercepting every message and modifying system to tamper user's data.

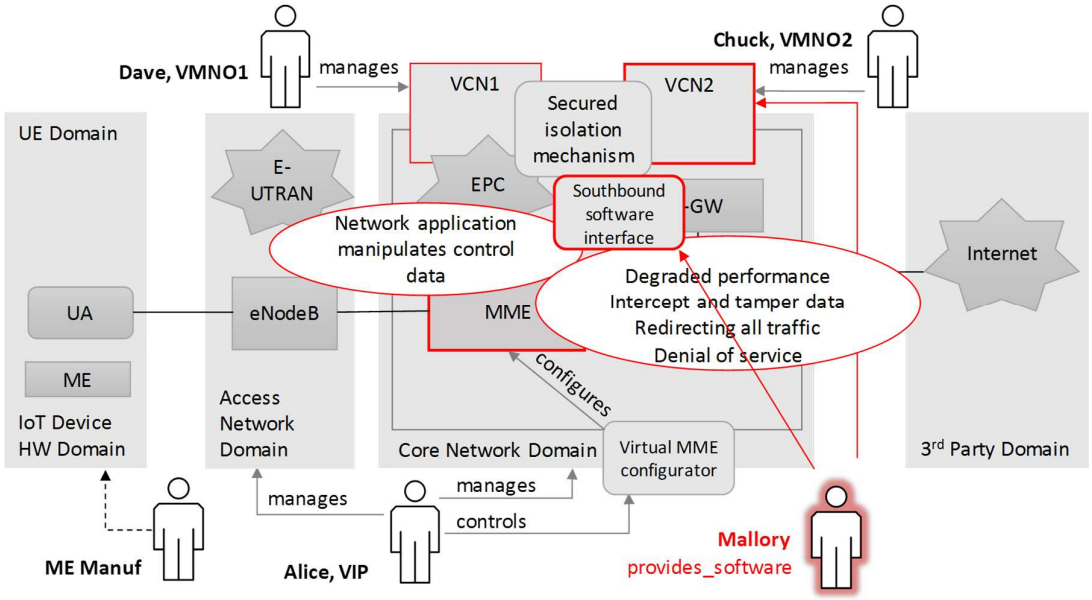

Figure 51. Manipulation of forwarding logic (T_UC5.2_3) - 'yet another rainy day'

Trust implications

Potential trust implications are the same as with T_UC5.2_2 or the following:

- Dave may lose trust to Alice, although Chuck or Mallory can be the real threat
- Chuck may not be aware of Mallory's malicious actions and his trust may not change at all
- If Chuck utilizes the leakage, he will lose some trust to Alice, if Alice does not notice the leak or if she cannot stop it
- Chuck can hardly trust Mallory, even if Mallory lets him use the leaked information
- Alice may lose trust to Chuck, even when Mallory is the only guilty stakeholder
- The end users of 5G network services may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.

Threat mitigation strategy

Potential way to mitigate this risk is the same as with T_UC5.2_2:

- Inserting a reference monitor at the southbound interface

B.13 Reactive Traffic Routing in a Virtualized Core Network (UC 5.3)

B.13.1 Use case description with architectural components

This use case concerns reactive forwarding of network traffic in a Virtual Mobile Network Operator's core network. Subscribers connect via third party access networks, acting as roaming subscribers with respect to the VMNO's network. When subscribers demand access to the physical core network, at the beginning there are any matching flow rules in the data plane components and the network application is triggered to install those rules. A (virtualised) SDN controller then reconfigure the flow tables of the switches to provide the required connectivity.

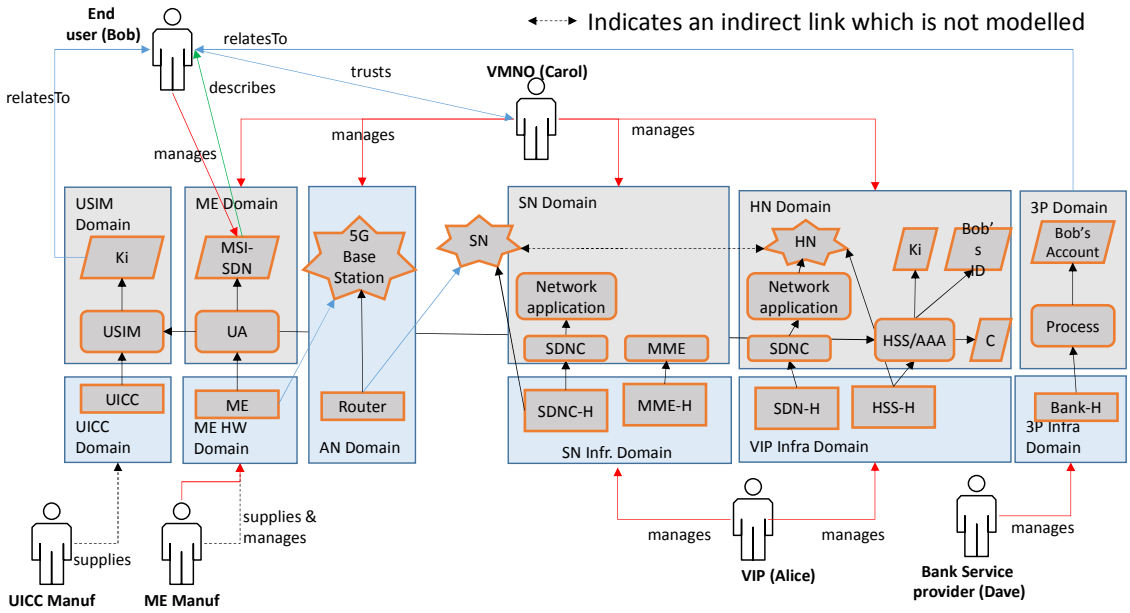

Figure 52. Reactive traffic routing in a virtualised core network (UC5.3): sunny day scenario

Figure 52 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). The subscriber (Bob) connects to the virtualised network provided by the VMNO (Carol), and uses it to access services such as a Bank Service from a service provider (Dave). This service provider may have an agreement with the VMNO to provide related services, such as enhanced authentication of subscribers, although this is not essential to the scenario. The VMNO provisions their core network as a slice obtained from a Virtualised Infrastructure Provider (Alice). The VMNO's core network is therefore implemented using VNFs running on the physical infrastructure, including a Software Defined Network Controller (SDNC) providing connectivity for the Home Domain. In Figure 52 we assume the VMNO has a similar arrangement to provide Serving Network domains connected to third party Access Network infrastructure, although this too is not essential to the scenario.

B.13.2 Identified threats

B.13.2.1 Fingerprinting attack on a virtualised network (T_UC5.3_1)

The threat in this case is a denial of service (DoS) attack against the VMNO's core network, caused by an attacker overloading the Home Domain SDNC. To do this, the attacker first carries out a fingerprint attack, measuring the response time of the network and determining how to trigger reconfiguration of the routing

tables at the SDNC. Having done this, the attacker provokes this reconfiguration by sending packets that force frequent updates and a massive increase in flow rules until the SDNC is overloaded and becomes unavailable.

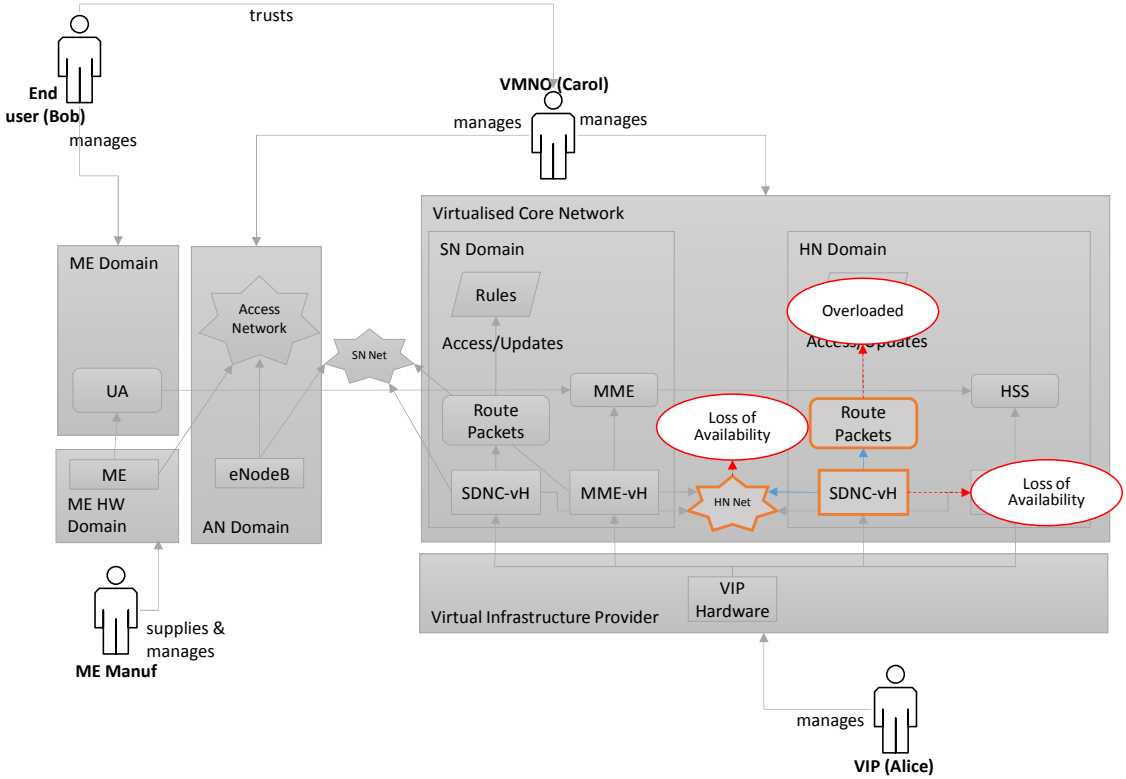

Figure 53. Fingerprinting attack on a virtualised network (T_UC5.3_1) – 'rainy day'

Figure 53 shows the primary threat by which this attack is carried out, and the architectural components involved in the attack. Essentially the routing function running on the (virtualised) SDNC in the HN domain is overloaded, the virtualised SDNC becomes unavailable, and the core network within the HN domain becomes unavailable.

Secondary effects caused by this attack include loss of access from the SN domain to control plane services in the HN domain such as the HSS, which prevents authentication of subscribers cutting them off from the Serving Network and in most cases also the Access Network. Another possible secondary effect is the overloading of the VIP Hardware (the physical SDNC and switches providing the virtualised HN domain core network), which may lead to a loss of availability in other slices supported by the physical infrastructure.

Trust implications

The trust implications of this are as follows:

- The Subscriber (Bob) cannot access the VMNO's network, which may also mean he cannot access specific services (like the Bank) if authentication depends on using that network. Bob cannot reasonably manage this risk, and depends on the VMNO to do that.
- In that case, the Bank becomes unavailable to customers they authenticate via that network. The Bank also cannot manage this risk, although any liability (towards Bob) might be transferrable to the VMNO via their service agreement covering authentication.

- The VMNO (Carol) suffers because her network is degraded and her customers (like Bob and possibly Bob's Bank) will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on behalf of her customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

The VIP provider could monitor loads from each slice, and constrain the physical network capacity made available to each slice. This does not prevent the primary threat, but would help to contain secondary effects that may damage the VIP provider.

B.14 Verification of the Virtualised Node and the Virtualisation Platform (UC 5.4)

B.14.1 Use case description with architectural components

This use case describes a situation where a virtualized network function (VNF) provider is running its VNF on top of a virtualized infrastructure and later wants to verify various security requirements through monitoring. In this use case we consider that the VNF is running on top of an ETSI network function virtualization (NFV) compliant architecture.

Figure 54 shows this scenario in relation to the ETSI NFV architecture for management and orchestration, in the absence of any threat (the sunny day scenario). In this case the management & orchestration (MANO) administrator performs its duties as agreed with the OSS/BSS provider i.e. storing the correct versions of the software images of the VNFs in the repositories. Before launching the VNF instance, the VNF manager (VNFM) checks the signature of the software images and verifies the integrity and authenticity. As a result, a legitimate instance of the VNF gets launched on the network function virtualization infrastructure (NFVI).

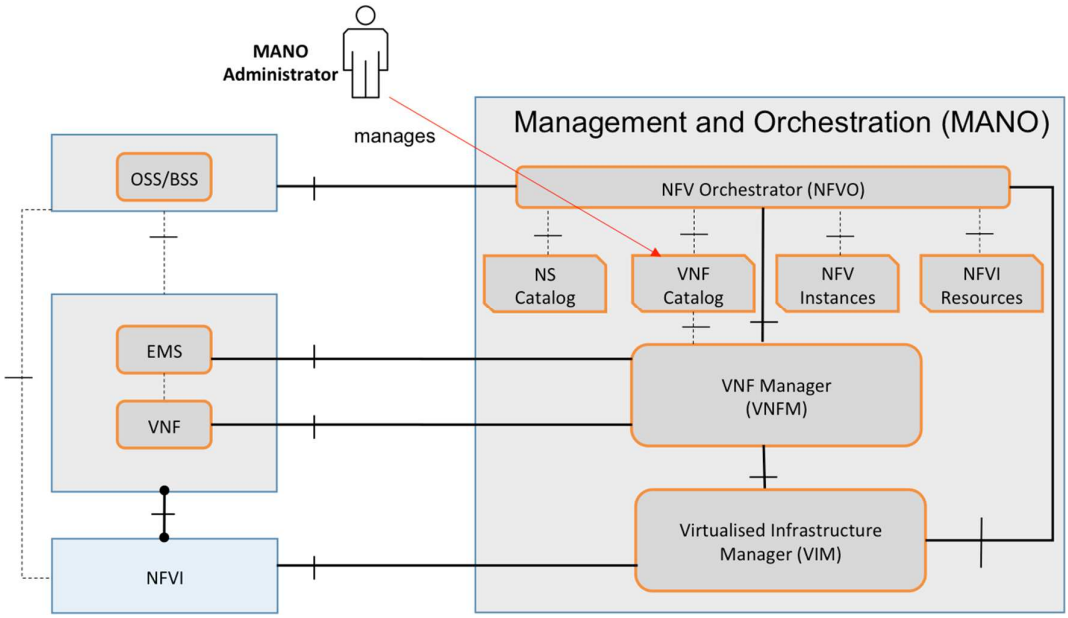

Figure 54. VNF instance running on NFVI in a sunny day scenario

B.14.2 Identified threats

B.14.2.1 Generic Location hacking (T_UC5.4_1)

We document four alternative threats that are related to falsified geographical data fed into the system. The actual ingress point of the falsified data depends on the implementation. The data may be fed from the hardware or from software layer, depending on the actors.

The main risk is that if the system cannot guarantee real geographical location information, any monitoring policies, notifications or alarms are effectively useless.

Alternative 1: Generic service disruption: If attackers manage to infiltrate the geographical data system and feed misinformation e.g. that the physical platform is located in another country, the automated counter-measure systems may cause cascading failures throughout the system.

First the virtualized node (VN) or any other party that monitors VNs will notice that the VN is in foreign country. The VN (or the manager) will request migration back to origin country immediately. This may overload the rest Virtual Platforms.

Alternative 2: Behaviour altering: Behaviour of the VN may change based on the geographical location. For example, the encryption requirements may be more relaxed in neighbouring countries, or legal interception warrant may be valid only in one country. By modifying the location data, the attackers may cause the legal interception functionality to stop working.

Alternative 3: Malicious operator: This threat arises from the fact that the operator may have temporary difficulties in containing all required VNFs within the data center in France. Since the operator is operating in multiple countries, they temporarily move the VNF into Germany, still within their own data centers. However, not to reveal the breach of contract, they feed wrong location information to the Virtualization Platform's location "sensors" (i.e. GPS jamming/IP routing tricks).

Alternative 4: Physical hardware relocation: In this threat, the actual physical platform is moved to another geographical location, either by mistake or intentionally. If an operator has data centers in more than one country (or other important geographical boundaries), a mistake may happen in shuffling hardware between the sites. The risk is elevated if one of the sites is used as a global assembly/configuration point for all physical machines, and then shipped to the final data centers.

The risk comes from the fact that any hardware secure modules likely contains an imprinted geotag set by the operator. If the hardware is moved to another country, but the geotag is not updated, any monitoring services querying for location information will receive invalid information.

Trust implications

If the attackers manage to feed false location data into the system, any location based systems and services are going to be compromised.

Threat mitigation strategy

For all alternatives, the key issue is detecting foul play.

For alternative 1 and 2, the physical hardware could be imprinted with the current location when it enters the data center. This minimizes the software footprint and the attack surface. It does not, however, help against a malicious operator.

For alternative 3, no real mitigation strategy. Depends also on how much effort the operator is spending in order to cover up the contractual breach. If the platform and the VNs support TPM/HSM binding, they could use that to detect the change. Otherwise, the VNs can try to perform statistical analysis on packet delays and other network characteristics to determine that they are further than they should be. This is costly and very hard to prove conclusively.

For alternative 4, no real mitigation strategy. This should be easier case than alternative 3 as the incident is likely unintentional. Network traces may provide an important clue. The TPM/HSM binding will not work, as the whole physical machine is relocated.

B.14.2.2 Manipulation of data stored in repository (T_UC5.4_2)

This is an attack against the integrity verification of the virtualised network functions (VNFs). The most likely attack scenario is that the attacker is an insider administrator of the repository of VNF images or has access to this image repository. With sufficient privilege the attacker is able to alter existing software image in image repository. In this attack scenario, we assume that the attacker is able to replace the legitimate image with an older vulnerable version of the same image. We assume that the infrastructure provider verifies the image integrity and authenticity during launch time by verifying the image signature. However, to bypass this verification process, the attacker uploads an authentic older image version with a known vulnerability that the attacker can exploit. Now, the verification still passes since this image is still signed by the VNF vendor and was not modified by the attacker anyway.

Figure 55 depicts the scenario of a rainy day where the MANO administrator is an attacker. In this case the MANO admin has access to the repositories of the software images and he/she replaces one or more software images with the older version of the same software images. Now, the verification of signature by the VNFM still gets passed since the replaced old image is still signed by the same vendor. Also, it is the lack of checking that the version is not verified during these phase will allow the attack to take place. After this verification, the vulnerable VNF instance is launched on the NFVI. Now the attacker can take advantage of exploiting the vulnerable VNF instance.

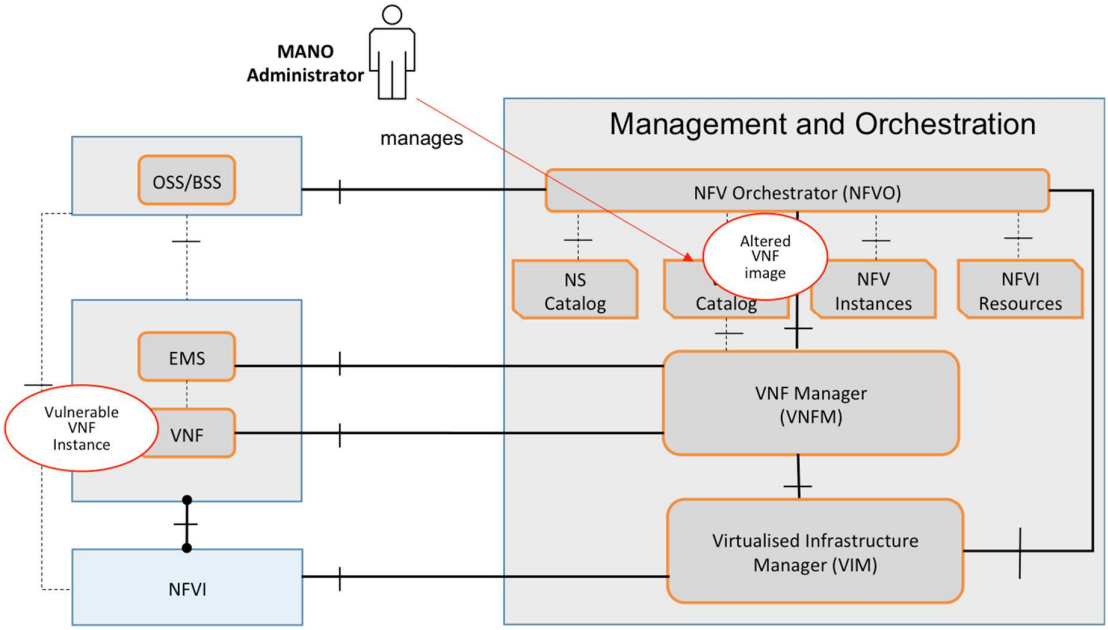

Figure 55. Vulnerable VNF instance running on NFVI in a rainy day scenario

Trust implications

The trust implications of this are as follows:

- The VMNO is not able to run the right version of the VNF. This makes a big risk for the VMNO from both security and cost perspective. In this scenario the VMNO is running a vulnerable version while it is still paying for the legitimate software to be run in the system.
- The attacker has the opportunity to exploit vulnerability. This may imply that the attacker is able to still data from the VMNO application.

Threat mitigation strategy

To mitigate this risk, first of all we need to ensure that the software version (or image version in this case) is verified before a launch of a VNF. So, basically three things need to be checked before a launch:

- During loading the virtualised infrastructure shall only load software image if the authenticity is verified.
- During loading the virtualised infrastructure shall only load software image if the integrity is verified.
- Verification shall include software image versions in the above two cases and the virtualised infrastructure should know which version to run.

Another alternative to the above three steps is that the VMNO verifies all the software images once it is launched. However, this alternative still gives a window of opportunity to the attacker to exploit the vulnerability after the VNF gets launched in the NFVI and before it gets verified by the VMNO.

B.14.2.3 Compromised software signing key (T_UC5.4_3)

Secret keys used by the software vendor to integrity protect the software are compromised, and the incident goes undetected. Such a case may arise e.g. when a malicious administrator/employee copies the keys. The attacker now can create a malicious binary, sign it, and distribute it to the clients.

Trust implications

The VMNOs will be executing untrusted and potentially malicious binaries, which may compromise the whole network.

Threat mitigation strategy

The software vendor must have strong security policies set for software release. Signing the software is not enough. Also a strong checksum of the content must be published in a separate place (e.g. a web page). That information must be signed with another (and physically disconnected) set of secrets.

B.14.2.4 Integrity of the testing machine is compromised (T_UC5.4_4)

According to the use case description, Carol runs a test on the Virtualization Platform to attest the security and privacy characteristics. The attackers have, however, compromised the test program (or the test machine), and give false results.

Trust implications

Carol is left with the impression that everything is fine in the system, when in reality not all is good.

Threat mitigation strategy

There should be a system where all concerned parties are able to extract kind of audit trail of the system, and then compare the result for any anomaly. While the attackers may fool parts of the system, it is unlikely they can do that for each different actor.

B.15 Control and monitoring of slice by service provider (UC 5.5)

B.15.1 Use case description with architectural components

A 3rd Party Service Provider requires a secure network with some QoS guarantees to be used by their customers (game players). The Service Provider has a contract with the VMNO for the VMNO to supply a suitable sub-slice of the VCN for the Service Provider's customers to use. The Service Provider is allowed to monitor the sub-slice and also to control the parameters of the sub-slice within some predefined bounds.

The term "sub-slice" is here being used to mean a portion of a network slice. This use case maintains most of its features, if the Service Provider is a direct customer of a MNO and the MNO provisions a "slice" of the core network for the SP.

Figure 56 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). Dave, an employee of the SP monitors the QoS provided to the game players (Bob and others) and notices that the capacity provisioned for the players may soon degrade to unacceptable level. Dave requests more capacity to meet the demand. The VMNO (Carol) first checks that Virtual Mobile Network can support the increased capacity and then accepts the request.

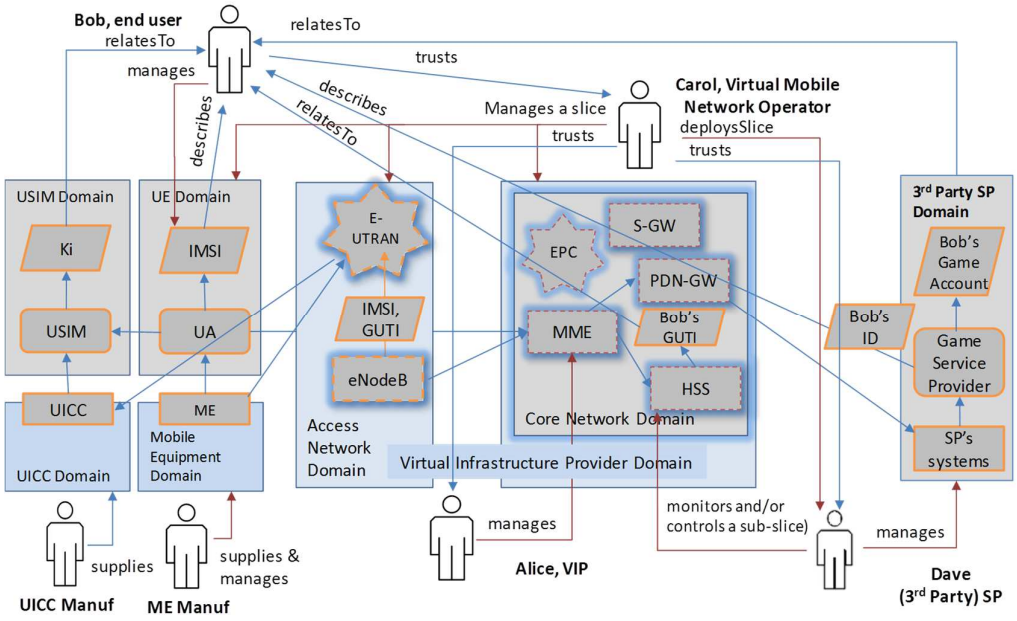

Figure 56. Control and monitoring of slice by service provider (UC 5.5): sunny day scenario

B.15.2 Identified threats

B.15.2.1 Misuse of open control and monitoring interfaces (T_UC5.5_1)

The SP (Dave) may misuse the access to control interfaces and cause service disruptions to other customers or an external party may exploit or attack SP's systems. Monitoring information and data flow may get captured to profile end-users.

When a sub-slice or slice exceeds its capacity limits, QoS offered to other users suffers, or service becomes unavailable, and core or access network may get overloaded. Figure 57 shows the VNFs involved in the occurrence.

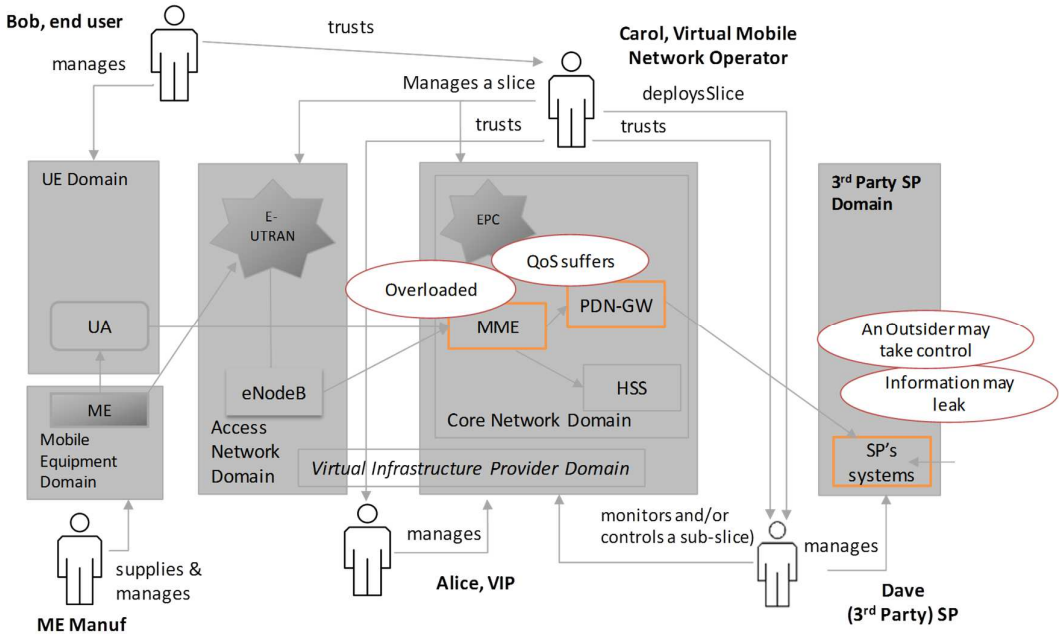

Figure 57. Misuse of open control and monitoring interfaces (T_UC5.5_1) – 'rainy day'

Consequence effects include potential loss of communication security and privacy in a VMN. An overloaded or congested PDN-GW may disturb adjacent systems as well and these may also get congested or unavailable. This use case indicates that when critical interfaces are opened for several service providers they may also become available for other adversaries.

Potential secondary effects include preventing authentication of subscribers through the HSS which denies access from them. Furthermore, if the identity of the end users leaks to outsiders, this information could be used in criminal actions against them.

Trust implications

Potential trust implications are the following:

- SP's customers (Bob) may get better service than they expected, if SP (Dave) intentionally gives them more resources and better QoS than VMNO (Carol) allowed. Bob's trust to Dave may only improve from these actions. Still, if Bob uses other services through the same VMNO, he may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.
- If the customer's (Bob) identification or other personal data leaks to outsiders, the customers may lose their trust completely, both to SP (Dave) and to VMNO (Carol).
- The VMNO (Carol) is responsible of that SP's (Dave) cannot control network outside their own slice or that they cannot exceed their allowed resources without a permission. And yet, the service level agreement between VMNO and SP should prohibit SPs from doing any unapproved actions and financial sanctions should follow, when this occurs.
- When VMNO (Carol) cannot control the VMN she loses trust of some or all customers. VMNO cannot transfer responsibility of her own customers to other stakeholders.

- VMNO should be able to trust that SP does not try to take control of other slices or the whole network and that SP's systems are not vulnerable. If the service provider (Dave) can prevent intrusion to his system, the service level agreement with VMNO (Carol) should cover liability of all consequences, to which SP's systems can be responsible.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- The VIP provider and VMNO should monitor and constrain the physical network capacity made available to each slice. As EPC especially is vulnerable to this threat, EPC monitoring and control systems should take care of counteracts.
- SPs should control their systems properly and also strictly monitor their customers since they may abruptly turn to hostile exploiters.
- SLAs should clearly specify each stakeholder's responsibilities and oblige to severe financial consequences from all potential violations.

VMNO may use the Micro-Segmentation Enabler, which is developed in 5G-ENSURE, to deploy sub-slices to SPs. This enabler can control and defend micro-segments in various ways. Furthermore, another 5G-ENSURE's enabler, the Security Monitor for Micro-Segments enables accurate security incident detection and also adaptation of micro-segment's defences against this type of threat.

B.15.2.2 Unauthorized access to a network slice (T_UC5.5_2)

If VMNO (Carol) misconfigures SP (Dave), she may authenticate and authorize SP to access or control resources that belong to the VMNO or other SPs. Such error may jeopardize availability and security of VMNO's and other SP's resources. Figure 58 shows the VNFs involved in the occurrence.

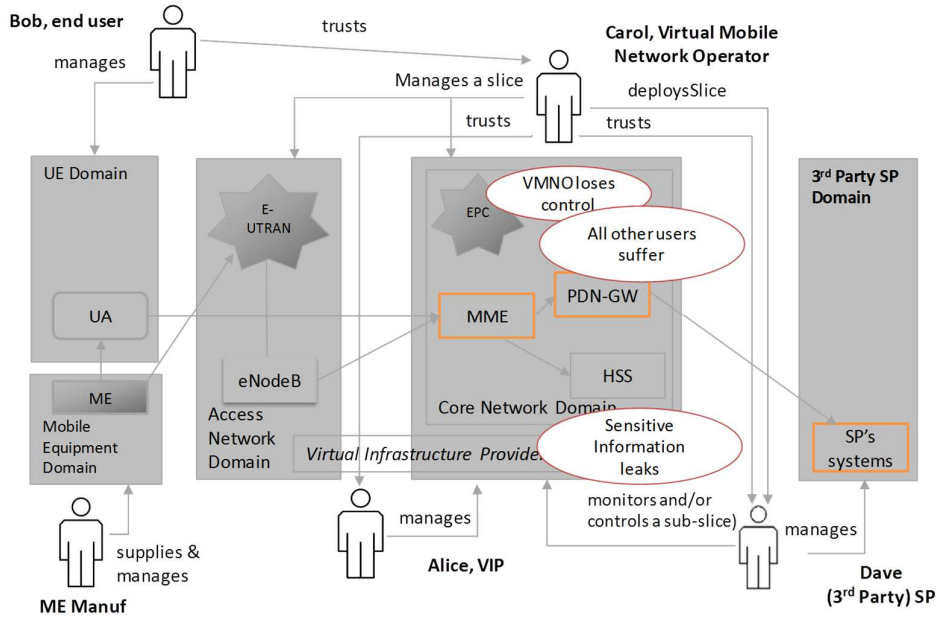

Figure 58. Unauthorized access to a network slice (T_UC5.5_2) - 'another rainy day'

Although this threat arises though a different procedure, its basic consequences are about the same as those mentioned with T_UC5.5_1. The effects include potential loss of communication security and privacy in a VMN.

Potential secondary effects include preventing authentication of subscribers through the HSS which denies access from them. Furthermore, if the identity of the end users leaks to outsiders, this information could be used in criminal actions against them. SP could also utilize or sell information from VMNO's and other SP's customers.

Trust implications

Potential trust implications are the following:

- SP's customers (Bob) may get better service than they expected, if SP (Dave) intentionally gives them more resources and better QoS than VMNO (Carol) allowed. Bob's trust to Dave may only improve from these actions. Still, if Bob uses other services through the same VMNO, he may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.

Threat mitigation strategy

Potential ways to mitigate this risk:

The VIP provider and VMNO should monitor and constrain the physical network capacity made available to each slice. As EPC especially is vulnerable to this threat, EPC monitoring and control systems should take care of counteracts.

B.15.2.3 Bogus monitoring data (T_UC5.5_3)

Tampered monitoring data or measurement procedures may cause control plane to perform wrong control actions. For instance, adversary may impair the availability of the system by getting nodes (which will appear malicious) to be dropped from the topology. The adversary may also change forwarding policies in order to affect availability or to direct data flows into nodes that are e.g. under the control of the adversary and may thus perform eavesdropping or tampering. Figure 59 shows the VNFs involved in the occurrence.

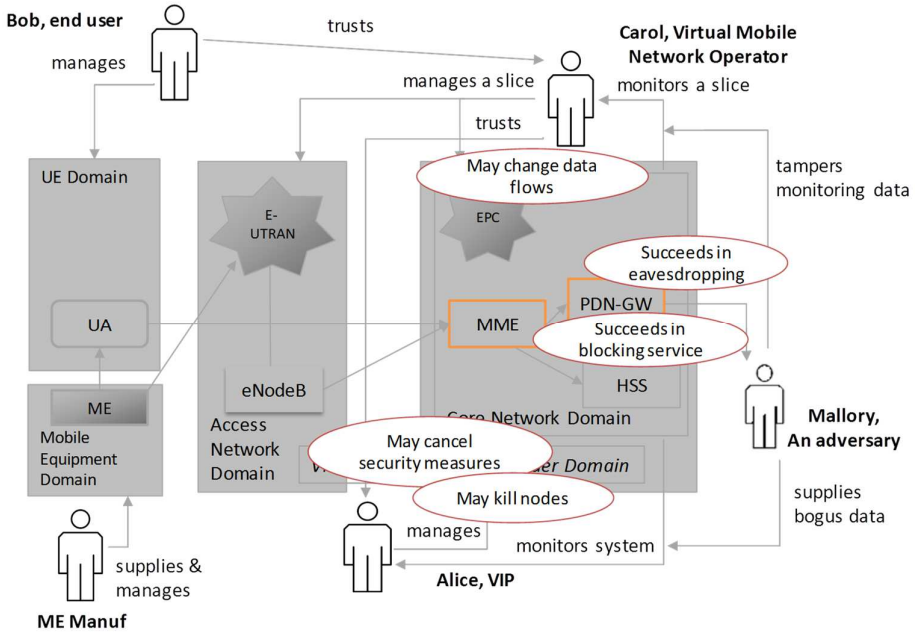

Figure 59. Bogus monitoring data (T_UC5.5_3) - 'another rainy day'

The adversary (Mallory) may utilize unauthorized measurement points or monitoring systems. The adversary may finally take full control of the system as some or all security measures can be cancelled. This may open a slice or the whole system for any type of malicious activities. The attacker may redirect traffic flows or block users, or take all resources for one user. The system may even lose some or all of its authentication, authorization and accounting functions.

Potential secondary effects include severe financial losses for the VMNO which may include reclaims from the end users (Bob).

Trust implications

Potential trust implications are the following:

- The Subscriber (Bob) cannot access the VMNO's network, which may also mean he cannot access any of the services that he typically uses. Bob cannot reasonably manage this risk, and depends on the VMNO to do that.
- The SPs cannot provide their services to their customers, which will cause them financial losses. The SPs cannot manage this risk, although any liability (towards Bob) might be transferrable to the VMNO via their service agreement covering authentication.
- The VMNO (Carol) suffers because her network is degraded and her customers will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on behalf of her

customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.

- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider may have to take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Sources of monitoring data should be authenticated and the source identity information should be available for the information user.
- In cases where monitored data is processed, or aggregated, and then made available for other parties, the original sources of data could be available to enable information users to make sufficient estimates on the reliability of the data.

The sources of bogus measurements may be detected by monitoring the measurements streams and analysing the data against correlated data sources.

B.15.2.4 No control of cyber-attacks by the Service Providers (T_UC5.5_4)

The use case features a Service Provider (SP) offering an online game service to gamers. The SP buys network service from a VMNO which itself relies on an Infrastructure Provider (VIP). The VMNO supplies a sub-slice to the SP with the required QoS.

The SP's system can be subject to cyber-attacks. SP signs a contract with a third party Security Service Operator (SSO) to monitor and remediate cyber-security attacks. Thanks to the terms of the contract between the SP and the VMNO, the SSO can benefit from network topology information and routing tables from the slice controller. Nevertheless, since SSO gets no information about the configuration of the VNF and their vulnerabilities, SSO cannot build a classical attack graph to monitor the cyber-attacks against the VIP.

SPs systems may seem protected while VNFs (MME, HSS, PDN-GW) can be under attack. Figure 60 shows the VNFs involved in the occurrence.

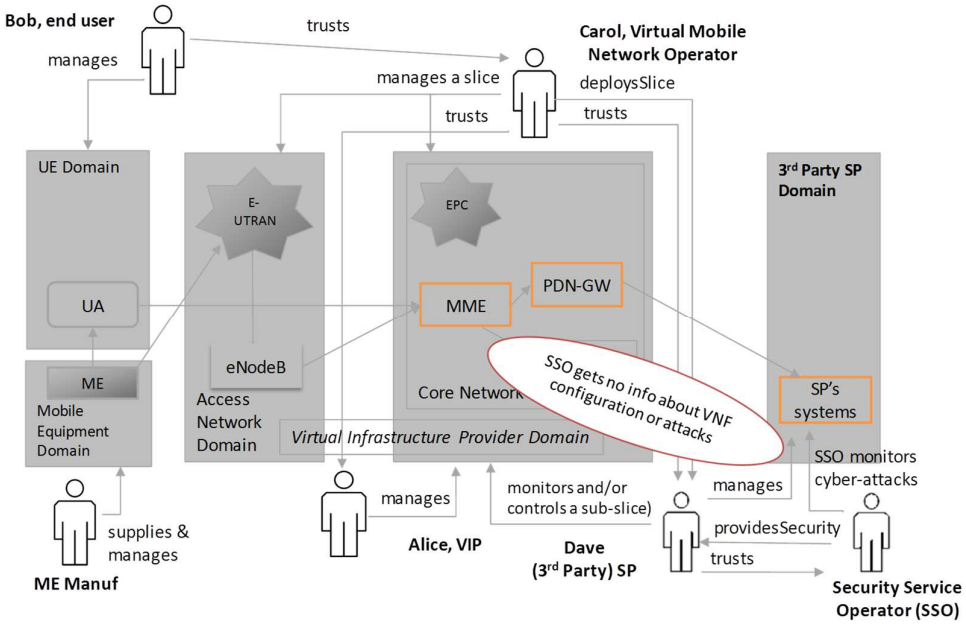

Figure 60. No control of cyber-attacks by the Service Providers (T_UC5.5_4) - 'rainy day'

Core network may get congested and SP (Dave) cannot provide the game service to end users (Bob) although SP expects SSO to resolve such cases. End users may lose communication or their communication privacy directly or as a consequence of secondary effects from these threats.

Trust implications

Potential trust implications are the following:

- Bob may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.
- If the customer's (Bob) identification or other personal data leaks to outsiders, the customers may lose their trust completely, both to SP (Dave) and to VMNO (Carol).
- When VMNO (Carol) or VIP (Alice) cannot control the VMN or VI she loses trust of some or all customers. VMNO or VIP cannot transfer responsibility of her own customers to other stakeholders.
- SP should be able to trust that VMNO's systems are not vulnerable. The service level agreement with VMNO (Carol) should cover liability of all consequences, to which VMNO's systems can be responsible.
- SP should trust that SSO can control all threats against SP's systems. When SSO cannot control VIP's system, there should be an agreement that limits SSO's responsibilities in these cases.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- A possible solution is to enable the SSO to get access to the information from the infrastructure domain, especially the type of software used to implement NFV in order to determine its vulnerabilities.

Another way to this threat is to separate the responsibilities by contract between the infrastructure domain and the VMNO. Then the SP may rely on the VMNO interface and will only control its cyber-threats at application level

B.16 Integrated Satellite and Terrestrial Systems Monitor (UC 5.6)

B.16.1 Use case description

This use case integrates the security methods used in satellite systems and terrestrial systems. Using this way, the SNO focuses on the monitoring of both system using a simple way where both security systems are accessible from the same server, using a centralized server for this task. The monitoring is done managing the alarms and events coming to the system in order to analyse the network involved. With the help of this method for monitoring combined in both systems, the issues detected in terms of security as threats can raise in a shorter period of time.

The system collects different data from events, indicators and alarms and the patterns of security threats from satellite and terrestrial systems to make a semi-automatic method of monitoring based on machine learning and the experience of past events.

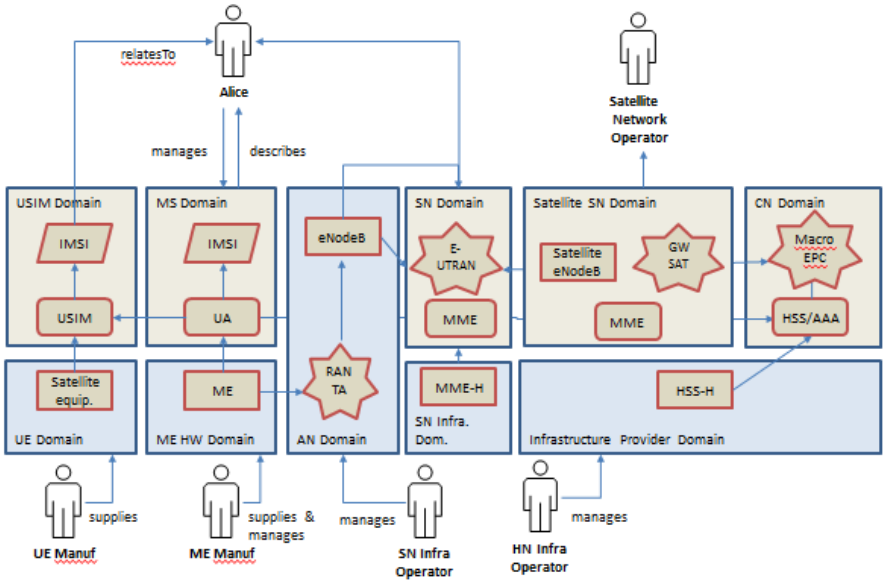

Figure 61. Integrated Satellite and Terrestrial Systems Security Monitor (UC 5.6): sunny day scenario

B.16.1.1 Security threats in a satellite network (T_UC5.6_1)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity with some QoS guarantees to be used by its customers. The service provider uses the behaviour known (in case of being a terrestrial operator) or rent this information to a terrestrial one to incorporate this knowledge and help the monitoring of satellite network under threats not known.

In this case an event never known (or not planned), i.e a threat in the satellite network occurs in the management system. A natural disaster occurs and the link communication between the satellite transmission system and the receptor antenna is cut due an obstacle placed between them. The operator cannot manage the satellite and it is vulnerable to attacks and different threats affecting to the satellite. Using a known system used in terrestrial networks as the reconfiguration of the topologies, the satellite system can learn of this and reconfigure the haze to focus in another point in order to re-establish the communication again.

Due the natural disaster nature, the public organizations and users (Alice) will re-establish the communications after some time, when the satellite's haze has been reallocated.

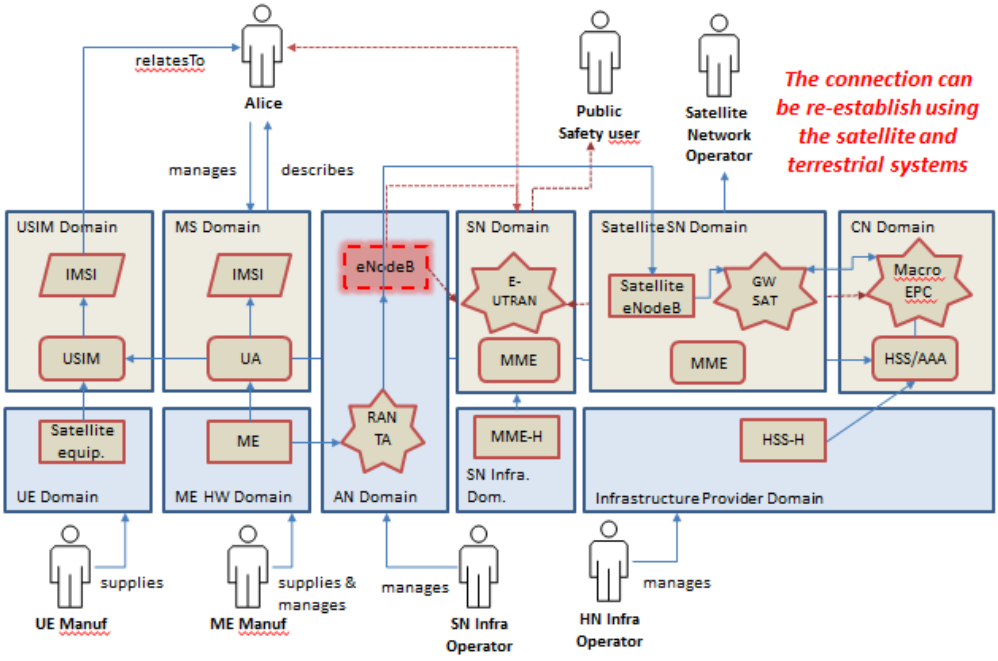

Figure 62. Re-establishing the communication, Security threats in a satellite network (T_UC5.6_1)

With the events and alarms received regarding the failure of communication, the system learns of the terrestrial monitoring system and focuses its haze to another antenna received not blocked with direct communication to the base station affected without direct contact to the satellite.

After the distribution of the signal, the affected base station receives the signal again just using a reconfiguration in the haze of the satellite to avoid the blocks due the natural disaster and the satellite operator can manage the satellite again.

Without the integrated system security monitor present, the recovery time of the service will be much higher and the human will be necessary in order to reallocate the service. Also during the time when there is no connectivity the security will leak, presenting a potential trouble in terms of security and loss of service.

Trust implications

Potential Trust Implications:

- Customer trust in the service provider or operator based on the lack of availability and the managing of facing issues under pressure.
- The service provider or operator seems not to have a plan for disasters or a system to recover the control as faster as possible based on recurrent events.
- The SLA, which can be associated to different contractual offers or contracts cannot be accomplished with the difficulties and the delay in the re-structuration of the topology network based on the threats.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Events and alarms management of real time data to control the network through network statuses and analysis.
- Establish clear action plans identifying critical elements, contentions actions and terrestrial networks as suggested in the rainy scenario can be key to mitigate the risks.
- Integrating Satellite and Terrestrial systems can be used the knowledge acquired in one or other system to mitigate threats in satellite networks. An example of this is a reallocation of the topology based on terrestrial networks.

B.17 Attach Request During Overload (UC 6.1)

B.17.1 Use case description with architectural components

This use case details a device attaching to an overloaded MNO network. This could be use to an emergency situation or simply access to the MNO network is overcapacity. Ideally all devices should be able to connect to the network without any issue, which is not always the case. The alternative is to apply quality of service (QoS) to certain device which will higher priority to connect first.

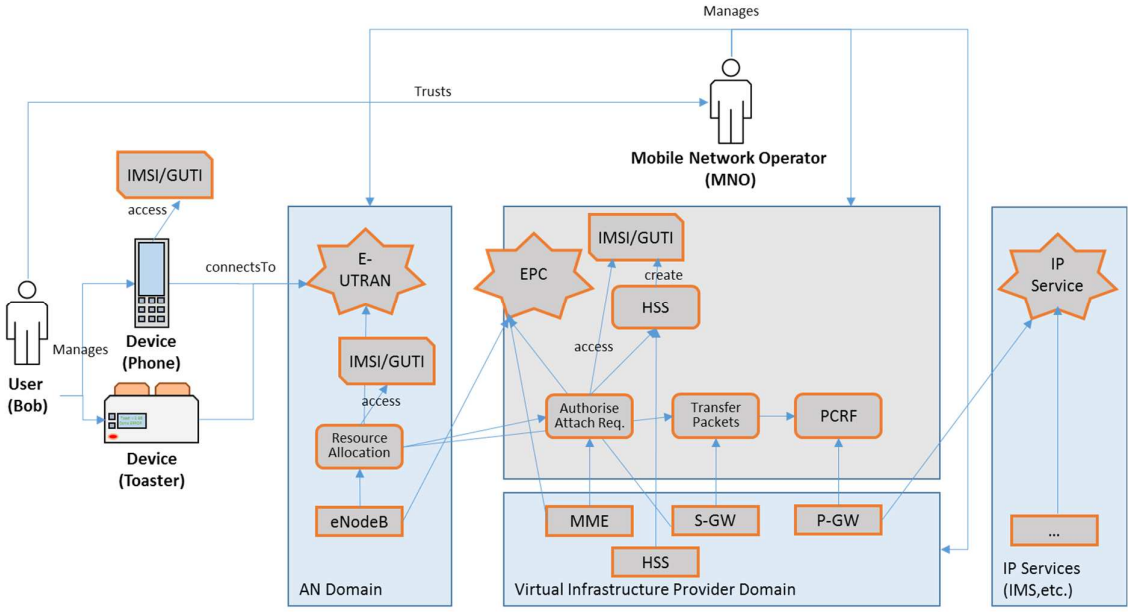

Figure 63. Attach Request during overload (UC 6.1): sunny day scenario

Figure 63 details the sunny day scenario. From left to right we see the entire sequence of how a user's device connects to the access network, and onwards to the MNO's service and out onto the wider internet. This use case is focused on the method which a device attaches to the MNO's network. When the user's device attaches it first connects to the eNodeB which will allocate resource and communicate back to the NMO's network so it can authorise the request. If all is well the user's device is authorised onto the 5G network. The MNO is in control of the eNodeB and the EPC. The end user, or subscriber, trusts that they can connect their devices to the 5G network without delay or issue.

B.17.2 Identified threats

B.17.2.1 Unable to attach when Overloaded (T_UC6.1_1)

The primary cause is a service in the path of a subscriber's device is overloaded resulting in the device being unable to connect to the MNO network. It may not involve a malicious attacker, but simply be down to high demand or inefficient design. This can threat can happen in more than one location, as shown in the figure below.

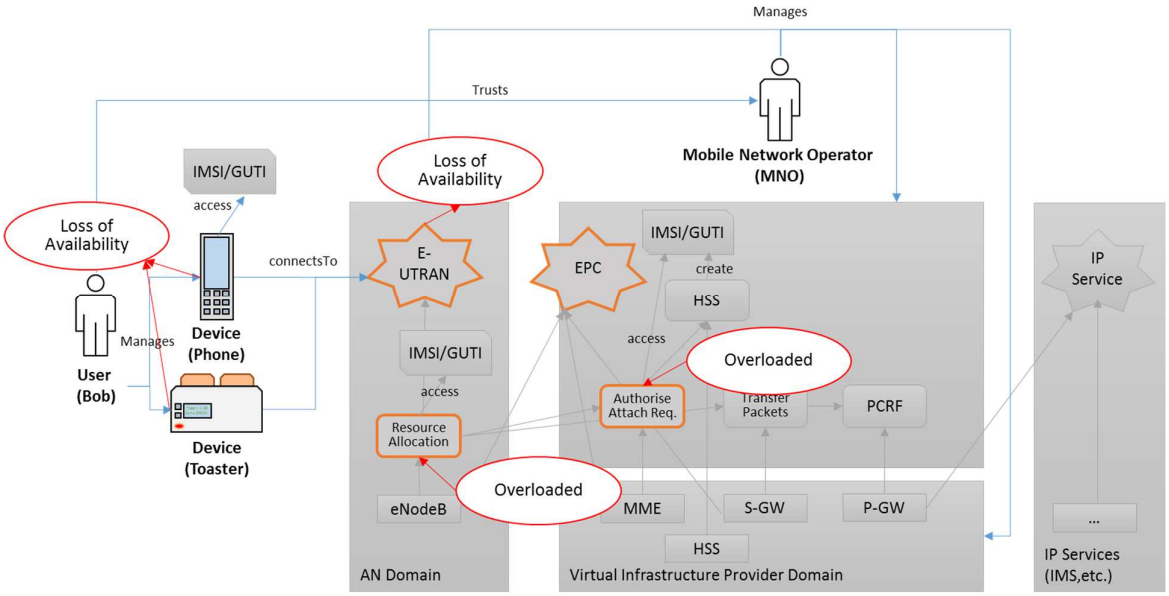

Figure 64. Unable to attach when overloaded (T_UC6.1_1) – 'rainy day'

As mentioned above it is possible that this attack could occur in multiple locations. The first being in the eNodeB, access network. If the eNodeB consumes too much resources it will be unable to accept new or existing refresh connections, due to being overloaded. The second location this risk could arise could be within the MNO network. If the MNO is unable to authorise a new device connecting to the network via the eNodeB then again the user's device will be unable to attach.

If there are multiple eNodeB's in a mesh styled formation, then when one becomes overloaded it will cause extra demand to on the others resulting in that device to become overloaded as well. Also, once the eNodeB becomes available again, it may cause devices which were attempting to attach one at a time to simultaneously attach. Resulting in an increased load on the MNO services, which could cause it to become overloaded.

Trust implications

The first implication is clearly between the user, Bob, and the MNO. Bob has expectations that the service he is paying for will reliably be available. If he is unable to attach to the network then he will lose trust in the service. If the eNodeB is provided by a MNO, and is used by a virtual MNO and the eNodeB becomes unavailable then the VMNO will lose trust in the MNO.

Threat mitigation strategy

A possible mitigation strategy is could be to enforce quality of service (QoS) and limiting access to the MNO or the eNodeB it would be possible to prevent overloading of the systems. It would be performed by the owner of the access network, which might be the VIP or MNO and in some cased the VMNO. Alternative mitigation methods would be to save resources by rejecting illegitimate or non-prioritised requests at an earlier stage that is done now. Another method would be to give priority to reconnecting devices to prevent them from becoming out of sync and allowing the attack to succeed. Again this are will be performed and located in the access network.

B.18 Unprotected User Plane on Radio Interface (UC 6.2)

B.18.1 Use case description with architectural components

This use case details issues which may arise from having insignificant protection of the user data plane. The signalling data between the UR and the network is protected via integrity validation. Though in in order to conserve battery power on the device, by minimising the signalling, it introduces a vulnerability in that the data plane lacks protection from both encryption and integrity.

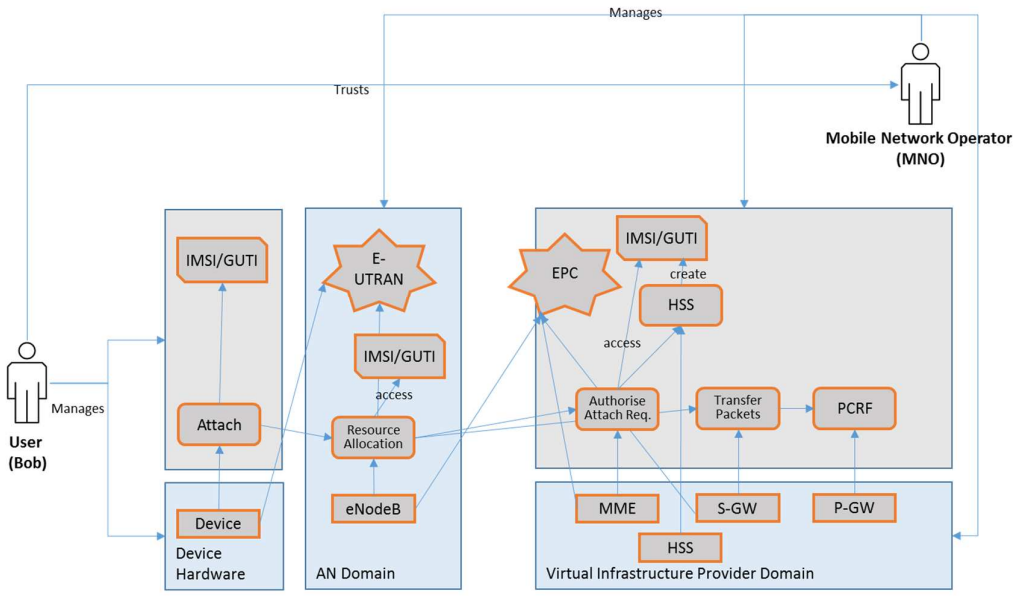

Figure 65. Unprotected User Plane on Radio Interface (UC 6.2): sunny day scenario

The sunny day scenario shows a user, Bob, attaching his device to the mobile network operator's network via the access network. The device communicates with the eNodeB, where it negotiates what resources are to be allocated to it. This is done via the signalling protocols which in this scenario are integrity protected. Which means there is no way for an attacker to interfere with negotiations between the device and the eNodeB. Once the resources have been allocated by the eNodeB, the drive can complete the attach request with the operator. Again, this communication between eNodeB and MNO are integrity protected. From this

we can infer that the device owner trusts the network operator to enforce integrity of the signalling channel to maintain a secure connection.

B.18.2 Identified threats

B.18.2.1 Unprotected User Plane on Radio Interface (T_UC6.2_1)

Due to an attempt to conserve battery power of the device connecting to the network, the amount of signalling traffic is reduced. Which leaves an authenticated channel open to attackers. This results in the network being unable to verify the authenticity of data from the user plane. This is where Malory is able to intercept user data passing between the Device and the eNodeB. Providing they have the equipment, such as a software defined radio and are in a suitable physical location to target the user's device. They are able to exploit the fact that neither the device nor the eNodeB verify the data it receives.

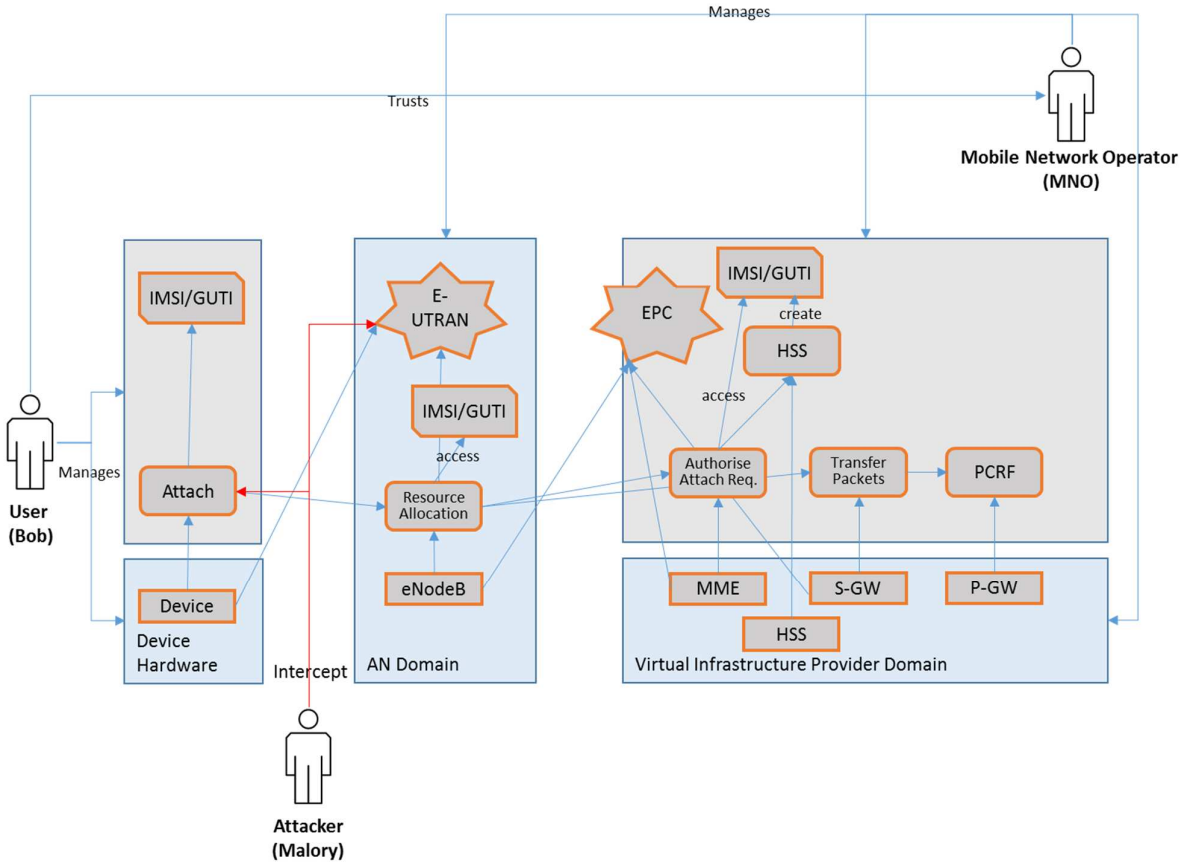

Figure 66. Unprotected User Plane on Radio Interface (T_UC6.2_1) – 'rainy day'

Secondary effects of this threat is any data passing through the network can be intercepted, modified, and replayed. If traffic is intercepted then the threat is the privacy of the content is affected. This could result in espionage or divulging of classified information. If traffic is modified this would undermine the trust a user has with the network. It would also allow an attacker to control any system which may use the network. Replaying traffic which has been previously captured could allow an attacker access to parts of the network allowed for specific users, such as administrators or restricted accounts.

Trust implications

The User of the device trusts the MNO to operate a network which is not vulnerable to this kind of threat. If this is not possible then the user should attempt to use end to end encryption, which would place the trust on the sender and receiver of the communications. The user data plane is not encrypted because of regulations see TS33.401. The network operators may transfer responsibility of this risk over to the regulators under which they are bound by law to obey.

Threat mitigation strategy

To mitigate the threat in its entirety, the network operators will should implement similar protections for the traffic as they do for the signalling plane. This is, to force integrity checking on packets to insure that they originate from the user's device and not the attacker imposing as the user. This control would be placed on the eNodeB, at the access network. If that is not possible due to resource, then it could be placed on the edge of the EPC network provided by the MNO.

To mitigate data between two users being compromised from this threat, it is possible to use end to end encryption. This force all communication between the users to be encrypted in transport and only decrypted at the destination. This would be suitable for certain types of users, it would allow for the network operators to still obey the regulations they are restricted by.

B.19 Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1)

B.19.1 Use case description with architectural components

This use case describes a subscriber's device, phone or sensor, attaching to the 5G network. I details the method which a device connects and how it can be subverted by an attacker, and the device will fail to attach as expected.

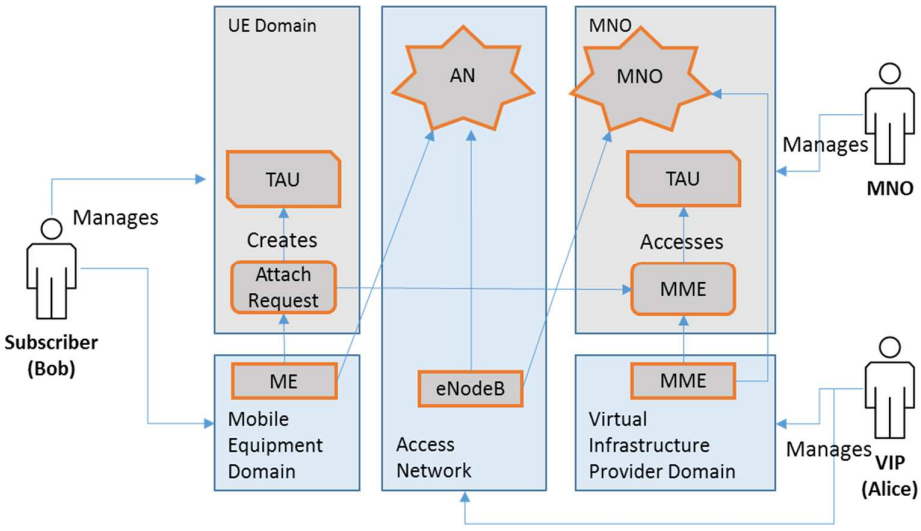

Figure 67. Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1): sunny day scenario

From right to left, we have the mobile network operator (MNO) and virtual infrastructure provider (VIP). The VIP manages the access network and the infrastructure for the MNO. The MNO manages their internal network and provisions access to it for the subscriber, Bob. When the subscriber wishes to attach to the MNO, their device (UE) will send an attach request. Once connected the UE will send periodic tacking area

updates (TAU) to the MME, via the eNodeB. The subscriber is required to trust that the VIP will deliver their requests unaltered and without a reasonable amount of delay. Likewise, the MNO trusts the VIP is also relaying their communications to subscriber. The subscriber may not be aware of the existence of the VIP, but only the MNO, as that is who they have come to an agreement with. The MNO must trust the VIP will provide them with secure and robust infrastructure. The security implications of this configuration are the eNodeB and subscriber. Since by their nature have a large exposure to public access, and are both designed to work under emergency conditions. These conditions might require foregoing security measures to maintain resilience and availability. For example, if there was a failure of the encryption module in the eNodeB, unless it falls back to unencrypted methods, subscribers might not be able to communicate in an emergency.

B.19.2 Identified threats

B.19.2.1 Denial of service due to Unprotected Mobility Management Exposes Network (T_UC7.1_1)

The threat is from a malicious attacker, in Figure 68 they are shown as Mallory. The root cause is due to the eNodeB being over powered with a stronger signal and the subscriber connecting to the Mallory service instead. Mallory intercepts the tracking area updates being sent from Bob to the MNO's MME. The intercepted TAU is modified before being relayed onto its original destination, the MME. The attacker can modify it so as to make the subscriber's device believe that the MME does not support certain services, and will downgrade to a service which Mallory wants.

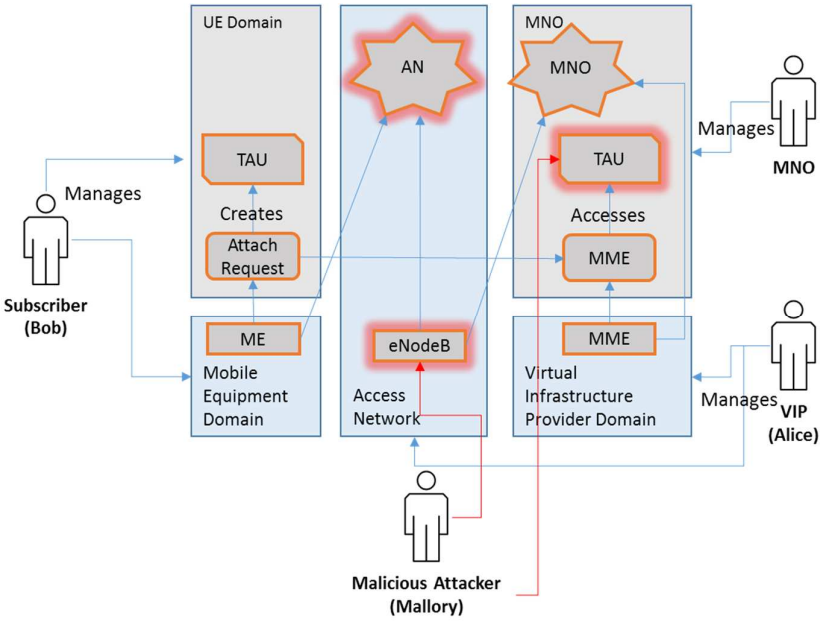

Figure 68. Denial of service due to Unprotected Mobility Management Exposes Network (T_UC7.1_1) – 'rainy day'

The eNodeB is directly involved, as the attacker is able to convince the subscriber to connect by impersonating the eNodeB. This allows for Mallory to compromise communication between them and the MNO. Mallory would be able to perform not only a DoS for the subscriber but also intercept communications between them. By forcing Bob to communicate over an insecure method, using the same method as the DoS, Mallory would be able to eavesdrop on Bob's communication with the MNO.

Trust implications

- The MNO trusts that the VIP will secure their equipment and detect any anomalous changes which might happen, such as the rouge eNodeB attack.
- The Subscriber trusts that the MNO will not allow and will actively prevent his communications from being intercepted. If this loss of trust occurs then it could result in a complete loss of trust with the MNO.

B.20 Satellite Network Monitoring (UC 8.1)

B.20.1 Use case description with architectural components

The SNO mainly focus on tasks related to network monitoring and issues detection, are visualizing the satellite terminals status and throughput associated to network and spectrum resource utilization. Other network operators responsible are making the same work in different slices and sub-slices as Figure 69 represents.

The SNO systems collecting different data indicator as network patterns use, authentication exchange schemes, to detect and mitigate the possible threats blocking the traffic or access at application layer for an Authentication Server with sensible information content.

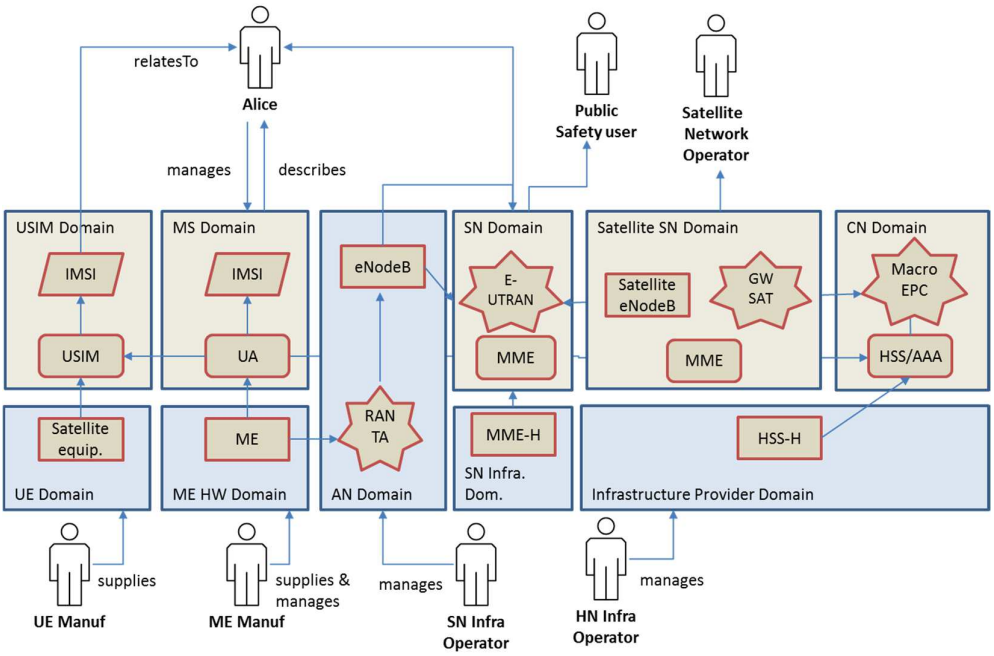

Figure 69. Use case title (UC 8.1): sunny day scenario

B.20.2 Identified threats

B.20.2.1 Service failure over satellite capable eNB (T_UC8.1_1)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity with some QoS guarantees to be used by its customers. Therefore, the Service Provider has to ensure that the SatNO is providing what is required by the contract (SLA).

This threat is particularly acute in ultra-reliable services (i.e. e-health, lifeline communications, and military scenarios).

In this case a natural disaster occurs and connection between Alice and eNodeB is lost, the network manager detects the failure event and proceed to performs topology calculation to guarantee ultra-reliable services. The new topology is configuration is populate across the network elements and the satellite-capable eNB activates the alternative route to Macro EPC via the satellite link. As a result the service lost is minimized and service restore is achieved.

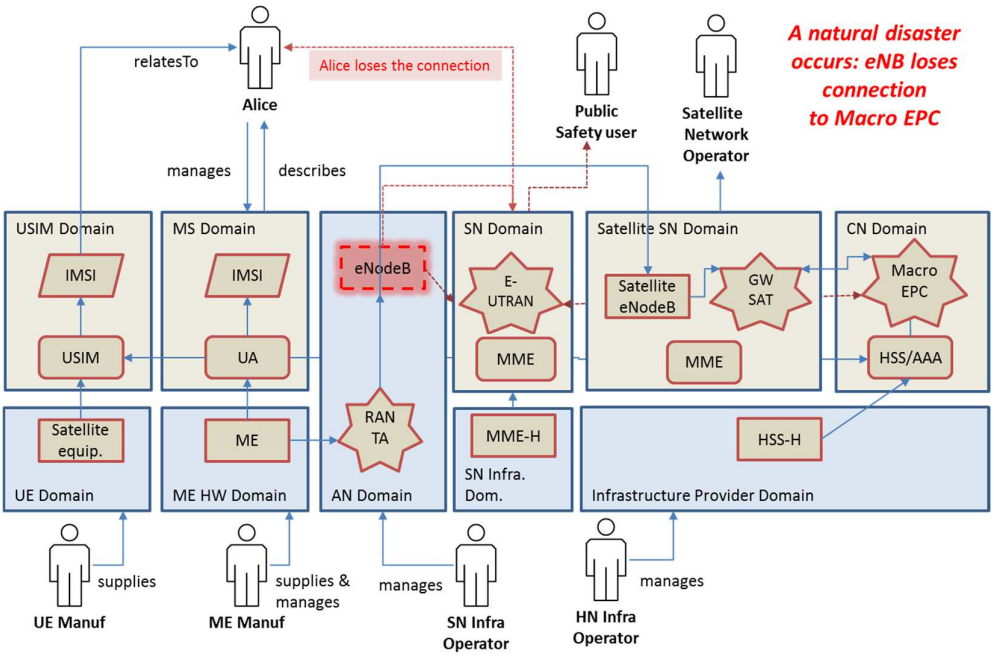

Figure 70. Service failure over satellite capable eNB (T_UC8.1_1) – 'rainy day'

Main domains involved in this actions are shown in the Figure 70, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite connections capabilities to the network increasing the recovery time and decreasing the service lost.

Without the mechanisms present, service lost time will be increasing, reliability of the system is decrease and mitigations actions are limited, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a lack of trust based on the network availability and the capabilities for the VMNO to guarantee their service level agreements.
- The VMNO needs to demonstrate a trustable recovery actions regarding to guarantee the control over the VNO, offering detailed action plans that cover typical operations issues in sensible highly exposed locations.
- In this use case, the threat is not specially focus in an insider attack, but can be extrapolate from a service unavailability in the eNodeB as root case, actions and actor can be implemented in the same way from a trust implications perspective.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Real time data gathering about network status and trends analysis can supply the foundations to accurate service lost detection.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.

Generate pre-emptive configuration policies across the elements can decrease the reaction time and automatize the network recovery process, decreasing the SNO / VMNO actions and dependencies.

B.21 Standalone EPC (UC 8.2)

B.21.1 Use case description with architectural components

This use case concerns standalone-capable eNBs that have the capability of standalone mode of operation, which provides commercial local IP connectivity to the UEs via a Standalone EPC. This is assumed to be a commercial service, and connection to the Macro EPC is still possible.

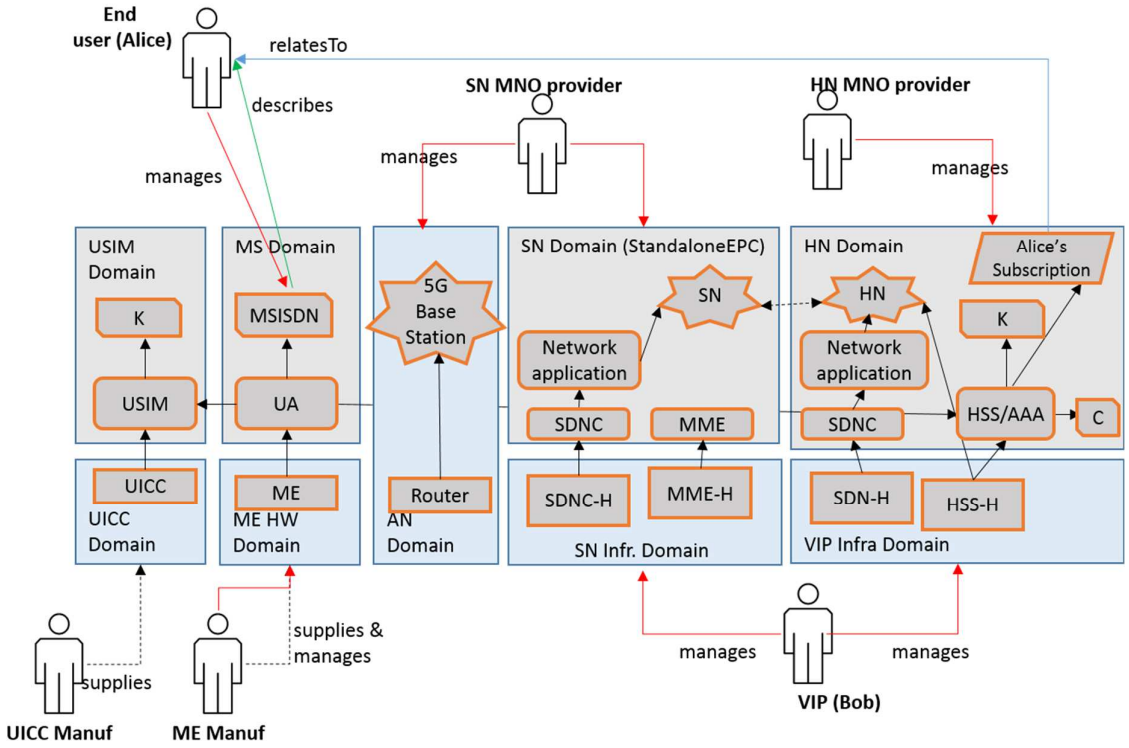

Figure 71. Standalone EPC (UC 8.2): sunny day scenario

Figure 71 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). Alice is in a mega event with 100.000 other people. She wants to use the services that are available in the standalone EPC. When the mega event starts, the standalone-capable eNB starts to broadcast support of the ad-hoc roaming mode to the local EPC. Alice's phone attaches to the standalone-capable eNB of the standalone EPC. The standalone EPC authenticates Alice's USIM with the help of the HN. Alice's HN authorizes the ad-hoc roaming to the standalone EPC by sending Alice's subscription profile to standalone EPC. Alice's phone does not lose the connection to the HN as the standalone EPC provides also connectivity to the HN. Alice uses the services in the standalone EPC, and also uses the services in the HN.

B.21.2 Identified threats

B.21.2.1 Standalone EPC loses connection to the Home Network (T_UC8.2_1)

The standalone-EPC-capable eNodeB fails to communicate to the subscriber's home network. This can be caused in a variety of ways, denial of service, system/hardware failure, or due to overloaded resources. By its nature this threat is can be exploited by a malicious attacker or an unintentional series of events. The crux of the threat is that some way the connection from the eNodeB to the Home Network will be disrupted, resulting in clients being unable to authenticate.

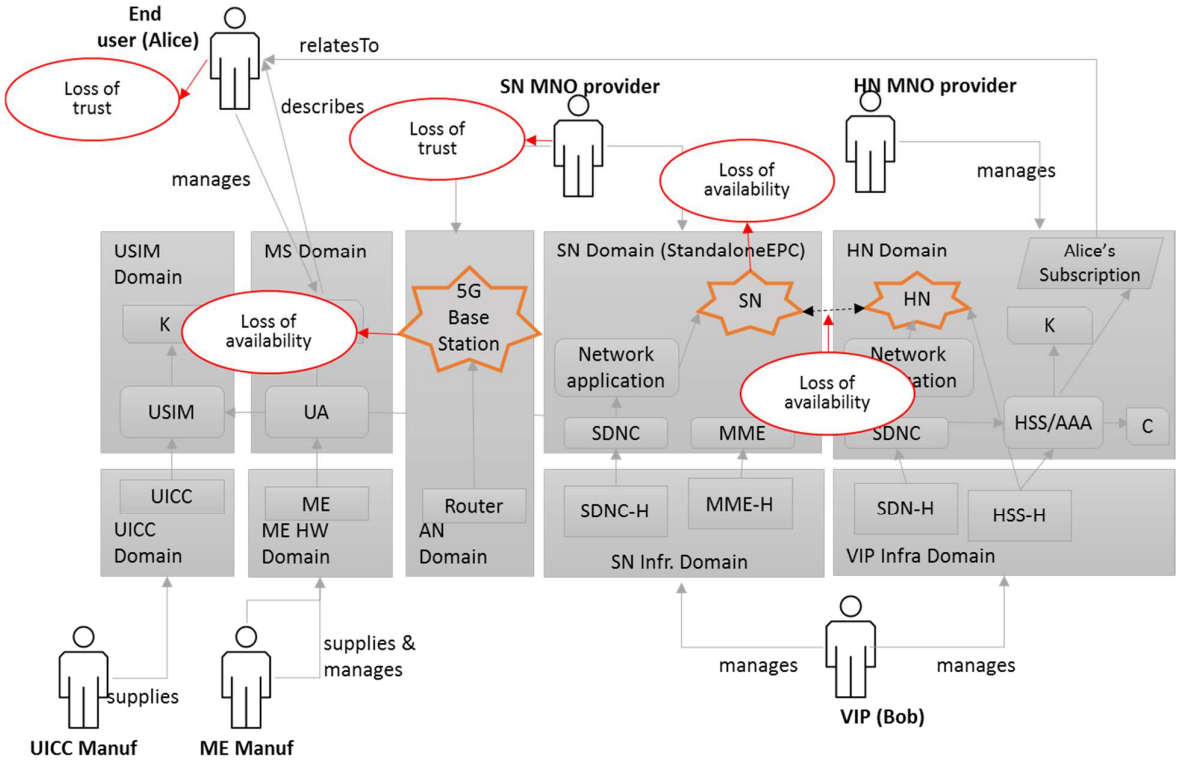

Figure 72. Standalone EPC loses connection to the Home Network (T_UC8.2_1) – 'rainy day'

The threat is the loss of connectivity between the serving network and the home network, this could be caused maliciously, or by a misconfiguration. Typically it would be caused by an overload in capacity of the hardware used to communicate with the HN. In this case the standalone EPC.

Secondary effects are such that devices looking to authenticate with the network are denied authentication and will be unable to communicate with any other devices, unless it is possible to communicate with their peers. With the eNodeB unable to communicate with the Home Network, it prevents other clients, which might not be using the isolated EPC service, from working.

Trust implications

Potential Trust Implications:

- The end users of the network, will loss trust with their VMNO, who is meant to provide them with access to the EPC. This is also not limited to a single virtual mobile network operator, due the physical eNodeB being unavailable.

- The HN MNO will lose trust with the SN MNO, since they are the ones who are maintaining the eNodeB. And are bound by contract to allow other operator's customers to use their equipment.

Since the eNodeB is shared by range of operators and the use of which is provisioned by a virtual infrastructure provider (VIP), when the eNodeB is unavailable there.

B.22 Alternative Roaming in 5G (UC 9.1)

B.22.1 Use case description with architectural components

Legacy mobile networks (GSM, UMTS, LTE) use an interconnect network based on SS7 or Diameter. In such an interconnect network, network entities often rely on the assumption that the traffic originating from a certain network is authentic, without having any way of checking this assumption. Unfortunately, this assumption is not always true in today's heterogeneous landscape of networks. This has led to a variety of attacks on the interconnect network based on spoofing of messages. In this use case, messages are instead bound to the correct entities, so that spoofing cannot take place.

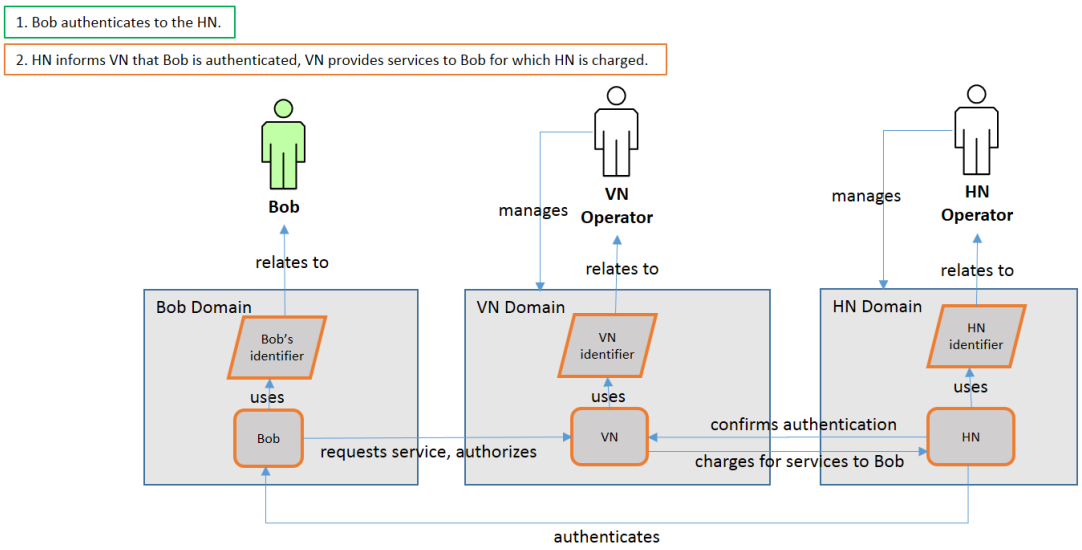

Figure 73. Alternative Roaming in 5G (UC 9.1): sunny day scenario

Figure 73 describes the use case in relation to the architecture, in the absence of any threat (sunny day scenario). The home network and the visited network have a roaming agreement. Bob needs the assistance of the home AAA infrastructure to authenticate himself to the visited network. The Home AAA issues the authentication challenge. This process also identifies both the visited network and the home network, so that the involved parties are identified. During this process, Bob also authorizes the visited network to provide services to him.

At the same time, accounting mechanisms are set up. The home network can therefore have assurance that any billing related information is tied to Bob. Thus, the visited network cannot make false claims. Similarly, Bob's false claims can be denied based on assured accounting information. Bob's device is involved in the process, so that there is transparency of the incurred costs to Bob as well.

B.22.2 Identified threats

B.22.2.1 Spoofed signalling messages (T_UC9.1_1)

If the authenticity of the messages related to the user cannot be verified, the integrity of the actions cannot be ensured. The actions can cause effects which lead to further compromises or have other unwanted consequences.

In Figure 74, the threat is explained in relation to the architecture. Mallory impersonates the visited network and takes actions that were not authorized by the user. This could relate to billing (customer gets extra charges that were not caused by them) or it could cause messages (such as SMS) redirected to somewhere else (potentially leaking information). Alternatively, Mallory could spoof management messages which change the infrastructure, potentially in a devastating way. There are different ways how Mallory could impersonate the visited network: insider attacks, hacking into the visited network's interconnect access, or simply by buying access to the interconnect from a network provider.

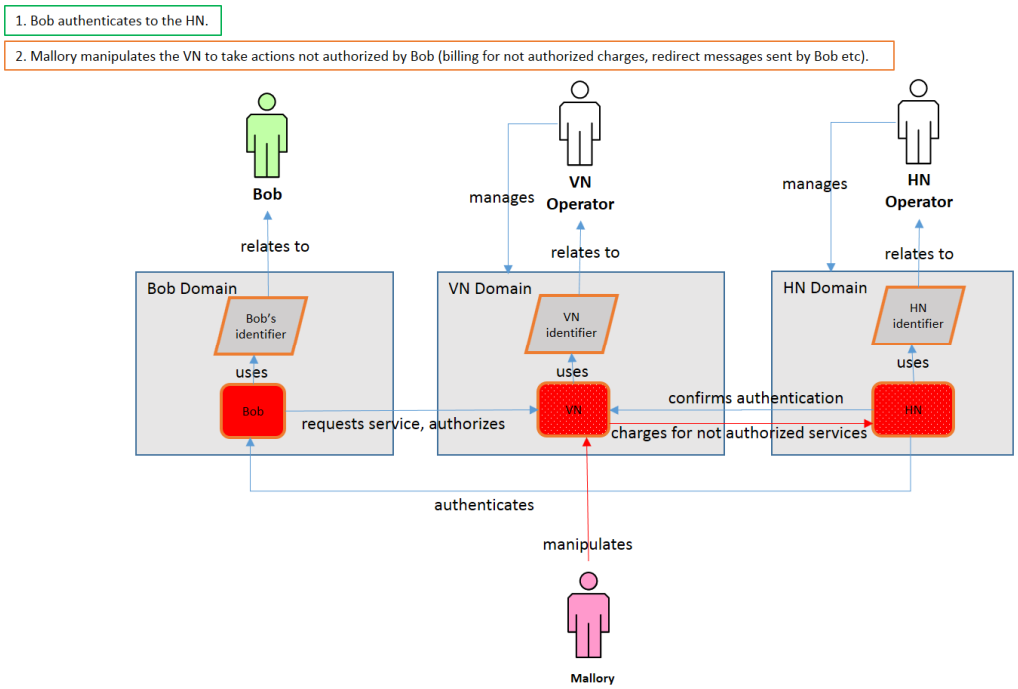

Figure 74. Spoofed signalling messages (T_UC9.1_1) – 'rainy day'

Trust implications

This threat is based on an outdated trust model between network operators. As said in the description of the use case (Use Case 9.1), in today's heterogeneous landscape of network operators the authenticity of a message cannot be guaranteed even if it originates from a trusted roaming partner, because not all trusted roaming partners may be trustworthy.

Besides mutual trust between network operators, the threat has strong implications on the trust of users to network operators in general and especially their home network operator. The user has no way to prevent non-authorized actions on their behalf, such as intercepting messages sent to the user, impersonating the user and originating charging records on behalf of the user.

Threat mitigation strategy

All signalling messages should be integrity protected and bound to the correct entities. Using cryptographic identities for all entities (networks and users) would be one possible solution. Additionally, authorization methods need to be in place, both from the entity that sends the message but also from the entity that receives the message and needs to ensure that the sender is authorized to perform a certain action.

B.22.2.2 Disputes in charging (T_UC9.1_2)

This threat is a special case of T_UC9.1_1 above. A user could dispute charges or an attacker on behalf of an operator could place unfounded charges on the user actions. Basically, an attacker impersonating the operator can produce billing records, but the customer has no way of proving whether they are correct or not.

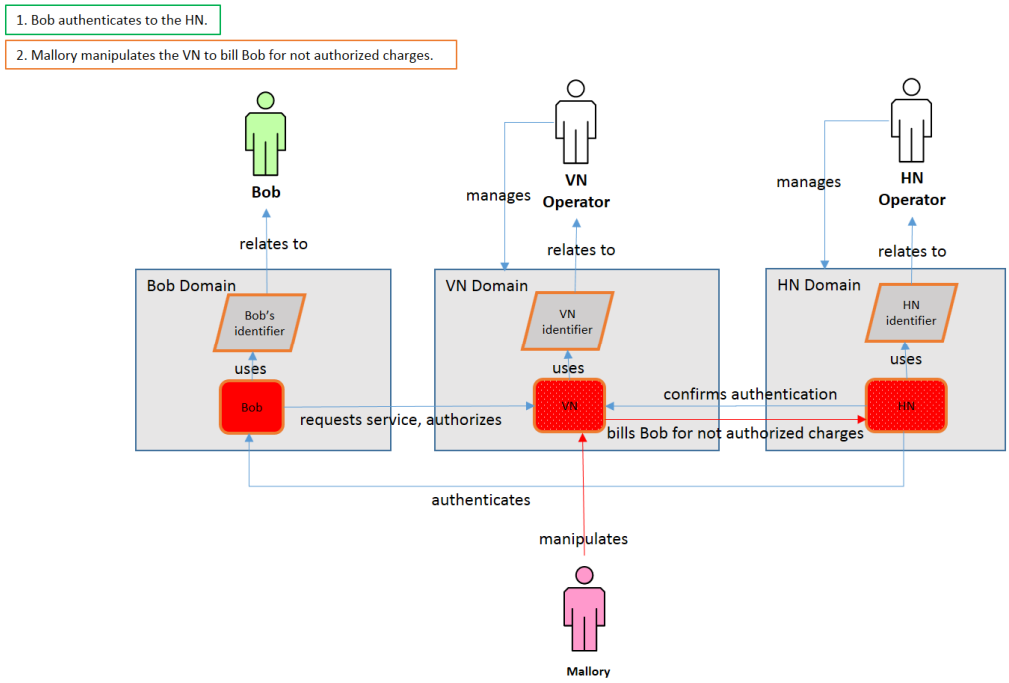

Figure 75. Disputes in charging (T_UC9.1_2) – 'rainy day'

In Figure 75, the threat is explained in relation to the architecture. Mallory impersonates the visited network and creates charging records not authorized by the user. As explained for the T_UC9.1_1 above, there are different ways for Mallory to impersonate the visited network.

Trust implications

This threat has mostly implications on the trust between user and home network operator. Users have no way to prove they have not originated the charging records, and the network has no way to check whether the user has originated the charging records.

Furthermore, this threat also has implications on the trust between network operators. A home network may realize that a trusted roaming partner was indeed not trustworthy.

Threat mitigation strategy

The charging related messages should have non-repudiation properties. Cryptographic identities could be one possible approach of creating records that are always strongly bound to the entity and cannot be disputed afterwards.

B.22.2.3 Disclose of sensitive data (T_UC9.1_3)

A request for sensitive information (such as authorization vectors) may come from non-trustworthy sources although they are received through a trusted channel. Obtaining sensitive information in unauthorized fashion could lead to further compromise of the network and possibly make it easier to spoof other entities.

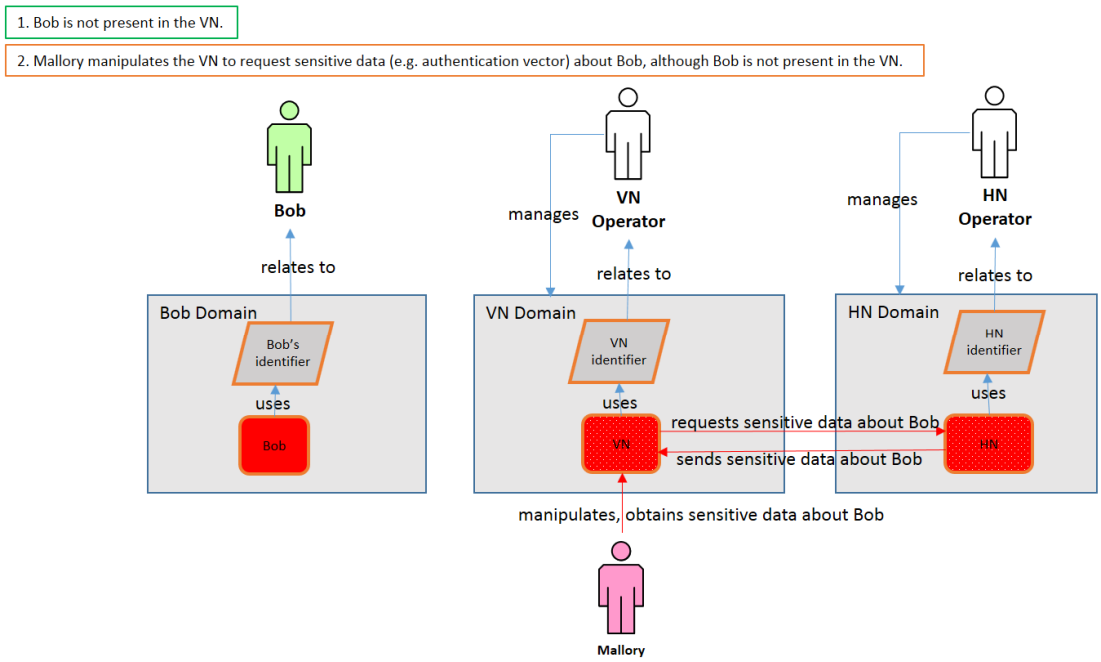

Figure 76. Disclose of sensitive data (T_UC9.1_3) – 'rainy day'

In Figure 76, the threat is explained in relation to the architecture. Mallory impersonates the visited network and manipulates the visited network to request sensitive data (e.g. authorization vectors) about Bob from the home network. Bob is not present in the visited network. Nevertheless, the home network sends the sensitive data to the visited network, and hence Mallory is able to obtain the sensitive data about Bob.

Trust implications

Similar as for the T_UC9.1_1 and T_UC9.1_2 above, this threat has implications for the mutual trust between operators as well as for the trust of users towards their home network operator and network operators in general.

Threat mitigation strategy

Similar as for the T_UC9.1_1 and T_UC9.1_2 above, the mitigation strategy should focus on providing authentication and authorization to the interconnect network.

B.23 Privacy in Context-Aware Services (UC 9.2)

B.23.1 Use case description with architectural components

The use case concerns the exchange of user context with third parties. User context can be used to provide enriched services to the user or otherwise communicate about his or her characteristics for the sake of network management in terms of flow semantics. This could especially take place in a roaming scenario, where the visited network and home network exchange information about the user. The user still needs to be in control of this disclosure of information so that the privacy of the user is not violated. Therefore, the users should be able to dictate the privacy policies to which they are willing to agree.

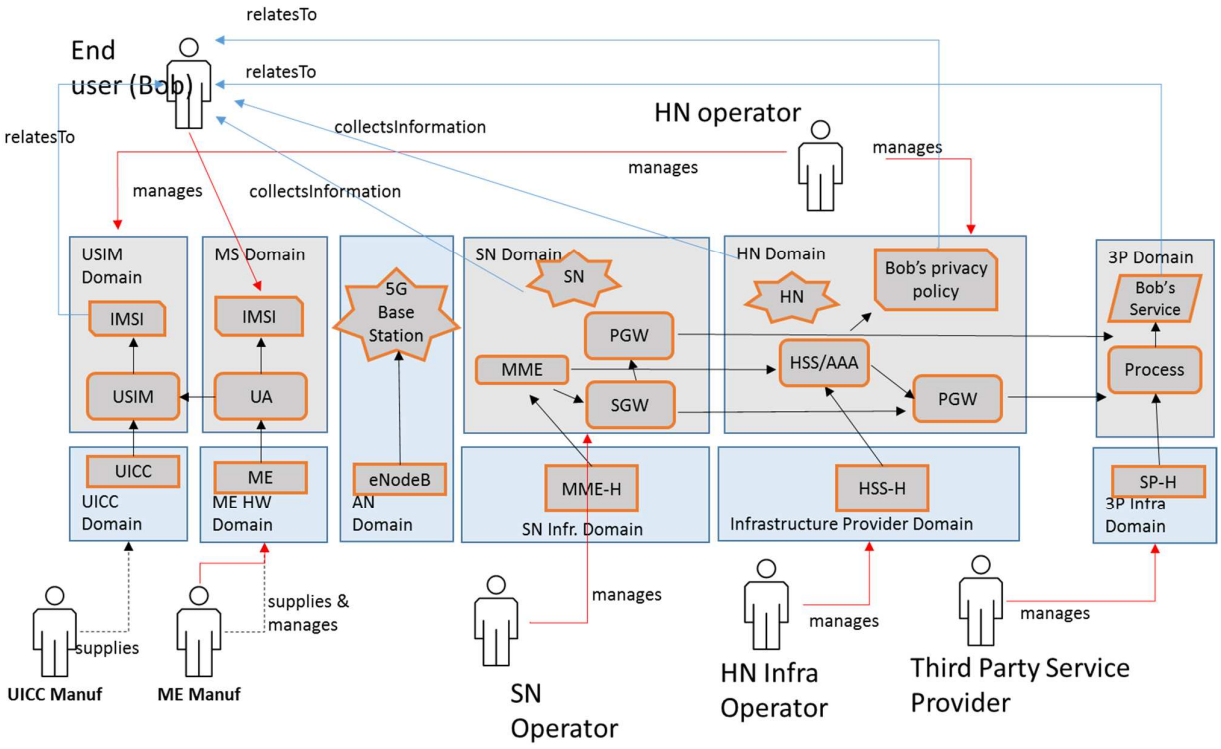

Figure 77. Privacy in Context-Aware Services (UC 9.2): sunny day scenario

In the simplest case the exchange of flow semantics information takes place within the network or between the visited and home network to communicate about the user context. This information generally does not need to reach service providers. A more evolved use case is the case where user context information (in terms of network perspective) is disclosed to an external service provider in order to provide better user experience or evolved services. This disclosure takes place according to the privacy policies the user has defined. This could also be predefined by the home operator, but the user has to explicitly agree to it. The user trusts that the home operator does not violate these policies. In addition, the user expects that the home operator has appropriate filtering mechanisms in place to ensure that no network internal information is not disclosed accidentally (e.g., header enrichment mechanisms used between the visited and home operator). The previous also has to apply to visited networks that provide local breakout, i.e., data to third parties does not traverse via home network.

Note that the application level end-to-end communication can be encrypted, so the operator cannot provide any added value to the context, at least not in-band. This is not in the scope of this use case.

B.23.2 Identified threats

B.23.2.1 User privacy policies are not respected (T_UC9.2_1)

Privacy of the user in this use case can be endangered by the operator that does not respect the privacy policy of the user. This could relate to business decision (e.g., contracts with third party advertisers) or be just lack of proper filtering (e.g., misconfiguration of egress filtering).

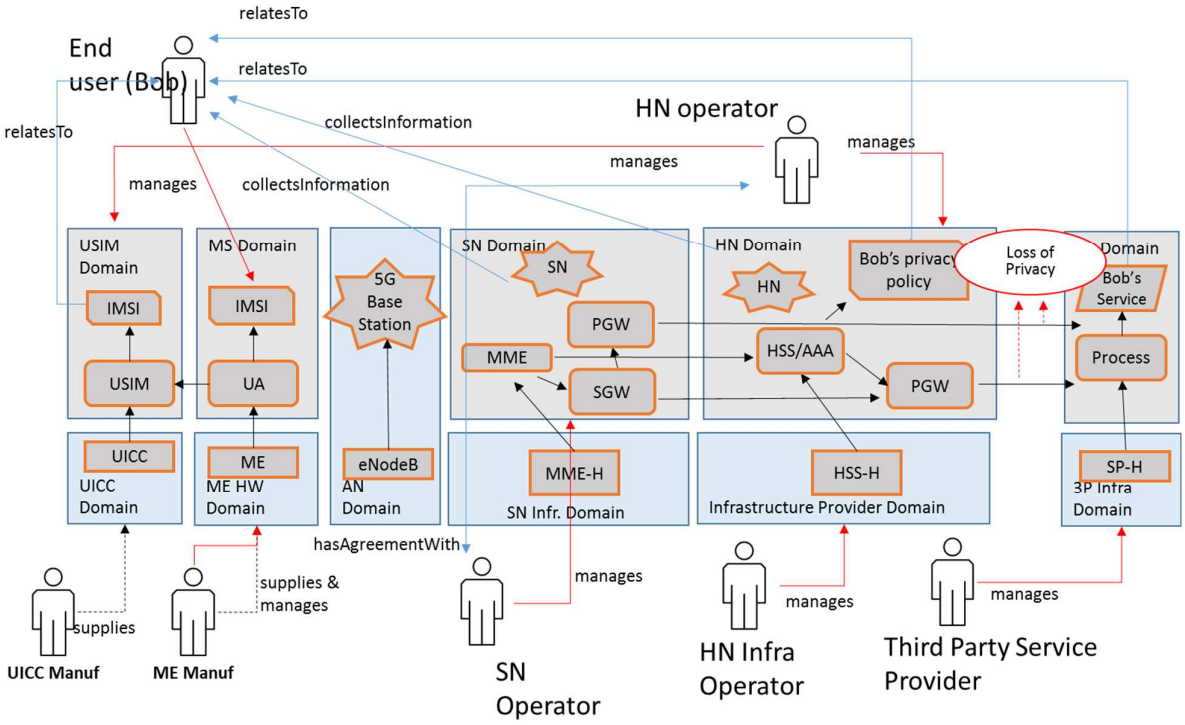

Figure 78. User privacy policies are not respected (T_UC9.2_1) – 'rainy day'

The figure above describes the issue in terms of architectural components. While the egress components in the final 5G architecture might be termed differently, they most likely will be called gateways (e.g., BGW as currently). If they do not filter the traffic properly, privacy breach is possible. Naturally, it could be that those components intentionally do not do filtering or add additional context information to the flow of information to serve the interests of third party partners, with whom the operator might have a business agreement. This might not serve the interests of the user.

It is also possible that the third party service provider further discloses information about the user. However, the service in question ought to in any case have a separate privacy policy for dealing with the user and that is outside the scope of 5G system.

Trust implications

The outcome of above could be that the overall trust of the user to the 5G system or to the operator very least decreases. Naturally, there could be legal (and therefore societal) implications if it is found out that the privacy related information is disclosed in violation of the user's privacy policy. Another thing is if the user has agreed to too relaxed privacy policy, often inadvertently. Regulatory schemes might expect certain basic level of user protection to be in place, though.

In the use case the user trusts that the privacy policy is honoured. As the user has an agreement with the home operator, he or she expects that the home operator takes care of this. On the other hand, if visited network can do local breakout in the roaming scenario, then the home operator expects that the user's privacy policies are still followed. In other words, home operator places certain amount of trust to the visited operator. It is worth noting that the user generally does not have an agreement with the visited network (unless some dynamic roaming agreement mechanisms are introduced as suggested in the alternative roaming use case).

Breach of this trust can take place if the home or visited network does not adhere to these policies. It can either happen inadvertently or on purpose. It is also worth noting that the home and visited operators could be operating under different privacy legislation.

Threat mitigation strategy

As the network originated context information can be collected by the network, the user can do very little to mitigate the threat, i.e., the operators control the way infrastructure works. If the home operator cannot trust the visited operator to employ sufficient privacy protection, then local breakout should not be allowed. Regulatory schemes can be used to protect the user in these cases. For ensuring that regulatory controls are followed, external audit of the system could be used.

For improving the transparency of privacy policies to the users the 5G enabler "Privacy policy analysis" could be used. This could help users better understand what sort of privacy policies the operator offers and whether that matches their needs.

B.24 Authentication of new network elements (UC 9.3)

B.24.1 Use case description with architectural elements

The use case deals with cases where it is possible to install new elements into the network. This could be logical components, such as virtual network functions, or physical devices. These components need to be authentic so that rogue elements are not introduced into the network.

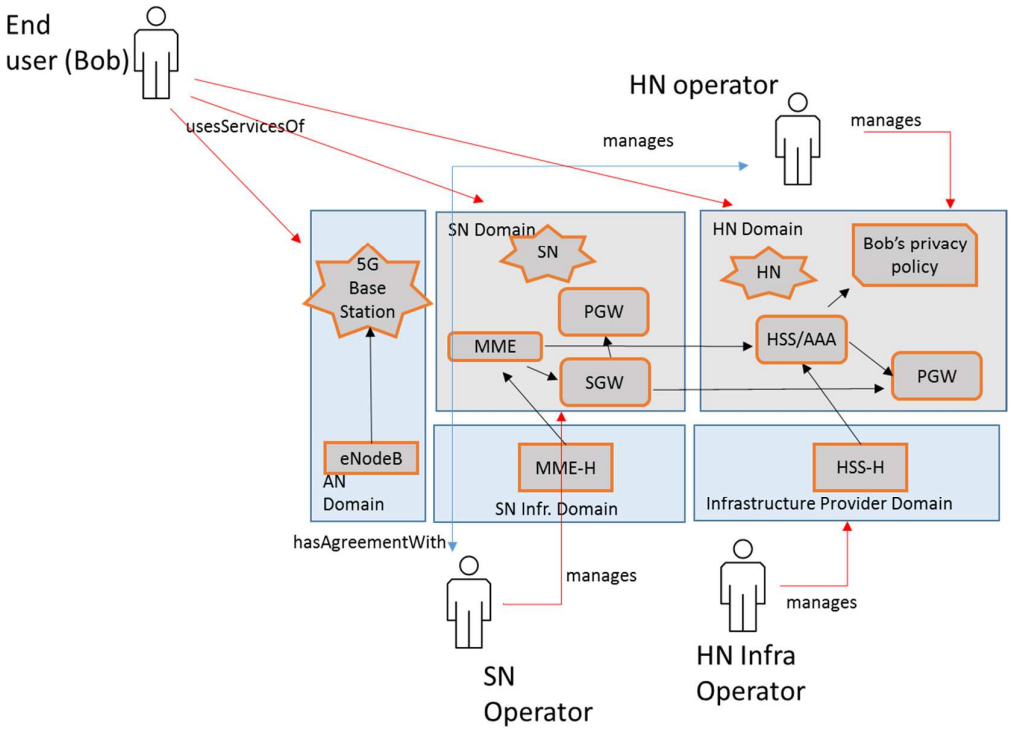

Figure 79. Authentication of new network elements (UC 9.3): sunny day

In the "sunny day" scenario the installation of new network elements can be made only by authorized parties and with guarantees that these new elements cannot endanger the integrity of the network or network flows. In other words, they cannot compromise other elements in the same network or inject traffic that could be considered authentic by other entities. In essence, it is not possible to spoof other elements or other users.

B.24.2 Identified threats

B.24.2.1 Hardening or patching of systems is not done (T_UC9.3_1)

If the systems in the networks are not hardened sufficiently or do not contain the latest security patches, it is possible that they can be compromised. This could lead to installation of new functionality, which performs malicious actions in the network, or the current functionality could be subverted to perform undesirable results. Especially in the 5G environment it is envisaged that it is possible to install new virtual network functions to enhance the working of the network. This could be especially detrimental if this can be done in unauthentic fashion (e.g., due to misconfiguration or a vulnerability in the system).

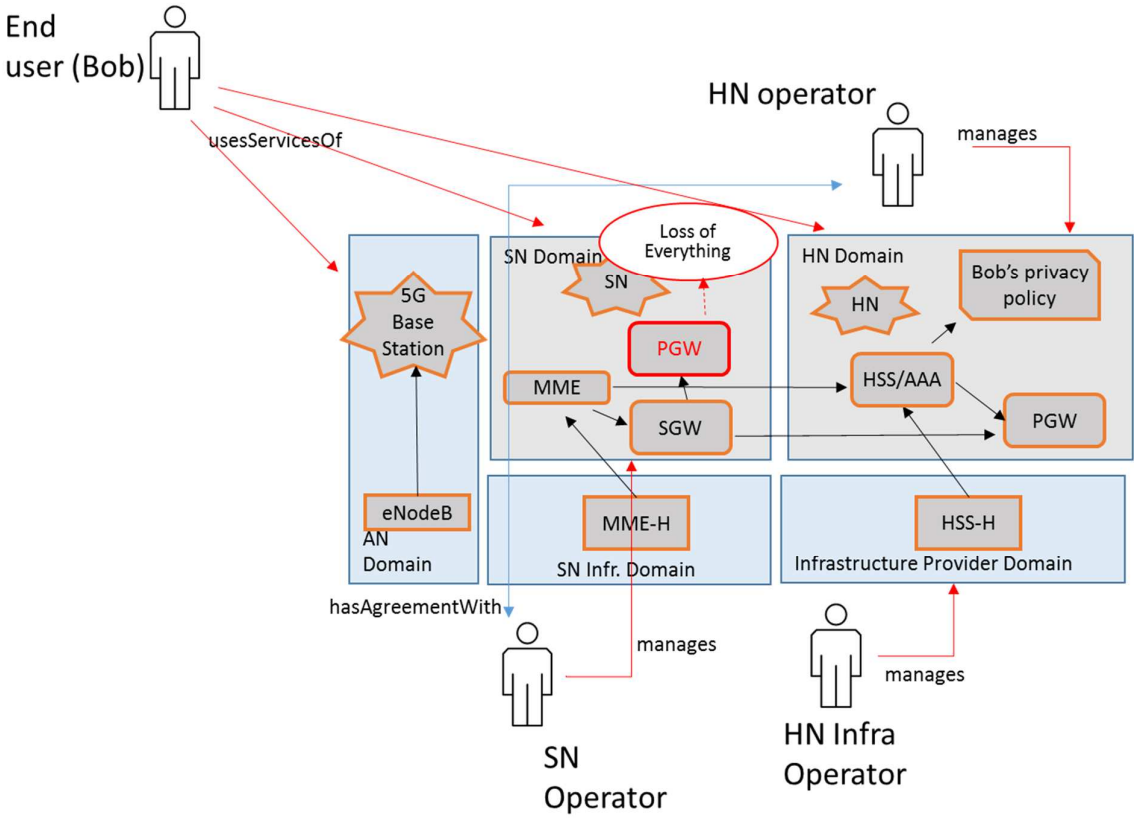

Figure 80. Hardening or patching of systems is not done (T_UC9.3_1): rainy day

While the above diagram portrays that one specific network element is compromised (shown in red), the compromise could happen with any element that is not sufficiently hardened. This compromise basically renders the component untrusted in every way and the component can be used to launch attacks against other elements. The components that expose external interfaces are at most risk, but the risk could materialize through other vectors as well. For instance, poorly managed maintenance system of the operator could be compromised first and then the attack could pivot to the "inner" elements.

Trust implications

If a system is subverted, one no longer can rely on integrity of it. Any action that is performed by that system can lead to various adverse effects, e.g., additional malicious traffic could be generated and further compromise of other systems could be attempted. In essence, the whole network could end up being untrusted.

In the roaming scenarios, the compromise of the visited network leads to the fact that the traffic coming from the other operator to the home operator cannot be trusted and making decisions based on that (e.g., billing) could result in further problems in terms of liability.

Threat mitigation strategy

Systems should be properly maintained by introducing vulnerability management processes. The configuration management should ensure that the systems are consistently hardened and systems have most

up-to-date security patches installed. This is even more important with 5G systems, as there are going to be more software components present through virtualization.

Monitoring of systems can help in detecting breaches. This can potentially be cooperative actions between different operators, so that indicators of compromise are reported to the operator of the source traffic. Proper segmentation of systems can isolate the breach to only one system. Thus, other systems should be considered potentially hostile instead of implicitly trusting devices just based on their network location.

A new VNF that is introduced into the network could also introduce vulnerabilities. The enabler "VNF Certification" could help mitigate this risk, if through it a certain level of assurance with regard the security posture of a VNF can be gained. In other words, there has been a pre-evaluation of the security of the component before it is approved to be installed into the network.

Additionally, the monitoring enablers ("System Security State Repository", "Security Monitor for 5G Micro-Segments", "Generic Collector Interface", "PulSAR") and the virtualization isolation enablers ("Access Control Mechanisms", "Component-Interaction Audits", "Bootstrapping Trust", "Micro Segmentation") help in detecting potential integrity problems and limiting the amount of damage a subverted component can cause.

B.24.2.2 Unauthentic device installed into the system (T_UC9.3_2)

If the physical security is lax, then it might be possible to install an unauthorized device into the network environment of the operator. This could be an act of malicious insider, but equally it could be performed by an external actor, who manages to get access to the physical infrastructure, e.g., by posing as a maintenance personnel. Unauthentic device could send traffic to the network and pose to be an authentic entity. This could lead to various man-in-the-middle or spoofing attacks. Additional attacks could be also performed against other system elements as well (see previous threat).

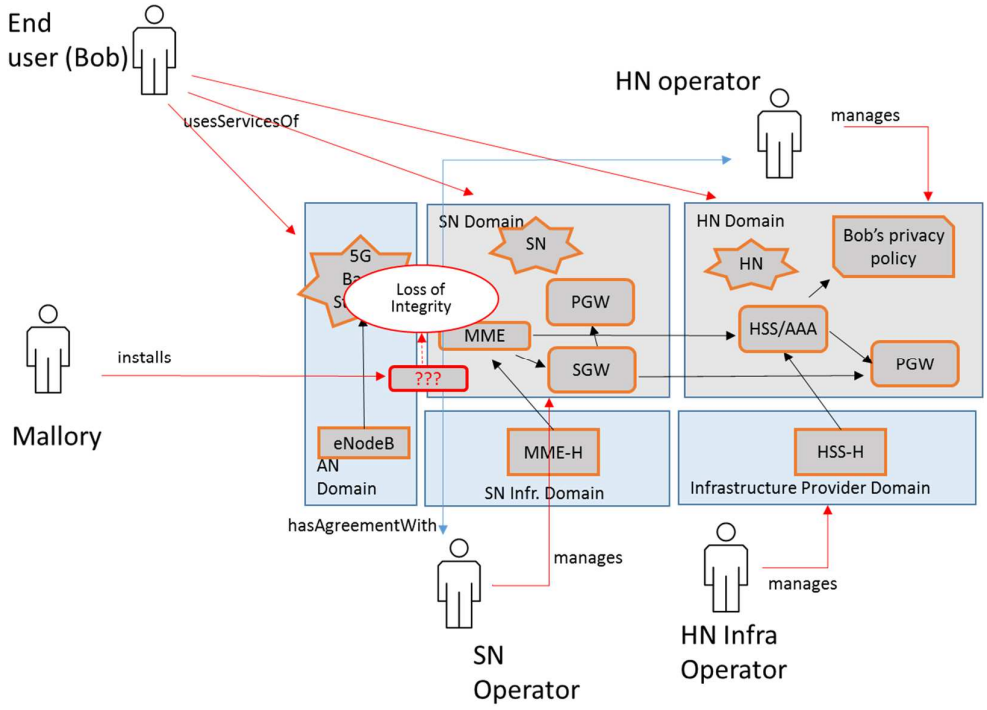

Figure 81. Unauthentic device installed into the system (T_UC9.3_2): rainy day

Trust implications

If the trust is based on the network location of elements, then it can be possible to misuse that trust as traffic coming from certain interface can be deemed authentic. For instance, if there are no other authentication elements in the information flow, data received from another, hacked operator could be interpreted to be legitimate. This could lead to the situation where, for instance, a user is incurred additional costs for the traffic that does originate from the actions of that user.

Threat mitigation strategy

Monitoring of the systems can help in detecting breaches. Also, if only authentic elements are allowed to connect to the system, them it is harder to install physical elements into the networks. For instance, the network ports that are not in use are not enabled. The new elements should first authenticate themselves before allowing them to communicate with the rest of the network.

It is worth noting that in 5G the infrastructure elements might reside in "normal" data centers as the functions might be running in more commodity hardware. One ought to be aware that the level of physical security might not be in the same level as current telecom data centers. Regulatory schemes should ensure that the physical security is taken care of in such locations as well.

The monitoring enablers ("System Security State Repository", "Security Monitor for 5G Micro-Segments", "Generic Collector Interface", "PulSAR") and the virtualization isolation enablers ("Access Control Mechanisms", "Component-Interaction Audits", "Bootstrapping Trust", "Micro Segmentation") help in detecting unauthentic components and limiting the amount of additional damage they can cause.

B.25 Botnet mitigation (UC 10.1)

B.25.1 Use case description with architectural components

A botnet is a network of hijacked agents/clients which are remotely controlled, often associated with introducing malicious software. Botnet infrastructure is increasingly being used for performing criminal activity that involves the use of computers or networks such as the Internet. Although the network operators are not highly impacted as yet, the situation will most likely change in the future, because of the rapidly growing trend of data traffic in mobile networks and increased capability of mobile devices. In this use case an attacker remotely instructs and end user mobile device to conduct malicious activities over MNO's network. This could, for instance, be scanning for additional victims, spamming, or directly attack other users.

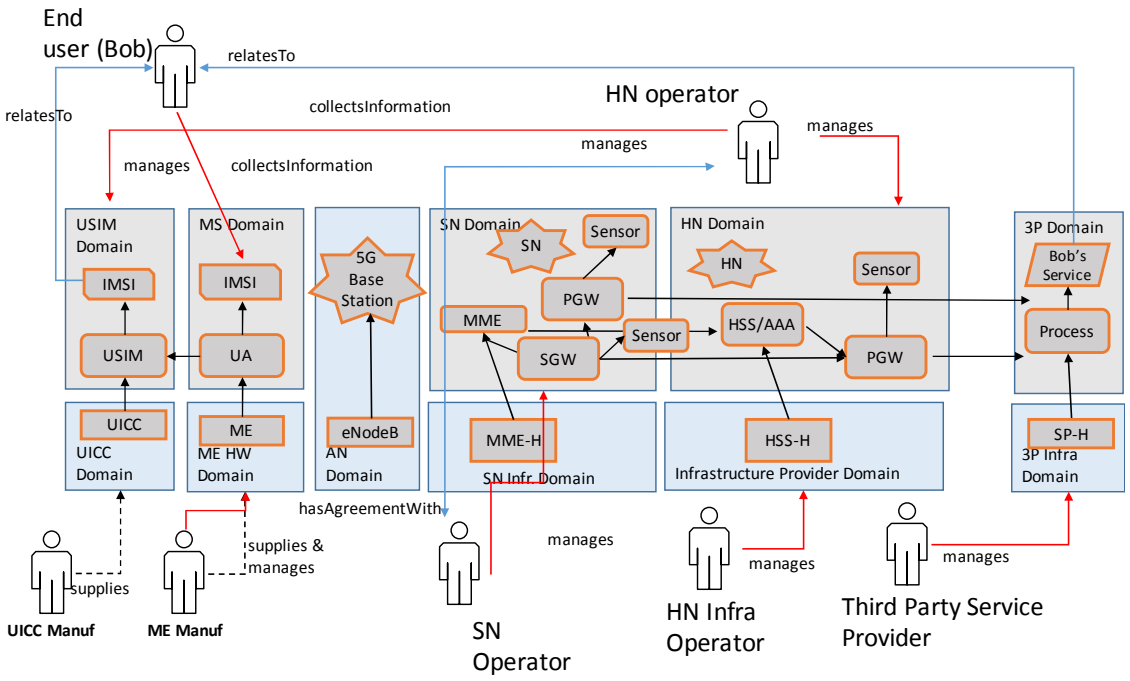

Figure 82. Botnet mitigation (UC 10.1): sunny day scenario

In the sunny day scenario a typical user activity should not be disturbed. This means that the end user could perform normal activities like phone calls, browsing Internet or sending short messages uninterrupted. Of course one has to take into account that the previously described standard activities could also take place during a case where the user device has been subverted. However, in the normal case any additional protection elements installed by the operator should not degrade the quality the user experiences. These elements could be used to alert (or stop) in case malicious traffic is detected.

B.25.2 Identified threats

B.25.2.1 Subverted user equipment (T_UC10.1_1)

The user downloads and installs an application of untrusted origin. This could be a modified version of a well-known application, which adds functionality to the normal operation of the application. This functionality could perform malicious activity, which includes, but not limited to, possibility to remotely control the application (and hence, the device itself) or perform actions that cause additional charges for the user, i.e., there is direct monetary impact.

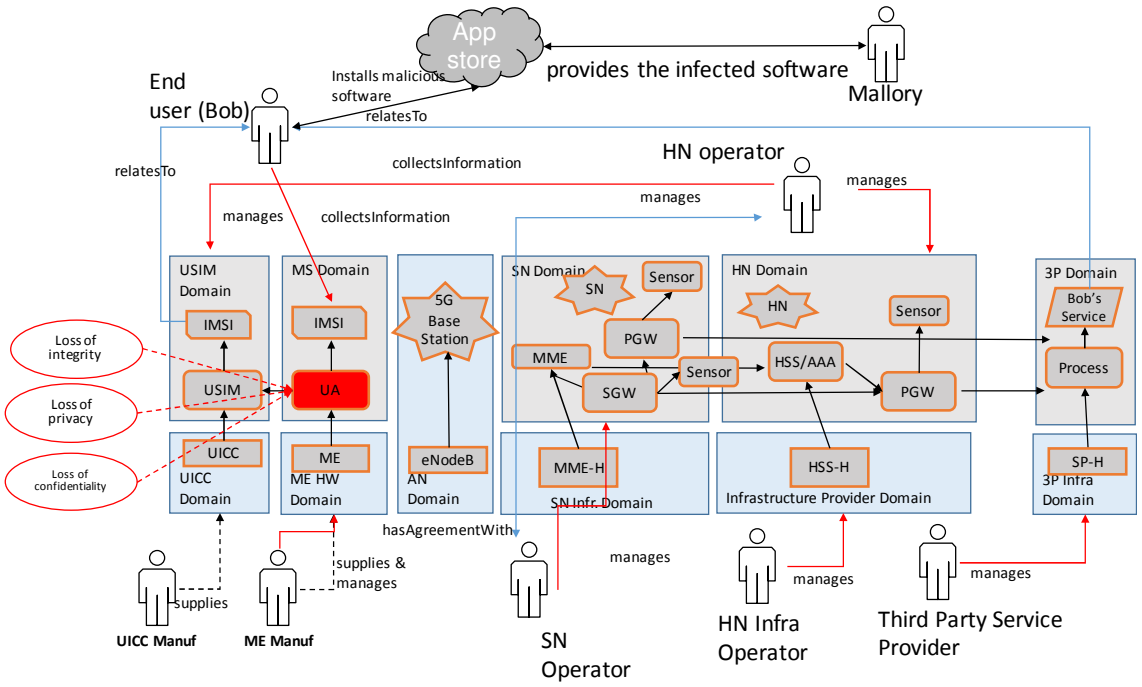

Figure 83. Subverted user equipment (T_UC10.1.1) – 'rainy day'

The figure above describes the process how Bob gets infected. Bob is staying at home and browses his Google Play (App Store, Windows Market). He founds a free version of a popular and trendy game (other application) uploaded by unknown publisher (i.e. Mallory) and decides to give it a try. Bob downloads it and installs it after accepting everything the game (application) requires to run. As a result, Mallory now has a full (or partial) control of Bob's UE. Therefore, this leads of loss of privacy, integrity and confidentiality for Bob.

Furthermore, as secondary consequences:

- There is an infected device operating in the customer network of the MNO
- UEs remotely controlled by Mallory
- UEs used for malicious activities within the MNO as from the MNO
- Monetary loss for the end users through their monthly bills, regardless how insignificant the amount is for each individual is (in case the UE is instructed to send SMSs to premium numbers)

Trust implications

- Loss of authenticity for Bob, resulting in Mallory impersonating him in front of the other users and the MNO.

Threat mitigation strategy

One way to approach this problem from the MNO point of view is to employ the services of an anomaly-based network intrusion detection or prevention system within the core network, so that the system detects atypical individual behaviour.

Another solution could be providing the end user with visually represented historical data of their activity within the MNO, which, in addition to the targeted number and the party who owns it, and also contains a

representation of which country and MNO that number is registered in. This would aid the users to identify anomalous activity from their mobile devices and to report this activity.

Furthermore, the MNO could offer services to the end users to define their own atypical behaviour in the MNO, so that users could, for instance, restrict any outgoing SMS to specific foreign countries, or display a message prior to sending any outgoing SMS.

B.26 Privacy Violation Mitigation (UC 10.2)

B.26.1 Use case description with architectural components

The use case relates to the use of an online service/application over the 5G network. Figure 84 shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

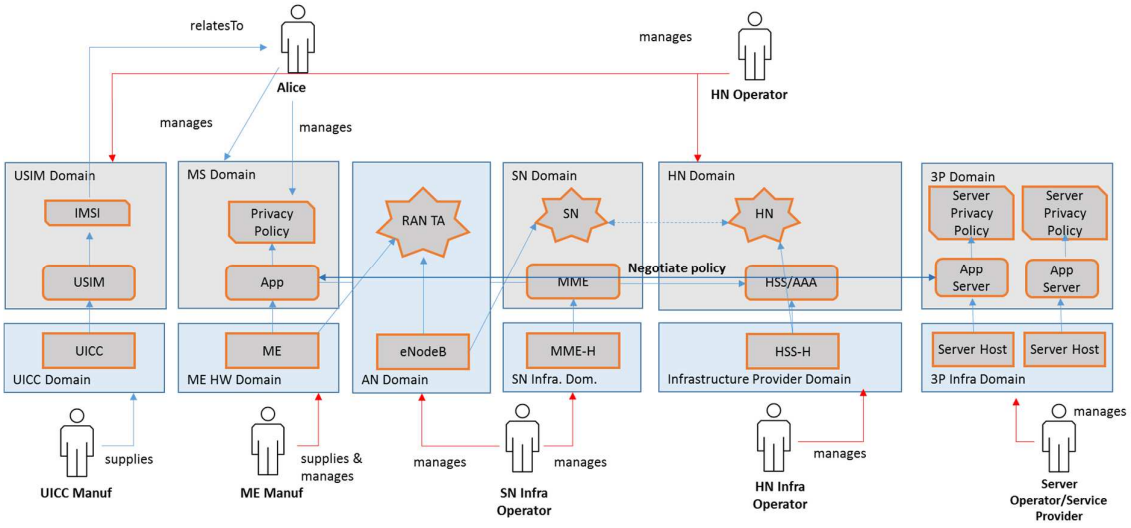

Figure 84. Privacy Violation Mitigation (UC 10.2): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure 84) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice get knowledge that a new technology company has created an inexpensive thermostat sensor for the house environment that learns about the temperature zone and movements around the house and potentially save the user's energy bill. It is programmable remotely.

Alice decides to buy this thermostat sensors. When Alice accesses via her ME the online service (provided by 3P domain) she is informed about the potential collection of some of her data as part of the privacy policy. Alice does not understand clearly the implication of these privacy policies. She uses the service and she is happy to be able to program and control by remote her house's temperature.

B.26.2 Identified threats

B.26.2.1 Nefarious activities (manipulation of information, interception of information): privacy violation (T_UC10.2_1)

Based on Figure 85, Mallory is either the provider of the web thermostat service itself or is an attacker that took control of the service. As a consequence Mallory is able to retrieve data about some of the basic

activities that take place in Alice's house like, when people are there and when they move from room to room. Additionally, Mallory also shares to third parties the data about Alice movements.

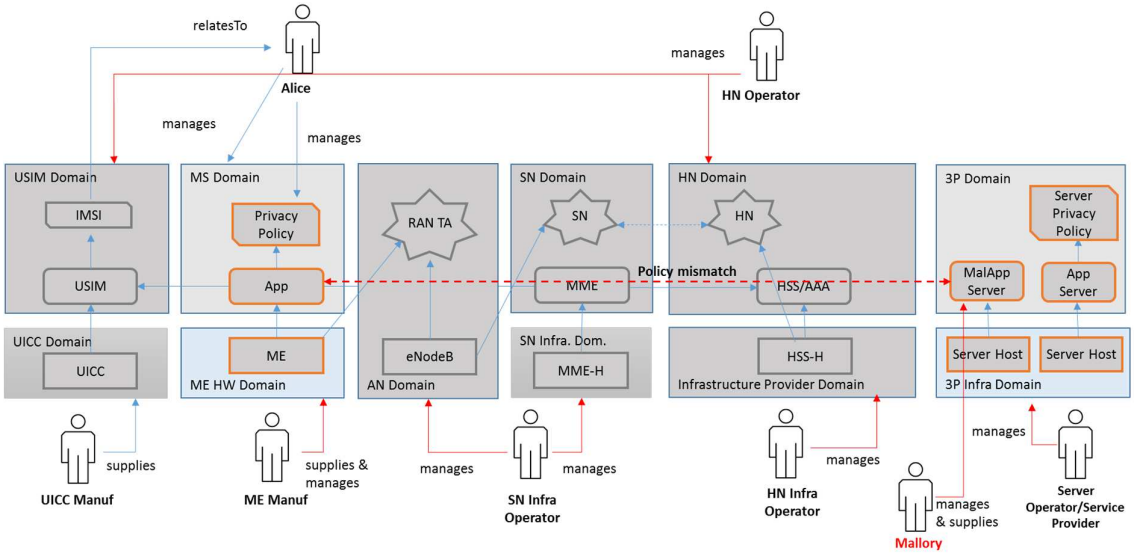

Figure 85. Privacy Violation Mitigation (UC 10.2): rainy day scenario

The consequence is that the provider (in the 3P domain) of the online service accesses more information than the one required to perform the stated functions. This creates privacy problems, in terms of uncontrolled and unauthorized access to sensitive user data. Secondary effects are that users may not know that personal data are shared with third parties; they don't know if data are effectively transmitted and stored securely, and what further use is made of it.

Trust implications

The use case involves the following actors: service provider and mobile application developer, the user (the phone user and the App/Service Provider subscriber), user equipment operating system developer/provider, user equipment/phone manufacturer (ME).

The current trust model is based on the following relationships:

- The user trusts the provider of the service. He/she assumes that the provider follows the privacy policy of the user regarding the collected data, which implies that only the data required for the correct service operation are retrieved, and the data is not leaked to third parties. Therefore, the user trusts that the provider does not further disseminate the collected information to additional parties, if not explicitly allowed by the user to do so.

The implications related to the trust model are that if the user's privacy policies are not honoured, then the privacy of the user is endangered. The implications are:

- The user has no effective way to detect/measure the real trustworthiness of the service provider.
- It is sometimes difficult for a user to understand the privacy implications of using a service: privacy policies (where they exist) are often not easy for users to read and commonly not presented upfront to the user.

- The user cannot control how her/his data are protected and used after being retrieved and sent back to the provider's servers.
- The user has no way to specify his/her privacy preferences including what type of data they he/she is willing to share, for what purpose and for what period.

Trust mitigation strategy

The type of trust required in this use case can be ensured/guaranteed by providing the user a way to analyse the privacy policy of a service and compare it to his/her pre-defined preferences.

The user shall be able to specify his/her privacy preferences including what type of data he/she is willing to share, for what purpose and for what period. This allows the user to make privacy-aware decisions regarding the use of 5G networks and over-the-top 5G services. Ideally, the analysis would be carried out prior to the service being used, for example, at the client application installation time or at the point of connecting to a 5G network.

A provider of a commercial Web site or online service, that collects personally identifiable information about individual consumers who use or visit its commercial Web site or online service, shall post its privacy policy in understandable and clearly way informing the user at a minimum about what precise categories of personal data the service wants to collect and process, why the data processing is necessary (for what precise purposes), whether data will be disclosed to third parties, what rights users have, in terms of withdrawal of consent and deletion of data.

B.27 SIM-based and/or Device-based Anonymization (UC 10.3)

B.27.1 Use case description with architectural components

The use case relates to user's sensitive data accessed by online services and mobile applications. Application running on user devices constantly transmit a steady stream of information to third parties, often sensitive, private, and identifying data ranging from a device's serial number like IMEI, unique operating system identifiers, phone number, voice mail number, SIM ID and even location information. Some of these identifiers are personally identifiable and linked to the devices the user has. The constant transmission of identifying data is important to delivering seamless and tailored services and content to users.

Figure 86. shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

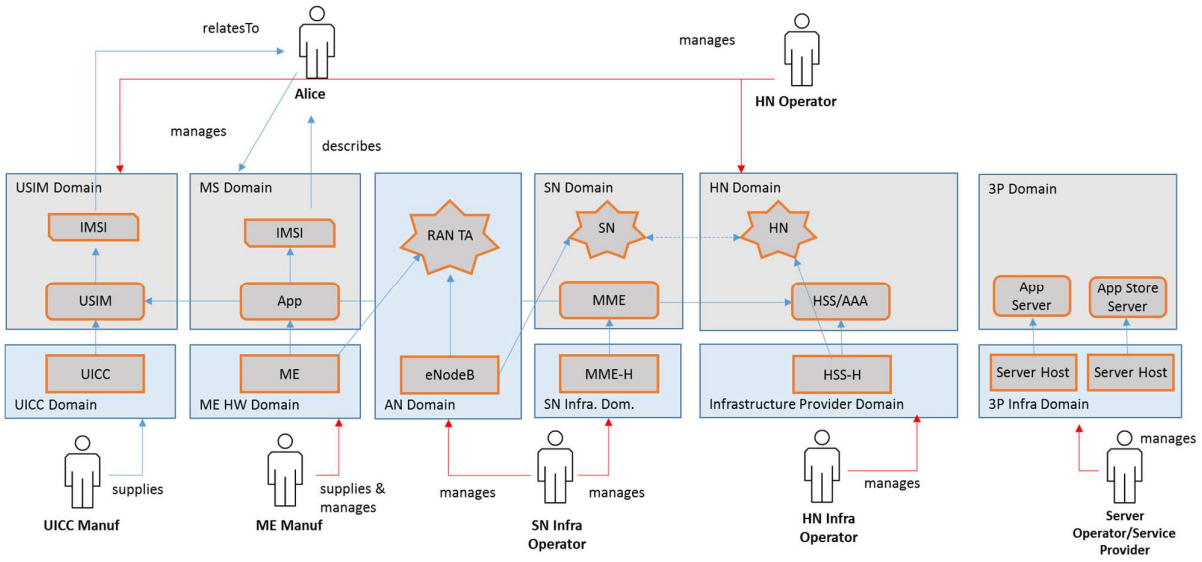

Figure 86. SIM-based and/or Device-based Anonymization (UC 10.3): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure 86.) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice needs to access via her ME an online service, e.g. a traffic road service to keep a check on the traffic situation and get real time information on traffic jams and road closures. Alice has to install on her ME the mobile application offered by the service provider (3P domain). During the installation process, the application notifies to Alice the data it needs to access as part of the 'permissions' list. Alice denies the permissions requested and the installation process fails. Few days later Alice travels away. She needs to reach a destination from the airport but since she does not have much time it is very useful for Alice to better plan the route and to know in real time any traffic situations that may affect her travel time. She tries to install again the application and this time she grants the permissions requested. The installation process ends successfully on the ME.

B.27.2 Identified threats

B.27.2.1 Nefarious activities (manipulation of information, interception of information): personal information disclosure (T_UC10.3_1)

Mallory can come into play in several places. Based on Figure 87., Mallory is the application developer/provider of the service itself. He/she develops the application to access a range of identifiers while providing the service. This "abuse" is also possible since many mobile operating systems reveal subscription and device identifiers, such as phone number, IMSI, IMEI, together with a plethora of other personal data. In a more extended scenario, Mallory may partner with advertising networks or other third parties, and share Alice's identifiers or personal information with these other parties. As a result, in addition to the apparent collectors of identifiers (i.e. the app developer/service provider) there are largely hidden collectors, such as those belonging to advertisers and analytics or crash report companies. The consequence is that the real-time traffic application installed by Alice requests a wide range of information from Alice ME, not all of which is clearly necessary by the advertised functionality of the application. Many of these identifiers are transmitted, collected and shared without Alice's consent. Moreover, the average mobile phone user does not have tools to monitor or control such leaks.

In another scenario Mallory exploits weaknesses in the real-time traffic application to hack into Alice's ME and to retrieve sensitive data transmitted to remote servers.

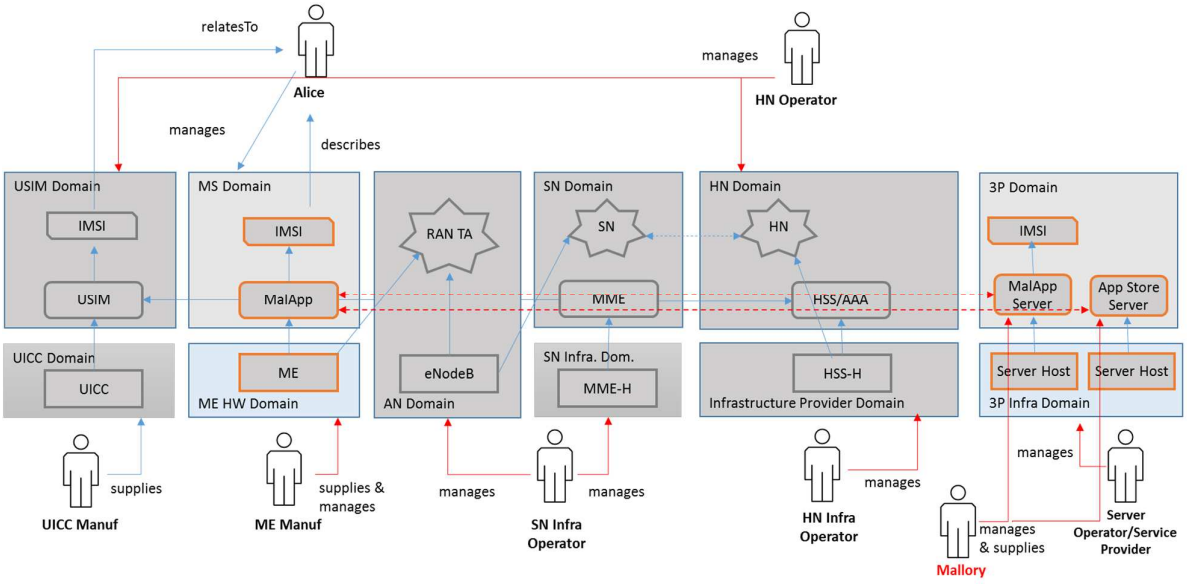

Figure 87. SIM-based and/or Device-based Anonymization (UC 10.3): rainy day scenario

The consequence is that the application accesses more information than the one required to perform the stated functions. This creates privacy problems, in terms of uncontrolled and unauthorized access to sensitive user data. Secondary effects are that users may not know that personal data are shared with third parties; they don't know if data are effectively transmitted and stored securely.

Trust implications

The use case involves the following actors: app ecosystem (Application store provider or service provider and User equipment application developer), phone users (Service Provider subscriber), user equipment operating system developer/provider, user equipment/phone manufacturer (ME).

In this scenario:

- An application store provider trusts an application submitted to the store only after the adoption of vetting process, during which the app is tested to ensure that it does not crash in any obvious way and that it conforms to all the appropriate application store rules. This means that an application store does not implicitly trust an application but it gives the trust only if the vetting process is passed.
- A user trusts the application store provider or service provider offering the application based on the security controls like the vetting process put in place to ensure that the stored applications are not infected by malware. Also the adoption of analyser tools on the app's binary code, to see whether it makes use of private functionality that is normally off-limits to developers, implicitly contributes in building user's trust in the application developer in terms of compliance to the software development guidelines. Finally, in some cases, security mechanisms like application signing provides to the users a way to verify the integrity of the downloaded application. Consequently the user implicitly assumes that applications downloaded from the trusted

application store provider are trusted. Moreover, the user trusts the user equipment (ME) both in the device manufacturer for firmware security, and, in particular, in the mobile OS security model in terms of permissions model implemented, vulnerabilities management process and built-in security controls like application isolation in a virtual "sandbox" that the operating system creates for it.

Even with the adoption of security measures in the different part of the trust chain, data leakage occurs very commonly showing that the trust model should be reviewed.

The implication related to the trust model are:

- The user has no effective way to detect the real trustworthiness of the APP provider
- There isn't a direct trusted relationship between the user and the application. The user does not have a mechanism to control what data an application really access and if they are really necessary. A user cannot prevent an APP from retrieving her identifying data when identifying data would not be really necessary for the service provided by an APP to the user
- The user cannot control how her identifying data are protected and used after being retrieved and sent back to the APP provider's servers.
- Most of the times users ignore applications asking permission to access personal info or they do not pay much care since they might not have much other options if they need to use the application. The risk of this model is that mobile apps can leak information to external sources by sending out device ID (IMEI/EID), contacts, location, etc.

Trust mitigation strategy

The type of trust required in this use case can be ensured/guaranteed through technical solutions (e.g. configurable format preserving anonymization techniques implemented on device) in addition to application security controls already performed by application stores and to security mechanisms built in the mobile OS. Potential solutions include an anonymization service that can be subscribed by 5G users needing it (5G users that have privacy concerns regarding their data). Network offers to subscribers a SIM (or a device) that implements anonymization algorithms like for example lightweight format preserving algorithms that can be implemented with little computational resources. Network offers to subscribers a means to configure their anonymization preferences.

The *Device-based Anonymization* enabler (R2) allows users to configure a fine grained data anonymization to distinguish between applications for which data needs to be protected and returned in an anonymized way to avoid unnecessary disclosure, and applications that need the real data (real IMSIs or MSISDNs) for their correct functioning. For example, some apps offer a mechanism to recover a lost password via SMS and therefore they need the real MSISDN of the user's profile. For compatibility with Internet services, format preserving encryption which generates the same pseudonym for the same identifier and service received in input should suffice. The enabler provides such an algorithm embedded in the mobile device OS, while being able to distinguish the calls coming from different applications installed on the user's device and apply data anonymization accordingly to the policy preferred by the user.

B.28 Lawful Interception in a Dynamic 5G Network (UC 11.1)

B.28.1 Use case description

In this use case, we attempt to show the implementation of a lawful interception. The sunny day is as follow (cf. D2.1 for further details). First, we assume that LEA identifies the suspected criminal (i.e., Bob) to be surveilled and that he (LEA) has an authorization from the court of justice in order to perform a lawful interception on Bob. On demand, the MNO should be able to answer any interception request regardless of the target entity / user or target service. At the beginning, LEA transmits the LI request and the granted authorization to the MNO to conduct the interception with regards to Bob. The MNO checks the validity of the request and depending on the intercept type and the service to be intercepted, the MNO instantiates, activates and initiates a Network function (we call it, in what follows, LI function) that will deliver to the authorities the required information. At the end of the authorized period, the MNO deactivates the LI function.

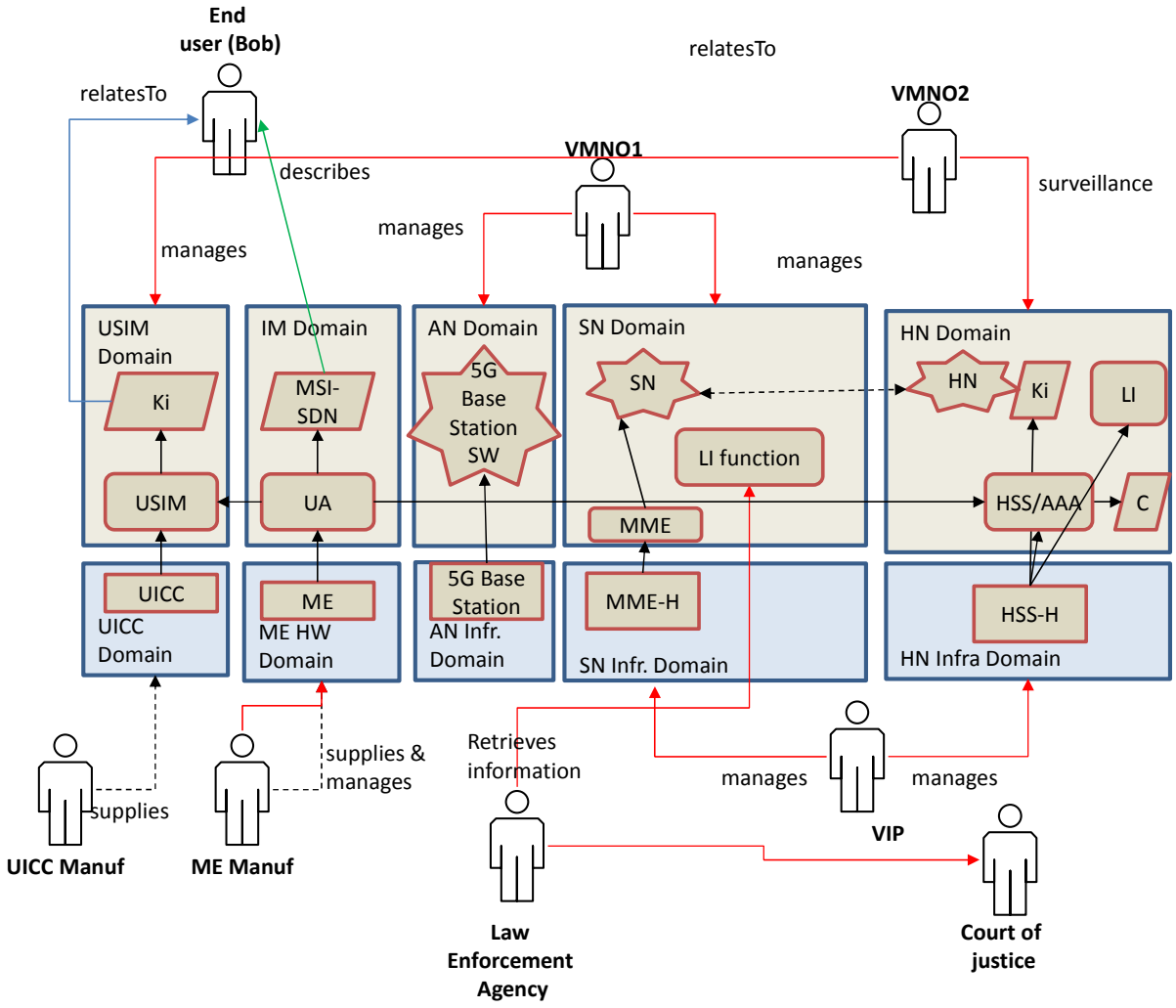

Figure 88. Lawful Interception in a Dynamic 5G Network (UC 11.1): sunny day scenario

B.28.2 Identified threats

B.28.2.1 Compromised / malicious LI (Lawful Interception) function (T_UC11.1_1)

In this threat, we have an attacker that will target the LI function. Attacking the LI function may result in various issues. The attacker may act either against the authorities by compromising the LI function in such a way that it delivers fake information about Bob or correct information about another user instead of Bob. The attacker may also compromise the LI function such that its functioning is not any more transparent (like required by LI) because it causes disruption or degradation of the service. Finally, the attacker may target the user privacy by providing to the authority more information than what is authorised.

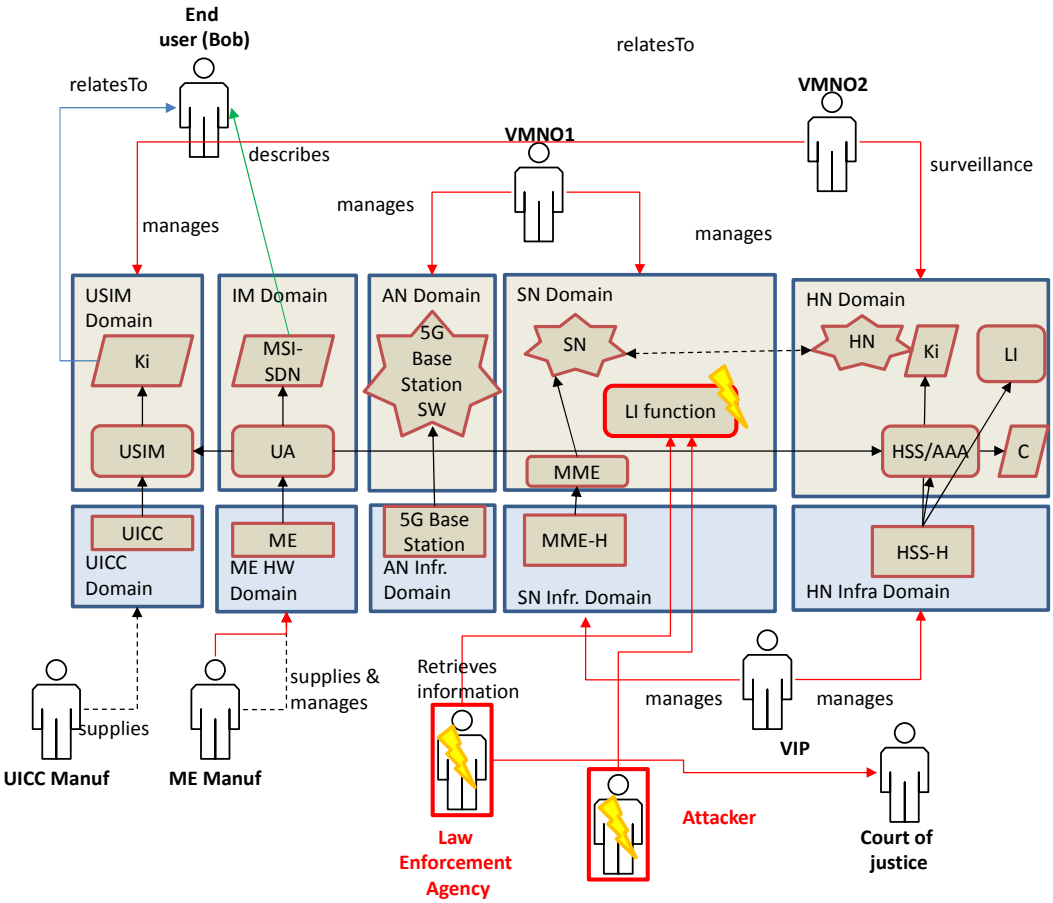

Figure 89. Lawful Interception in a Dynamic 5G Network (UC 11.1): rainy day scenario

Trust implication

The user trusts the MNO that only authorized LI are executed and only authorized authorities have access to collected data during the LI. The user also trusts the MNO that an LI lasts only the time designated in the authorization and only on the users indicated in this authorization. The authorities trust that the MNO will provide correct data.

Threat mitigation strategy

In order to protect against this threat, the MNO needs to consider the validity of the LI function. We can consider the state of the art about remote attestation mechanism and software integrity verification.

B.29 End to end encryption in a LI aware network (UC 11.2)

B.29.1 Use case description with architectural components

The use case relates to the user communication over 5G network. Figure 90. shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

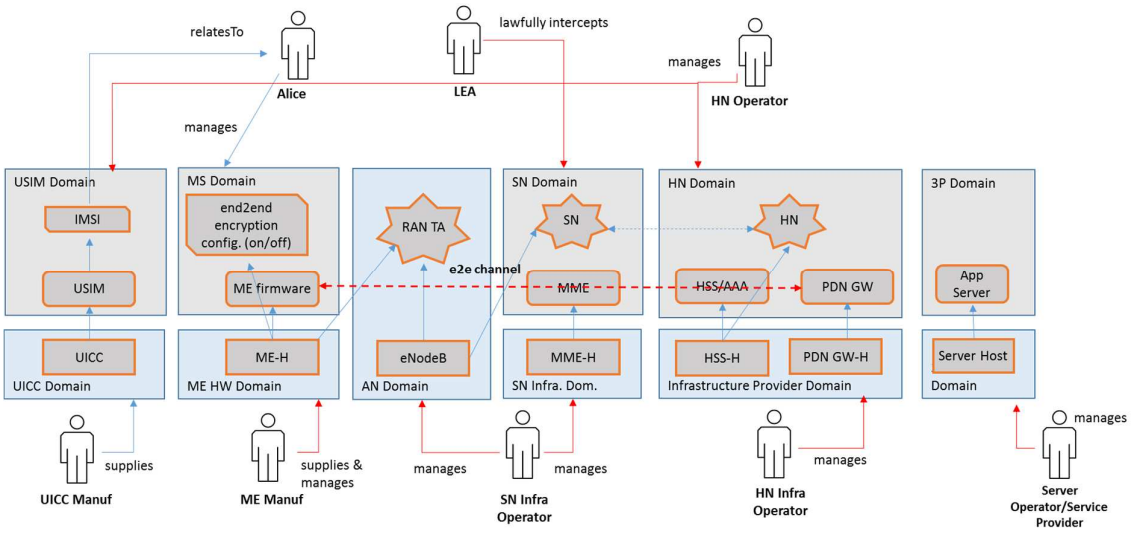

Figure 90. End to end encryption in a LI aware network (UC 11.2): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure 90.) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice needs to communicate in an encrypted manner with Bob. She wants her call or SMS/MMS to be encrypted but she does neither share a secret key with Bob nor an application to encrypt the communication. Alice uses the encryption service provided by the 5G Operator, as shown in Figure 90.

Alice is connected to the 5G network (it has been authenticated). Alice, with the help of the network operator, negotiates a session key with Bob. If LEA wants to intercept Alice communications, the LEA, the mobile operator (provider of the encryption service), the court of justice and may be other entities collaborate to retrieve or reconstruct the session key. One entity alone should not be able to retrieve or reconstruct this key. This operation needs at least the cooperation of the LEA, the mobile operator and the court of justice.

Therefore if LEA wants to intercept Alice's calls, LEA asks the 5G operator to provide access to the intercepted communications. 5G operator as provider of the encryption service acts as an escrow agent. The session key is retrieved or reconstructed and used by LEA to decrypt the session key and consequently Alice's communication by completely respecting the terms of the interception authorized by the court of justice.

B.29.2 Identified threats

B.29.2.1 Nefarious activities (manipulation of information, interception of information) over LI-aware network (T_UC11.2_1)

Based on Figure 91., Mallory is a malicious LEA or a malicious key escrow actor. The main potential flaws of an end-to-end encryption service is to provide LEA (or any other key escrow agents, e.g., a 5G operator) full control of the decryption keys or to somehow enable a backdoor which might be used for undetectable mass

surveillance. In such a case, the malicious LEA or any entity in control of the backdoor may get information exchanged by one of the users involved in LI out of the designated period in the authorization and/or about users not actually in the authorization list (Unauthorized disclosure).

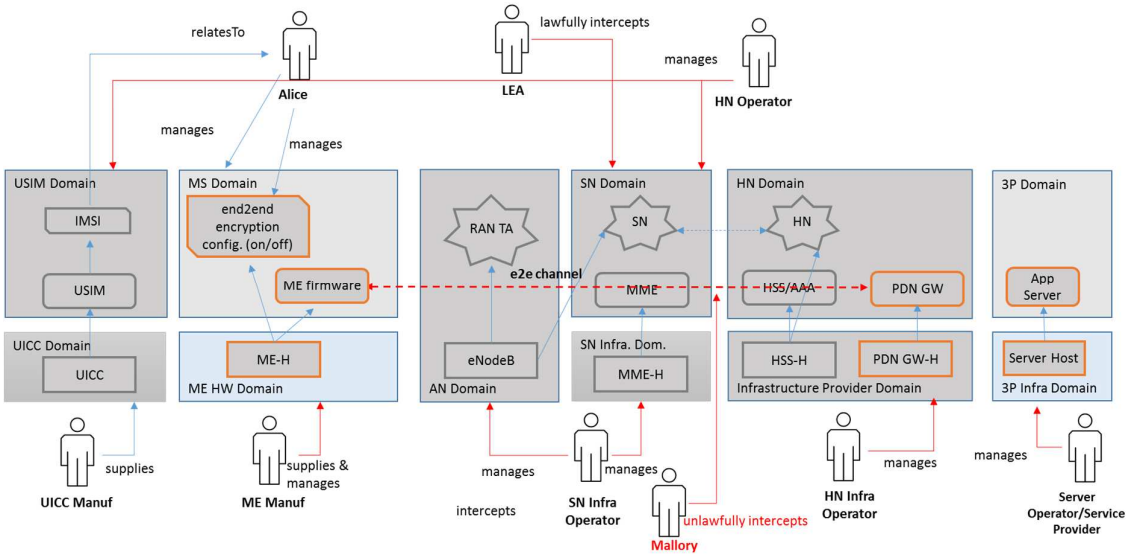

Figure 91. End to end encryption in a LI aware network (UC 11.2): rainy day scenario

In this way the user data privacy is not guaranteed when the LI is active for an end to end encrypted communication.

Trust implications

The use case involves several actors: the end-user (e.g., Alice), the MNO (HN) to which the user has a subscription, the SN (and the AN) provider, the law enforcement agency (LEA) that needs to intercept a suspected user communications, the court of justice which delivers the lawful interception authorization. The current trust model is based on the following relationships.

- the user trusts its HN as part of the direct service agreement.
- The HN trusts the SN as part of the roaming agreement contract and it confers full trust in the SN with regards to its subscriber.
- Both HN and SN trust their interconnection provider.
- The user and the HN trusts the SN for the privacy aware implementation of LI. Given that the service is developed / offered by the mobile operator and that it is a key-escrow-like service, users need to trust that the mobile operator developed a system that requires at least k agents to retrieve / reconstruct the session key.

The implications related to the trust model are:

- The user has no way to detect the trustworthy of either the SN or the HN as far as the key escrow mechanism implementation is concerned.
- The user has no way to detect the trustworthy of LEA as far as the key escrow mechanism implementation is concerned.

- On the other hand if users trust the privacy fairness of the encryption service provided by the mobile network and this trust is broken, users may stop using this service.

Trust mitigation strategy

The type of trust required in this use case can be ensured/guaranteed through technical solutions (e.g. configurable end to end encryption) with privacy aware LI.

The properties that an end-to-end encryption service should satisfy are:

- *On-demand service*: The service should be turned on and off by the subscribers.
- *Backward secrecy*: LEA must not have access to exchanged information before the designated period in the authorization.
- *Forward secrecy*: LEA must not have access to exchanged information after the designated period in the authorization.
- *Security*: The end-to-end encryption service may be applicable on IP or higher layer independently by the type of UE using an application which is installed as part of the service.

The encryption key may be part of an escrow system provided by the 5G operator to enable secure communication and at the same time enable lawful interception. For example the session keys can be encrypted using a master key. To this end, we can use a threshold (k, n) secret sharing scheme. In such a case, less than k agents (e.g., LEA, 5G operator, etc.) cannot get any information about the master key and any k (possibly smaller than n) or more agents can recover the master key. In this way a malicious LEA cannot recover the session encryption key.

C Annex C: Positioning wrt 3GPP SA3

3GPP SA3 WG has started in March 2016 a study on the security aspects of the next generation system. The study has produced a dedicated technical report TR33.899 (Rel-14) "*Architecture and Security for Next Generation System*". Within this TR, SA3 studied preliminary threats, requirements and solutions for the security of next generation mobile networks.TR 33.899 has been stopped in August 2017during the sa3#88 meeting mainly due to time shortage. The content of TR 33.899 reflects the state of the work when the study item was stopped. Proposed requirements and solutions are not fully evaluated. In the meantime SA3 has started to work to a (Rel-15) System Wide Work Item on 5G System and Security Architecture - Phase 1. Within this Work Item (i.e. 5GS_Ph1-SEC), SA3 aims to develop the Stage 2 normative specification of Phase 1 of the 5G security architecture based on the prioritizations and interim agreements captured in TR 33.899 and on requirements from other working groups, e.g. SA2, RAN2 and RAN3. A new TS 33.501 on Security Architecture and Procedures for 5G System have to be delivered in March 2018 (R15) according to the current planned SA3 time scale.

Part of the content of the new 33.501 has been taken from the 33.899, by selecting only the most mature and agreed proposals from each security area. In fact the complete or partial conclusions of this study will form the basis for the normative work and/or for any further study.

For this reason we report hereby a short analysis of the security requirements of the latest version of the TR 33.899 (version 1.3.0, 21 august 2017).

C.1 Analysis of 3GPP TR 33.899

As already said, the TR 33.899 is a collection of proposed security requirements, and solutions that were collected during the study of the next generation architecture (or 5G). The study item was stopped in August 2017. Proposed requirements and solutions are not fully evaluated.

In the scope of this TR there are the threats, potential requirements and solutions for the security of next generation mobile networks.

33.899 contains 17 main sections, corresponding to 17 research area or security area. They are:

1) Security architecture deals with architectural aspects of the security for NextGen system.

2) Authentication deals with authentication framework, identifiers, and credentials, authentication methods.

3) Security context and key management deals with security aspects related to management of security context and security keys.

4) RAN security deals with the security for Next Generation radio interface and radio access network.

5) Security within NG-UE deals with the security of sensitive data handled within the NG-UE.

6) Authorization deals with both, authorization of the UE to access the network and authorization of the network to serve the UE.

7) Subscription privacy deals with various aspects related to the protection of subscribers' personal information, e.g. identifiers, location, data, etc.

8) Network slicing security covers security aspects related to the network slicing concept such as service access, network function sharing and isolation.

9) Relay security deals with security of the NextGen connectivity over relays.

10) Network domain security deals with security of the signalling protocols in the network domain such as authentication, integrity, and availability.

11) Security visibility and configurability deals with presentation of security information to a user of a UE, and management of security configuration by a user or a UE.

12) Credential provisioning deals with security aspects of provisioning 3GPP credential(s) on equipment that will access the NextGen system.

13) Interworking and migration deals with security aspects related to the interworking and migration scenarios between radio technologies and possible core network concepts.

14) Small data deals with massive number of IoT UEs that usually send small amounts of data sporadically and also moves around.

15) Broadcast/Multicast security deals with security for broadcast services that will be used in verticals, for example MCPTT, Critical Communication, V2X, and massive MTC.

16) Management Security deals with security related to management plane and deployment scenarios.

17) Cryptographic algorithms deal with cryptographic algorithms to be used for security mechanisms and protocols within Next Generation System.

Each security area contains a list of threats, requirements and proposed solutions. The SA3 groups didn't define any specific methodology to identify the security requirements, but the TR has been used as a means to collect the ideas and solutions to "old" security issues already known from 3,4G experiences, following a bottom-up approach.

The TR33.899 collects more than 250 requirements, most of them not fully analyzed by the SA3 group. Said that, it is difficult to position the present document and its results with respect to the TR33.899 requirements. Instead it has been decided to follow a double approach:

- to take into account only the most general ones, that the TR call "High level security requirements", then
- to analyze only the requirements which security areas have a mapping with the ones addressed by 5G-ENSURE.

High level security requirements

TR 33.899 High level requirements
3GPP specifications shall provide mechanisms to verify the integrity of 3GPP radio messages to a common point in the visited network. These mechanisms shall allow the detection of unauthorised radio messages, detection of "false base stations" and verification of an authorised network. The mechanisms shall be extensible so that suitable security can be maintained of the life of the NextGen implementations. The mechanisms defined should cater for the high speed communications envisioning in NextGen and for battery efficient low volume data.
The security mechanisms defined in NextGen shall be able to be configured to comply with local lawful interception laws and regulations.
The security mechanisms defined in NextGen shall be able to be configured to confidentially protect voice, data and signalling.
The security mechanisms defined in NextGen shall be able to be configured to protect subscriber's privacy.
The security mechanisms defined in NextGen shall be able to be configured to provide authorisation services for users, devices and networks both at a bearer level and at a services level.
The security mechanisms defined in NextGen shall be able to be configured to provide authorisation, integrity protection and confidentiality between network elements and between networks.
The security mechanisms defined in NextGen shall be able to be configured to provide authorisation, integrity protection and confidentiality for new NextGen services.
As NextGen networks may be active upto and beyond 2030 and as the ability to attack security mechanisms increases over time, the security mechanisms specified for NextGen shall be extensible to new algorithms and procedures that will be defined during the lifetime of the specifications, where appropriate.
The control plane shall be protected against denial of service attacks from UEs. Mechanisms should be specified which limit the effect which signaling attacks may cause to the network. Signaling caused by UEs should not be able to degrade the network performance for other end users and the network itself, this is especially the case for NextGen where the amount of signaling may increase.
UEs shall be protected against denial of service attacks from network. Mechanisms should be specified which limit the effect which signaling attacks may cause to UEs. Signaling caused by the network should not be able to degrade the network performance for end users, this is especially the case for NextGen where the amount of signaling may increase.
UEs and NextGen network should be protected against denial of service attack from external networks, e.g. the internet, and from other UEs. Impact to network and end user signalling or data processing due to external attacks should be minimized. Signaling and data processing caused by external network traffic should not degrade the network performance for end users and the network itself, as well as the UE performance, e.g. the power consumption.

C.2 5G-ENSURE security areas versus 3GPP SA3 TR 33.899

At the ETSI Security week, during the second 5G-ENSURE workshop, the invited chairman of SA3, Anand Prasand, presented the status of study "*Architecture and Security for Next Generation System*" i.e. TR 33.899 and provided a mapping between the security areas addressed by 5G-ENSURE project and the ones which are part of the study. The mapping is reported in the following figure.

Figure 92. 3GPP SA3 security areas mapping against 5G-ENSURE

In particular the following areas have been identified:

- Subscription Privacy
- RAN Security
- Authentication
- Architectural aspects of next generation security

As part of the standardization work performed within WP5, 5G-ENSURE has contributed to the TR 33.899 by providing several requirements mainly related to the Subscription Privacy area which have been accepted a token into account also in the normative phase.

For the other areas, that is RAN Security and Network Slicing and Authentication, in the table below are reported some of the requirements coming from the use cases threat analysis (Mitigation Hints) and when there is a mapping with potential requirements in TR 33.899 that has been reported.

Area	5G-ENSURE Use case	5G-ENSURE Requirements	TR 33.899 Requirements
Privacy	(UC 2.1) Device Identity Privacy	R1. Enhanced privacy for network attachment protocols should be provide by limiting exposure of device identifiers and prior points of attachment R2. IMEI should be sent only in a confidentiality protected message (e.g., through encryption). R3. Anonymous and optimised address selection (e.g. MAC address) for network attachment protocols should be provided to protect device identifiers	Permanent equipment identifiers shall be concealed in communication, whenever feasible.
	(UC 2.2) Subscriber Identity Privacy	R4. Encrypted identifiers when possible should be used	Permanent subscriber identifiers shall not be transmitted in clear-text, whenever feasible. It shall be possible to anonymize or conceal permanent subscription identifiers when appropriate. For example anonymization might be required by regulations, or the receiving node might not need to identify the subscription Permanent subscription identifiers shall be concealed in communication, whenever feasible.
		R5. Frequent changing of temporary identifiers should be ensured	5G-CN temporary subscription identifiers (e.g. S-TMSI) shall be

			refreshed regularly with a frequency that avoids their persistent use. Common parameters should be specified that can be used to define the required refresh period.
		R6. Improved pseudo-identifiers should provide for unlinkability of subscriber	From one or more temporary identifiers, it shall not be feasible for an unauthorized party to identify the corresponding permanent identifier. From one or more temporary identifiers, it shall not be feasible for an unauthorized party to predict the next corresponding temporary identifier (i.e. the next temporary identifier of the same subscription).
		R7. Temporary subscription identifiers shall be used instead of permanent subscription identifiers in communication, whenever feasible	Temporary subscription identifiers shall be used instead of permanent subscription identifiers in communication, whenever feasible
Network Slicing	(UC 5.1) Virtualized Core Networks, and Network Slicing		
	(UC 5.2) Adding a 5G Node to a Virtualized Core Network	R8. Applying security verification procedures – technical and organisational - for assuring that the added nodes are trustworthy.	

		R9. Only authenticated and authorized entities should be allowed to add nodes.	
	(UC 5.3) Reactive Traffic Routing in a Virtualized Core Network		
	(UC 5.4) Verification of the Virtualized Node and the Virtualization Platform		
	(UC 5.5) Control and Monitoring of Slice by a Service Provider	R10. Strong isolation is needed to prevent resource access outside a slice. R11. Should be allowed access only those control interfaces that are required to minimize service providers potential to escape	Platforms supporting network slice should be able to ensure that resource of network slice instances is not impacted from each other (e.g. by reserving resource per network slice instance).
		R12. Strong isolation between slices is needed.	The 3GPP System shall have the capability to provide a level of isolation between network slices which confines a potential cyber-attack to a single network slice. It should be possible to isolate slices from one another, to minimize attacks on data confidentiality (e.g., data leakage between network slices) and integrity when a single NG-UE is accessing services over more than one network slice.
		R13. Authentication and authorization over the access to control and data plane	The capabilities to manage network slices should be under control of authorized operators.

	(UC 5.6) Integrated Satellite and Terrestrial Systems Security Monitor		
RAN	(UC 6.1) Attach Request During Overload	R14. A secure method for priority of access requests should be supported R15. illegitimate or non-prioritized request should be rejected at early stage, to save resources (i.e. enable integrity protection at a low layer in the radio network stack) R16. Priority for re-attachment to devices losing radio synchronization should be given	The network (gNB) shall be able to perform UE verification to be able to detect a malicious UE acting on behalf of a real UE The network (gNB) shall be able to perform UE verification in order to be able to detect a malicious UE acting on behalf of a real UE.
	(UC 6.2) Unprotected User Plane on Radio Interface		
Authentication	(UC 1.1) Factory Device Identity Management for 5G Access		
	(UC 1.2) Using Enterprise Identity Management for Bootstrapping 5G Access		
	(UC 1.3) Satellite Identity Management for 5G Access	R17. fine-grained access control for resource constrain devices should be provided e.g. based on tokens	
	(UC 1.4) MNO Identity Management Service		
	(UC 3.1) Authentication of IoT Devices in 5G	R18. Group-based authentication mechanism should be supported to mitigate traffic spikes towards the network	The lightweight but secure enough authentication scheme for energy consuming sensitive devices is required in NexGen network. The 3GPP system shall support an authentication method which is resilient to DoS attacks caused by massive number of UEs

			authenticating at the same time.
	(UC 3.2) Network-based Key Management for End-to-End Security	R19. isolation techniques – e.g. micro-segmentation – may be utilized to control which applications may access key management server	
	(UC 4.1) Authorization in Resource-Constrained Devices Supported by 5G Network	R20. authorization mechanisms, for example based on tokens should be used in Resource-Constrained Devices.	
	(UC 4.2) Authorization for End-to-End IP Connections		
	(UC 4.3) Vehicle-to-Everything (V2X)		

D Annex D: Abbreviations

List of abbreviations used throughout this document.

AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
AN	Access network
BTS	Base Transceiver Station
CN	Core Network
D2D	Device-to-Device
DNS	Domain Name System
(D)DoS	(Distributed) Denial of Service attack
EAL	Evaluation Assurance Level (EAL1 through EAL7)
EAP	Enhanced Authentication Protocol
eNB	Evolved Node B
ENISA	European Union Agency for Network and Information Security
EPC	Evolved Packet Core
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HAPS	High Altitude Platforms
HSS	Home Subscriber Server
ID	Identifier
IM	Identity Management
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOT	Internet of Things
ITU-T	ITU (International Telecommunication Union) Telecommunication Standardization Sector
LI	Lawful Interception
LTE	Long Term Evolution
M2M	Machine-to-Machine
MBB	Mobile Broadband
MME	Mobility Management Entity
(m)MTC	(Massive) Machine-Type Communication
MNO	Mobile Network Operator
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
OTT	Over-the-Top (Provider)
PLMN	Public Land Mobile Network
PUA	Potentially Unwanted Application
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
SatAN	Satellite Access Network
SatNO	Satellite Network Operator
SDN	Software Defined Networks
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SN	Serving Network

SP	Service Provider
SSO	Security Service Operator
SW	Software
TAU	Tracking Area Update
TCAM	Ternary Content Addressable Memory
TMSI	Temporary Mobile Subscriber Identity
TNA	Transport Network Architecture
TVRA	Threat Vulnerability and Risk Assessment
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
V2X	Vehicle-to-Everything
VMNO	Virtual Mobile Network Operator
VIP	Virtual infrastructure provider
VNF	Virtualized Network Function(s)
WSN	Wireless Sensor Network