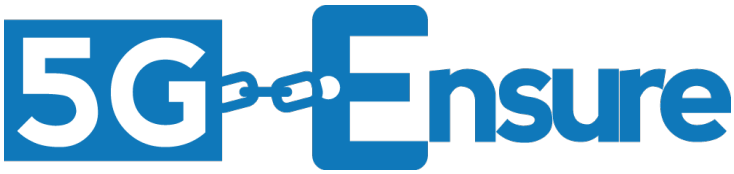

Deliverable D2.1
Use Cases

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	2016-02-01	
Dissemination Level:	Public	
Lead beneficiary	EAB	Göran Selander, goran.selander@ericsson.com
Authors	EAB: Mats Näslund, Göran Selander IT INNOV: Stephen Phillips, Bassem Nasser LMF: Vesa Torvinen, Vesa Lehtovirta NEC: Felix Klaedtke NIXU: Seppo Heikkinen, Tommi Pernilä, Alexander Zahariev ORANGE: Ghada Arfaoui, José Sanchez, Jean-Philippe Wary UOXF: Piers O'Hanlon SICS: Martin Svensson, Rosario Giustolisi TASE: Gorka Lendrino, Carla Salas TIIT: Madalina Baltatu, Luciana Costa VTT: Janne Vehkaperä, Olli Mämmelä, Jani Suomalainen	

Executive summary

This document describes a number of use cases illustrating security and privacy aspects of 5G networks. Based on similarities in technical, service and/or business-model related aspects, the use cases are grouped into *use case clusters* covering a wide variety of deployments including, for example, the Internet of Things, Software Defined Networks and virtualization, ultra-reliable and standalone operations. The use cases address security and privacy enhancements of current networks as well as security and privacy functionality needed by new 5G features. Each use case is described in a common format where actors, assumptions and a sequence of steps characterising the use case are presented together with a short analysis of the security challenges and the properties of a security solution. Each use case cluster description is concluded with a "5G Vision" outlining the associated enhancements in security and privacy anticipated in 5G networks and systems. A summary of the 5G visions and conclusions are provided at the end of the document.

Foreword

The overall objective of 5G-ENSURE (see Section 1.1) is to become the reference project for everything that concerns security and privacy in 5G while contributing to 5G resilience. To achieve this overall ambition a number of specific objectives are targeted, including:

- Collect, analyse and prioritize 5G security and privacy requirements
- Define a security architecture for 5G
- Specify, develop and test an initial set of security and privacy enablers for 5G

These three objectives are in part dependent on analysing 5G security relevant use cases, which is the content of this deliverable D2.1. Hence D2.1 provides input to the work on Trust Model (Task 2.2), Risk Assessment, Mitigation and Requirements (Task 2.3) and the Security Architecture (Task 2.4) within the project. The use cases presented herein also serve to provide initial "blue-prints" for the required functionality of the so-called *security enablers* developed by WP3 of 5G-ENSURE.

D2.1 is one instance of the 5G-ENSURE measurable results and one of the milestones (MS2) of the 5G-ENSURE project. D2.1 is the first technical deliverable of the project and hence is not dependent on any previous technical deliverable within the project. The external sources for this deliverable, however, include other parallel projects running within the overall 5G-PPP and, conversely, cross-PPP coordination activities are in place to disseminate the results to other 5G-PPP projects.

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 logotype 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.

All Use Cases investigated in this deliverable are in the research context of a future 5G network and do not entail any commitment to be implemented in existing 2/3/4G standards. All references to 4G/LTE or EPC platforms are used for illustration of Use Cases and are not committing the project in any way to a predefined 5G infrastructure (as an iteration only of existing 4G standards for instance).

Copyright notice

Contents

1 Introduction

This document describes use cases illustrating security and privacy aspects of 5G networks. These use cases provide a basis for understanding 5G security and will be used in several ways within the 5G-ENSURE project (see Section 1.1):

- The project will analyse potential threats and vulnerabilities, and identify security and privacy requirements based on these use cases.
- The use cases will be used to define a trust model between the various actors in a 5G system addressing the multiplicity of actors and also taking into account the machine-to-machine interactions characterising next generation networks.
- The use cases provide input to the *security enablers* in scope of the project covering the areas AAA, Privacy, Trust, Security Monitoring, and Network Management & Virtualisation Isolation.
- The items above, as well as the use cases themselves, are the major building blocks used to define the 5G security architecture in the project. Cross-PPP coordination activities are in place to disseminate the results to other projects of the 5G-PPP.

The use cases illustrate specific 5G related security challenges. There are two categories of use cases and associated challenges:

1. For *use cases illustrating security issues inherited from current generation networks*, the challenge is to provide an improved level of security and privacy.[1]

2. For *use cases illustrating new features introduced in 5G,* e.g. support for Machine Type Communications (MTC) and Software Defined Networks (SDN), the challenge is to provide an appropriate level of security and privacy, as well as potential new security functionality illustrated by the use case.

In the first category of use case, the focus is on the vulnerabilities and potential counter measures addressing the identified security issues. In the second kind of use case the focus is on the additional security functionality needed to support the new features.

This process of generating use cases may hypothetically result in new desired 5G security features for which it is hard or even infeasible to provide solutions which are both cost-efficient and adequate. However, the purpose of this deliverable is neither to do risk analysis, nor to specify detailed solutions for which there are other activities within 5G-ENSURE (see Foreword). Hence, the resulting use cases should not be interpreted as functionality that unconditionally will be supported in 5G, but as an exploration of interesting relevant scenarios, and a starting point for further analysis.

This document is organised as follows: The remainder of Section 1 contains a glossary and a list of abbreviations of terms used. Section 2 provides a background on the use case clusters and how they are compiled. Sections 3 to 13 contain the actual use case clusters and the constituent use cases. Section 14 summarises the use case clusters and Section 15 provides the main conclusions derived from this use case compilation activity. References are provided at the end.

[1] This should not be understood as a statement that current networks are not secure, but rather that changes in the threat landscape warrants considerations of additional counter-measures.

1.1 5G-ENSURE

5G-ENSURE belongs to the 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.

1.2 Glossary

This section contains terminology for threat analysis used when discussing the vulnerabilities of the use cases. The terms are based on the Internet Security Glossary [RFC4949].

- Adversary
  - An entity that attacks a system.
- Attack
  - An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat.
- Counter-measure
  - An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- Deception
  - A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
- Disruption
  - A circumstance or event that interrupts or prevents the correct operation of system services and functions.
- Threat
  - A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.
  - Threats do not have to be linked to an *attacker*: a *vulnerability* combined with human error for instance can also lead to consequences such as *exposure*, *corruption* or *incapacitation*.
- Unauthorized disclosure
  - A circumstance or event whereby an entity gains access to information for which the entity is not authorized.
- Vulnerability
  - A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

1.3 Abbreviations

AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
B/OSS	Business and Operational Support Systems
CC	Content of Communication
CN	Core Network
EAP	Enhanced Authentication Protocol
eNB	Evolved Node B
EPC	Evolved Packet Core
ESIM	Embedded Subscriber Identity Module
GAN	Generic Access Network
GUTI	Globally Unique Temporary Identity
HN	Home Network
HSS	Home Subscriber Server
ID	Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LI	Lawful Interception
MME	Mobility Management Entity
mMTC	Massive Machine-Type Communication
MNO	Mobile Network Operator
NMS	Network Management System
PLMN	Public Land Mobile Network
SA	Security Association
SatAN	Satellite Access Network
SatNO	Satellite Network Operator
SDN	Software Defined Networks
SIM	Subscriber Identity Module
TA	Tracking Area
TAU	Tracking Area Update
UE	User Equipment
uMTC	Ultra-reliable and low-latency Machine-Type Communication
xMBB	Enhanced Mobile Broadband
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VMNO	Virtual Mobile Network Operator
VN	Visited Network

2 Background

The use cases described in this document were selected to illustrate security or privacy aspects relevant for 5G systems.

These use cases are based on input from external sources (e.g. other 5G-PPP projects, 3GPP New Services and Markets Technology Enablers (SMARTER) [TR22.891], publications of vulnerabilities and potential attacks on cellular networks, etc.) combined with the expertise and experience provided by the partners. The externally sourced dedicated 5G use cases turned out to be of limited direct applicability since most of these do not have sufficient security focus, see further discussion in Section 15.

The use cases are grouped into clusters according to topic, see Table 1. The cluster topics have been defined based on commonalities in the use cases in terms of provided security functionality or common technology. Each cluster contains the description of the actors involved in the described use cases, the actual use cases, and the "5G vision" – illustrating the security functionality which a 5G system is envisioned to encompass. The focus on the actors is motivated by their critical role in the upcoming trust modelling work in the project.

Each use case is structured as follows. First the pre-conditions are listed, illustrating the setting before the actual use case takes place. This is followed by a description containing the sequence of steps illustrating the use case. The step-by-step description is intended to pave the road for the upcoming threat and risk analysis in the project. Subsequently, there is optionally a short analysis of the use case in question, followed by an outline of security properties of a solution. Finally, the use case is classified in terms of relevant candidate security enablers in the project (see Section 1), and applicable next generation radio technology use cases: Enhanced Mobile Broadband (xMBB), Massive Machine-Type Communication (mMTC), Ultra-reliable and low-latency Machine-Type Communication (uMTC) [METIS2015]. These classifications are included to position the use case both within the 5G-ENSURE project and in the context of other 5G-PPP projects, and also to simplify the location of the use cases of relevance to the reader.

Table 1: Table of use cases and clusters

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

3 Cluster 1: Identity Management

3.1 Introduction

Cluster 1 contains four use cases describing various aspects of identity management in 5G networks.

In use case 1.1 we learn how to secure 5G connectivity and mobility of factory devices with pre-existing AAA credentials managed by the factory owner. Use case 1.2 demonstrates another way to gain 5G access, by establishment of SIM credentials to bootstrap enterprise employee credentials. Use case 1.3 elaborates on identities and authentication for roaming into a satellite network. Use case 1.4 describes an MNO providing an identity management service to a service provider on behalf of a user.

3.2 Actors

The actors in this cluster are:

- Mobile Network Operator (MNO)
- Mobile device users (Alice, Bob)
- Malicious party (Mallory)
- Factory Robot (Rob)
- Factory Owner (FO)
- Service Provider (SP)
- Satellite Network Operator (SatNO)

3.3 Use Cases

3.3.1 Use Case 1.1: Factory Device Identity Management for 5G Access

3.3.1.1 Introduction

Industry automation today uses proprietary radio access technologies, or non-3GPP technologies such as WLAN. New 5G radio accesses are foreseen to be designed to offer competitive advantages in terms of cost, quality of service, mobility, etc., that makes them attractive for industry automation. Thus, 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, assuming that the MNO can agree to such a configuration. This setting is also discussed in [TR22.891]. The factory owner installs 5G base stations in the factory but will rely on MNO to perform services such as IP connectivity and mobility.

The agreement between FO and MNO covers aspects such as charging policies, security policies and configuration data (e.g. certificates), liabilities of the parties, etc. It should be noted that such agreement would require a major change in the trust model compared to current roaming agreements, which today only exists between MNOs.

3.3.1.2 Preconditions

The preconditions are illustrated in Figure 1.

- The Factory has its own AAA server for robots.

- The MNO has a dedicated Industrial Automation Control (IAC) server to connect to the factory AAA server for AAA purposes. The IAC may comprise parts of MME functionality or an interface to the operator's MME. The full functionality and its realization, e.g. in terms of virtualization, is out of scope of the use case.
- 5G base stations owned and deployed in factory, but the factory has no other 5G network core equipment. The base stations use some spectrum allocated to the MNO.
- FO and MNO have an agreement allowing factory base stations to connect securely to the MNO core network over an interface we denote "S1" (see below) and allowing the factory's AAA server to connect securely to the MNO's IAC over an interface we denote "S6" (see also below) in order to establish network access credentials.
- "S1" denotes a presumed 3GPP reference interface between the Radio Access Network and Core Network (CN) handling e.g. authentication signalling between the IAC and UE via 5G base stations. The S1 interface is assumed to be secured by, for instance, IPsec Security Associations (SA) established using credentials which are part of the agreement between the FO and MNO.
- "S6" denotes a presumed 3GPP reference interface between the serving network (MNO IAC) and a subscriber data-base (a AAA-type server). The S6 interface is assumed to be secured by, for instance, IPsec SAs established using credentials which are part of the agreement between FO and MNO.

3.3.1.3 Description

When power is switched on, Rob, a factory robot, connects to the Factory Network using factory credentials as illustrated in Figure 1.

Basic flow of events:

1. Rob is powered up
2. Rob requests access to the factory 5G base station presenting a FO identifier
3. Rob is not yet authenticated and the base station contacts the IAC in the MNO CN over S1
4. The IAC recognizes, e.g. using name space analysis of the FO identifier, that Rob belongs to the factory and this IAC connects to the factory AAA over S6
5. The FO AAA provides, based on Rob's FO identifier, a temporary credential to the IAC which enables the IAC to authenticate Rob to this session
6. Mutual authentication, based on Rob's temporary credential, is performed between Rob and the MNO network. As a result, cryptographic keys are made available for the purpose of protecting the connection between the robot and the factory base station, and between the robot and the IAC
7. Rob is provided IP connectivity and mobility

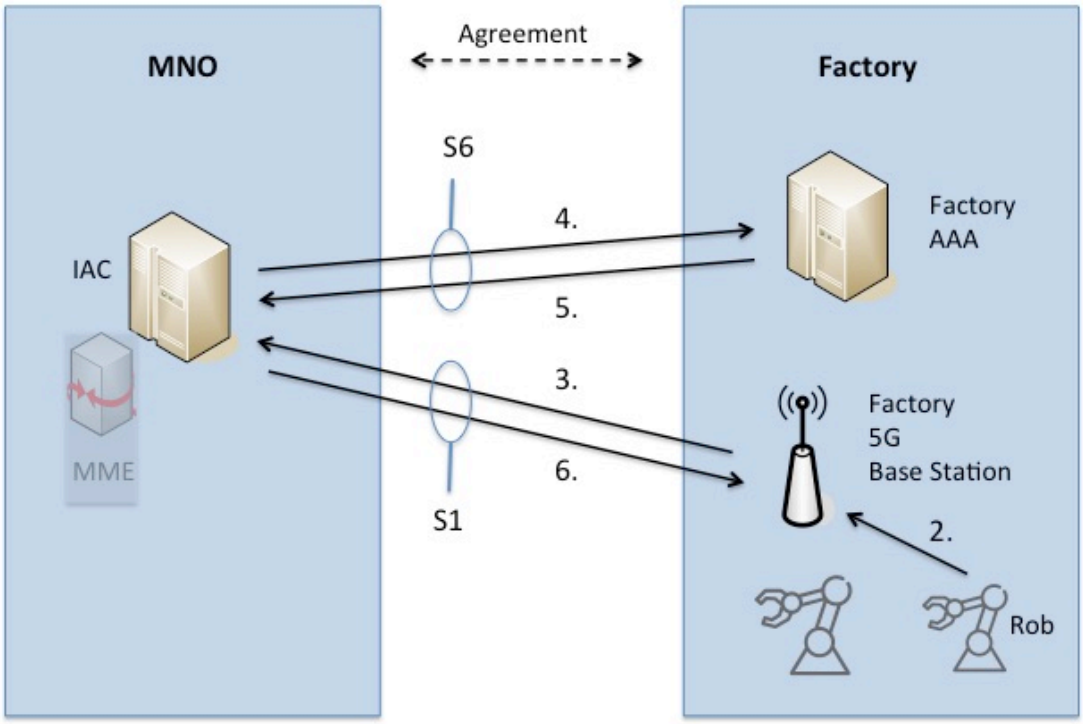

Figure 1: Factory 5G deployment

3.3.1.4 Properties of a solution

- Secure connections between factory and MNO, for example IPsec on S1 and S6, where the agreement between MNO and Factory should contain the credentials for establishing IPsec.
- EAP-based authentication to factory AAA. Which EAP methods to be allowed could be specified in the agreement between MNO and Factory, but weak methods such as passwords will most likely not be allowed in any such agreement.
- The 5G authentication procedure can be designed to be compatible with whatever factory credentials that are used.
- The MNO never distributes the customer's credentials (whether MNO related or FO related) to any third party
- A candidate solution is using an MNO implementation of GBA [TS33.220]

3.3.1.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC

3.3.2 Use Case 1.2: Using Enterprise Identity Management for Bootstrapping 5G Access

3.3.2.1 Introduction

The enterprise wants to provide its employees' devices with 5G connectivity to use in the office or when being mobile. Since the enterprise in any case needs to manage the employees' credentials it is convenient

to use these credentials to bootstrap 5G credentials used for connectivity. However, the enterprise does not want to manage an HSS. The enterprise and MNO sign an agreement that the employee devices can become provisioned with 5G credentials, assuming that the MNO can agree to such a configuration. The enterprise may extend coverage and capacity of the 5G network by installing additional (e.g. indoor) 5G base stations, but this is not necessary if the existing 5G access suffices.

It should be noted that this kind of agreement would require a change in the trust model compared to current subscription provisioning models.

3.3.2.2 Preconditions

- MNO has its own IAC to cover industry needs
- The enterprise has its own AAA for the employees.
- Bob, an enterprise employee, has a UE (e.g. mobile phone, laptop, etc.) which is provisioned with enterprise keys.
- The enterprise and MNO have made an agreement allowing subscription parameters associated with new employees to be stored in the MNO IAC. The MNO IAC generates these credentials by request from the enterprise AAA. The credentials could for example be (U)SIM-compatible parameters to be used with the Authentication and Key Agreement (AKA) protocol. The agreement covers aspects such as how to secure the credential provisioning, charging policies, liabilities of the parties, etc. To this end, the MNO and enterprise are assumed to have made a risk assessment that the enterprise AAA is sufficiently secure, and has an acceptable risk level, when entering into the agreement.
- After being authenticated and authorized by the AAA, Bob's UE is being provisioned from MNO IAC with credentials for establishing a 5G session. The credentials are protected in transport between MNO IAC and Bob's UE based on the enterprise AAA.

3.3.2.3 Description

Bob, an enterprise employee, switches on his UE which attaches to the MNO base station and authenticates to the network. This authentication procedure may be different depending on how/what credential that was provisioned. The flow is depicted in Figure 2.

Basic flow of events:

1. Bob requests 5G credentials from the Enterprise AAA. The request is authenticated using Bob's enterprise keys.
2. The Enterprise AAA requests to the MNO IAC provisioning of 5G session credentials
3. Bob's UE is securely provisioned with (U)SIM-type credentials from the MNO IAC based on the employee AAA credential
4. Bob's UE authenticates to the 5G network
5. Bob's UE is ready to use

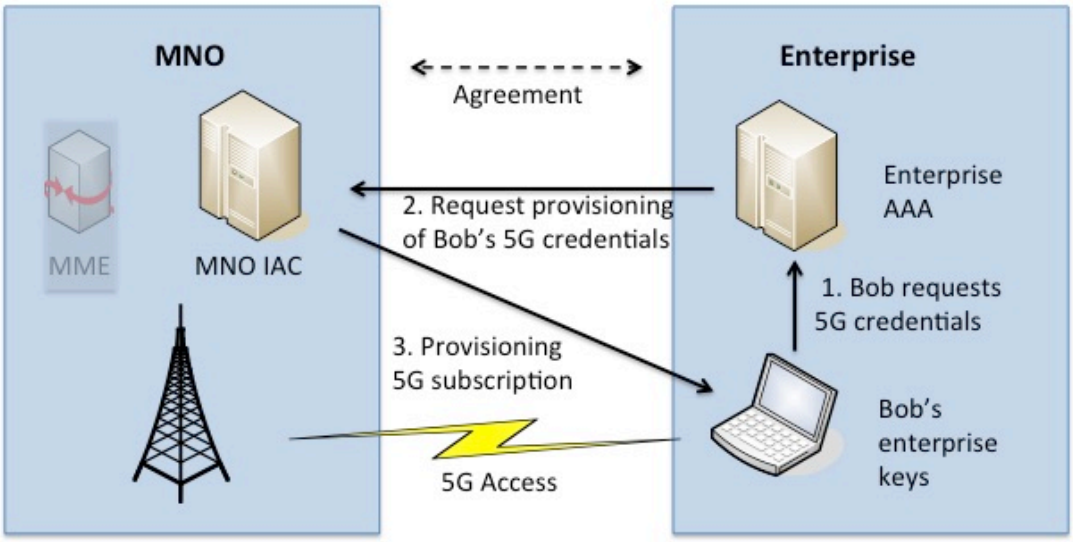

Figure 2: Enterprise 5G deployment

Alternative flow of events:

In this flow, instead of (U)SIM-type credentials, some non-SIM credential of sufficient strength is assumed, under the condition where the secure storage and use of those credentials in Bob Device has been qualified by the MNO as sufficient in term of secure storage, assurance etc. in relation to existing USIM card, and could be controlled by MNO. In particular the security level of this storage should prevent credential cloning. A protocol such as e.g. EAP may be used to carry the authentication signalling.

1. Bob's UE been provisioned with non-SIM type credentials via the MNO IAC
2. Bob's UE authenticates to the 5G network using the credentials, e.g. by means of EAP
3. Bob's UE is ready to use

3.3.2.4 Properties of a solution

- ESIM provisioning initiated by enterprise network
- EAP based authentication to enterprise AAA
- In the first flow, no new credentials need to be supported by the 5G authentication protocol

3.3.2.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB

3.3.3 Use Case 1.3: Satellite Identity Management for 5G Access

3.3.3.1 Introduction

This use case explores two identity-management situations involving satellite networks and a dual satellite and terrestrial 5G access: one in which the 5G device attaches to the satellite network; the other one in which the 5G device identifies in either the satellite network or the terrestrial network, and then due to coverage issues the 5G device performs a roaming to the other network.

3.3.3.2 Preconditions

- SatNO has its own AAA for its subscribers.
- SatNO and MNO has a roaming agreement allowing each other's users to roam in the other's network.

3.3.3.3 Description

Bob switches on his dual satellite and terrestrial 5G UE with a set of credentials that allows access to both networks, and is initially connected to the satellite network (see Figure 3). Due to coverage issues he may need to roam between the networks (see Figure 4).

Please note that AAA Servers depicted in Figure 3 and Figure 4 are depicted separately for logical reasons, but their physical location might be the same – they can physically even be one single AAA Server.

Basic flow of events:

1. Bob's UE, located for instance in a moving truck in an isolated area, can only offer Bob connectivity through satellite when he turns on the UE.
2. Bob chooses to connect the UE through satellite, and the authentication and authorization process is performed between the UE and the satellite AAA Server and between the satellite AAA Server and the 5G AAA Server.

The fine-grained access policies at 5G AAA Server process the authentication request from Bob's UE and establishes that, for the credentials provided, access can be granted to the UE into the satellite network, with an authorization level A (which may consist for example of certain peak data rate, certain sustained data rate, certain services enabled, etc.).

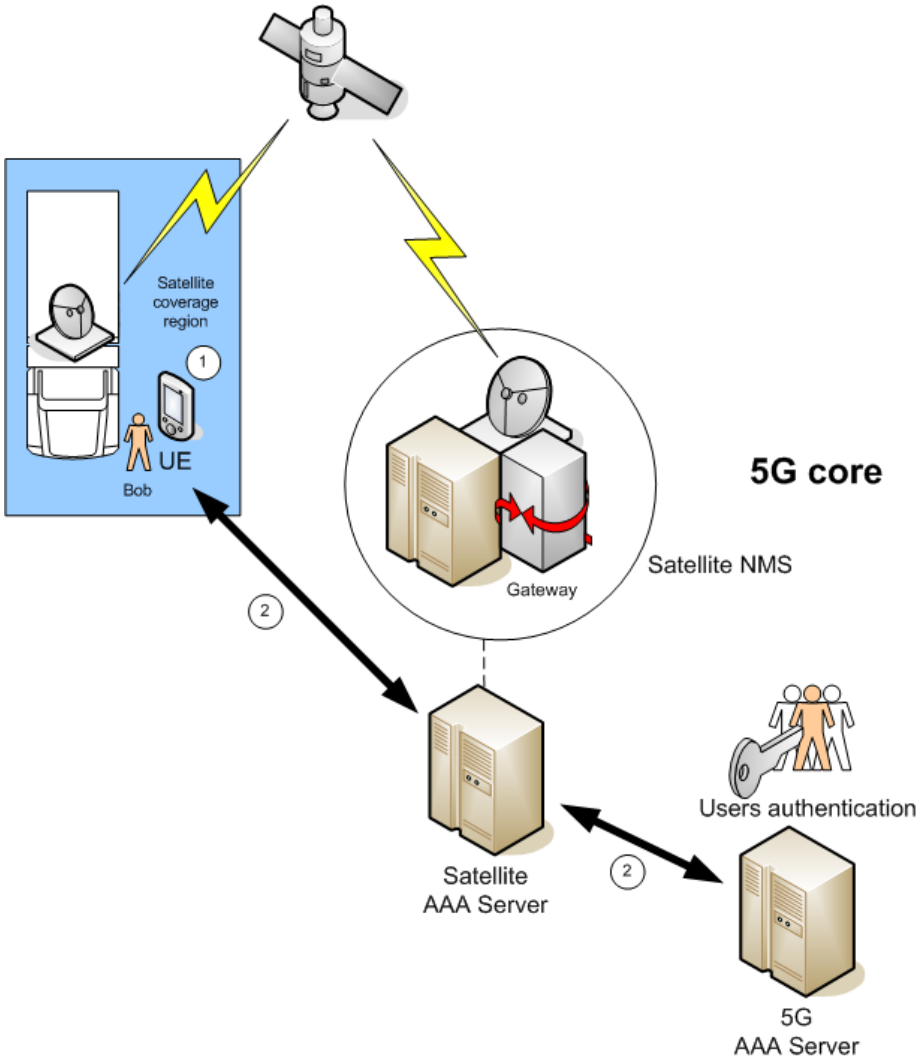

Figure 3: Integration of AAA system mechanisms in 5G device with satellite coverage

Alternative flow of events:

The events can be seen as an extension of the basic flow in which the roaming aspect is incorporated.

1. Bob's UE, located for instance in a moving truck in an isolated area, can only offer Bob connectivity through satellite when he turns on the UE.
2. Bob chooses to connect the UE through satellite, and the authentication and authorization process is performed between the UE and the satellite AAA Server and between the satellite AAA Server and the 5G AAA Server
3. Bob parks and takes his UE inside a building under terrestrial coverage compliant with UE terrestrial connectivity
4. The UE detaches from the satellite network and automatically tries to attach to the terrestrial network using the relevant credentials.
5. The credentials are roamed from 5G AAA Server to Terrestrial AAA Server and Terrestrial network authorizes Bob's UE. At this point the 5G device has regained connectivity after a roaming process that has been virtually seamless to Bob.

As explained in the basic flow of events, the fine-grained access policies at the 5G AAA Server process the authentication request from Bob's UE and establishes that, for the credentials provided, access can be granted to the UE into the satellite network, with an authorization level A (which may consist for example of certain peak data rate, certain sustained data rate, certain services enabled, etc.).

Now, during the roaming process, a roaming request from the Terrestrial AAA Server arrives at the 5G AAA Server, which process the authentication credentials from Bob's UE (given by the Satellite AAA Server) and establishes that, for the credentials provided, access can be granted to the UE into the terrestrial network, with an authorization level B (which may consist for example of certain peak data rate, certain sustained data rate, certain services enabled, etc.).

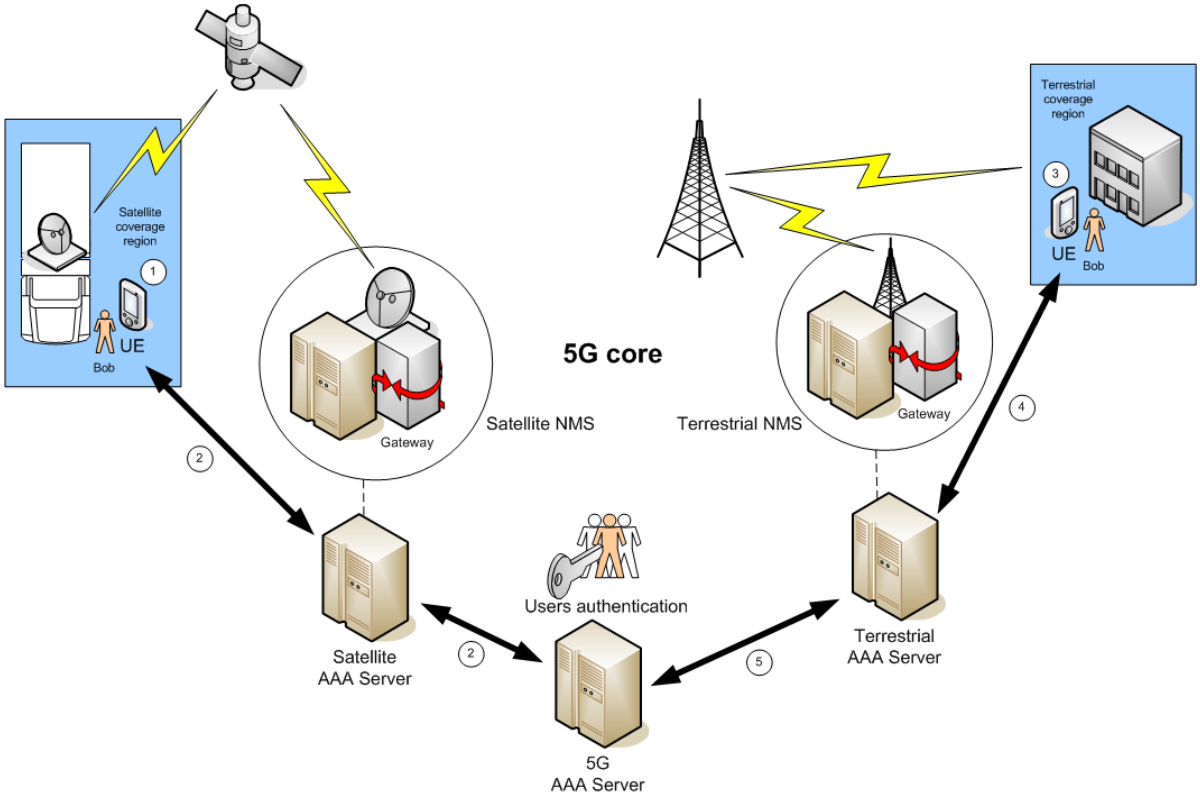

Figure 4: Integration of AAA system mechanisms with 5G roaming from satellite to terrestrial networks

3.3.3.4 Properties of a solution

- (U)SIM-type credentials for satellite access may be one approach to allowing roaming from terrestrial network into satellite network, e.g. using EAP-AKA authentication [EAP-AKA].

3.3.3.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

3.3.4 Use Case 1.4: MNO Identity Management Service

3.3.4.1 Introduction

This use case describes an MNO providing an identity management service to a 3rd party service provider on behalf of a user.

3.3.4.2 Preconditions

- User Bob is a subscriber of an MNO
- The MNO associates to Bob a "Network ID" (e.g., a mobile phone number to Bob's UE)
- Bob uses a service, S, provided by a 3rd party service provider SP (e.g. a bank)
- Bob subscribes to a customised service, S, provided by a 3rd party service provider SP (e.g., a bank) based on some information that can be provided by the MNO. The service agreements (between the user Bob and MNO and SP, respectively) detail what information can be collected by the MNO, what information can be shared with the SP, the deactivation of this option, etc.
- The service provider assigns to Bob a local identity (i.e. an identity associated to this service such as a bank account number)
- The service local identity of Bob encompasses some attributes related to his "Network ID"

3.3.4.3 Description

For the sake of concreteness, we consider a banking service example, see Figure 5.

Bob would like to access some resources associated to his bank account, e.g., perform a transfer of money, change his secret code, etc. The bank requests the operator information with respect to Bob such as Bob's access network type, Bob's equipment, used authentication scheme, location, and so forth. Depending on the provided information, the bank adjusts its security policy. The bank may for example ask Bob for further (second factor) authentication or modify the way to deliver the service.

As a consequence, the bank will manage to have the same security level when delivering a service, e.g. if the user is connected via a public hotspot then perhaps additional authentication and protected communication is needed. This is owing to dynamic security policies that are based on information provided by the MNO.

Basic flow of events:

1. Bob's UE is authenticated to the MNO
2. Bob's UE requests access to a service at a service provider (Step (a) in Figure 5)
3. Upon request, the operator collects information about Bob (and/or his UE) and shares it with the service provider according to the terms of the service S (Steps (b), (c) and (d) in Figure 5)
4. The service provider authorizes or personalizes a service to Bob based on the received information (Steps (e) and (f))

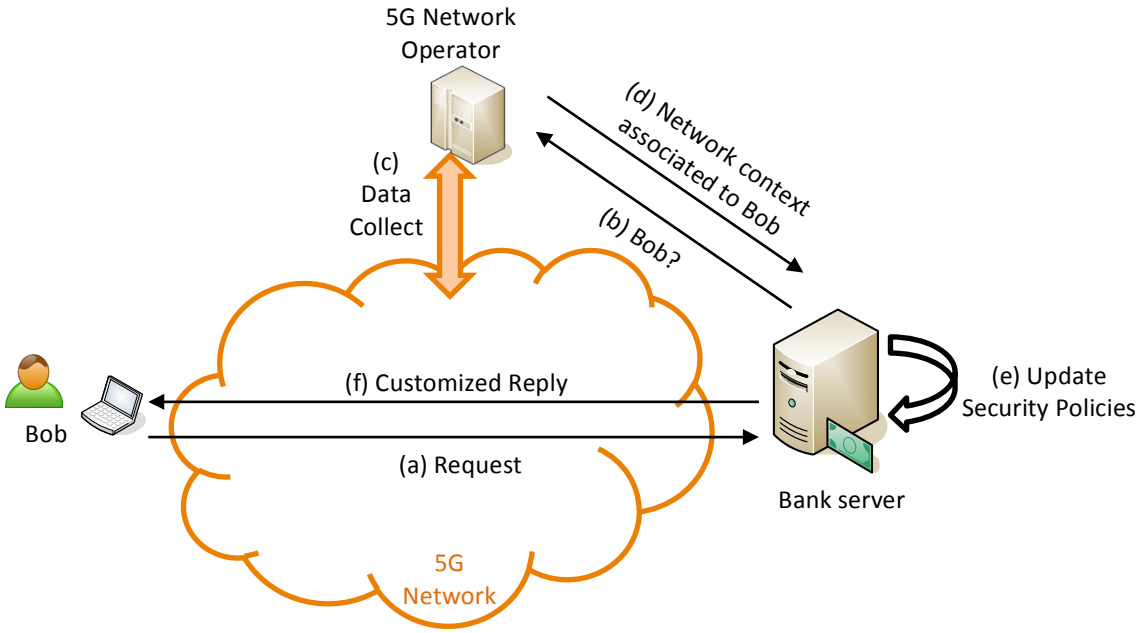

Figure 5: 5G Network Operator as Trust Provider

3.3.4.4 Properties of a solution

- Use of suitable (secure) attribute sharing mechanism.

3.3.4.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB

3.4 5G Vision

5G provides a variety of identity management services which expands the capabilities of devices and networks beyond the legacy UE to RAN service. A device provisioned with appropriate credentials can get 5G access in a flexible way driving down cost in large scale deployments. New subscribers or machines can be enrolled in 5G networks, using their pre-existing identity management schemes, while respecting their privacy. This attracts new categories of users to the 5G ecosystem.

5G identity management provides for better integration between cellular and satellite networks, including roaming. 5G AAA Servers include specific intelligence to confer an authorization level suited to the authentication credentials for a particular access network, in particular they assign the authorization level seamlessly to the end user during the roaming between two access networks. Moreover, the 5G AAA Servers in satellite networks offer ultra-fast logins with optimized data exchange in order to lower the latency and maximize the spectral efficiency. Finally, 5G AAA Servers are capable of supporting hundreds of thousands of simultaneous logins, in compliance with the requirements imposed by 5G.

An MNO can offer identity management services such as trusted assertions and secure identifiers of subscribers, while respecting the agreed upon privacy policy.

4 Cluster 2: Enhanced Identity Protection and Authentication

4.1 Introduction

These use-cases address the area of enhancements to identity protection and authentication in 5G compared to existing 3G and 4G networks. Specifically they focus on three use-cases, the first of which tackles privacy for device identifiers which need to be appropriately protected and/or anonymised. The second use-case addresses the area of subscriber identity privacy which also needs to be suitably protected and/or anonymised, particularly when traversing access networks. The final use-case tackles the provision of perfect forward secrecy to combat the threat of passive attacks, particularly in the case of subscriber key compromise.

4.2 Actors

The actors in this cluster are:

- User (Alice)
- Alice's UE (UE)
- Malicious user (Mallory)
- Mobile Network Operator (MNO)

4.3 Use Cases

4.3.1 Use Case 2.1: Device Identity Privacy

4.3.1.1 Preconditions

- Alice's UE is switched on

4.3.1.2 Description

Alice's UE connects to the mobile network and wants the identity of her UE to be private.

Basic flow of events:

1. Alice's UE connects to the 5G network over the Air Interface or via Generic Access Network (GAN)
2. Alice's UE authenticates to the 5G network using (U)SIM credentials
3. Alice's UE responds to the MME's request for the International Mobile Equipment Identity (IMEI) of her UE, and request validation
4. Alice's UE is ready to use

Alternative flow of events:

1. Alice's UE connects to the 5G network over the Air Interface or via Generic Access Network (GAN) with an Attach Type "Emergency"
2. Alice's UE includes the IMEI in plain text in the Attach request during an emergency call situation, where it does not have a valid Globally Unique Temporary Identity (GUTI) or International Mobile Subscriber Identity (IMSI)
3. If the network is configured to support emergency services, Alice's UE gets emergency bearer allocated

4.3.1.3 Vulnerabilities and consequences

- Users do not want to be tracked via their UE identifiers
- Certain user groups do not want their subscriber identity and their device's identity linked

4.3.1.4 Properties of a solution

The solution space includes exploration of protocol enhancements and investigation into state-of-the art end-to-end anonymization techniques, offering protection against device identity disclosure and unauthorized device tracking. As with LTE, 5G should ensure that the IMEI is sent only in a confidentiality-protected message, as opposed to GSM and UMTS, where the network, and hence an attacker, may request delivery of the IMEI in the clear. In addition the enhancement aims to also address the emergency call case where the IMEI is sent over the network unprotected, since a security context cannot be created and used to provide for confidentiality.

4.3.1.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

4.3.2 Use Case 2.2: Subscriber Identity Privacy

4.3.2.1 Preconditions

- Alice's UE is switched on.
- Mallory sets up a fake Base Station (for active attacks) or monitoring (for passive listening of transmissions of legitimate base station).

4.3.2.2 Description

Alice's UE connects to the mobile network and wants her subscriber identity and location to remain private.

Basic flow of events:

1. Alice's UE connects to the 5G network, identified by her GUTI/IMSI
2. Mallory observes GUTI/IMSI, or elicits Alice's IMSI, and can track Alice's UE
3. Alice's UE authenticates to the 5G network using the SIM credentials
4. Alice's UE is ready to use
5. Mallory tracks Alice's current location by triggering the mobile network into initiating the generation of paging messages to Alice's UE (e.g. by using social media application to initiate unobtrusive communications)
6. Mallory observes the paging messages sent and can potentially correlate the contained GUTI with Alice's social network identity

Alternative flow of events:

1. Alice's UE connects to the 5G network, identified by her GUTI/IMSI
2. Mallory observes GUTI/IMSI, or elicits her IMSI, and can track her
3. Alice's UE authenticates to the 5G network using the SIM credentials
4. Alice's UE is ready to use

5. Mallory forces Alice's UE to connect to Mallory's rogue eNB by exploiting the feature "*absolute priority based cell reselection"*
6. Mallory initiates a "*RRC Connection Reconfiguration"* message
7. Alice's UE responds with a *"Measurement report"* and the GPS coordinates of her UE, if her UE supports the *"locationInfo-r10"* feature
8. Mallory is able to determine Alice's location by trilateration, or the supplied GPS coordinates

4.3.2.3 Vulnerabilities and consequences

- The subscriber's identifier or temporary identifiers allows for tracking of a user
- Temporary identifiers (pseudonyms like GUTI or TMSI) are broadcasted in clear text so that Alice's UE can identify targeted communications. If such identifiers are not changed (re-pseudonymized) before Mallory is able determine which belongs to Alice, Alice's location can be tracked
- Broadcasting a GUTI, 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. However, location tracking based upon tracking identifiers alone does not always provide a precise location for Alice. Alice may be in different location to her UE, or her UE's communication may be relayed, at the physical layer, to another location
- Users do not want their subscriber identity and their device's identity linked
- The current standards allow measurement reports to be sent without security, which enables Mallory to retrieve the reports to determine the location of Alice's UE [Shaik2015]

4.3.2.4 Properties of a solution

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.

4.3.2.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

4.3.3 Use Case 2.3: Enhanced Communication Privacy

4.3.3.1 Preconditions

- Alice's UE is switched on
- Mallory has a 5G access network monitor and is in possession of Alice's user-specific key, K

4.3.3.2 Description

Alice's UE connects to the mobile network and wants her communications to be private to passive monitoring, despite compromise of her user-specific key. The assumption that Mallory has obtained K is normally an extremely unlikely event. Nevertheless claims of such situations arising have occurred [SchahillBegley2015].

Basic flow of events:

1. Alice's UE connects to the 5G network

2. Alice's UE authenticates to the 5G network using the (U)SIM credentials
3. Mallory observes the authentication and derives the session keys (CK, IK), using Alice's key, K
4. Alice's UE is ready to use

4.3.3.3 Vulnerabilities and consequences

- Users' communications may be decrypted through passive monitoring of access network traffic
- Users may be impersonated

4.3.3.4 Properties of a solution

A potential solution would be to introduce mechanisms to provide for perfect forward secrecy of the communications. Thus only an active attacker could ascertain the session keys in the event of a user-specific key compromise.

4.3.3.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

4.4 5G Vision

It is essential that users have control over the privacy of their subscriber and device identifiers in 5G and have even higher assurance that privacy of their communications are upheld. The pervasive nature of 5G means there will be many more deployment options for devices. Thus users want to have wider scope and control over their subscriber and device identities, and to ensure that communications are secured against wider threats. 5G networks should guarantee user privacy by providing security properties including confidentiality to subscriber and device identities, untrackability of the user location, perfect forward secrecy for encrypted communications and unlinkability between the user subscription information and the device identity.

5 Cluster 3: IoT Device Authentication and Key Management

5.1 Introduction

This use case cluster focuses on IoT device authentication and key management and it includes two use cases: “Authentication of IoT devices in 5G” and “Network-based key management for end-to-end security”.

The first use case focuses on authentication of constrained IoT devices [RFC7228] which might not have direct access to the 5G network or might benefit from group-based authentication, where massive groups of IoT devices are authenticated simultaneously. The group is defined by one or more attributes, such as the device location, type of device or type of application, etc. Thus, group-based authentication consists of a set of protocols that allows members of the group to be authenticated.

The second use case focuses on network-based key management where the network provides a service for key exchange to be used for secured end-to-end communication.

5.2 Actors

The actors in this cluster are:

- 5G Network Operator (MNO)
- Mobile device user (Bob)
- AAA Server in 5G network
- Key management service in 5G network
- IoT device 1 (Sensor1)
- IoT device N (SensorN)
- IoT gateway
- IoT backend service (operated by Alice)

5.3 Use Cases

5.3.1 Use Case 3.1: Authentication of IoT Devices in 5G

5.3.1.1 Preconditions

- Mobile device user and IoT gateway have 5G credentials
- A large number of IoT devices (Sensor1, SensorN) require access to services/Internet
- IoT devices (Sensor1 and SensorN) may not be able to access services/Internet by themselves

5.3.1.2 Description

The group of IoT devices (Sensor1, SensorN) are constrained devices with different network access and security technologies and may need access services/Internet, which are reachable by means of a 5G network. The IoT devices can be grouped into two categories: IoT devices with an onboard radio interface, hence are capable of radio signalling with the 5G network; and IoT devices without 5G radio access, but with other communication technologies, e.g. WiFi or Bluetooth, therefore requiring an IoT Gateway that provides the 5G connectivity. The presence of the IoT gateway may potentially obstruct the possibility to

robustly identify individual devices at the application layer. While a group identity may of course be used (e.g. related to IMSI), this use case seeks to enable more robust identification also of individual devices by leveraging the strong security of the SIM credentials.

Existing authentication protocols, e.g. LTE-AKA, might not be suitable to efficiently support the expected number of authentication requests generated by the boom of connected IoT devices. This might result in unwanted latencies when numerous devices in the same group initiates simultaneous authentication requests. This is especially important in highly mobile devices due to the many requests of authentication vectors to the home network. A solution to this can be group-based authentication, in which overhead may be reduced as each device of a given group does not have to execute the complete authentication protocol [Chengzhe2013].

Additionally, a third scenario is that the network broadcasts a session request to a group of devices, on behalf of a user or service. One of the group members will authenticate with the 5G network, presenting its unique identity, and its group identity [TS22.368]

Basic flow of events:

1. The IoT gateway authenticates to the AAA server, or the mobile device (Bob) authenticates to the AAA server, using USIM AKA. Thus, the 5G subscriber's identity, i.e. IMSI, is ensured and can be collected by the network.
2. The IoT Sensor (Sensor1, SensorN) authenticates to the IoT gateway or to the mobile devices using radio access specific technology. The IoT sensors and the connected IoT gateway or mobile devices are owned by the same subscriber.
3. The IoT sensors have access to services/Internet and are able to send and receive data, either via Bob's device or via the IoT gateway. In their request to services they might reuse the 5G subscriber's identity.

Alternative flow of events:

1. The IoT gateway authenticates to the AAA server, or the mobile device (Bob) authenticates to the AAA server, using USIM AKA. Thus, the 5G subscriber's identity, i.e. IMSI, is ensured and can be collected by the network.
2. The IoT Sensor (Sensor1, SensorN) authenticates to the AAA server, by assistance of the IoT gateway or the mobile device (Bob), to establish itself as a point of presence in the 5G network to enable a service differentiation on a network level, e.g. different QoS classes. The IoT sensors will be uniquely identified in the network in addition to the IoT gateway or mobile device (Bob). All involved equipment are owned by the same subscriber.
3. The IoT sensors have access to services/Internet and are able to send and receive data directly, either via Bob's device or via the IoT gateway.

Alternative flow of events:

1. The IoT devices dynamically form groups according to their similarity (type of device, location, application). The IoT devices have the necessary credentials to authenticate with the AAA server.

2. Group-based authentication is performed for a group of IoT devices with the AAA server authenticating a group of devices simultaneously.

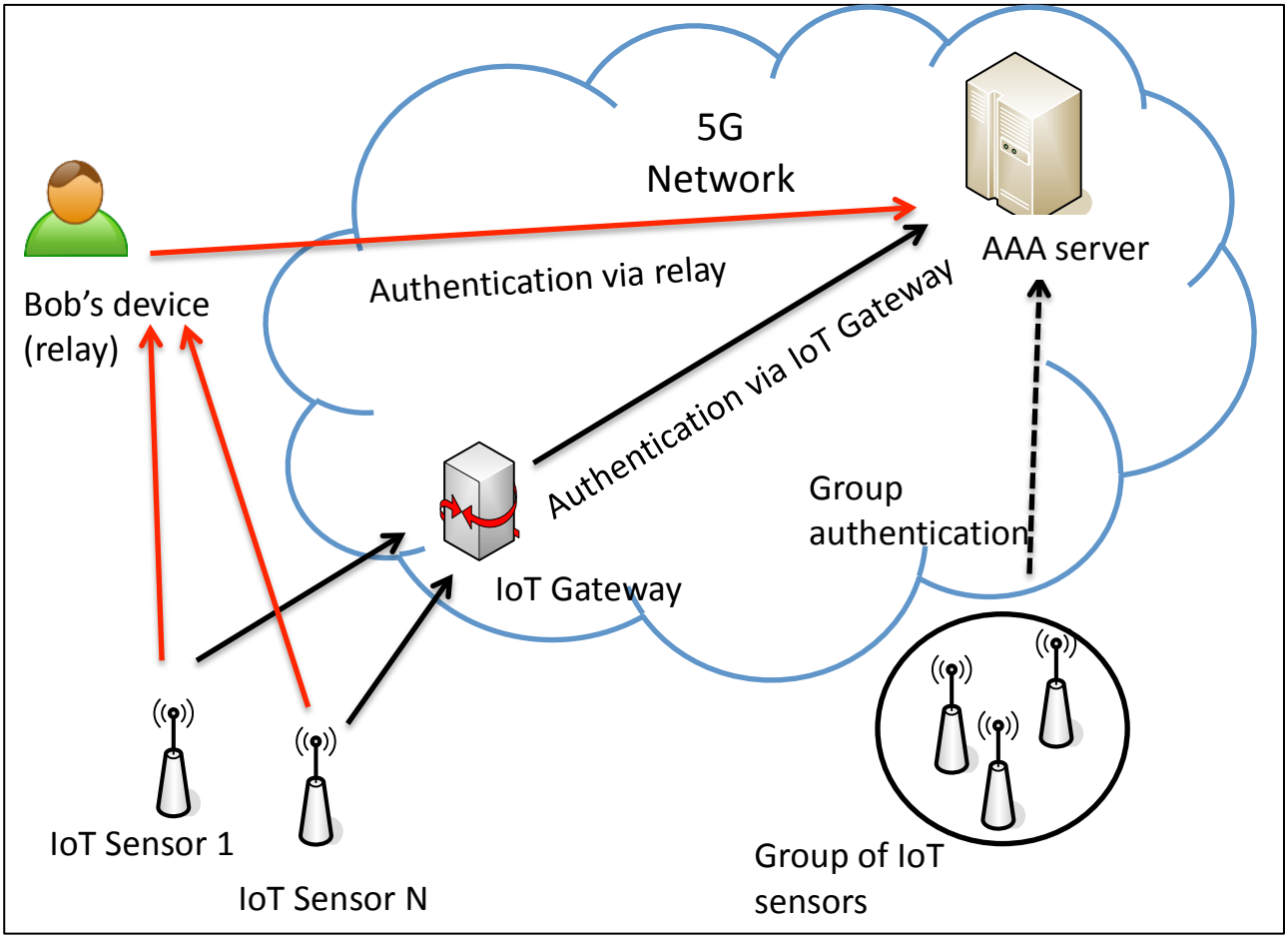

Figure 6: Authentication of IoT/M2M devices in 5G

5.3.1.3 Vulnerabilities and consequences

The security threats could be related to a man-in-the-middle taking part into the bootstrapping procedure. A specific security threat related to the alternative flow could be related to a malicious IoT device which is grouped with other IoT devices and is authenticated together with other IoT devices. In addition, the constrained nature of IoT devices might make it easier to subvert the security of these devices (e.g., they don't have enough processing power to use stronger algorithms).

5.3.1.4 Properties of a solution

5G User Equipment (Bob's mobile device or IoT gateway) may act as a 5G bootstrapping device for a number of constrained devices, sensors, and actuators that are not able to access the 5G network themselves.

Group based authentication, where IoT devices can form a group based on physical location, type of sensor/actuator, type of application, or other similarity factor, IoT gateway or mobile device acting as a relay could perform simultaneous authentication for group of devices. In a group based authentication scenario, the AAA overhead will be greatly reduced as each device does not have to execute the complete protocol.

5.3.1.5 Use case categories

Ensure Enablers	AAA
Next Generation Radio Technology Usecases	mMTC, uMTC

5.3.2 Use Case 3.2: Network-Based Key Management for End-to-End Security

5.3.2.1 Preconditions

- IoT devices (endpoints) have 5G credentials
- IoT backend service (endpoint) operated by Alice has 5G credentials
- 5G network provides network-enabled key management service
- The key management service can authenticate actors with 5G credentials using the AAA server in 5G network
- Alice is able to provide policies for the key management service to control which endpoints can share keys

5.3.2.2 Description

An IoT device is connected to 5G network and authenticated to use the network. The IoT device needs to communicate with the backend service (operated by Alice). 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 connected IoT device utilizes a network-enabled key management service provided by 5G network to achieve secure end-to-end communication between the device and the IoT backend service located, e.g., in the cloud.

Basic flow of events:

1. The IoT service is connected to the key management service and authenticated
2. Alice (operating IoT service) provides policies controlling which IoT devices may share a key with the IoT service
3. IoT device is connected to 5G network and authenticated
4. IoT device negotiates security keys for data encryption using the key management service provided by 5G network
5. IoT device encrypts and authenticates data to be transmitted using keys provided by the network and starts sending the data to the IoT server
6. The IoT server decrypts and verifies received data using the key negotiated with the key management service

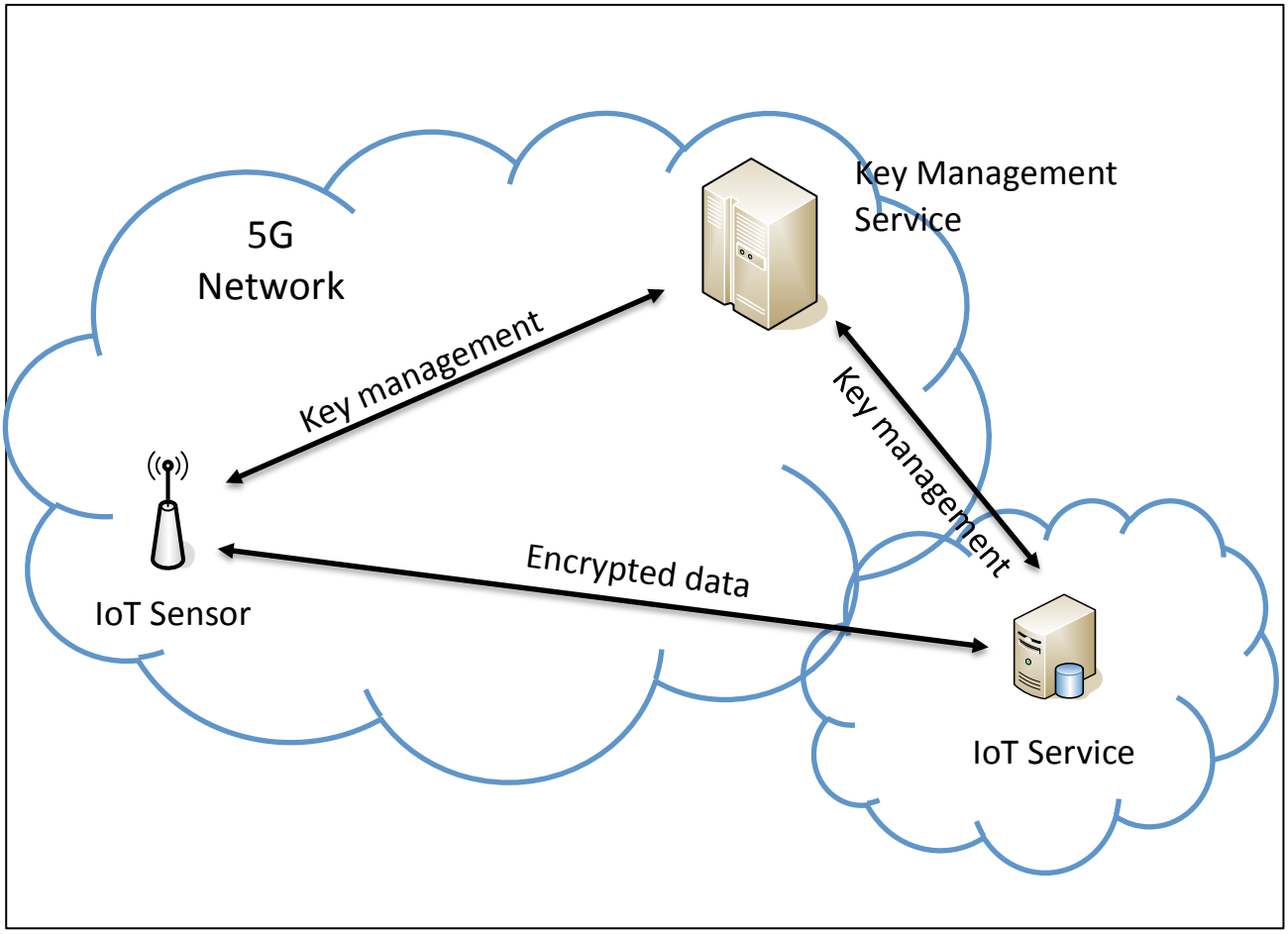

Figure 7: Network-based key management for end-to-end security

5.3.2.3 Vulnerabilities and consequences

Missing end-to-end security leaves communication vulnerable for compromised or malicious network components. End-to-end security, where keys are managed by the services/devices themselves, prevents lawful interception and may waste resources as operators' may still secure core network communication with their own mechanisms.

The key management solution provided by 5G operators is suitable for cases where the end-points trust the operator and operator's capabilities (e.g. to provide truly random keys which do not leak to adversaries). In highly critical applications such trust assumptions may not always be justified. Availability of end-to-end connections may in these cases achieved by replacing the key management that is provided by a 5G operator with a more trusted alternative.

5.3.2.4 Properties of a solution

Network-enabled key management available in 5G enables communication to be encrypted and authenticated from end to end. The connected device can utilize network-enabled key management provided by 5G network to achieve secure end-to-end communication between the device and the service located e.g. in the cloud. By providing network-enabled key management, 5G network can provide secure communication and at the same time enable lawful interception.

The key management service may provide both device specific key for unicast communication as well as group specific keys for multicast communication.

The solution may be linked to service/device discovery. An IoT device is not required to provide any configuration interfaces that would enable its owner to input configuration data such as the address of the remote IoT service. A device that has been bought directly from a shop may e.g. have only an interface to insert 5G credentials (like USIM card). Alice may provide this configuration through the 5G mobile operator (key management service) who forwards the configuration information alongside with the keys for the authenticated and authorized devices. Authentication (or SLA) between key management service (provided by an operator or third party) and devices/services utilising the key management service is needed before the actual key exchange.

In terms of LI, the solution proposed should be transparent, which means that 5G Network operators should be able to support interception without the need of Key Management Server (in case it is operated by third party to be involved). This point is related to country sovereignty.

5.3.2.5 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC

5.4 5G Vision

5G should support group-based authentication, where IoT devices can form a group based on the similarity (location, type of sensor/actuator, application, …) to reduce AAA overhead where each device does not have to execute the complete AAA protocol. 5G should also be able to serve IoT devices behind a relay/gateway securely even when IoT devices do not have direct access to 5G network.

5G networks should also provide a security enabler for the key management which enables communication to be encrypted and authenticated from end to end. The connected device can utilize network-enabled key management provided by 5G network to achieve secure end-to-end communication between the device and the service located, e.g., in the cloud. By providing network-enabled key management, 5G network can provide secure communication and at the same time comply with the lawful interception requirements.

6 Cluster 4: Authorization of Device-to-Device Interactions

6.1 Introduction

This cluster contains three use cases about authorization of device-to-device interactions: the first use case considers the authorization in resource-constrained devices [RFC7744] by means of token based on 5G credentials; the second use case considers the authorization by a 5G operator of direct IP connections; the last use case considers authorization in vehicle-to-everything communications.

6.2 Actors

The actors in this cluster are:

- User (Alice)
- Sensors' Owner
- Sensors' Owner's AAA Server
- Sensor1
- Sensor2
- 5G operator
- Vehicle1 (Ann)
- Vehicle2 (Bob)
- Pedestrian (Charlie)
- Vehicle Manufacturer

6.3 Use Cases

6.3.1 Use Case 4.1: Authorization in Resource-Constrained Devices Supported by 5G Network

6.3.1.1 Preconditions

- Every actor holds 5G credentials
- The AAA Server can authenticate users with 5G credentials
- The AAA Server maintains a database that stores access rights to the sensors.

6.3.1.2 Description

Sensor1 and Sensor2 are resource-constrained devices [RFC7228] that want to outsource authorization services to a AAA Server. Thus, the AAA Server should support an interface that allows the sensors' owner to issue security policies via the 5G network. Also, the AAA Server should support an interface to issue authorization tokens based on the 5G credentials (see Figure 8).

Basic flow of events:

1. The sensors' owner issues security policies to the AAA Server concerning access to its sensors.
2. Alice authenticates to the AAA Server and requires access to the sensors.
3. The AAA Server issues an authorization token based on 5G credentials of Alice according to the security policies.
4. Alice has access to the sensor(s) using her token and 5G credentials.

6.3.1.3 *Vulnerabilities and Consequences*

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).

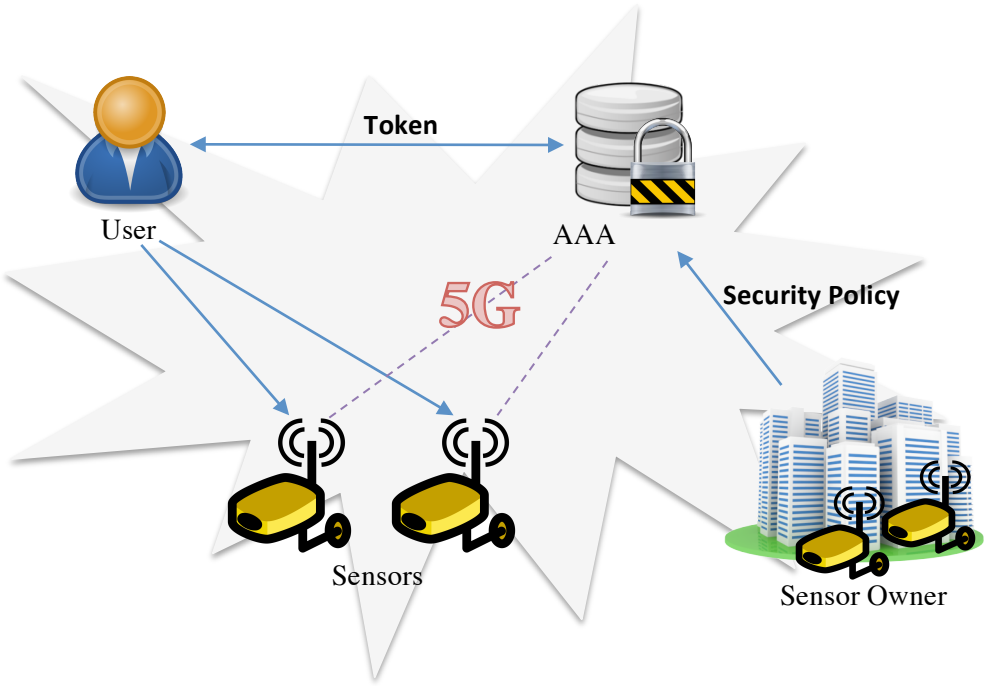

Figure 8: Setting for Authorization in Resource-Constrained Devices

6.3.1.4 *Properties of a solution*

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.).

6.3.1.5 *Use case categories*

Ensure Enablers	AAA
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

6.3.2 Use Case 4.2: Authorization for End-to-End IP Connections

6.3.2.1 *Preconditions*

- Alice and Sensor1 hold 5G credentials

- 5G operator can authenticate both Alice and Sensor1
- Sensor1 is able to perform access control

6.3.2.2 Description

Alice wants to access the data provided by Sensor1, hence she wants to build end-to-end IP connections through the 5G network. The 5G operator should be able to authorize such connections.

Basic flow of events:

1. Alice and Sensor1 are authenticated by the 5G network and configured to the same 5G slice
2. Alice bootstraps a direct IP connection with Sensor1 via 5G network
3. The 5G operator authorizes the direct IP connection
4. Sensor1 sends its data through the established secure direct IP connection

6.3.2.3 Vulnerabilities and Consequences

One potential vulnerability appears if the solution would allow a direct IP connection without authorization. In other words, a malicious user might then establish such a connection even though the 5G operator should have blocked it.

6.3.2.4 Properties of a solution

To prohibit unauthorized access and illicit traffic, using the direct IP connect, the 5G network may require that direct connections must first be authorized by the network, or use an IP whitelist, combined with a services whitelist. The 5G operator might also do a layer 7 verification of the IP traffic sent to the sensors, to detect known exploit attempts.

6.3.2.5 Use case categories

Ensure Enablers	AAA, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

6.3.3 Use Case 4.3: Vehicle-to-Everything (V2X)

6.3.3.1 Preconditions

- Every actor holds 5G credentials
- 5G operator can authenticate vehicles
- Mutual authentication between vehicle and vehicle manufacturer

6.3.3.2 Description

Ann and Bob may want to exchange data (Vehicle-to-Vehicle (V2V) communication) via 5G network to share knowledge in order to provide more intelligent services, such as traffic jam information. Ann may also want to exchange data with Charlie (Vehicle-to-Pedestrian (V2P) communication) via 5G network to support cooperative collision warning. Finally, Ann may want to connect with her vehicle manufacturer infrastructure (Vehicle-to-Infrastructure (V2I) communication) to download a software update, or to send analytics reports from the vehicle to the repair shop.

V2V, V2P, and V2I have different security needs, and the 5G operator should grant authorization to the 5G network accordingly.

Basic flow of events:

1. Ann establishes a connection with Bob
2. Bob sends to Ann information about his location and speed
3. Ann processes Bob's information to generate the traffic status

Alternative flow of events:

1. Ann establishes a connection with Charlie
2. Charlie sends his position to Ann, and Ann hers to Charlie
3. Ann and Charlie process the information according a collaborative collision warning system.

Alternative flow of events:

1. Ann establishes an IP connection with a vehicle manufacturer
2. Ann sends her software version information to the vehicle manufacturer
3. The vehicle manufacturer sends a software update to Ann

6.3.3.3 Vulnerabilities and Consequences

Indication about traffic jams might use a group security association where identifying and authenticating an individual sender may not be required. However, if group security association is used for sending analytics to the repair shop from a vehicle, a malicious group member (e.g. Eve) could be able to send unauthorized analytics data to the repair shop on behalf of the victim (Ann).

6.3.3.4 Properties of a solution

- Enrolment in national traffic management infrastructure, as soon as border is passed.
- Symmetric keys for encryption
- Asymmetric keys for signature, providing non-repudiation

6.3.3.5 Use case categories

Ensure Enablers	AAA, Trust, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

6.4 5G Vision

5G should support authorization of device-to-device operations at different levels. At the application level, the 5G infrastructure provides the credentials to support the generation of security policies and authorization tokens. At the network level, the 5G operator should be able to authorize direct and secure end-to-end connections between devices. Moreover, the use of licensed spectrum of 5G should be authorized in a secure way. 5G should cope with the different levels of trust, for instance, according to the V2X scenario, and also take the relevant legislation and regulation into account in the design of the 5G solution.

7 Cluster 5: Software-Defined Networks, Virtualization and Monitoring

7.1 Introduction

To lower the cost and allow more flexibility, e.g. rapid deployment of new network functionality, 5G will rely on virtualization. In addition, network virtualization in the form of network slices can be a means to isolate different types of traffic and to provide better security and network attack resistance.

By “network slice” we mean a portion of the underlying network used to provide network services with particular properties. For example a slice could be used to provide:

- High QoS for real-time streaming/video
- Delay tolerant networking
- Special enterprise or M2M traffic
- Strong security properties (e.g. "isolating" traffic from potential eavesdropping, DoS etc.)

The use cases on in this cluster are divided into three categories:

1. The user plane of an SDN network: This category comprises uses cases that deal with the virtualization of the network, i.e., the 5G Core Network in the form of a Network Slice. The first use case belongs to this category.
2. The control plane of an SDN network: This category comprises use cases that deal with mechanisms of virtualizing the network, and how the virtualized network is operated. This includes the tools for creating, maintaining, and removing Network Slices, and Network Nodes in these Slices. It also includes the router infrastructure, SDN programming interfaces, clouds, and the VNFs (Virtualized Network Functions). The second and third use cases belong to this category.
3. Monitoring and control of the virtualized 5G network and of the virtualization infrastructure: This category comprises uses cases that describe monitoring, verifying, and controlling the virtualized 5G Core Network, and in the virtualization infrastructure. The fourth, fifth and sixth use cases belong to this category.

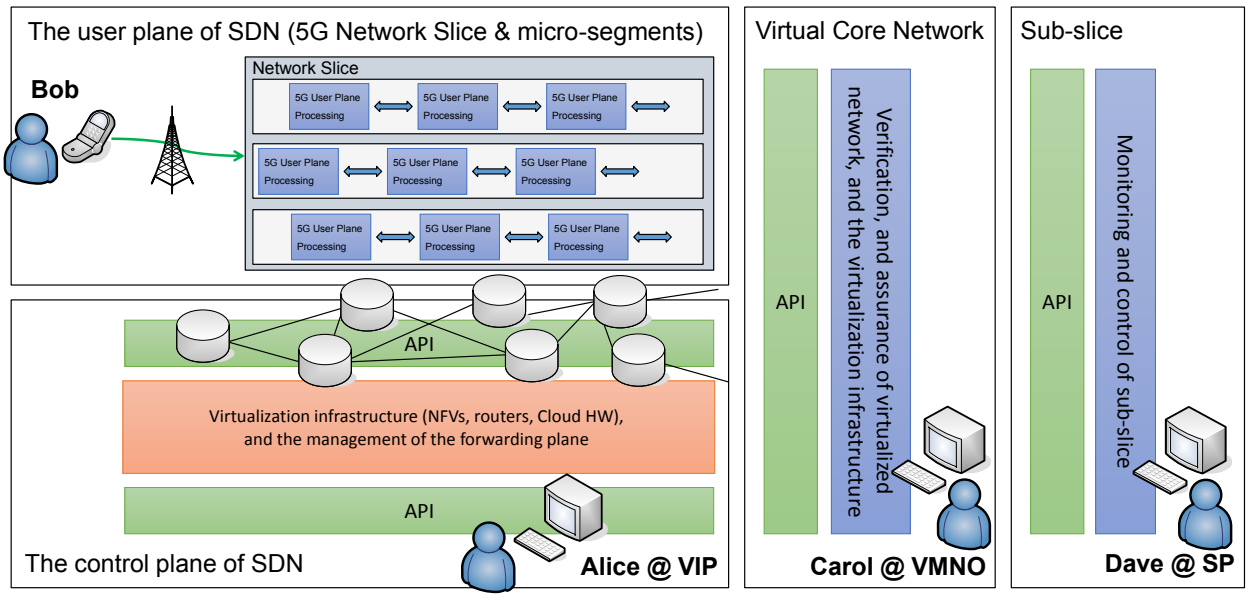

Figure 9: User plane, control plane in SDN and monitoring and control of virtualized 5G network

7.2 Actors

The actors in this cluster are:

- Virtual Mobile Network Operator (VMNO)
- Virtualized Infrastructure Provider (VIP)
- Infrastructure components, these are the network components (physical or virtualized)
- 5G Node Provider (5GNP), this is the software vendor of a 5G node that is running on top of the Virtualized Infrastructure
- Service Provider (SP) running a service on top of the VMNO's network
- Employee (Alice) using the API in Infrastructure side, could be an employee of SatNO, VMNO or VIP
- Consumer (Bob) and his 5G devices (e.g. xMBB or mMTC devices)
- Employee (Carol) using the monitoring/assurance API, could be an employee of VMNO, VIP, 5GNP
- Employee (Dave) of the SP using an API to the VMNO.

7.3 Use Cases

7.3.1 Use Case 5.1: Virtualized Core Networks, and Network Slicing

This use case belongs to category 1: the user plane of an SDN network.

7.3.1.1 Preconditions

- The Virtualized Infrastructure Provider (VIP) and the Virtual Mobile Network Operator (VMNO) have a business agreement, and they have installed, and configured a Virtual Core Network (VCN) consisting of two Network Slices. One slice is serving xMBB subscribers, and the other mMTC subscribers.
- The VCN is connected to an infrastructure of 5G base stations that in this use case are shared between multiple VMNOs. The RAN consists of components owned by different VMNOs.
- The Network Slices are configured in such way that one slice does not accept commands from another slice.
- Micro-segmentation splits 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.
- Bob has a 5G xMBB device, and a subscription of VMNO to that device.
- Bob has also a sensor that is a 5G mMTC device, and includes a subscription of VMNO.
- VMNO is providing an Internet accessible API for 5G mMTC device subscribers to control the behaviour of the mMTC devices.

7.3.1.2 Description

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 to the corresponding network slices. Devices and the network negotiate security mechanism and algorithms in a secure way, and after the security is turned on, the devices have access to the services in the different network slices.

This use case assumes that the devices are authenticated after they have access to the slice, however, there are other options like authentication of the device at a special slice selection function.

Basic flow of events:

1. The 5G xMBB device, and 5G mMTC device are powered up.
2. The devices attach to the 5G base station.
3. The devices are authenticated after the attachment.
4. The base station contacts the MMEs in the VMNO network slices for xMBB and mMTC.
5. 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.
6. Before creating the micro segments, the devices and the slices mutually authenticate. Authentication could happen also in an earlier phase between the device and a special slice selection function.
7. The micro-segments are allocated for the devices that are authorized for it. The micro-segment has a security mechanism of its own.
8. Bob uses his 5G xMBB device to configure the behaviour of the sensor via the API.

7.3.1.3 Vulnerabilities and consequences

Having large segmented security zones can create significant attack surfaces and enable threats to move throughout large portions of the 5G software network unrestricted.

7.3.1.4 Properties of a solution

By dividing the network into smaller parts, i.e., network slices, sub-slices and micro-segments it would be easier to monitor and respond to anomalous behaviour. In this way, the surface for attacks and threats can be reduced significantly. 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.

7.3.1.5 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Trust
Next Generation Radio Technology Usecases	uMTC, mMTC, xMBB

7.3.2 Use Case 5.2: Adding a 5G Node to a Virtualized Core Network

This use case belongs to category 2: the control plane of SDN.

The general SDN approach that could be used to implement this use case, would typically use the following concepts. The control plane of SDN intermediates between the application plane and the data plane, whereas the user plane of SDN is composed of network applications that send instructions to the control plane, the SDN controller, via the northbound application interface. Those instructions will be translated by the SDN controller into suitable actions sent via the southbound protocol interface to the data plane. For instance, to install an end-to-end path between two nodes, the SDN controller will take this instruction sent by a network application and it will generate a series of flows to be installed on the appropriate switches e.g. via OpenFlow, to ensure that path.

7.3.2.1 Preconditions

- There are two Virtual Mobile Network Operators, VMNO1 and VMNO2.
- Each VMNO has its own virtual core network, VCN1 and VCN2.
- VCN1 and VCN2 share the same physical network.
- A multi-slice system, where the slices consist of virtual topologies simultaneously deployed over the same core network (physical infrastructure). This physical infrastructure is operated by a Virtualized Infrastructure Provider (VIP).
- Both core networks VCN1 and VCN2 are isolated by using an isolation mechanism.
- VMNO1 has requested the VIP to construct a new Network Slice. This request has been done in a secure way.

7.3.2.2 Description

Network Applications in each Virtualized Core Network modify the forwarding logic of the shared physical network.

The Network Applications (such as an MME) are not able to read or modify physical network resources belonging to the other Virtualized Core Network. Furthermore, modifications to the physical network, which might originate from a reconfiguration of one of the virtual core networks, should not conflict with the current configurations of the other virtual core network. In the flow below, the MME is assumed to be associated with a slice. Thus, this only supports the model in which UE devices are assigned to slices before they have been authenticated, even if, as mentioned, other options are possible.

Basic flow of events:

1. Alice, an employee of a VIP, starts configuring a new Network Slice on VCN1 by creating a new virtual MME. The MME software is coming from a 5G Node Provider (5GNP).
2. Alice creates the virtual space for MME, and installs the MME software on top of that.
3. Alice configures the forwarding logic related to the new MME.

7.3.2.3 Vulnerabilities and consequences

The MME software in the VCN1 should not be able to see or modify the forwarding logic related to VCN2. There may be policy conflicts when different network applications in each virtualized core network try to modify the forwarding logic of the shared physical network elements, because those can inject contradictory policies, or even one non-authenticated network applications can try to inject malicious policies to the SDN controller.

On the other hand, the high dynamicity in SDN and NFV-based environments comes from the fact that the SDN controller ensures the connectivity among virtual nodes comprising the slices by choosing a physical path at run-time. Apart from this, when SDN is combined with NFV the network becomes even more dynamic, since virtual nodes host VNFs which may be migrated, leading to subsequent recalculation of the path allocated by the SDN controller. This dynamicity leads to a lack of control on the established dependencies between the slice topologies and the physical infrastructure, since it depends on the SDN controller which may change those dependencies dynamically. As a consequence, fault isolation on multi-slice systems needs to be ensured. Fault isolation ensures the resilience of VNFs and virtual links composing the slices, and it consists of ensuring that those virtual resources are disjointly allocated (i.e. ensuring those slices do not share resources) in the network infrastructure or at least ensuring there is enough redundancy

to migrate them to avoid service outages. Otherwise, a failure on the shared physical resources could propagate to both slices.

7.3.2.4 Properties of a solution

Security policies:

The authenticity and integrity of the received data and commands in each slice must be ensured. To control the access between slices, security mechanisms must be able to check if the received data / commands, originated from within the slice or not (from a legitimate entity). In other words, it must be able to check its trustworthiness, to prevent access from other slices.

The security system must ensure the different SLA objectives for the different slices are met. The SLA objectives will be different depending on the use case (e.g. autonomous driving, health, massive IoT, etc.)

The policies sent by network applications should be first injected to a policy checker block [Paladi2015] to analyse the policies from network applications towards the VCNs to avoid incoherencies between policies and/or security issues. This policy checker block verifies and enforces policies and controls the access of network applications to the SDN controller. This block has two components: a real-time policy checker block that verifies the incoming policies and tags them whith issuing entity, and a offline policy checker block that ensures isolation, network reachability and liveness. In this use case, the network applications should not be able to read or modify network resources of other VCNs, so the rules sent from network applications should be injected into a policy checker block able to understand their origin, identify whether or not they are not allowed to access to that VCN and reject them if necessary. The SDN controller should only install those policies accepted by the policy checker block, once this block checks that those policies come from authenticated and authorised network applications.

- In a 5G network, the isolation of slices (isolation assurance within 5G nodes) must be ensured. This assurance must be provided at two levels, at security level (threats propagating through the slices) and at resiliency level (faults in the physical infrastructure propagating through the slices).
- A compromised slice may compromise the security of other slices sharing the same physical 5G nodes.
- Unavailability of a physical network resource (physical 5G node) serving N slices, due to intentional or accidental intentions, may propagate to the N slices (a.k.a cascade effect)
- Integrity and authenticity of the data/commands uploaded/downloaded by a 5G controller/a 5G object must be ensured to avoid any security issues.

Resiliency policies:

A resilient system must prevent cascade effects between different slices, by checking in real time which part of the physical infrastructure is ensuring the integrity of a given slice topology and propose migrations when detecting vulnerable, attacked, compromised or affected physical resources. For that, it is necessary to support the retrieval on-the-fly of the dynamic dependencies between the slices and the physical infrastructure in order to calculate the propagation of faults and attacks in a given slice.

7.3.2.5 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

7.3.3 Use Case 5.3: Reactive Traffic Routing in a Virtualized Core Network

This use case belongs to category 2: the control plane of an SDN network.

7.3.3.1 Preconditions

- There is one Virtual Mobile Network Operator, VMNO1.
- VMNO1 has its own virtual core network, VCN1.
- Network traffic in VCN1 is routed (reactively) by a network application. The function of this network application is to receive packet-in messages and reconfigure the flow tables of the switches accordingly.
- This use case assumes that the virtual 5G core is aware of virtualization. (It could also be possible that the dynamic behaviour is done transparently to the virtual 5G core.)
- A consumer of VMNO2, Bob, accesses with his mobile device a service in the internet. Bob is a roaming subscriber in the VCN1.

7.3.3.2 Description

When Bob accesses the physical core network for which no matching flow rules are installed, the VCN1's network application is triggered. The reconfiguration of VCN1 is compiled down to a reconfiguration of the physical network. The reconfiguration handles Bob's network flow to access the remote internet service.

Basic flow of events:

1. Bob's device starts sending network packets to the core network.
2. Since the network packets do not match any flow rule, the core network generates a corresponding packet-in message for VCN1.
3. VCN1 triggers its network routing application for the received packet-in message.
4. The network application establishes a network flow in VCN1.
5. The reconfiguration of VCN1 is compiled down so that a corresponding network flow in the physical network is established.
6. Bob starts communicating over his mobile device with the internet service.

7.3.3.3 Vulnerabilities and consequences

The time of reconfiguring the physical network can be measured by an attacker. In this way, an attacker can gain information about which and when a network packet triggers a reconfiguration of network components. This can be exploited to mount powerful denial-of-service attacks, where an attacker overloads the controller of VCN1 by sending packets that, with high probability, trigger a reconfiguration of the networks. Furthermore, note that installing flow rules in state-of-the-art hardware switches is a costly operation. This means that even the performance of the physical network might be decreased.

7.3.3.4 Properties of a solution

A solution should not decrease network performance significantly. This means, for example, that delaying every network packet that does not trigger an interaction with the control plane at a switch before

forwarding it is not a workable solution. Although an adversary would not gain any knowledge when measuring the timings of sending and receiving packets, the whole network traffic would significantly be slowed down. However, one can delay a few packets of a network flow to obfuscate the timing measurements of an adversary. The few delayed packets fake an interaction between the network's data plane and control plane. These delays can be done directly at the switches or a dedicated, new data-plane component. There is no need for any interaction with the control plane. The selection of the packets and the delay is specific to a network, and needs to be configured.

7.3.3.5 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

7.3.4 Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform

This use case belongs to category 3: the monitoring of the virtualized 5G network and of the virtualization infrastructure.

7.3.4.1 Preconditions

- A new MME has been virtualized, and it is running on top of a Virtualization Platform.
- The MME is deployed as part of a VCN, and a Network Slice.
- There is a certification system for Virtualization Platforms that issue "level 1 certification" to third party products.

7.3.4.2 Description

Carol is running various tests on the Virtualized Node, and the Virtualization Platform. Carol needs to check that the new node meets the requirements of the Virtual Mobile Network Operator. This slice is used for eHealth services, and it needs to fulfil certain safety, security and privacy standards: in this example we assume that all parts of the VCN are physically within France.

Basic flow of events:

1. Carol starts by checking that the physical computer of the Virtualization Platform is located in France. The physical computer is the one where the Virtualized Node is to be installed.
2. Carol adds a monitoring policy that allows her to receive a notification if the location is changed, and an alarm message if the location moves outside of France.
3. Carol runs a test on the virtual machine of the Virtualization Platform, and verifies that it is able to fulfil the security and privacy requirements. Carol is able to verify that the Virtualization Platform has been certified by an external party, and it has "level 1" certification.
4. Carol then checks the integrity of the MME software that is running on top of the virtual machine.
5. Carol verifies that the security towards the other nodes in the Virtual Core Network is configured correctly, and only authenticated and protected data/commands are able to pass/access the MME.
6. Carol checks that the slice topology corresponds to a physical infrastructure whose physical nodes comply with the geographical constraints for this use case.

7.3.4.3 Vulnerabilities and consequences

In this e-health service, the slice should depend only on 5G nodes located in France or operated by a given MNO, that is why Carol is checking that the underlying nodes of the slice provided comply with such a geographical constraint.

Privacy and security issues should be respected, especially in highly sensitive services like e-health. For instance, if the e-health flow of a given country goes through any non-French 5G nodes, it may not respect the service security or privacy policy.

A 5G operator must be able to ensure at all times that a given slice (service) resource are located in a given geographical area. A service provider must be able to check that the data flow of the service transits within a given area. This is possible if we are able to retrieve the underlying physical node identifiers belonging to every slice at run-time and verify their geographical location in order to ensure that their location does not violate the geographical constraints imposed by the e-health case.

VNFs can be provided by third parties, so another threat is when VNFs become compromised. A network operator must be able to check, in real time, the integrity of the running code in a NFV and that it (the NFV) is compliant to what he previously defined, that is why one of Carol's role is to check the integrity of the MME software running on the VM.

Another threat is when SDN is the underlying infrastructure of NFV-based services, where SDN is ensuring the connectivity among VNFs. In this scenario, the SDN controller can become compromised, because SDN controllers are vulnerable to DDoS attacks (Distributed Denial of Service).

7.3.4.4 Properties of a solution

One basic approach is to verify and thoroughly test the deployed software that controls the network. There should be dedicated tools that support these verification and testing tasks. Another, complementary approach is to monitor the interactions between the network's planes. These interactions are checked against given security policies. Noncompliant, malicious, and suspicious interactions (or sequences of interactions) are reported. The checking can either be done online or offline. In the latter case, the interactions are logged and then collected and audited later.

7.3.4.5 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Security Monitoring, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

7.3.5 Use case 5.5: Control and Monitoring of Slice by Service Provider

This use case belongs to category 3: monitoring and control of the virtualized 5G network.

7.3.5.1 Preconditions

- There is a Virtualised Infrastructure Provider (VIP).
- There is a Virtual Mobile Network Operator (VMNO).
- The VIP has deployed a Virtual Core Network (VCN) for the VMNO.
- There is a Service Provider (SP).
- The VMNO has deployed a sub-slice for the SP with certain SLA constraints.

7.3.5.2 Description

A Service Provider, for instance a massively multiplayer online game (MMOG) host, 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 needs to be able to monitor the sub-slice to ensure that the VMNO is providing what is required by the contract, and also needs to be able to vary the parameters of the sub-slice within some predefined bounds as the service's popularity changes.

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. By having the SP interact with a VMNO we demonstrate a further potential level of complexity.

Basic flow of events:

1. Dave, an employee of the SP, using the tools provided by the VMNO, monitors the QoS being provided to the game players in the sub-slice.
2. Dave, using the Service Provider's game monitoring system, predicts that the number of players this evening will increase beyond the capacity that the sub-slice was provisioned for and that the performance of the game for the players will degrade to an unacceptable level.
3. Dave requests that the capacity of the sub-slice is increased to deal with the additional demand.
4. The VMNO determines (automatically or manually) that the VCN can support the increased capacity of the sub-slice without degrading the QoS of other customers and so increases the sub-slice capacity.
5. The VMNO charges the SP for the extra capacity.

7.3.5.3 Vulnerabilities and consequences

The use case demonstrates that a customer of a VMNO can request, use, monitor and control a sub-slice of the network. This requires re-selling of capacity by a VMNO along with QoS terms contained in an SLA. The use case also demonstrates the dynamic nature of allocations by allowing the Service Provider to have some degree of control over their sub-slice. To ensure an acceptable level of service for their customers, the Service Provider would need to be able to assess the trustworthiness of the VMNO before entering into a contract with them. The VMNO's systems dependence on (at least) the VIP makes the chain of trust quite complex.

7.3.5.4 Properties of a solution

- control of sub-slice may be addressed with delegation
- hierarchical asserted identities of actors
- SLA where parts of the agreement relates to establishing new SLAs
- a tool to assess the trustworthiness of a system (including network components and actors) based on known threats and prior experience

7.3.5.5 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Security Monitoring, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

7.3.6 Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor

7.3.6.1 Introduction

This use case belongs to category 3 and is related to broadband telecommunication systems or telecommunication ground user segments. The infrastructure for building the SatAN (Satellite Access Network) comprise the following network components (see Figure 10):

- Satellite Hub: satellite earth station connected to the 5G network.
- Satellite-capable eNB: traditional eNB improved with a satellite link.
- Different UEs:
    - Satellite Terminals (Ka band): satellite terminal with a Ka band antenna.
    - Satellite Modems: end-user satellite terminal connected to a satellite antenna using a communications satellite as a relay.
    - 5G devices.

These network components are distributed in a wide-area and due to the satellite support ensure high network availability and service reliability with a 100% geographic coverage.

These network components periodically collect information from themselves (hardware status, alarms…) and counters from the specific business logic (transfer rate, number of requests…). This information, called indicators, is used to monitor the network.

These indicators can be classified in three categories:

- Health status:
    - Intrusion detection.
    - Alarms scanned by satellite network devices.
    - Excessive load.
- Configuration state:
    - Network status.
    - Credential status.
- Counters:
    - Volume counters.
    - Efficiency counters.

These network components are supervised and controlled using a network management system. This network management system is composed of:

- Security monitor: receives such indicators and is in charge of carrying out an active security analysis to detect attacks and malicious behaviour. Furthermore, the security monitor uses data analytics

and intelligence-driven security to response to the identified threats (e.g. notify the operator, balance the load, …). 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.

- B/OSS (Business and Operational Support Systems) monitor: receives such indicators and is in charge of service provisioning, network configuration and billing.

7.3.6.2 Preconditions

- The network components periodically collect indicators.

7.3.6.3 Description

Once registered, network components deliver to the security monitoring the indicators collected. Later, security monitoring uses active security analysis with these indicators in order to detect threats.

SatNO connects to the security monitor to check the systems status (e.g. fault management, performance monitoring) and, if needed, responds to the identified threats.

A Service Provider (i.e. telecommunications company) has a contract with the SatNO to supply a suitable system capacity with some QoS guarantees to be used by its customers. The Service Provider implements pre-paid/post-paid services and connects to the B/OSS monitor to ensure that the SatNO is providing what is required by the contract and performs some control tasks (management of system bandwidth and power to optimize global capacity, configuration of network components, …).

Basic flow of events:

1. Upon activation, each network component identifies itself with the network and registers with the network management system
2. The security credentials of these network components need to be periodically updated
3. Once registered, network components deliver periodically the collected indicators to the network management system
4. Network management system receives from the network components a large amount of indicators
5. Security monitor uses active security analysis with these indicators

Alternative flow of events:

1. Alice, a SatNO, connects to the security monitor to check the system status and the security analysis provided by the security monitor
2. Security alarms (e.g. attacks, malicious behaviour detected, …) may require a response from Alice (e.g. allow/deny access to one network component)

Alternative flow of events:

1. Carol, an employee of the SP, connects to the BSS/OSS monitor to check the QoS
2. Carol may request increase capacity to deal with additional demand

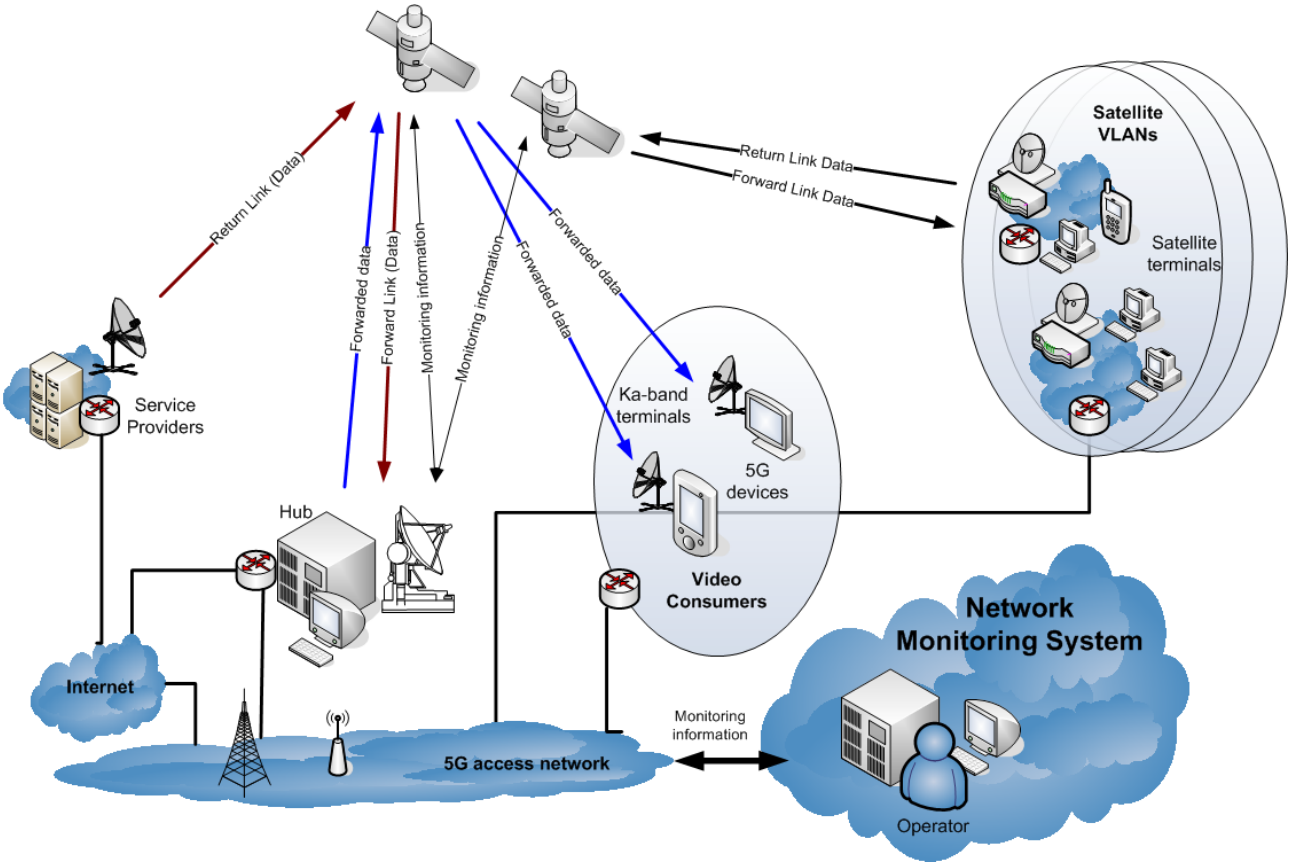

Figure 10: Satellite and 5G Monitor.

7.3.6.4 Vulnerabilities and Consequences

The use case demonstrates the dynamic nature of allocations by allowing the Service Provider to have some degree of control over their micro-slice. The security credentials of these micro-slice components may have been compromised and it is needed to force an update of these credentials to maintain the security of the network.

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.

7.3.6.5 Properties of a solution

The use-case requires re-selling of capacity by a SatNO along with QoS terms contained in an SLA.

- Secure mechanism to store and update the security credentials for the network components
- Generic secure interface to provide indicators from a heterogeneous network and to update the security credentials
- Real time data analytics and intelligence-driven security to detect threats based on security metrics

7.3.6.6 Use case categories

Ensure Enablers	Security Monitoring, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	mMTC, uMTC

7.4 5G Vision

It is envisioned that the virtualization of the core network is an essential feature of 5G. A virtualized core is described here as a “network slice”. Mobile operators are able to provide different core network slices for different types of subscribers. This includes different UE types, such as mMTC or xMBB but also customer specific slices such as eHealth or satellite communications. Network slices may provide different services, and share a common radio network. The virtualization may also include more fine-grained features, such as micro-segmentation within the slice. Isolation of network slices is essential.

Techniques that are available for implementation of the virtualization are many, e.g. Software-Defined Networking, Virtualized Network Functions and Cloud techniques. Virtualization is most likely to be transparent to many 5G nodes, however, there might also be some 5G node components that are actively modifying the structure and behaviour of the core network, adapting to e.g. subscriber/device context. Virtualization is most likely and desirable to be transparent to the User Equipment (UE), and the subscriber. The UE does not need to be aware of the internal structure or implementation of the core.

Virtualization bring new types of actors, and roles into the picture. It is envisioned that it is possible to separate the roles of the 5G Node Provider, the Virtualization Infrastructure Provider, and the Virtual Mobile Network Operator. This also means that new types of secure monitoring and assurance interfaces are needed if all the new roles are taken by separate actors. Actors that are operating on top of virtualized platform need to monitor, verify and control what is happening in the virtualized network as well as in the virtualization infrastructure.

8 Cluster 6: Radio Interface Protection

8.1 Introduction

This cluster describes two use cases addressing availability and integrity of the radio interface. Use case 6.1 considers overload and denial of service attacks of the radio interface and how devices with priority should be prioritized in order to be able to attach even during a high load situation. Use case 6.2 considers user plane data integrity protection.

8.2 Actors

The actors in this cluster are:

- Mobile Network Operator (MNO)
- Communication device (D)
- User (Bob)

8.3 Use Cases

8.3.1 Use Case 6.1: Attach Request During Overload

8.3.1.1 Preconditions

- The RAN is serving multiple recent attach requests
- Available radio resources are depleted

8.3.1.2 Description

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.

Basic flow of events:

1. D makes an attachment request to the base station
2. The base station is busy serving other recent attachment requests or has no radio resources available
3. D gets no access or becomes delayed

Alternative flow of events:

1. D is attached to the network
2. D loses radio synchronization
3. D is re-attaching
4. Available radio resource are depleted and the network can't offer D access
5. D does not regain connectivity

8.3.1.3 Vulnerabilities and consequences

- Current networks perform preliminary radio resource allocation and signalling procedures which consumes processing and other resources in the RAN and on the backhaul, before the authentication procedure
- Illegitimate requests cannot be rejected at an early stage, and there are no means to give priority to important requests
- An adversary can saturate the radio network (or the uplink resources), e.g. using software defined radios (SDR), or using multiple legitimate devices, e.g. like in a botnet setting
- When attached devices loses radio synchronization, they are required to perform the random access procedure and may be unable to reconnect, despite being allocated radio resources

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

8.3.1.4 Properties of a solution

- 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

8.3.1.5 Use case categories

Ensure Enablers	AAA, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

8.3.2 Use Case 6.2: Unprotected User Plane on Radio Interface

8.3.2.1 Preconditions

- The UE is in Connected Mode
- Signalling is integrity protected
- User plane data is not integrity protected
- Encryption may not be allowed on the radio interface due to regulatory constraints

8.3.2.2 Description

Signalling between the UE and network is integrity protected, but in some scenarios, the amount of signalling needed before sending user data is minimized to save battery, sometimes signalling before sending user data is completely removed. The data connection is left open to the network when the UE goes to sleep mode.

User plane data is not encrypted due to regulatory constraints. Since user plane data is not integrity protected either [TS33.401], this leaves the user plane data totally without protection.

Basic flow of events:

1. D attaches to the network and establishes integrity protection for signalling. Encryption is not used for signalling nor for user plane data
2. The network receives unprotected user plane data from D
3. D goes to sleep. The data connection is left open.
4. D wakes up and sends data on the data connection

Alternative flow of events:

1. D attaches to the network and establishes integrity protection for signalling. Encryption is not used for signalling nor for user plane data
2. The network receives unprotected user plane data from D
3. D goes to sleep. The data connection is left open
4. Adversary sends data on the open data connection

8.3.2.3 Vulnerabilities and consequences

- The network cannot verify authenticity of the received user plane data
- An adversary may use the open user data connection

As a consequence, the user plane data is completely unprotected and the MNO cannot provide any service relying on the content.

8.3.2.4 Properties of a solution

- Introduce integrity protection of user plane in addition to integrity protection of control plane
- Replace specific integrity protection of control plane with common integrity protection on user and control plane lower in the radio network stack

8.3.2.5 Use case categories

Ensure Enablers	AAA, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	mMTC, uMTC

8.4 5G Vision

The 5G network should be robust against overload and denial of service attacks of the radio interface. Prioritized devices should be getting priority and be able to attach even during high load situations. Also, already attached devices losing synchronization should regain access during high load situations. User plane data should be integrity protected enabling trustworthy services to be built on top, and illegitimate and low priority requests should be rejected at an early stage.

9 Cluster 7: Mobility Management Protection

9.1 Introduction

This cluster describes different techniques to cause a persistent denial of service attack of the UE, illustrated by three different flow of events. The denial of service attacks are possible since none of the exploited messages require confidentiality or integrity protection in the current 3GPP standard, thus enabling the attacker to intercept, decode and alter the messages.

9.2 Actors

The actors in this cluster are:

- Mobile phone subscriber (Bob)
- Malicious attacker (Mallory)
- Mobile Network Operator (MNO)
- Sensor1

9.3 Use Cases

9.3.1 Use Case 7.1: Unprotected Mobility Management Exposes Network for Denial of Service

9.3.1.1 Preconditions

- Bob has a valid subscription with the MNO
- Mallory's rogue equipment is physically located in the same area (TA or Cell) as Bob or Sensor1
- Mallory has access to her own rogue eNB

9.3.1.2 Description

Bob 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).

This use-case is valid for all types of connected devices, i.e. Bob can be substituted with Sensor1.

Basic flow of events:

1. Bob is at work and has his phone turned on and is connected to his MNO
2. Bob's phone sends a TAU request message to the MME of his connected MNO
3. Mallory 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".* See Figure 11 and Figure 12.
4. Bob's phone accepts the TAU Reject message and acts accordingly
    a. If EMM cause number 7, Bob'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, Bob's phone will consider itself invalid for all services and enter the state EMM-DEREGISTERED.

Alternative flow of events:

1. Bob powers on his phone.
2. Bob's phone sends an "*Attach request*" to the MNO.
3. Mallory intercept the *"Attach request".*
4. Mallory alters the message and replace the "*Voice domain preference and UE's usage setting*" with *"Additional update type – SMS only*" and forwards the message to the MNO.
5. The MNO accepts the message and proceeds with the AKA protocol, furthermore the MNO configures the profile of the UE in the MME with the capabilities sent by Mallory, thereby rejecting all voice capabilities.

Alternative flow of events:

1. Bob's phone continuously sends registration requests to the networks with the best coverage.
2. Mallory responds with the reject message "*Forbidden PLMN".*
3. Bob's phone accepts the unprotected reject message and reconfigures the USIM accordingly, hence denying all services to the indicated public land mobile network (PLMN) until the phone has been turned off/on or the USIM has been re-inserted.

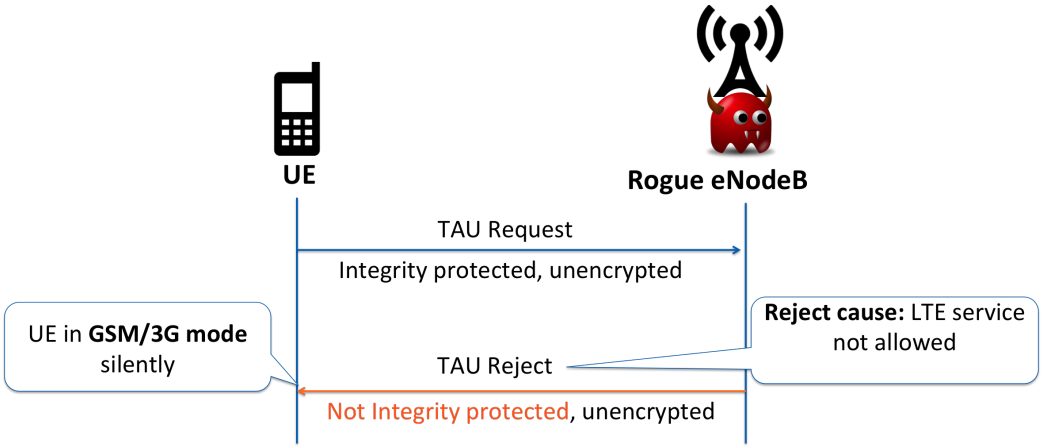

Figure 11: (from [Shaik2015]) DoS attack - denying LTE network services

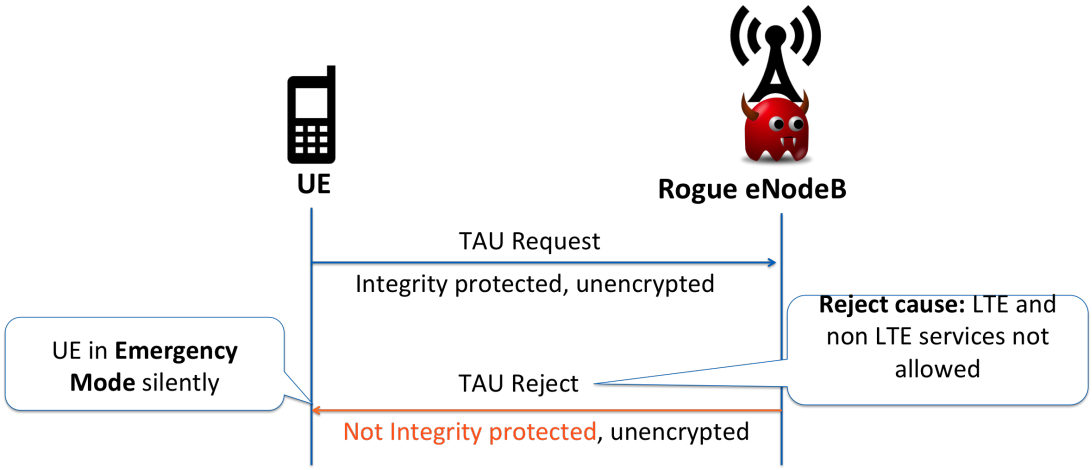

Figure 12: (from [Shaik2015]) DoS attack - denying all mobile network services

9.3.1.3 Vulnerabilities and consequences

- 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.

9.3.1.4 Properties of a solution

Security monitoring could be one solution to capture those attacks where UE is 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.

9.3.1.5 Use case categories

Ensure Enablers	AAA, Network Management & Virtualisation Isolation, Security Monitoring, Privacy
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

9.4 5G Vision

5G provides robust network services with considerable availability guarantees. The signalling messages exchanged between the user equipment and the 5G network should have the appropriate protection to combat known weaknesses in LTE. Such protection can be built from existing mechanisms, which in LTE provide a matching history of the user equipment's security capabilities. In 5G these mechanisms can be expanded to include a similar check of the network capabilities. Additionally, the introduction of an operator public key can bring the necessary protection of capability lists that are broadcasted by the network.

10 Cluster 8: Ultra-Reliable and Standalone Operations

10.1 Introduction

This cluster includes two use cases for ultra-reliable and standalone operations. The first one is the satellite-capable eNB that provides connectivity to the core network if the normal backhaul is lost. The second case describes standalone core network services that are similar to isolated public-safety services but are in this case commercial.

The use cases talk about Macro EPC which is the 5G core network that is used in normal mode of operation. Macro EPC provides services to the subscribers that are in the home network, or which are roaming in some visited networks. The Macro EPC is reached via the satellite in the first use case when the normal route is not possible because of a natural disaster.

The standalone EPC is an entity which provides functionality that eNBs in standalone mode of operation use, instead of the Macro EPC, in order to support local services. This is assumed to be a commercial service, and connection to the Macro EPC is still possible.

10.2 Actors

The actors in this cluster are:

- Ad-hoc roaming user (Alice)
- SatNO (Bob)
- Visited Network (VN)
- Home Network (HN)

10.3 Use Cases

10.3.1 Use Case 8.1: Satellite-Capable eNB

10.3.1.1 Introduction

This use case focuses on evolving the Transport Network Architecture (TNA) by combining both satellite and terrestrial transport architectures. The infrastructure comprises the following components:

- Satellite Hub: satellite earth station connected to the 5G network.
- Satellite-capable eNB: traditional eNB improved with a satellite link.
- Network manager: performs topology calculations and distributes the updated network configuration.

The main goal is the ability to offer resilience to cases of link failure. The satellite connectivity adds flexibility to backhauling networks. Also, this use case provides offloading capability via satellite to the backhaul network in case of congestion. This is a key enhancement in 5G, as this use case can only be served by satellites, or for which satellites provide a more efficient solution.

The topology management objective is that no nodes in the mesh network are left un-connected, while covering all the needed area. Topology algorithm shall be based on user priority and bandwidth.

10.3.1.2 Preconditions

- Macro EPC: the EPC which serves an eNB in normal mode of operation.
- There is a satellite-capable eNB that has the capability of connecting to the Macro EPC via satellite, and provides IP connectivity to the UEs when the eNB has lost the wired route to the Macro EPC.
- In the event that the satellite-capable eNB does not belong to the HN and that there is no static roaming agreement between the VN and the HN, the roaming agreement is dynamic, and valid only when special conditions like a natural disaster occur.

10.3.1.3 Description

Alice is in holiday in an area which is abruptly turned into a natural disaster area. Alice is able to communicate even when there is no static roaming agreement between the HN and the VN.

Basic flow of events:

1. The natural disaster occurs. The eNB looses the connection to Macro EPC.
2. The network manager detects the failure event and performs topology calculations to guarantee ultra-reliable services
3. The new topology is forwarded to the network components
4. The satellite-capable eNB activates the alternative route to Macro EPC via the satellite.
5. The satellite-capable eNB starts to broadcast that it supports the ad-hoc roaming mode. It offers SMS services to everyone in the area. The voice services are now reserved for public safety users only.
6. Alice's phone looses the connection to the network.
7. Alice's phone attaches to the satellite-capable eNB of the VN.
8. Alice's HN authorizes the ad-hoc roaming in the VN.
9. Alice receives an SMS from the embassy asking if she and her family are safe.
10. Alice informs the embassy that everyone in her family is safe.

10.3.1.4 Properties of a solution

- Dynamic roaming
- Non-satellite 5G device using satellite-capable eNB
- Satellite-based 5G topology reconfiguration

10.3.1.5 Use case categories

Ensure Enablers	AAA, Trust, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

10.3.2 Use Case 8.2: Standalone EPC

10.3.2.1 Preconditions

- There is a standalone-capable eNB that has the capability of standalone mode of operation, which provides commercial local IP connectivity to the UEs via a Standalone EPC.

- There is a standalone EPC which provides functionality that eNBs in standalone mode of operation use, instead of the Macro EPC. Standalone EPS provides IP address assignment and local routing within the standalone EPC.

10.3.2.2 Description

Alice is in a mega event with 100.000 other people. She uses the services that are available in the standalone EPC.

Basic flow of events:

1. When the mega event starts, the standalone-capable eNB starts to broadcast support of the ad-hoc roaming mode to the local EPC. It offers local IP connectivity within the standalone EPC.
2. Alice's phone attaches to the standalone-capable eNB of the standalone EPC. Alice's phone does not loose the connection to the HN.
3. Alice's HN authorizes the ad-hoc roaming to the standalone EPC.
4. Alice uses the services in the standalone EPC.
5. Alice also uses the services in the HN.

10.3.2.3 Properties of a solution

- Dynamic roaming
- Commercial standalone EPC

10.3.2.4 Use case categories

Ensure Enablers	AAA, Trust, Network Management & Virtualisation Isolation
Next Generation Radio Technology Usecases	xMBB, mMTC, uMTC

10.4 5G Vision

5G network is more reliable in terms of having dynamic, alternative routes from the radio network into the core network (such as satellite connection) and more flexible in terms of dynamic roaming. eNBs having satellite capabilities are especially interesting because they can provide satellite capabilities to non-satellite 5G devices. New commercial possibilities on stand-alone radio networks, and stand-alone core networks are also envisioned.

11 Cluster 9: Trusted Core Network and Interconnect

11.1 Introduction

These use cases deal with trusted core network and interconnection between different entities. The 5G network should be such that it is able to ensure that the interacting entities are authentic ones and spoofing of messages cannot take place. This should not be based on implicit security assumption, but rather use explicit security solutions.

11.2 Actors

The actors in this cluster are:

- Mobile phone subscriber (Bob)
- Adversary (Eve)
- Home Network (HN)
- Visited Network (VN)

11.3 Use Cases

11.3.1 Use Case 9.1: Alternative Roaming in 5G

11.3.1.1 Introduction

When entities are roaming in a visited network, it still needs to be ensured that the related messages are authentic instead of implicitly relying on the assumption that the traffic is originating from a certain network. Thus, messages need to be bound to the correct entities, so that spoofing cannot take place. The entities also should have clear understanding which entities they are communicating with. This is especially important when there are real world consequences, such as charging.

11.3.1.2 Preconditions

- The HN and the VN have a roaming agreement

11.3.1.3 Description

Bob needs the assistance of the home AAA infrastructure in order to authenticate himself to the VN. Home AAA issues an authentication challenge. This process also identifies both the VN and the HN, so that the involved parties are identified. In the course of this process, Bob also authorises the VN to provide services to him.

At the same time, accounting mechanisms are set up. The HN network can therefore have assurance that any billing related information is tied to Bob. Thus, the VN 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.

Basic flow of events (see Figure 13):

1. The VN is advertised to Bob
2. Bob identifies his HN and authorises the VN to offer services to his identity
3. The HN detects that risk status of the VN is such that interaction can proceed
4. The HN sends an authentication challenge to Bob and also identifies the VN to be used

5. Bob checks that he is using the correct network and responds to the challenge
6. The HN verifies the challenge-response and informs the VN that Bob is authentic
7. Authentication result is transmitted to Bob
8. Bob negotiates the use of services for his identity
9. The VN binds its own identity to the service negotiation
10. Non-repudiable service records are created

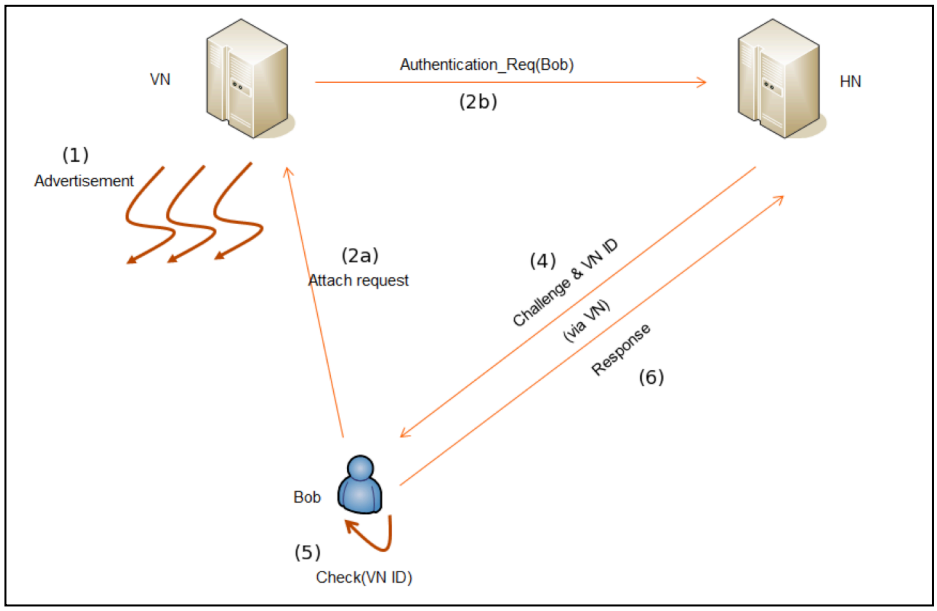

Figure 13: Bob attaches to the VN while roaming abroad

11.3.1.4 Vulnerabilities and consequences

This use case depicts the following vulnerabilities and their consequences.

- Unauthorised disclosure of sensitive information
  - If core network elements, interconnect networks, or other operators are expected to be trusted entities with no additional verification, sensitive information will be disclosed to unauthorised entities [Nohl2014]
- Spoofing of signalling messages
  - If unauthentic signalling messages can be sent and accepted, the behaviour of the network can be changed in an unauthorised way, i.e., integrity of the network is compromised
  - If traffic that has impact on charging is neither authenticated nor clearly bound to the entity which is responsible for the traffic, fraud can be performed. This is likely to decrease the user trust to the system.

11.3.1.5 Properties of a solution

If network entities have cryptographic identities, then messages can be bound to them strongly. This provides more flexibility, when referring to other entities outside the two-way interaction.

Service usage can be negotiated in such a way that both parties have an understanding of the incurred costs. This involves using the said identities guaranteeing that assured accounting records can be created.

11.3.1.6 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Use cases	xMBB

11.3.2 Use Case 9.2: Privacy in Context-Aware Services

11.3.2.1 Introduction

The context of the user is beneficial for providing better services. However, privacy issues arise as there might be unintentional disclosure of user related information [Vallina-Rodriguez2015]. Another side of the coin is that if purely encrypted traffic is used, then it is harder to take advantage of flow semantics to optimise the user experience [Smith2015].

11.3.2.2 Preconditions

- The HN and the VN have a roaming agreement

11.3.2.3 Description

The VN and the HN may exchange information regarding the Bob's context. This information can be used to customise the network in order to satisfy Bob's service requirements without revealing any unnecessary information.

Basic flow of events (see Figure 14):

1. On demand, the VN sends information about Bob's context to the HN
2. The HN shares some of the context information with content providers as allowed by (privacy) policies

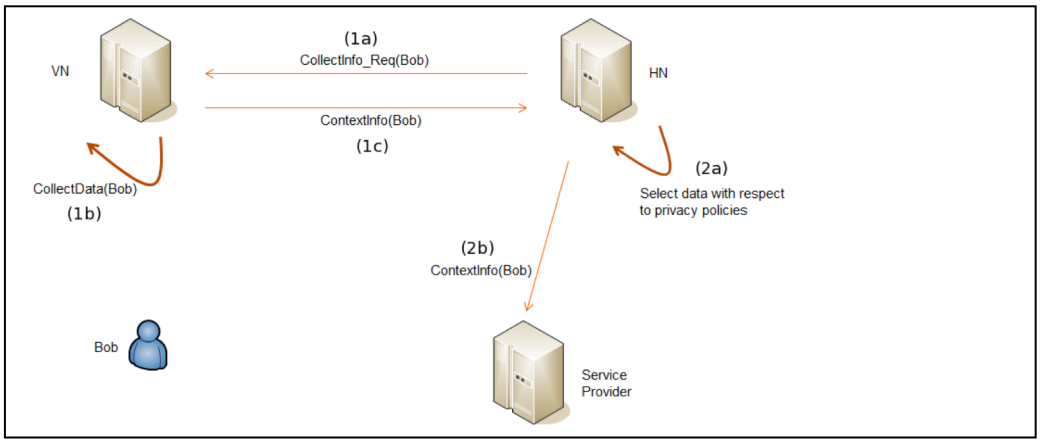

Figure 14: Disclosure of user context information controlled by Home Network

Alternative flow of events:

1. Bob authorises visited network to disclose some of the context information as per his defined privacy policies
2. The VN shares some of the context information with content providers

11.3.2.4 Vulnerabilities and consequences

User traffic can be enriched in various ways, such as proxies including additional headers to the user traffic. However, this information can leak and be abused by parties for which the information was not intended. This violates user privacy.

It is worth noting that in the above alternative flow the control of disclosure lies within the visited network. Even though the user can state his privacy policies, he cannot verify how well this is honoured as the user's contractual relationship is with his home network. On the other hand, nothing (save regulatory sanctions) prevents visited network from disclosing this information anyway.

11.3.2.5 Properties of a solution

Context information is disclosed in controlled fashion and it is made available in a standardised way so that it is not necessary to devise non-interoperable or potentially vulnerable schemes. In addition, the context information can be used in case of encrypted flows.

11.3.2.6 Use case categories

Ensure Enablers	Privacy, Trust
Next Generation Radio Technology Use cases	xMBB, uMTC

11.3.3 Use Case 9.3: Authentication of New Network Elements

11.3.3.1 Introduction

5G networks allow more dynamism through virtualisation and new functions can be introduced to the network on the fly. As these environments are more virtualised, there is always a danger that someone manages to introduce a malicious function into the network. Similarly, unauthorized physical elements could be attached to the network, if their authenticity is only based on the location in the network.

11.3.3.2 Preconditions

- The HN and the VN have a roaming agreement
- The VN does not have up-to-date patch management
- There is an exploitable vulnerability in the VN infrastructure
- Poor physical security of the VN has resulted in the installation of unauthorised device

11.3.3.3 Description

Unbeknown to Bob, Eve has managed to infiltrate the VN and installed a device into the local network (Figure 15). The device is not recognised as an authorised node, so it cannot inject network traffic, however, it detects an unpatched vulnerable server and installs malicious network function to subvert user traffic. However, as all the signalling related to Bob is strongly bound to his (temporary) identity, Eve's attempts to inject messages masquerading as Bob, so that Bob would suffer the incurred costs, are detected as spoofing attempts. Based on this finding, the HN network reports the possible misuse to the VN. Based on its policies, the VN will consider some measures to address the problem.

Basic flow of events:

1. Eve installs a malicious network device

2. Even attempts to inject signalling messages, but they are rejected because of an unauthorised sender
3. Local network has an unpatched server and Eve is able to take advantage of the existing vulnerability
4. Malicious virtual function is installed on the server
5. Malicious function attempts to send spoofed message claiming to come from Bob
6. The HN network detects Bob's spoofed identity coming from the VN
7. The VN is informed of the misuse

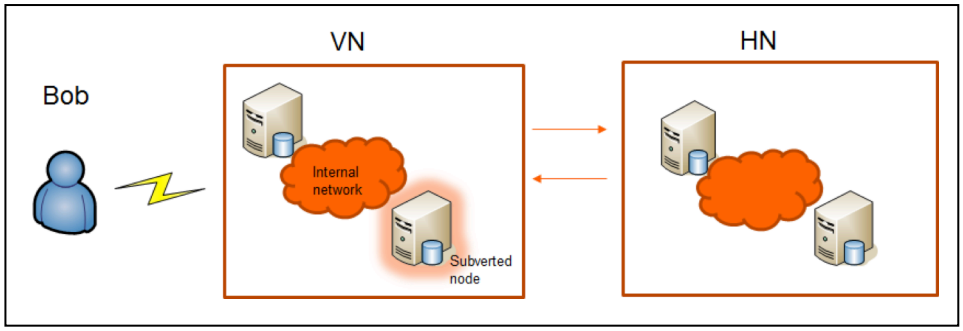

Figure 15: Eve has infiltrated VN and tries to subvert Bob's traffic

11.3.3.4 Alternative Description

Unbeknown to Bob, Eve has managed to infiltrate the VN and installed a device into the local network. The device is recognised as an authorised node, so it can inject data to Bob's user traffic. Eve's injection is detected as spoofing attempts because of behavioural analysis on Bob's traffic profile in the HN network. Based on this finding, the HN network reports the possible misuse to the VN. Based on its policies, the VN will consider some measures to address the problem.

Alternative flow of events:

1. Eve installs a malicious network device
2. Network has a vulnerable AAA server and Eve is able to take advantage of the vulnerability
3. The device is recognised as an authorised node
4. Malicious device injects spoofed messages
5. The HN network detects abnormal traffic behaviour for Bob coming from the VN
6. The VN is informed of the misuse

11.3.3.5 Vulnerabilities and consequences

The following vulnerabilities can be introduced when more dynamism is introduced.

- Unauthorised network elements are deployed into the core network
  - If an adversary is able to deploy devices or functions into the network, various man in the middle attacks can become possible. The adversary has a potential to eavesdrop, modify, delete or inject new traffic. In the case of signalling traffic, the whole network could be compromised. Depending on the level of trust relationships, the propagation of the attack to other networks might be additionally facilitated.
- As more elements rely on software and virtualisation, proper patch management needs to exist

- If elements are not kept up-to-date, lack of patching may lead to existence of exploitable vulnerabilities in the software.

- Composition of networks or network elements is not authentic (or authorised)
  - If new 5G architecture allows dynamic composition of networks or network elements, lack of authentication and authorization can lead to compromised network similarly as in the previous case. The composition needs to define the constraints on the level of integration, i.e., what resources are available and what sort of security levels are expected. Liability aspects need to be taken into account as well.

11.3.3.6 Properties of a solution

When new elements are introduced into a dynamic network, it has to be ensured that they are authentic components. Monitoring and testing of the environment can help in detecting possible violations of system integrity. Monitoring of traffic patterns can also help in detected subverted elements.

11.3.3.7 Use case categories

Ensure Enablers	AAA, Trust, Network Management & Virtualisation Isolation, Security Monitoring
Next Generation Radio Technology Use cases	xMBB, uMTC

11.4 5G Vision

5G networks are envisioned to dynamically adapt to the user needs. This dynamism sets more requirements on the authenticity of the entities as new entities emerge in the network and old ones are removed. Operators should not be forced to resort of implicit security assumptions about the security of the core network of the interacting partner, i.e., there should be more assurance that the traffic is indeed originating from a legitimate entity and is bound to a legitimate entity. This is especially important when any signalling has effect on charging, thus it should be ensured that the users do not face unfounded service charges. This applies to the identity of the users as well, i.e., it should not be possible to spoof the identity of the user. On the other hand, the service charges ought to be attributable to the user so that the user is not able to deny the use of service.

In order to enrich and optimise the user experience, context information ought to be available for use. However, one also should ensure that when doing so the user privacy is honoured. Thus, there ought to be a controlled and standardised way of providing context-aware services.

As the network could be constantly evolving due to virtualisation and dynamic interaction, one should ensure that the security of the network is monitored as well. While monitoring of the network is commonplace activity even nowadays, it is mainly done by add-on devices that may not have a holistic view of the network. In some cases it might be even envisioned that dynamic composition of elements would warrant security testing of those components before they are allowed to interact. This could simply be straightforward vulnerability scanning, but more complex scenarios could involve, e.g., sandbox testing. Correlation of information from several sources should in any case be used to make more educated guesses regarding the possible existence of ongoing attacks.

12 Cluster 10: 5G Enhanced Security Services

12.1 Introduction

Cluster 10 contains three use cases describing various enhanced security services that can be offered in 5G networks.

In use case 10.1 we learn a possible way to counter act mobile botnets BotNet by offering a service to aid the users to identify anomalous activity from their mobile devices and to report this activity. Use case 10.2 proposes a service that can help protect the user's privacy at the application layer, by means of apps and device privacy checks. Use case 10.3 offer an anonymization capability to all 5G subscribers having an anonymization SIM. In addition to this capability more services may be envisioned that are able to anonymize user/device identifying data and, therefore, can help to protect the user's privacy.

12.2 Actors

The actors in this cluster are:

- Mobile phone subscribers (Bob, Alice)
- Home Mobile Network Operator (HMNO)
- Malicious attacker (Mallory)

12.3 Use Cases

12.3.1 Use Case 10.1: Botnet Mitigation

12.3.1.1 Introduction

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 send a premium SMS to a number controlled by the attacker.

12.3.1.2 Preconditions

- Bob has a valid subscription with the MNO
- Mallory's infected application is uploaded to Bob's preferred applications store/market

12.3.1.3 Description

Bob is staying at home and browses his Bob's preferred applications store/market. He finds a free version of a popular and trendy game (or any other application) uploaded by an 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. How Bob's device gets infected is irrelevant here, it could be also by attaching his phone to an infected PC/laptop, or by opening a link received in phishing mail. The salient aspect is that the infection propagates through mobile traffic. Here we observe the case how Bob's device gets infected via operator's network.

The free version of the popular and trendy game application is modified in a way that in addition to the main functionality it also adds the SMS sending functionality, and transforms the phone into a bot remotely controlled, by a Command and Control Centre (C&C) piloted by Mallory. After Bob's device has been infected, Mallory can remotely perform various malicious activities on the device, such as SMS sending in the background. For this particular attack, Mallory had registered a premium number with an operator, which could be even located in another country, and once (or twice) per month Mallory could configure the C&C to instruct all of his "puppets" (i.e. remotely controlled mobile devices) to send SMS to that premium number. Bob and thousands of other users will very unlikely be able to detect the increased monthly bill, especially if the increase amounts to only a couple of euros.

Basic flow of events:

1. Mallory registers a premium number with an operator.
2. Mallory configures the Command and Control Centre (C&C) robot to instruct all puppets to send SMS to that premium number.
3. Bob is connected to the MNO and browses the application market on his mobile device.
4. Bob installs an infected application and becomes one of the C&C's puppets unknowingly.
5. Without Bob's knowledge, his mobile device is used for botnet activity such as SMS sending and Bob's monthly bill is increased

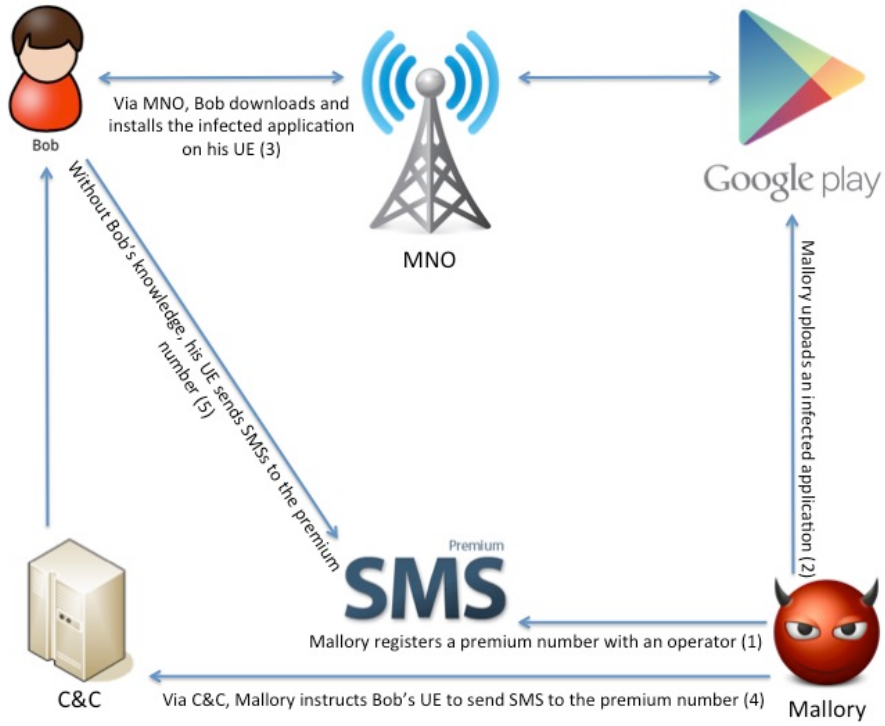

Figure 16: Malware infected UE sending premium SMS

12.3.1.4 Vulnerabilities and consequences

Vulnerabilities in mobile devices as well as the ingenuity of their users can lead to subverting the integrity of the device and installation of malware. As a result

- Mobile device could be controlled remotely
- Mobile devices could be used for malicious activities

Unwanted communication could lead to monetary loss for the end users through their monthly bills, regardless how insignificant the amount is for each individual.

12.3.1.5 Properties of a solution

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.

12.3.1.6 Use case categories

Ensure Enablers	Network Management & Virtualisation Isolation, Security Monitoring, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

12.3.2 Use Case 10.2: Privacy Violation Mitigation

12.3.2.1 Introduction

Mobile devices and the installed applications disclose a large amount of private information both personal and device-related information. There are many misbehaving apps, PUAs (Potentially Unwanted Applications), adware and ransomware in the wild and spyware is not so uncommon even in official app stores! Currently the mobile network has no means to protect the user's privacy at the application layer.

Some mobile subscribers have privacy concerns and would like to know if their device and the applications installed therein are involved in activities that violate their privacy.

12.3.2.2 Preconditions

- Alice has a valid subscription with the MNO
- Alice also subscribes to the privacy service provided by her mobile network operator (and possibly installs a privacy app).

12.3.2.3 Description

Alice has just installed a new game app on her mobile device (UE) from a link received inside an SMS from a Whatsapp contact. She is concerned that app may violate her privacy in some way and so uses a service (and possibly a local app) to check.

Basic flow of events:

1. Alice activates the privacy service.
2. Alice launches her new game app.

3. The privacy service on the 5G network detects some anomalous event from the UE (e.g., botnet related communications) and sends a notification to Alice to ask her to activate a privacy related analysis.
4. Alice agrees to the request, and data (e.g. a list of installed applications) is sent from her phone to the privacy service for analysis.
5. The privacy service responds with a notification containing the name of the non compliant app if any, a summary of its privacy violation activity, and the suggestion to uninstall it.

Alternative flow of events:

1. Alice starts the privacy app and configures her privacy preferences.
2. Alice installs the new game app, starts it and the game attempts to access the corresponding server which has also configured its privacy policy.
3. The privacy app checks Alice's and the server's privacy policies.
4. A privacy-related warning containing the name of the violating app and server is shown to Alice if the policies do not match.
5. Alice can decide if to proceed with the app/server or not.

12.3.2.4 Properties of a solution

- The 5G network deploys some anomaly detection or malware activity detection mechanisms or privacy violation mechanism [Razaghpanah2015], [Ren2015].
- 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.

12.3.2.5 Use case categories

Ensure Enablers	Privacy, Security Monitoring, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC, xMBB

12.3.3 Use Case 10.3: SIM-based and/or Device-based Anonymization

12.3.3.1 Introduction

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.). If such private information is accessed by applications, the users would like to be able to protect it with appropriate (e.g., format preserving) anonymization algorithms residing preferably on the SIM. This service can be offered by the MNO at the application layer e.g., through an application running on the device and/or on the SIM itself. A device implementation should preferably be integrated into the OS to provide protection against misbehaving applications. On the other hand, a SIM-based implementation may have even stronger security advantages and also provides "plastic roaming", e.g., the service can be enjoyed even if the user changes device. We stress a difference to Use

Cases 1.4 and 2.2. In the first case, the identity protection is provided through a *network-based* function. In the second case, the identity protection is, as in his use case, provided in the device, but the protection is targeting the *lower (radio) layers* of the protocol stack, rather than the service/application layer.

12.3.3.2 Preconditions

- Alice has a valid subscription with the MNO and a SIM that has anonymization capabilities
- Alice has a means to configure and activate her anonymization preferences (profile).

12.3.3.3 Description

Alice configures her anonymization profile such as, for example the IMSI is never disclosed to the applications requesting it, but returned in an anonymized way (e.g., with format preserving anonymization).

Basic flow of events:

1. Alice browses application market on her mobile device
2. Alice installs an entertainment application that can read the IMSI and send it to a remote server together with other app related data.
3. Alice activates the anonymization profile and starts the app.
4. When the application asks for the IMSI, it gets it anonymized and sends the anonymized IMSI to the remote server together with other app related data.

12.3.3.4 Properties of a solution

- Network provides an anonymization service that can be subscribed by users needing it (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.

12.3.3.5 Use case categories

Ensure Enablers	Privacy, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC

12.4 5G Vision

In 5G, MNOs should build and drive internationally coordinated Anti-BotNet activities or programs. All detection and prevention methods should be embedded in the MNO infrastructure, since the MNOs do not have controls on the end user devices and how users use the connected devices.

The 5G networks can offer additional (optional) enhanced security services to users that subscribe them, especially users concerned with security and privacy issues arising from mobile malware and misbehaving or unwanted applications. Such services may detect and notify to the user botnet-related activity and privacy violation activity. SIM-based (or possibly even device-based) anonymization services can as well be provided to users who want to be able to control and protect the privacy of their own data.

13 Cluster 11: Lawful Interception

13.1 Introduction

In this cluster, we introduce the use cases that are relevant to lawful interception in a 5G context. As described in Figure 17, Lawful interception involves several actors that we detail in what follows. For every use case, we give one or multiple flows of events, the potential vulnerabilities that may arise and its associated consequences, the security properties that a solution should satisfy, and the use case category. At the end of this section, we give an indication of the potential enhancements in 5G.

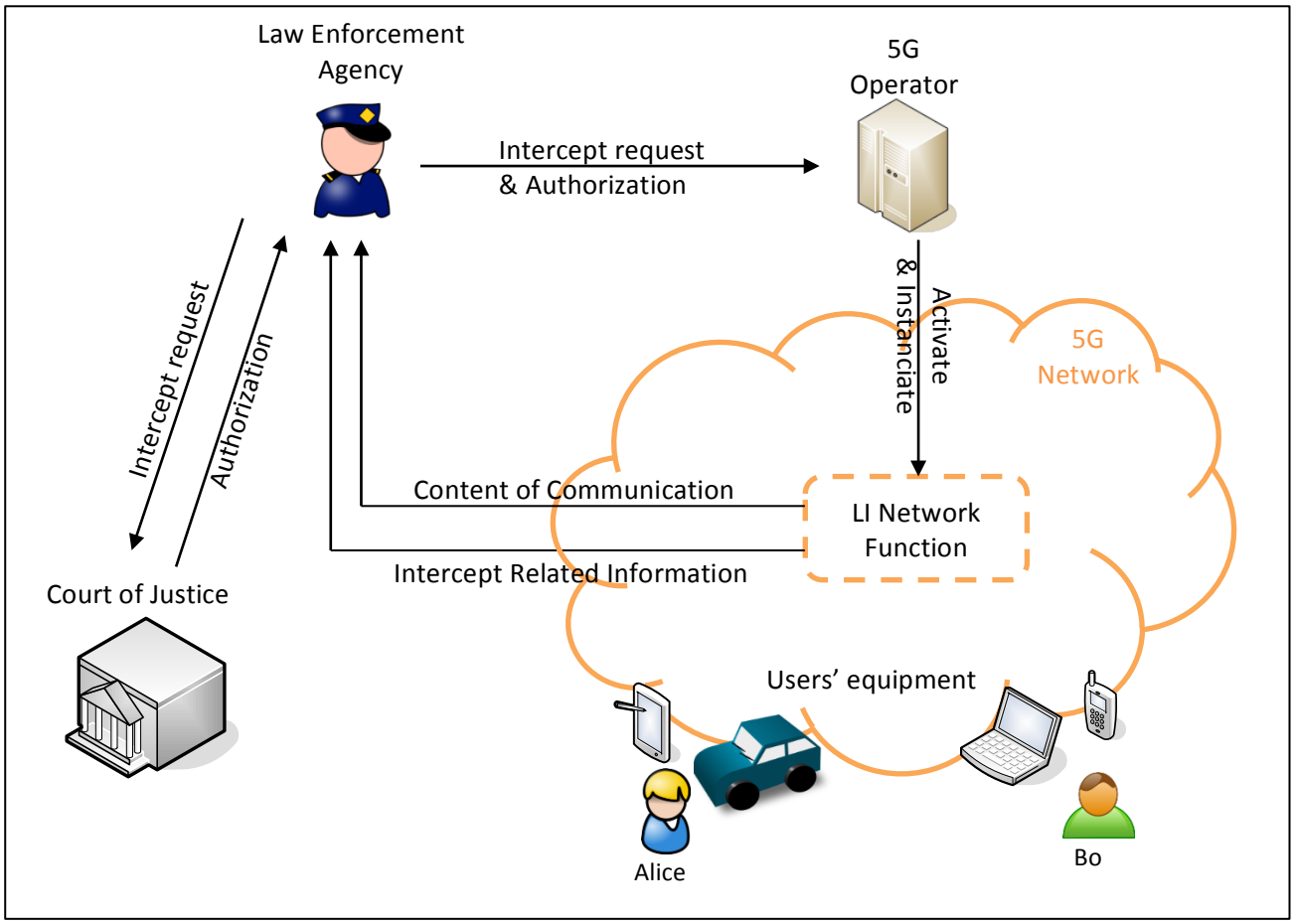

Figure 17: Lawful Interception Ecosystem

13.2 Actors

A lawful Interception ecosystem, as described in Figure 1, involves four actors.

- Law Enforcement Agency (LEA): this is the authority that intends to carry out a lawful interception on a user, a list of users, a service or a list of services.
- A mobile phone subscriber (e.g., Alice, Bob)
- A 5G Operator
- Court of justice: this is the authority that delivers the authorization to perform a lawful interception.

13.3 Use Cases

13.3.1 Use Case 11.1: Lawful Interception in a Dynamic 5G Network

13.3.1.1 Introduction

5G involves the emergence of new technologies such as SDN and NFV, and new concepts like slicing. The network is evolving from a static one to a programmable, hence dynamic, one. An MNO will, therefore, have new responsibilities. In addition to managing hardware-based network equipment's, MNO will have to ensure the management and security of virtualized resources. Virtualization, in 5G, brings out new opportunities mainly a dynamic network topology. This dynamicity would enhance the network resource management, so as to have the ability to support different services with different requirements, e.g. ultra-reliable use cases, massive IoT use cases.

In these circumstances, we attempt to show the necessary arrangements in order to ensure the LI functions. In what follows, for the sake of simplicity, we consider that LEA would like to intercept Bob's activities in a given telecommunication service.

13.3.1.2 Preconditions

- LEA identifies the suspected criminal (i.e., Bob) to be surveilled.
- LEA requires an authorization from the court of justice in order to perform a lawful interception on Bob.

13.3.1.3 Description

On demand, a 5G operator should be able to answer any interception request regardless of the target entity / user or target service [TS33.106].

Basic flow of events:

1. LEA transmits the LI request and the granted authorization to the designated service of the 5G operator to conduct the interception with regards to Bob.
2. The designated service of 5G operator checks the validity of the request.
3. Depending[2] on the intercept type (i.e., only Intercept Related Information (IRI-only), IRI and Content of Communication (CC))and the service to be intercepted, the 5G operator instantiates / activates / initiates a Network function (we call it, in what follows, LI function) that will deliver to the authorities the required information.
4. At the end of the authorized period, the 5G operator deactivates the LI function.

[2] The step 3 may be interpreted differently depending on the 5G architecture. For instance,

- In a virtualization-based architecture for 5G network, the LI function should be a virtualised network function (VNF).
- In a slice-based architecture for 5G network, the LI function should be able to detect the involved slice. If the user is subscribed to various services (i.e., slices), the LI function should be a common VNF to all slices.

13.3.1.4 Vulnerabilities & consequences

The main issues that may arise are resulting from a compromised / malicious LI function. We give further details about these issues in what follows.

- Unauthorized disclosure:
  - A compromised LI function may be activated / initiated without being triggered by the 5G operator.
  - A compromised LI function may provide to LEA information about users that do not belong to the declared list in the authorization.
  - A compromised LI function may deliver information to an external attacker.
  - A compromised LI function may continue delivering information even after the end of the designated period in the authorization.

- Disruption:
  - A compromised LI function may impact the quality a given service.

- Deception:
  - A compromised LI function may deliver to LEA fake information (e.g., services to which the user is subscribed (slices)) about the suspected user.

13.3.1.5 Properties of a solution

In this section, we describe the properties that a LI implementation should satisfy and some possible ways to do so. Those choices may vary based on the adopted 5G network architecture.

- Transparency
  - The LI function, when activated, should not be detectable. Any third party (e.g., through observation) or user (e.g., through quality of service) should not notice any change when this function is activated.

- Confidentiality
  - Only concerned entities (i.e., the 5G operator LI service and LEA) have access to the list of the wiretapped.
    → The 5G operator must be able to answer the LI request without requiring **any third part**y even when the user is subscribed to services that are not offered by the Network operator, but are delivered by the 5G network.
    → This property impacts two aspects: the LI function "location" within the network and its behaviour.
    Regarding the LI function location, two candidate solutions arise: a LI function per service (hence, within a slice) or a common LI function. The first candidate solution may violate the first and second properties (i.e., transparency and confidentiality) if the 5G operator will have to ask the service provider (i.e., slice owner) to activate the LI function. Now, if we consider that the 5G operator will not make any request to the slice owner, this may question the integrity of the service / slice. This is why, we promote the second candidate solution (i.e., a common LI function for all the slices). Of course, a common LI must be implemented in a way to still ensure it does not provide unauthorized information leakage between slices.

Regarding the LI function behaviour, the main two points are to authenticate the incoming requests from the 5G operator, and the target authority (i.e., LEA) before delivering any information.

- Dependability & reliability
  In a highly dynamic network including multiple slices and a floating topology, contrary to 3/4G, assuring trustworthiness of the delivered information.
  - The 5G operator should be able to provide high assurance that the wiretapped user / entity is indeed the required one.
  - The 5G operator should be able to provide high assurance on the validity of the collected information.
  - The 5G operator must ensure that only those under surveillance are wiretapped, e.g., Authorities cannot use the LI function to wiretap users / entities not on the list.
  - In case of an end-to-end encryption managed by the network, the 5G operator should be able deliver plain data or the encrypted data along with the decryption key.
    → Contrary to 3/4G, this property implies the protection of transmitted information in terms of integrity, confidentiality and assurance about the source of information. Cryptographic mechanism may be used in such cases, e.g., ciphering, signature.

- Security
  - Only the 5G operator should be able to activate the LI function. This would prevent fraudulent interceptions. → This property will also impact the choice of the LI function location within the network.

13.3.1.6 *Use case categories*

The LI requirements should be part of all the 5G enablers and use cases. Indeed, any 5G use case may be considered as a service where the target user or entity is subscribed.

Ensure Enablers	Privacy, Network Management & Virtualization Isolation, Security Monitoring, AAA, Trust
Next Generation Radio Technology Use cases	xMBB, mMTC, uMTC

13.3.2 Use Case 11.2: End-to-end Encryption in LI-aware network

13.3.2.1 Introduction

5G should push forward a strict privacy for users. An end-to-end (device-to-device) encryption is the only solution to ensure this requirement, especially when the communications are to or from different networks, areas or countries with unknown security level or unacceptable one. The main goal is to offer stronger protection of user data and user related information while being able to securely answer any LI request.

This use case describes how a 5G operator can prevent eavesdropping attacks on all possible paths the user data traffic follows through the mobile network. This is by augmenting identity management with additional cryptographic keys.

13.3.2.2 Preconditions

- Alice and Bob subscribe to an add-on end-to-end protection service supported by the 5G operator.
- There is a key management and key escrow server in the 5G network.

13.3.2.3 Description

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 18.

Basic flow of events:

1. Alice is connected to the 5G network and has been authenticated.
2. Alice wants to call Bob. Alice's device uses the key management service and negotiates a session key with Bob's device to be used for call encryption.
3. Alice calls Bob with encryption turned on.
4. LEA wants to intercept Alice's calls. LEA asks the 5G operator to provide access to the intercepted communications.
5. 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 communication.

13.3.2.4 Vulnerabilities & consequences

The main potential flaws of an end-to-end encryption service is to provide LEA (or any other key escrow agents, e.g., 5G operator) full control of the decryption keys or to somehow enable a backdoor which might be used for undetectable mass surveillance [Murdoch2016]. In such a case, LEA or any entity in control of the backdoor may get information exchanged out of the designated period in the authorization and/or about users not in the list (**Unauthorized disclosure**).

13.3.2.5 Properties of a solution & candidate solutions

In this section, we describe the properties that an end-to-end encryption service should satisfy and some possible ways to do so. The main idea is to encrypt session keys 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 what follow, we give further details.

- 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.

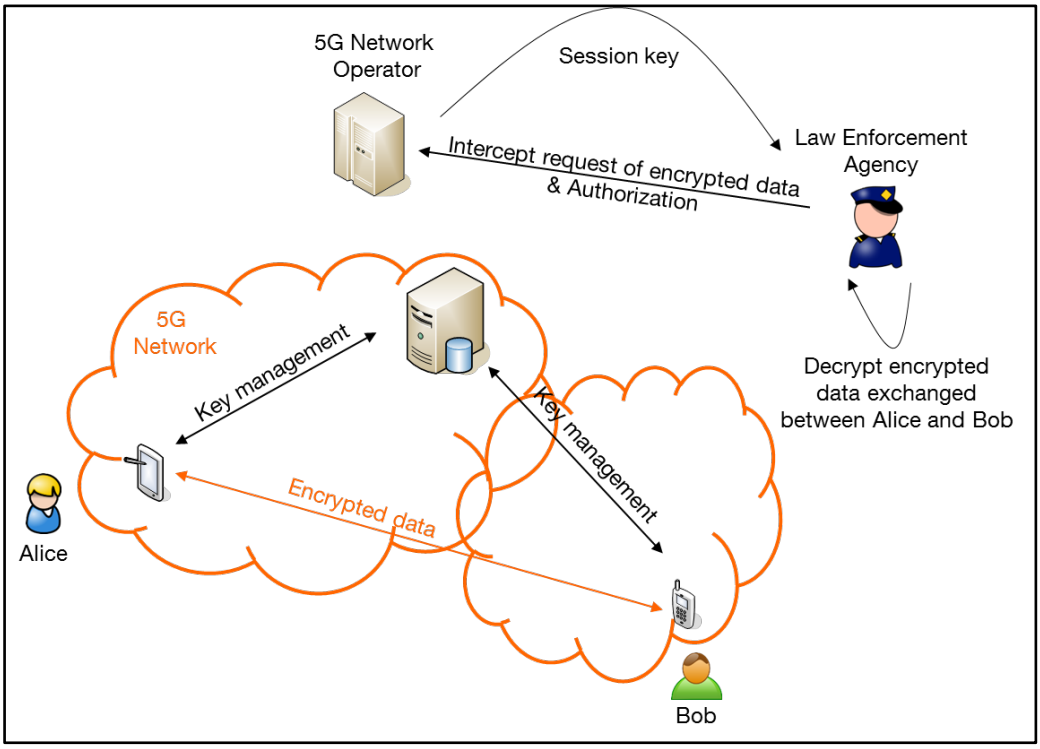

Figure 18: The operator as a trusted provider of an end-to-end encryption service

13.3.2.6 Use case categories

Ensure Enablers	AAA, Privacy, Trust
Next Generation Radio Technology Usecases	mMTC, uMTC

13.4 5G Vision

5G should be able to answer any LI request in a secure way (i.e., without compromising the privacy of any of the network users). Moreover, information delivered, in case of a LI, must be provably trustworthy.

5G should be able to support end-to-end encryption for confidential device-to-device communications (e.g., calls and SMS/MMS communications), in conjunction with key escrow for reasons of lawful intercept.

14 Summary: Use Case Clusters

This document presents 31 use cases grouped into 11 clusters illustrating the enhanced scope of security and privacy in 5G networks and systems.

Clusters 1-4 focus on **Identities, Authentication, Authorization and Privacy**:

5G should provide a variety of identity management services which expands the capabilities of devices and networks beyond the legacy Device to Radio Access Network service. For example, new subscribers or machines should be able to enrol in 5G networks, using pre-existing identity management schemes; or be able to support identity schemes enabling devices to roam between terrestrial and satellite networks.

An MNO should be able to offer additional identity management services such as trusted assertions used by third party providers, and key management enabling communication to be authenticated and encrypted end-to-end. 5G should also be able to serve Internet-of-Things devices behind a gateway and support authorization of device-to-device operations at application layer or at network layer.

Due to the pervasive nature of 5G it is essential that users have control over the privacy of their device identifiers by providing properties like confidentiality to subscriber and device identities, untrackability of the user location, perfect forward secrecy for encrypted communications and unlinkability between the user subscription information and the device identity.

Cluster 5 focuses on **Software Defined Networks, Virtualization and Monitoring**:

5G networks should provide different virtualized Core Network (slices) for different types of subscribers including different Device types, such as mMTC or xMBB, but also customer specific slices such as eHealth. Network slices may be able to provide different services, and share a common radio network. Isolation of network slices is essential. Virtualization is most likely to be transparent to many 5G nodes and also to devices and subscribers, but some 5G node components should be able to actively modify the structure and behaviour of the core network.

Virtualization bring new types of roles and actors into the picture such as the 5G Node Provider, the Virtualization Infrastructure Provider, and the Virtual Mobile Network Operator, which require adequate trust relations to be established and enforced. This also means that new types of monitoring and assurance interfaces are needed if all the new roles are taken by separate actors. Actors that are operating on top of virtualized platform should be able to monitor, verify and control what is happening in the virtualized network as well as in the virtualization infrastructure.

Clusters 6-10 focus on **Availability, Reliability and Integrity**:

5G should provide robust network services with considerable availability guarantees, in particular robustness against overload and denial of service attacks of the radio interface. Also in high load situations should prioritized devices should get priority to attach and already attached devices losing synchronization should be able to regain access. User plane data should be integrity protected enabling trustworthy services to be built on top, such that illegitimate and low priority requests should be rejected at an early stage. Threats of cyber-attacks directly targeting 5G access networks needs to be dealt with in the 5G design.

In 5G networks there should be increased assurance that the traffic is indeed originating from a legitimate entity and is bound to a legitimate entity. MNOs should not be forced to resort to implicit security assumptions about the security of the core network of interacting partners.

5G network should be more reliable in terms of having dynamic, alternative routes from the radio network into the core network (such as satellite connection). New commercial possibilities on stand-alone radio networks, and stand-alone core networks are also envisioned.

5G should provide means for coordinated botnet mitigation schemes with prevention and detection embedded in the network infrastructure, leveraging established and adding new techniques for restricting traffic.

5G networks should offer subscribers additional (optional) enhanced security services for anonymization capabilities as well as addressing security and privacy issues arising from mobile malware and misbehaving applications.

Cluster 11 focuses on **Lawful Interception**:

A 5G system should be able to answer any Lawful Intercept (LI) request in a secure way without compromising the privacy of network users, and the information provided by the LI function must be provably trustworthy and securely delivered. For this reason there is a need for a common LI function for services delivered via the 5G network which authenticates and authorizes the incoming requests and target law enforcement authority. The operators can provide trusted key escrow services within this framework.

15 Conclusions

The use cases presented in this document illustrate the need for enhanced security and privacy in fifth generation mobile networks.

The use cases exhibit a wide range of security concerns including user privacy, identity management, authentication, authorization, key establishment for IoT, air interface protection, botnet mitigation, isolation of core network functionality, secure virtualization and verification of virtualized node and platform, security monitoring and control, and lawful interception.

The use cases address security enhancements of current networks as well as security functionality of new 5G features in a balanced mix. Just to highlight a few take-aways:

- 5G encompasses a variety of radio access systems expanding the capabilities of mobile devices and networks. To allow extended offerings in terms of access or other services there is a need to support alternative authentication schemes and associated identity management, while not compromising the high security of legacy authentication and identity management.

- The increased emphasis of user privacy, including unlinkability between subscriber information and device identifiers and untrackabilty of user's location, needs to be met by new protection schemes.

- 5G networks should provide various kinds of virtualized Core Network functions (slices) for different types of subscribers or corporations which need totally different isolation properties. Virtualization bring new types of roles and actors and new types of monitoring and assurance interfaces as well as the need to verify and control the actions and entities corresponding to the various actors.

- The increasing trend of connecting important functions in society and corporations through mobile network technology leads to an increased demand for robustness and reliability in overload and denial of service situations. The balance between law enforcement and privacy revealed by the developments in the society during the last years calls for enhanced schemes for separating the concerns of the involved parties.

Most of these security and privacy enhancements requires being built-in into the radio access and core networks and cannot be added as an afterthought. The continued analysis on security enablers and security architecture within 5G-ENSURE will assess more into details the relevance of these use cases and their impact on the 5G system. However, it is already clear that security and privacy considerations such as those made in this document need to enter the development of 5G standards at an early stage to have the required impact on the security and privacy characteristics of next generation mobile networks.

References

[Chengzhe2013] L. Chengzhe, L. Hui, L. Rongxing, and S. Xuemin, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, vol. 57, pp. 3492-3510, 2013.

[EAP-AKA] J. Arkko and H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation, Authentication and Key Agreement (EAP-AKA)", IETF RFC 4187, 2006.

[FooKune2012] N. H. Foo Kune, John Koelndorfer and Y. Kim, "Location leaks on the gsm air interface," in 19th Network and Distributed System Security Symposium, 2012.

[METIS2015] "Deliverable D6.6, Final report on the METIS 5G system concept and technology roadmap", ICT-317669-METIS/D6.6, 2015.

[Murdoch2016] S. Murdoch, "Insecure by design: protocols for encrypted phone calls", Bentham's Gaze, 2016. https://www.benthamsgaze.org/2016/01/19/insecure-by-design-protocols-for-encrypted-phone-calls/

[Nohl2014] K. Nohl "Mobile Self-Defense", Chaos Communication Congress, 2014.

[Paladi2015] N. Paladi, "Towards secure SDN policy management. In: 1st International Workshop on Cloud Security and Data Privacy by Design", 7-10 December 2015 , Limassol, Cyprus.

[Razaghpanah2015] A. Razaghpanah, N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, P. Gill, M. Allman, V. Paxson "Haystack: In Situ Mobile Traffic Analysis in User Space", 2015. http://arxiv.org/abs/1510.01419

[Ren2015] J. Ren, A. Rao, M. Lindorfer, A. Legout, D. Choffnes "ReCon: Revealing and Controlling Privacy Leaks in Mobile Network Traffic", 2015. http://recon.meddle.mobi/papers/recon-sep.pdf

[RFC4949] R. Shirey, "Internet Security Glossary, Version 2", IETF RFC 4949, 2007. https://tools.ietf.org/html/rfc4949

[RFC7228] C. Bormann, M. Ersue, A. Keränen, "Terminology for Constrained-Node Networks", IETF RFC 7228, 2014. https://tools.ietf.org/html/rfc7228

[RFC7744] L. Seitz, S. Gerdes, G. Selander, M. Mani, S. Kumar "Use Cases for Authentication and Authorization in Constrained Environments". IETF RFC 7744, 2016. https://tools.ietf.org/html/rfc7744

[SchahillBegley2015] J. Schahill, J. Begley, "The Great SIM Heist --- How Spies Stole the Keys to the Encryption Castle", The Intercept, Feb 2015. https://theintercept.com/2015/02/19/great-sim-heist/

[Shaik2015] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems", October 2015. http://arxiv.org/pdf/1510.07563v1.pdf

[Smith2015] K. Smith, "Network management of encrypted traffic", IETF Internet Draft draft-smith-encrypted-traffic-management-04, Nov 2015.

[TR22.891] 3GPP TR 22.891 “Feasibility Study on New Services and Markets Technology Enablers; Stage 1”, Sections 5.20, 5.22, 5.72

[TS22.368] 3GPP TS 22.368 “Service requirements for Machine-Type Communications (MTC); Stage 1”

[TS33.106] 3GPP TS 33.106 “3G security; Lawful interception requirements”

[TS33.220] 3GPP TS33.220 “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)”

[TS33.401] 3GPP TS 33.401 “3GPP System Architecture Evolution (SAE); Security architecture”

[Vallina-Rodriguez2015] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, V. Paxson “Header Enrichment or ISP Enrichment? Emerging Privacy Threats in Mobile Networks”, HotMiddlebox’15, 2015.