electronics

MDPI

Article

Network Slicing Security Controls and Assurance for Verticals

Tomasz Wichary [1], Jordi Mongay Batalla [1,*], Constandinos X. Mavromoustakis [2], Jerzy Żurek [3] and George Mastorakis [4]

[1] Institute of Telecommunications, Warsaw University of Technology, 00-665 Warsaw, Poland; tomasz.wichary.dokt@pw.edu.pl
[2] Department of Computer Science, University of Nicosia, Nicosia 1700, Cyprus; mavromoustakis.c@unic.ac.cy
[3] Faculty of Electrical Engineering, Gdynia Maritime University, 81-225 Gdynia, Poland; j.zurek@we.umg.edu.pl
[4] Department of Management Science and Technology, Hellenic Mediterranean University, 72100 Crete, Greece; gmastorakis@hmu.gr
* Correspondence: jordi.mongay.batalla@pw.edu.pl

Abstract: This paper focuses on the security challenges of network slice implementation in 5G networks. We propose that network slice controllers support security by enabling security controls at different network layers. The slice controller orchestrates multilevel domains with resources at a very high level but needs to understand how to define the resources at lower levels. In this context, the main outstanding security challenge is the compromise of several resources in the presence of an attack due to weak resource isolation at different levels. We analysed the current standards and trends directed to mitigate the vulnerabilities mentioned above, and we propose security controls and classify them by efficiency and applicability (easiness to develop). Security controls are a common way to secure networks, but they enforce security policies only in respective areas. Therefore, the security domains allow for structuring the orchestration principles by considering the necessary security controls to be applied. This approach is common for both vendor-neutral and vendor-dependent security solutions. In our classification, we considered the controls in the following fields: (i) fair resource allocation with dynamic security assurance, (ii) isolation in a multilayer architecture and (iii) response to DDoS attacks without service and security degradation.

Keywords: 3GPP; 5G; security controls; management and orchestration; network resource model; network slicing; security attributes; slicing profile

Citation: Wichary, T.; Mongay Batalla, J.; Mavromoustakis, C.X.; Żurek, J.; Mastorakis, G. Network Slicing Security Controls and Assurance for Verticals. *Electronics* **2022**, *11*, 222. https://doi.org/10.3390/electronics11020222

Academic Editors: Juan M. Corchado, Stefanos Kollias and Javid Taheri

Received: 15 December 2021
Accepted: 7 January 2022
Published: 11 January 2022

1. Introduction

Vertical customers are interested in what 5G with network slicing may offer. The new improvements and capabilities that 5G brings include fast data transfer, ultrareliable and low-latency communication, mass device connectivity and better coverage and capacity. We can tailor these functionalities for a created solution and customize network slicing according to the various service requirements from vertical industries. Network slices provide critical services where unauthorized access to sensitive data and communication failure are unacceptable. It requires that service, including the network slice, be secured. In addition, it is essential how the infrastructure is deployed because the network slice should not exhaust resources from other slices under attacks such as Distributed Denial-of-Service.

We understand a network slice as a set of expected infrastructure behaviours that must maintain business continuity even when the slice is compromised. One solution is to put the network slice in quarantine, partially or entirely, and then recreate the expected infrastructure behaviours with noncompromised components.

The introduction of virtualization technologies has put new challenges on the need for high reliability, including network slice security, due to sharing resources. Virtualization raises many concerns about network slice security related to the impact of one slice on

another. These concerns come down to isolating network slices to avoid the consumption of other network slice resources. We may consider isolation at different levels: (i) quality of service isolation and quality of experience isolation, where traffic from one slice could not impact traffic and services belonging to other slices in the same network, (ii) data leak isolation, where the attacker can access sensitive information, and data breach due to poor security protection and accidental actions, (iii) data processing, where packets and information are processed independently and do not affect other slices, and so on.

We can as well consider network slice protection in terms of security levels. The design pattern of network slice specification allows defining the required security protection level. As an example, we can consider the following cases: the higher-security level for high reliability and low-latency communications requires robust reliability, strict authentication protocols and strong cryptographic protocols and methods; however, the moderate-security level for network slices with high connectivity specifications requires security enhancements from LTE and the lower-security level of constraining devices with long battery life requires concurrent security access, privacy protection and lightweight security mechanisms. Cybersecurity offenders may use lower-security slices as entry points for their attacks. Such compromised slices may cause problems for higher-security protected slices due to shared resources between slices.

The vertical requirements [1] indicate that the most desirable 5G feature is network slicing with reliability, availability and latency. The network slicing with shared infrastructure may reduce these requirements' implementation costs, as shown in [2]; however, forefronting technologies developing shared infrastructures, such as cloud computing, impose other severe problems with security and privacy [3]. Thus, the security management and orchestration of slices must overcome these challenges when implementing shared services and avoid human burden operations, which is a critically important reason for automating security operations. The main challenges, from the point of view of security, for managing slices and their orchestration are (i) services recovery for multitenant and multivendor environments, (ii) multicomponents interoperability, (iii) security risk management based on well-known threats and possible countermeasures and (iv) isolation of end-to-end network slicing in complex systems. The network slice controller can handle the orchestration of various 5G functions and infrastructure components to manage slice requirements. In this case, the orchestration process of the 5G system, network resources with provisioning capability of security controls, such as safeguards and countermeasures, are employed to reduce identified risk for services.

The heterogeneity of resources generates challenges for management and orchestration. One essential approach is to deliver services where various technology domains communicate with each other [4]. In a hierarchical orchestration model, a high level of abstraction hides the orchestration complexity process distributed over multiple technology domains (see Figure 1). The orchestrator (network slice controller) makes decisions based on attributes describing how the network slice serves the service. Such attributes are a high-level abstraction that provides requirements for selected network parts to enforce specific behaviour. The attributes represent delegate operations in the domain level, e.g., radio access network, fixed access network, transport network and 5G core domains. The delegation approaches rely on declarative languages to specify the resource needs (e.g., for containers at the cloud-native approach, virtual machines (VNF) or physical elements), which is a desirable approach for security safeguards and countermeasures when infrastructure employs many underlying technologies (e.g., firewalls, resource separation in virtualization platforms [5], carrier-grade network address translation). The top-level/service orchestrator sends the instructions to domain/lower-level orchestrators in order to construct service and fulfil the requirements from the service order. A low-level orchestrator has a limited scope of operations to orchestrate resources used for building domain-specific services. It translates the high-level abstraction layer to a more concrete form and converts it to low-level configuration parameters. The top-down hierarchical orchestration management instructions are called metadata attributes or parameters. The

decision process is centralized over the resource management for the end-to-end network slice, including radio [6].

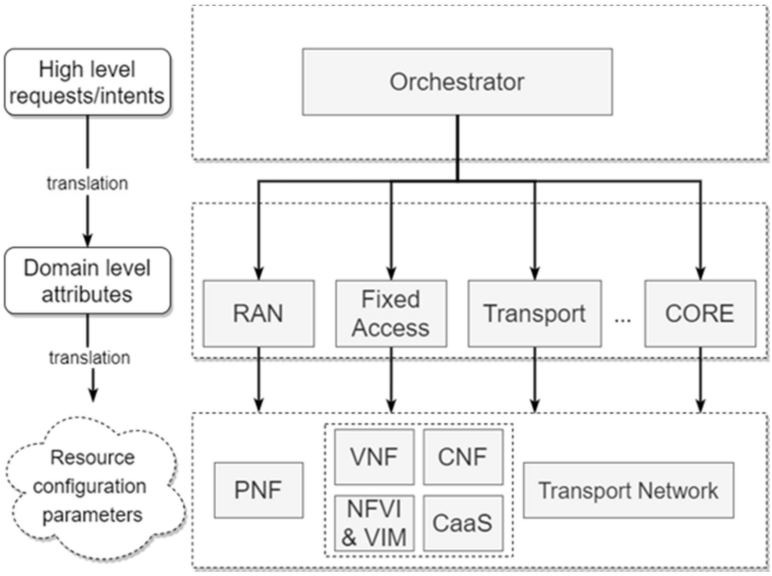

Figure 1. Orchestration management hierarchy for 5G network slicing.

The translation procedure of high-level attributes depends on how the orchestration model adopts it. The service delivery model generally represents a closed system with a finite number of states that specifies actions based on established policies and rules. The orchestration system may perform many actions simultaneously; for example, it enforces contradictory management, which requires detection and resolution of policy conflicts; at the same time, intent-driven management introduces a new layer between user or application and service and policy model. The translation of the abstract layer to underlying models could be synchronized and implemented step by step between layers or by auditing the underlying layer in alignment with the intent.

The problem is that metadata for security controls are not defined sufficiently and causes difficulties in selecting appropriate security mechanisms. Therefore we need a metadata framework that maps attributes to security controls in order to manage security. The lack of security control attributes in 5G network slicing is due to a lack of a comprehensive framework for implementing such controls.

In conclusion, network slice requirements are based on an agreement between mobile operators and verticals. These requirements are called Service Level Specifications (SLS) and include data rate, traffic capacity, user density, latency, reliability and availability, among others. These SLS define how the slice controller should orchestrate the network to fulfil these requirements. The standardized parameters do not specify comprehensive security aspects of network slicing, especially when considering many underlying technologies (e.g., virtualization platforms, cloud, firewalls and Application Content Filtering). It takes effect in that when we consider different underlying technologies, many researchers have required a more comprehensive approach to security. We also support this request in our prior research studies [7,8]. In the proposal shown in this paper, we propose a comprehensive selection with the definition of the classes of the parameters that impact slice security so that those parameters may be included in slice specification and be part of the orchestration procedure for initiating the slice configuration. In this way, the lower-level orchestrators may map the parameters to concrete technologies at the underlayers.

The remainder of this paper is organized in the following fashion: Section 3 goes through the 3GPP Network Resource Model and Service-Based Management Architecture and presents the slice profiles concept with standardized attributes by 3GPP and GSMA. We analyse safety-related attributes and define the security classes for isolation at different

levels. In Section 4, we present security domains for security attributes. Our analysis intends to open a security model based on security architecture with eight security domains. This model is based on standardized technical specifications so that the security controls may be mapped to security attributes in slice profiles. Section 5 analyses technology and security controls out of the 3GPP scope and proposes several security solutions. We perform the functional classification of security controls, adding non-3GPP safeguards and countermeasures. Section 6 presents an example of the requirements and security constraints based on predefined and available security controls for two slice profiles. Finally, Section 7 includes the main conclusions of the paper concisely.

2. Related Work: The Standards

In the 5G White Paper [9], the NGMN Alliance provides security recommendations for increasing the security level of the access network by introducing automated network management and control networks while minimizing the number of repetitive tasks. Automation limits the burden of repetitive manual tasks and human presence and thus minimizes the possibility of human error, increasing the security of the network and its management [10]. The architecture for autonomous networks has been analysed in the context of interaction between autonomous components, see [11]. The management has been structured hierarchically to reduce the overhead exchange communication. However, managing resources with child components challenges the complexity of network management systems, thus risking scalability capacity. The recognized security practices for all kinds of communication, including critical national infrastructure (CNI), was considered by the NGMN Alliance in security recommendations [12].

The management solution with an automation monitoring and enforcement process may protect cloud services effectively by detecting and replacing automatically compromised components. Automation of security risks and analysis of well-known and new threats jointly to enforce countermeasures is the subject of many research studies, e.g., [13,14]. The models are designed for one specific solution and do not follow the target automation capabilities required by the telco.

More general approaches may be found in ISO 27000 series standards from the International Organization for Standardization (ISO). The standard ISO 27005 [15] provides a methodology for implementing information security risk management. It does not recommend any risk management methods. Still, it shows a process of structured sequences activities concisely so that it is possible to build a risk security index (RSI) based on this process. Such an RSI may be helpful to create an automation process model for security incident prioritization.

The input point of any RSI should be the requirements of the service specified in the SLS and, concretely, in the slice profile. This profile focuses on functional requirements. As security is an inseparable component of network slicing and 5G systems, there is a need to build a security model for managing security risks for network slices with slice profiles that contain security requirements. In addition, it is critical to have the relevant model to address specific security problems, including data protection and privacy for the complete 5G system. The complexity of 5G network slicing security models arises when the infrastructure needs to be shared, e.g., a network function using shared resources. In Release 16 (a set of documents standardizing some mobile network features), the network management includes a modular framework, which allows the orchestration of components coming from different vendors. This framework is based on Service-Based Management Architecture (SBMA) that provides the fundamental building blocks of Management Service (MnS) producers and MnS consumers.

The MnS producer provides MnS capabilities to MnS consumers [16]. Three MnS components types are defined: A, B and C. MnS component Type A (MnS Type A) provides notification and management operation, for example, creating, deleting and updating information objects. Manipulating the signature of operation and creating a performance report are examples of MnS Type A. These activities are generic and do not manipulate informa-

tion from the managed element. In its part, MnS component Type C (MnS Type C) provides alarm, malfunctioning information and performance measures of managed data [17]. Examples of MnS Type C are:

- the measure of modification attempts for requested PDU session modifications initiated by UE and received by SMF and
- the measure of modification attempts for N4 session modifications.

At last, MnS component Type B (MnS Type B) is a so-called network resource model (NRM) and represents management aspects of 5G networks.

A Management Function (MnF) comprises at least two element types, with MnS Type A and B or MnS Type A, B and C (see Figure 2). The MnF may have multiple customers and consume multiple MnS from producers.

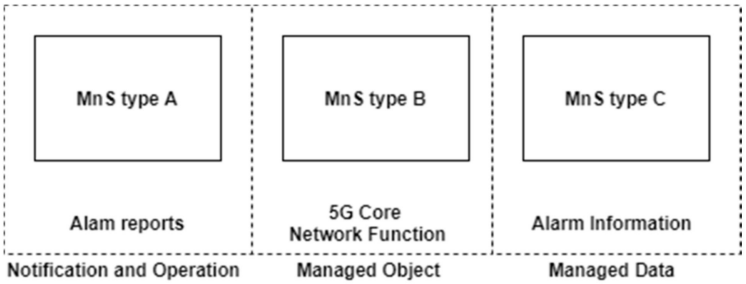

Figure 2. Management Service with MnS types A, B and C for 5G Network Function [18].

The management capability governance exposes MnS and MnF that should access to the MnS producer [19]. A Network Function (NF) may be one example of MnF. The NF may provide management services, such as configuration, performance and fault supervision services for, e.g., a network slice. The scope of possible management operations depends on the type of MnS components. MnS Type B is essential for our metadata security framework as it may keep information (e.g., security attributes) about security controls.

The following information models can be found in the 3GPP TS 28.541 [20]:

- The 3GPP 5G NRM supports modelling RAN (radio access network) and core network slicing from a generic NRM definition [20];
- A generic NRM template is defined in TS 28.632 [21];
- The NG-NRM (NRM for Next Generation RAN) is defined in Clause 4 of TS 28.541 [20];
- An NRM for E-UTRAN (4G) and updated for NG-eNB (4G base station connected to 5G core network) is defined in TS 28.658 [22];.
- 5GC (5G core) Network Functions (NF) such as AMF (Access and Mobility Management Function), SMF (Session Management Function), UPF (User Plane Function) or UDM (Unified Data Management) are required to define many end points and attributes for defining the NRM. These NRMs for 5GC NF are defined in Clause 7 of TS 23.501 [23], and 5GC NRM is defined in Clause 5 of TS 28.541;
- Network Slice (and Subnet) are a set of Management Functions (MnFs) that also require resources (e.g., CPU, memory and network) and, therefore, are also based on 5G NRM. Network Slicing NRM with models of NSI (Network Slice Instance) and NSSI (Network Slice Subnet Instance) is defined in Clause 6 of TS 28.541 (see Figure 3).

The NGMN [24] defines network slice capabilities employing service instance, Network Slice Instance and resource layers, and it provides a high-level understanding of the network slice concept and positioned requirements. The instance constitutes components of the slice inherited from the slice profile that describes the slice requirements. A Service Instance represents each service from end-users, enterprises and verticals, whereas the Network Slice Instance (NSI) provides the network behaviours based on service instance requirements and may have none, one or many of the Network Slice Subnet Instances (NSSI). These NSIs/NSSIs may be shared between SIs and are represented by Network Functions and resources. The Network Functions may utilize physical, logical and virtual

resources. The NF may share resources, which can be shared or dedicated to the NS(S)I. The idea of Network Slice as a Service (NSaaS) [25] refers to this generic network slice model.

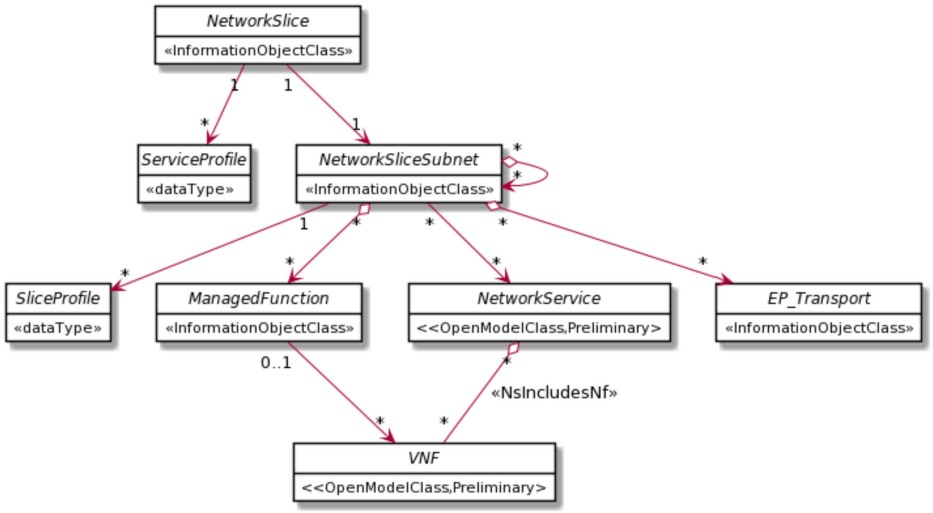

Figure 3. Network Slice NRM relationship [20]. Note * denotes zero or more.

On top of NSaaS, Security as a Service (SECaaS) [26] integrates security controls and monitoring into infrastructure and network functions to provide more cost-effective solutions. The SECaaS is a multitenant, scalable, virtual and customized service offered in usage/subscription-based pricing. Finding the appropriate security controls and monitoring is fundamental for the modularity of the offers to the market. It is challenging to steer these mechanisms from orchestrators at the management layer.

We mentioned earlier that NRM (MnS Type B) is necessary for managing security requirements and storing metadata (attributes). The following section shall explain where the attributes of the network slice are and how the slice profile is created with information data.

3. The Security Model for Hierarchical Resource Isolation

The NRM differs depending on the technology domain and the hierarchical management model (NSI/NSSI). Each technology domain expects specific infrastructure behaviours. It is relevant for many use cases for vertical industries. The use cases, with their characteristics and network slice requirements, need a standard method for describing the characteristics. The 3GPP proposes mapping the network slice subnets with service level requirements to the network slice subnets' components. We have the technology-agnostic attributes represented by slice profile (NSP) in the information model for the Slice NRM.

The NSP constitutes a set of metadata. The metadata provide structured references for identifying the attributes of the various infrastructure layers, network stack layers and services they describe. The Telecommunication Management Network (TMN), defined by ITU-T, provides general architecture requirements for telecommunication networks and services. The TMN groups functions into many layers [27], such as (i) business applications/management, (ii) service orchestration/management, (iii) network control and management, (iv) VNF control and management and (v) network and resources.

Different layers provide different scopes and levels of abstraction. Their purposes are different and required by the various departments in the organization. The Network Functions (NFs) become the general computation processing capable nodes in a cloud-enabled environment. The NFs are virtualized, decomposed and placed in different locations. The flexibility of NFs allows for providing, e.g., eMBB communication at centralized cloud and during a URLCC communication with latency constraints at the edge. Standards development organisations (SDOs), such as 3GPP, do not analyse Network Function (NF) itself. NF internal implementation remains vendor-specific. According to 3GPP TS 28.531 [19], slice profiles are some of the key elements used for the allocation process of the network

slice and how it utilizes NFs and resources across various infrastructure domains. The standardized values used in slice profiles can differentiate network slice types, and we may take them from the Generic Slice Template (GST) [28]. Slice profiles, understood as network slice types (NEST), are GST templates with filled values [20]. We may distinguish two types of NEST:

(i) Standardized NEST (S-NEST), with values provided by SDOs, e.g., 3GPP, GSMA, 5GAA and 5G-ACIA, and
(ii) Private NEST (P-NEST), with attributes defined by slice providers themselves.

The 3GPP indicates that the network slice should be supported by network service [20]. The service functionalities include service (de)registration, authorization, discovery and interservice communication.

The management services are built by a set of MnS components. The number of available components increases with new 3GPP releases. The NRM parts are defined for various management tasks to construct information models tailored to specific network management services. The examples of NRM parts are state and configuration, performance metrics and service assurance control. The attributes proposed by 3GPP are based on functional and QoS requirements. The top-level slice profiles with attributes and corresponding values are translated to the subslice profiles and finally to resources and configuration parameters. An attribute that is a pure security and isolation attribute is resourceSharingLevel with possible values: shared, nonshared (see Figure 4).

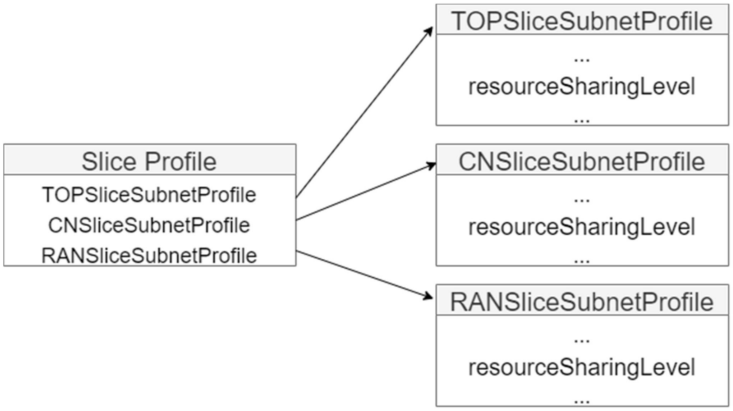

Figure 4. Network slice modelling by the 3GPP. Note: TopSliceSubnetProfile represents the top slice network slice subnet.

The 3GPP SA5 work closely with GSMA to align slice network slice management and orchestration. The GSMA provides a standardized list of attributes that characterize network slices. The parameters define high-level requirements and do not indicate how they should be implemented. The attributes responsible for security include 'Isolation level', 'Network functions owned by Network Slice Customer', 'Simultaneous use of the network slice' and 'Network Slice Specific Authentication and Authorization (NSSAA) Required'.

In the 3GPP Slice Profile and Generic Slice Template, we have an attribute that represents a level of isolation. Isolation is a critical mechanism in the 5G system and the security domain, and it is expected to play a crucial role in network slicing. GSMA define isolation levels as:

- physical with separation of memory, network and processes and
- logical with virtualization on different abstraction-resources, networks and tenants.

The 'Network Functions owned by Network Slice Customer' attribute provides a set of network owners and is provided by the customer. It also provides an implicit mechanism of isolation. The attribute 'Simultaneous use of the network slice' describes whether User Equipment (UE) can use a slice with other slices. It limits the risk of malicious interslice traffic, where UE could operate as a router or proxy service.

Further study is ongoing, and some research updates about a hybrid usage of isolation levels are expected in the next 3GPP releases. The relatively new attribute 'Network functions owned by Network Slice Customer' provides a list of network functions owned by MVNO, which has its own MCC+MNC codes and, for example, could require storing all the subscribers in its UDM. Another new security attribute is 'Network Slice Specific Authentication and Authorization (NSSAA) Required'. This attribute requires a secondary authentication method by the AAA server (Clause 5.15.10 of 3GPP TS 23.501).

This approach limits the number of potential slice types. The mobile network, such as a 5G system, is not a one-size-fits-all type of bit pipe with extreme speed. The network has full virtualization, sophisticated SLAs, simultaneous mass connections, security protection levels and various possible isolation mechanisms.

The attributes with a hierarchical model allow for taking into account the impact of attributes on the various levels between them. It, in turn, allows different levels of isolation to be distinguished. When creating multiple virtual networks, such as network slices in a shared infrastructure, isolation mechanisms become fundamental in ensuring that network slices are independent of each other. Figure 5 proposes an approach with new security classes for attributes. A high-level mapping of attributes to low-level configuration parameters is easiest to develop when grouping the attributes into classes.

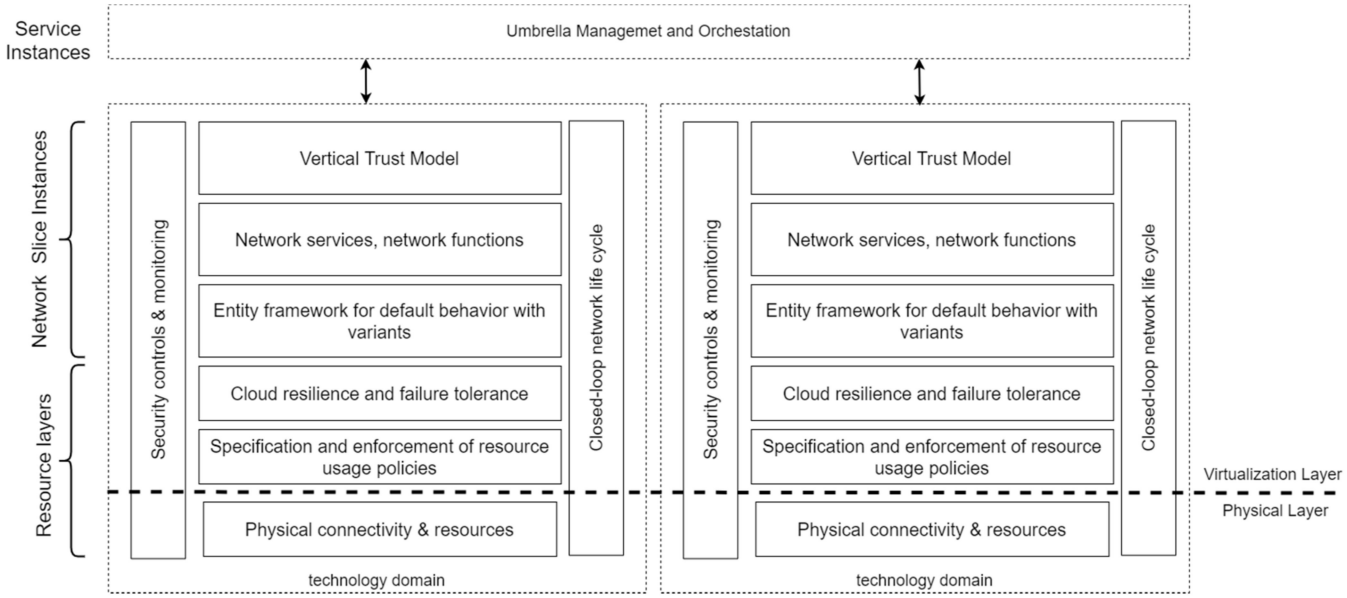

Figure 5. Network slice isolation classes.

As depicted in Figure 5, we associate the isolation classes with layers and instances defined by MGMN to understand the security model better. We will discuss these classes in the following points.

The **Vertical Trust Model** is relevant when we need to separate, e.g., for the Mobile Network Virtual Operator (MVNO), verticals and enterprises in many use cases. The specific use cases depend on the number of services and their requirements. The alternative approach to shared infrastructure with network slicing is a nonpublic 5G network that isolates resources to have QoS autonomously, the proximity of ultra-low-latency and secures stored data locally. Our model combines these two approaches: network slicing with S-NSSAI and private network with NID identifiers [23]. The NID identifier can be used to distinguish vertical private networks further. The S-NSSAI identifier is deployed within the private network to realize service provided in the network slice for vertical identified by NID. The S-NSSAI is composed of slice type and slice differentiator (SD), where the SD is used to differentiate tenants, e.g., verticals, enterprise and services [20,29]. The network

deployment with the above identifiers provides the flexibility to define many types of network separation with virtual networks and for isolation approaches (see Figure 6).

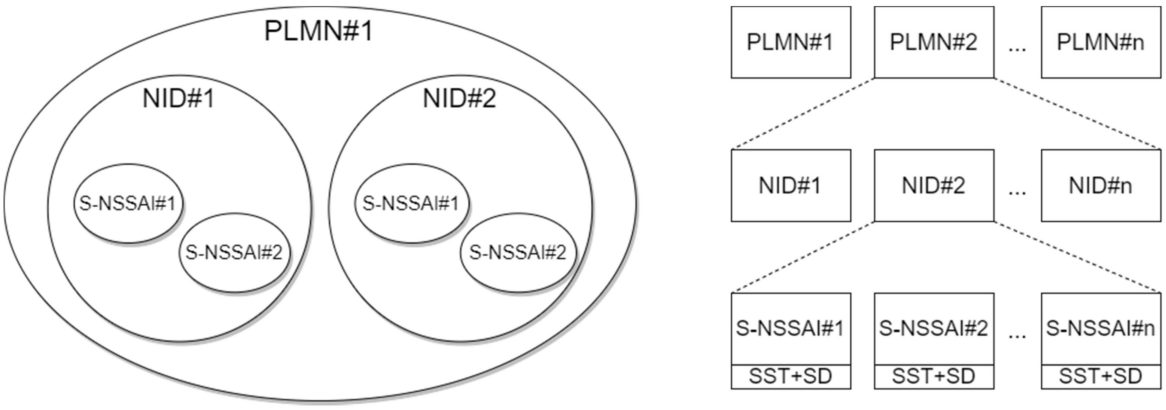

Figure 6. Hierarchy of network identifiers.

The behaviour of network slices refers to the service/slice type (SST) included in network slice identity. This approach is to share standardized slice behaviour to tenants distinguished by SD. It is a convenient solution because it simplifies management and reduces the effort to launch similar services such as video streaming. A combination of PLMN and NID identifies many set-ups of the 5G nonpublic network. This combination is globally unique and enables the connection between different MNOs. Filtering the 5G network resources with identifiers such as PLMN + NID + S-NSSAI (see Figure 7) provides a new view of trust domains.

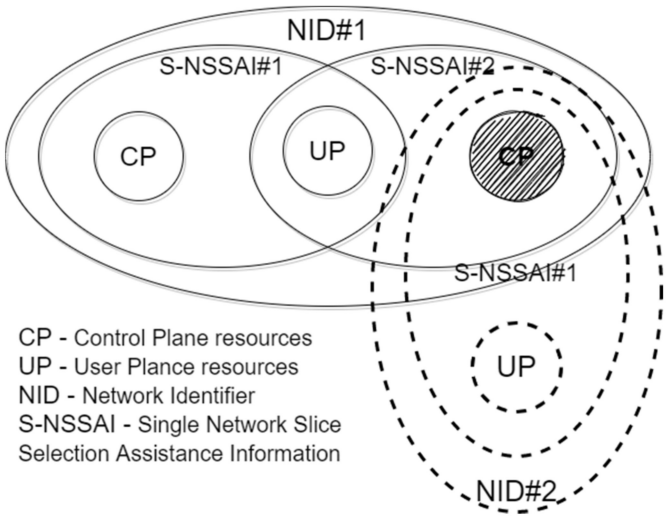

Figure 7. Trust domains in a hybrid private network with shared resources and network slices.

The trust model [30] provides an approach where services with similar characteristics (the same SST) may share elements prepared to handle such services to meet joint QoS/QoE requirements. Figure 7 presents examples where two S-NSSAIs share the same UP resources, while two S-NSSAIs belonging to different network IDs may share resources from the signalling part.

Our qualifiers are:

- QoS/QoE isolation supports by grouping resources with the same network identifier, which allows us to take away some resources and move to private premises, mainly supporting time-sensitive communication;

- Isolation and processing of sensitive data/databases on-premises, which may avoid data leaks;
- Sharing of service components without critical security, latency and reliability in this isolation class;
- Signalling protection, which is critical to mitigating any attackers' use of CP signalling and trusted relationships.

Network services, network functions. This class is an underlayer of the Vertical Trust Model. It is not entirely detached and inherits risks with better resource accuracy. Trustiness defines how the network function and service are deployed and defines the traffic boundaries for unconditional access to services.

- In the control plane, we may define a trust boundary in Service Base Architecture with Network Repository Function (NRF) acting as OAuth2 Server for secure communication between NFs.
- Separating the UPF from the network defines the trust domain for the data plane.

Our qualifiers are:

- Access tokens coordinating signalling isolation and trust boundaries [31];
- Validation of network function with slice identity belonging to the network slice;
- Network entities being shared or nonshared between slices.

Entity framework and specification for default behaviour with variants. The slices can have special requirements, different from predefined standard solutions. For example, the network slice requires access to slice with secondary authentication access control for mitigating DDoS attacks. The standard solution may involve an authentication and authorization server hosted by the Mobile Network Operator (MNO) and a firewall with DDoS protection embedded in the User Plane Function (UPF). The UPF can prevent DDOS attacks, including volume-based and protocol attacks (e.g., SYN floods). This solution consists of changing the authentication and authorization server configuration or changing the server to an alternative one and may also mitigate DDoS type attacks for the Application Layer (e.g., GET/POST floods). The variant configuration is created by modifying existing network slicing components and may influence other slices.

Our qualifiers are:

- The system needs an error-prone configuration and
- A process of decision support for supporting configuration alternatives that understand configuration limitation, dependency and restriction [32].

Cloud resilience and failure tolerance. This class defines the criteria of end-user service agreement. Resilience is a measure of cloud capacity and application to continue to operate in the presence of system degradation and failure [33]. Cloud resiliency requires adaptation to changing conditions, self-healing and autonomous recovery. When the cloud system notices a failure, the rest of the cloud usually continues to function.

Failure tolerance is when failure does not impact service except for, e.g., some delay during service failover. Failure prevention and convergence of recovery require a strategy and a model with recovery service algorithms and adaptation to a new operation state of the system. The component of the network slice needs to be recovered and the failure prevented from being expanded to other slices.

It is important to define metrics correctly to measure resilience and monitor violations. The potential resilience issues are relevant to security issues, e.g., sniffing, session hijacking and flooding attacks. The reliability metrics/attributes are: mean time to failure and mean time to repair, but other attributes also affect service directly or indirectly [34].

Our qualifiers are:

- Availability pattern measured in percentage of uptime;
- Geographical redundancy, the system composed of decentralized locations;
- Resiliency refers to continuing work without interruption during increased security disruption, e.g., volumetric attacks.

Specification and enforcement of resource usage policies. Slices may have various resource requirements, and resource isolation may prevent cloud infrastructure overload. This attribute class may solve problems with consistency in infrastructure for critical communication within the slice. It means that any other slices cannot leverage the resources assigned to a network slice, but it does not mean that all slices have a fixed amount of resources available. For example, it could be a minimum guaranteed amount of resources. Resource isolation may reduce the influence of the overloaded infrastructure or DDoS attacks on the network slice. In addition, the system needs to have a mechanism that prevents any potential attacker threatening one slice from accessing other slices in the same infrastructure.

Our qualifiers are:

- Resource management policies: do not accept workload in violation of policy; limit workload per instance; optimize resource allocation with localization constraints; load balance resource allocation with optional constraints, e.g., energy consumption or vulnerabilities scanning score reports; guarantee traffic quality parameters and
- Policy enforcement points: the components that enforce resource policy decisions.

Physical connectivity and resources. Physical connectivity is the protection mechanism from any physical actions or events, which could cause severe loss and damages. The physical protection can be measured and considered during a closed-loop network slice life cycle. The server room can be equipped with a surveillance cam monitor. The presence of unauthorized personnel will lower the security ranking. It also concerns servers without physical backup or active removable media, e.g., USB ports.

Our qualifiers are:

- Access control to the facility; identification and accountability of personnel; detection of unauthorized system access; authorization, e.g., with access cards or fingerprints.

In addition to all levels of slice resource isolation, we should consider automating creating a network slice. Therefore, we need to ensure that this process of managing the slices also incorporates the required security level to enforce isolation at all levels. In our vision, we introduce two vertical levels where security and isolation must be considered:

Closed-loop network life cycle. The network slice is not a static concept. It must be created, updated, terminated, tested and verified before deploying or extending the use to other slices. The network slice may require quarantine due to the threat of an attack and needs to be reconfigured in real time. The manual resource management for network slicing is not an optimal resolution. Hence, the life cycle process enables dynamically reacting heterogeneous service requirements. The whole network slice process of reconfiguration can use a machine learning algorithm that needs to tune some parameters to meet formed requirements, e.g., the quality of service and experience or predefined security level.

The **security controls and monitoring** functions minimize the impact of isolation classes on each other. The isolation mechanisms prevent information flows between other (non)security components at various isolation classes. It is sometimes impossible to achieve strict isolation, and we can only minimize security risks. Implementing the layered structure with continuous monitoring as well as collecting and measuring potential security threats enables isolation against network complexity.

The sharing infrastructure reduces operational costs and increases possible applications. The isolation of (un)trusted slice components across all isolation classes may be considered as one of the dimensions of the network slicing security model.

4. The Proposed Solution for Attribute Definition and Model

The provided isolation classes define only one aspect/dimension of the security model and the methodology for separating resources on the same platform (virtualized or physical machine). Another problem is securing the end-to-end service itself. Our model aims to extract the subsystems of the 5G system where security attributes could be defined and implemented. Those domains provide the next dimension and extend isolation classes

with security domains into the SECaaS model. Concretely, we propose the following eight security domains of the 5G system for deploying and mapping the security attributes. Three of the proposed domains are at the user plane (transport of users' data), three are at the control plane (transport of control data), and two domains are common to both planes.

The security domains only for the user plane are: (i) Service-oriented Safeness, (ii) Secure Application Layer and (iii) Secondary Authentication (also requires the involvement of the control plane).

The security domains only for the control plane are: (iv) Service-Based Architecture Security, (v) Exposure Security and (vi) Authentication and Key Management. Last, the security domains common for both control and user planes are (vii) Network Access Security and (viii) Network Transport Security.

As depicted in Figure 8, we associate the security domains with control, user planes and instances defined by MGMN. This figure positions them in the 5G system, provides an overview of possible security challenges and slices orchestrator views within the management domains: UE, Access Network, Core Network and Services. The management domains show where the life cycle automation processes are needed. Altogether, they are referred to as an end-to-end system from UE to the service or SECaaS supported by security domains. In the background of the figure, the components of the 5G network architecture include Network Slice Selection Function (NSSF), Authentication Server Function (AUSF), Network Repository Function (NRF), Unified Data Management (UDM), Policy Control function (PCF), Network Exposure Function (NEF), Access and Mobility Management Function (AMF), Session Management Function (SMF) for control planes and User Plane Function (UPF) for the user plane. The eNodeB is connected to the UPF to transfer application data and the AMF for control plane signalling.

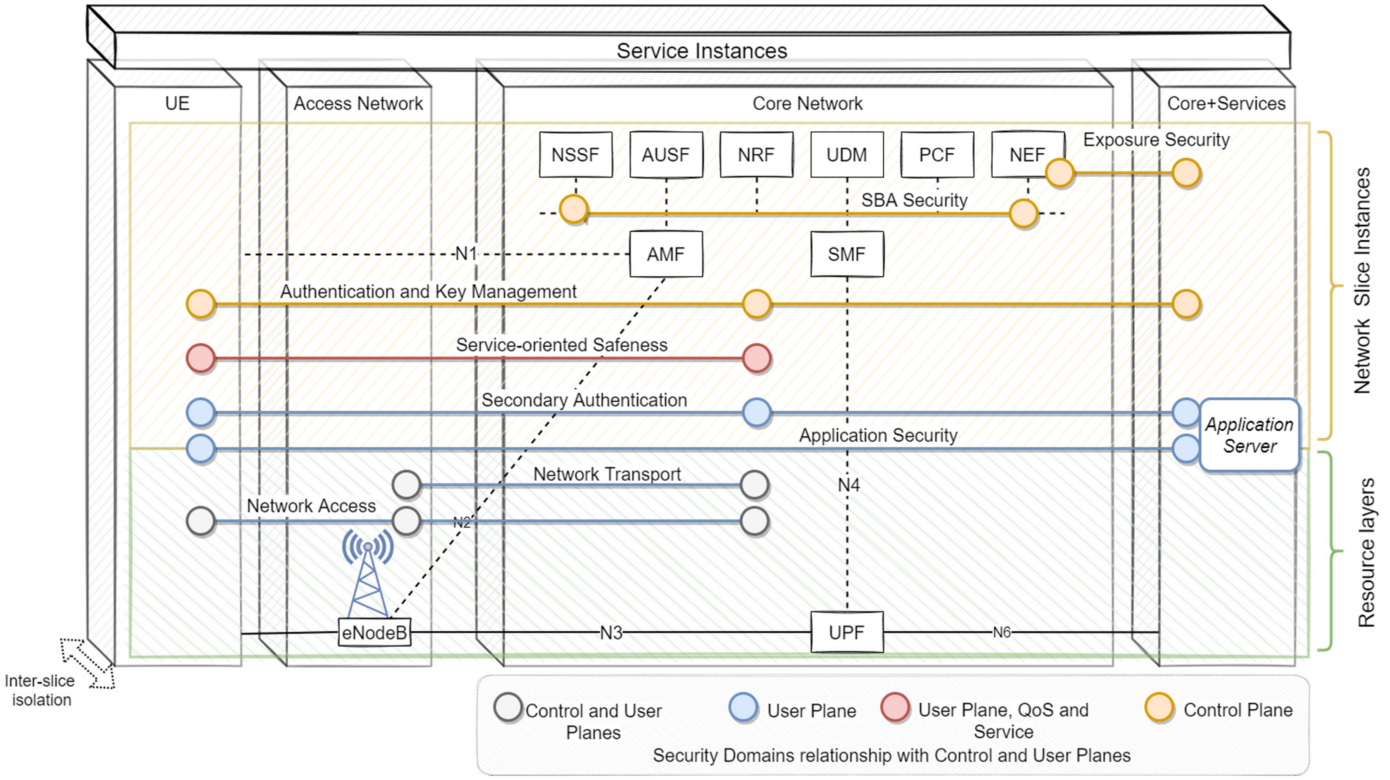

Figure 8. Security domains of 5G networks.

On top of security domains, we have different security management areas to support end-to-end security. Security Assurance Management implements controls to protect the network, the services and the information; however, Security Assurance Management does not guarantee that controls will protect the network from all external attackers. Therefore,

the Mobile Network Operator (MNO) needs to employ continuous vigilant surveillance of its network resources and slice components to complement this effort. For example, Security Assurance Management should be supported by Security Policy Enforcement Management to ensure secure network assurance management, Detective Security Controls to detect and respond to security incidents and noncompliance with security standards and Device Policy Management to establish rules and security policies for User Equipment to prevent cybersecurity attacks.

The domains with the necessary security attributes are:

Service-oriented Safeness. The 5G network evolved to service-oriented architecture, which is capable of implementing end-to-end quality of service (QoS) and quality of experiences (QoE) [35]. The service-oriented architecture guarantees Service Level Agreement (SLA) and Security Level (SL) requirements towards the network service. The control plane functions map the service requirements concerning QoS, QoE and security to data plane functions' behaviours. The QoS and the QoE are based on different measures and cannot guarantee each other: while the QoS measures network performance and its metrics typically are bandwidth, latency and jitter [36], the QoE focuses on individual user experience and satisfaction of offered service. An example of QoE is the Mean Opinion Score (MOS), where the user rates the service quality on a scale from 1 to 5, where 5 is excellent and 1 is bad.

In our model, service security could be an additional aspect that the network provides In addition to the QoS/QoE such that the service would require confidentiality and integrity in the transmission path and specific security controls in radio and core networks. The identified problems are the following:

- Encryption can introduce additional latency;
- Attacks may be directed to protocols negotiating QoS;
- Resource allocation problems conflict with constraints from QoS and security;
- Security control may overuse resources and deny service.

Our qualifiers are:

- When we consider security as part of the quality of service, the QoS mechanisms must be resistant to various conditions, including security control, which introduces latency to protect service from attacks, and
- When mapping security controls, they should define the security attributes and be mapped to required security levels.

Our expected outcome is a new security level with graduation protection and detection security controls and remote QoS service monitoring.

Secure Application Layer. Application security is the set of security features that allow an application to securely communicate with the service provider. In current networks, when the User Equipment (UE) sends sensitive data to the application server, the MNO does not have access to that data.

We propose that the MNO offer application layer-based services to verticals with the functionalities specified in 3GPP TS 23.434 [29]. This document presents the Service Enabler Architecture Layer (SEAL), including procedures, Application Programming Interfaces (APIs) and flows to support vertical applications over the 5G system. We propose that the application require similar core capabilities to the ones presented in SEAL, and, concretely, the application will require: group management, configuration management, location management, identity management, key management and network resource management.

A way to introduce such capabilities at the application layer is to support interconnection between distributed SEAL server deployments and interservice communication between SEAL servers, as presented in Figure 9.

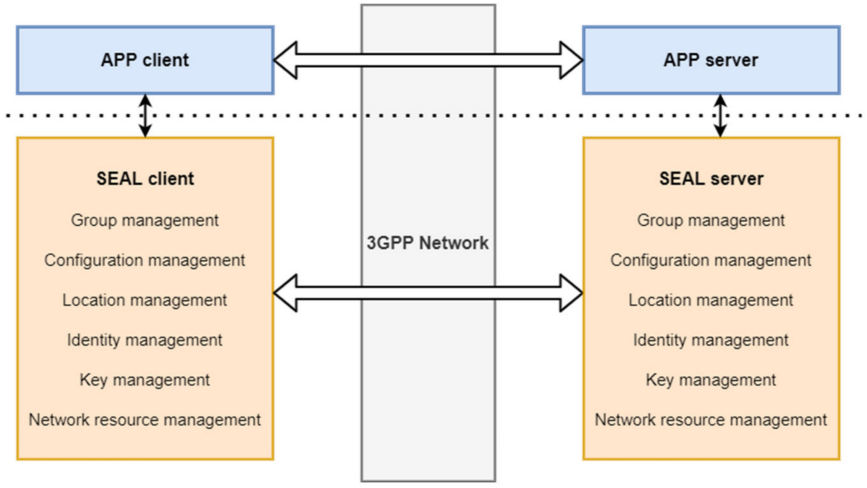

Figure 9. Simplified functional model of SEAL Architecture, 3GPP TS 23.434.

In that case, security attributes should be defined in the three main security areas of SEAL, i.e., security requirements for interfaces, user authentication and authorization, as well as SEAL key management procedure and deployment scenario [37]. The identified problems are:

- API exposure outside Trust Domain, e.g., PLMN, and
- distributed architecture with a specific vertical application, e.g., service discovery and resource adaptation.

And our qualifiers are:

- Fine-grained access control policies and controls;
- Strong authentication;
- Security controls and measures, specific per application to protect services.

At last, the expected outcome is the availability to describe the security level using security attributes per application.

Secondary Authentication. The Extensible Authentication Protocol (EAP) supports both primary and secondary authentication. Primary authentication is conducted during the first registration of the UE into the network. The Authentication and Key Agreement Scheme (5G-AKA) and Extensible Authentication Protocol (EAP) are supported by 5G. The EAP, defined in IETF RFC 3748, provides authentication for 3GPP and non-3GPP Access Networks. The main goal of this authentication scheme is mutual authentication between the UE and the network.

Secondary Authentication is completed during collated user plane connection.

In addition, Network Slice Specific Authentication provides authentication of the UE to the slice. It is defined in 3GPP TS 33.501 (Clause 16.3). It defines the network slice specific authentication (NSSAA) procedures between UE and AAA (Authentication, Authorization and Accounting) servers and specifies the Security Anchor Function (SEAF) of the AMF as the EAP authenticator.

Secondary Authentication is necessary for opening new sessions and for transporting data. In this authentication phase, security attributes should be mapped from higher levels of abstraction to concrete security enforcement mechanisms.

In this case, the identified problems are:

- Different heterogeneous devices can cause security problems when communicating with each other and
- Performance and operation issues can cause devices not to use the same authentication and authorization protocols.

Our qualifiers are:

- Access control policies with the second authentication process;

- Communication between devices requiring mutual authentication;
- Integrity and confidentiality ensuring authentication and authorization;
- Lightweight versions of security mechanisms for group device authentication and authorization.

The expected outcome is the following:

- Creation of security levels based on access mechanisms and
- Access of security attributes, which can describe security access and control levels.

Service-Based Security. Introduction of Service-Based Architecture (SBA) moves from monolithic (reference point) to modular architecture. New instances of a Network Function can be deployed without impacting existing NFs. The Consumer–Producer service model makes communication among NFs feasible. API calls replace the communication request-response or subscribe–notify between Network Functions.

Service-based communication requires the following security mechanisms: (i) authentication and authorization and (ii) confidentiality, integrity and replay protection.

In Release 15 of 3GPP, direct communication without proxy between NFs was introduced with mutual authentication and transport encryption based on TLS protocol and token-based authorization based on OAuth2.0 protocol. In 5G, the NRF offers a Nnrf_AccessToken service for Oauth2 authorization [38] following the Client Credentials authorization grant [39].

In Release 16 of 3GPP, the SBA evolved to indirect communication: a Service Communication Proxy (SCP) in the path between consumers and producers. The NRF needs to be aware that the SCP can request tokens on behalf of consumers. With token-based authorization, with the NRF and the SCP, we can define and enforce the trust domain inside the 5G network per network slice. According to Clause 6.1.6 of the 3GPP TS 29.510 [40], the NRF can authorize based on the attributes presented in Table 1.

Table 1. Authorization information for Isolation Slice.

Authorization Information	Description
allowedPlmns	PLMNs allowed to access the NF instance.
allowedSnpns	SNPNs allowed to access the NF instance. If this attribute is present in the NFService and in the NF profile, the attribute from the NFService shall prevail.
allowedNfTypes	Types of NFs allowed to access the NF instance.
allowedNfDomains	Pattern representing the NF domain names within the PLMN of the NRF allowed to access the NF instance.
allowedNssais	S-NSSAI of the allowed slices to access the NF instance.

The NRF acts as an authorization server, provides Network Functions tokens on the predefined information (Table 1) and defines the trust domain. It also controls separation between slices (see Figure 10). In the case of a compromised NF, the communication is limited to the trusted domain. Network Domain Security (NDS/IP) can still be used for network layer protection for non-SBA interfaces.

The identified problem, in this case, is mainly that the Network Function needs to be identified, authenticated and authorized, and our qualifiers are:

- Token-based authorization to identify trust domain NFs with authorization token grants;
- Mutual authentication with digital certificates;
- Encrypting communication with encryption policies;
- Traffic filtering capabilities.

The general outcomes are:

- Creation of trust domains and isolation of slice components with security principles and

- SBA security attributes, which can describe security access and control levels for Network Functions.

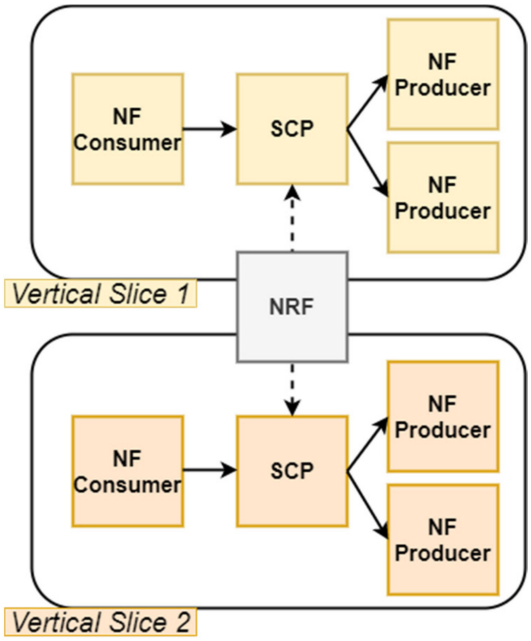

Figure 10. Trust domain for isolated slices within 5G Service-Based Architecture.

Exposure Security. The Exposure Security should define the security attributes of any information exposed in the APIs defined in the Common API Framework (CAPIF), which defines exposed capabilities for all 3GPP Northbound APIs.

CAPIF Security defines interface protection, security method negotiation and authentication and authorization.

The APIs' development was reduced and harmonized by the standardization that allows for the rapid implementation of 3GPP APIs [41]. The identified problems are:

- Data breaches due to attack vectors;
- Man-in-the-middle attacks;
- Credential stuffing attacks;
- Injection malicious code attacks.

Our qualifiers are:

- Encrypting transit traffic;
- Rate limiting of the request sent, DdoS protection;
- Rate limiting to control brute-force attacks;
- Sanitizing and validating all API requests data.

The general outcome is the availability to define API protection with security attributes.

Authentication and Key Management. Key management is a crucial component of a cryptographic access control system with access to a large range of resources. It secures data from risks escalation and privileged users and ensures regulatory compliance. Key management is in charge of ciphering keys: generation, creation, protection, storage, exchange, etc. [42].

The evolution of EPS AKA (Authentication and Key Agreement of the 4G Evolved Packet System) from the 4G network has resulted in 5G AKA. In addition to 5G AKA, 5G allows EAP-AKA for non-3GPP access and, optionally, for 3GPP access. The operator selects the authentication procedure based on its policy: 5G AKA or EAP-AKA. However, the UE and serving network shall support EAP-AKA and 5G AKA authentication methods [40]. EAP-AKA authenticates users in its Home Public Land Mobile Network (HPLMN), while EPS AKA authenticates users in its Visiting Public Land Mobile Network (VPLMN), and,

at last, 5G AKA allows VPLMN and HPLMN authentication. The 5G AKA protocol offers resistance to all known attacks and provides required security features such as mutual authentication, confidentiality and anonymity. It relies on public-key encryption to hide the real identity and cryptographic capabilities available in the universal subscriber identity module (USIM) hardware such that the UE is always connected to a serving network authorized by the home network.

Authentication and Key Management are critical for mobile networks to protect users and their communications. It may support a variety of use cases, and the requirement is to support multiple authentication methods. AKA naturally requires the description and enforcement of security attributes. The identified problems in this case are:

- Access to keys that can read sensitive data;
- Securely managing keys, which may be highly complex;
- Heterogeneous environment, likely composed of different encryption and protocols;
- Regulatory requirements are growing and becoming more complex.

Our qualifiers are:

- User equipment identity protection;
- Home-network control;
- Key separation in the key derivation;
- Key trust models: shared symmetric key and public key certificate;
- UE identity type: IMSI and SUCI/SUPI.

The general outcomes are:

- Availability to describe Authentication and Key Management rules with attributes to achieve the required protection level and
- Attribute property providing specifications that define authentication source, availability, integrity and confidentiality.

Network Access Security. UE encryption is a security property that allows the UE to authenticate, access services securely and protect against attacks on the radio interfaces.

The user plane provides security to ensure that traffic is not modified during transit. The Session Management Function (SMF) shall provide a user plane security policy to the base station. The UP security policy indicates what confidentiality and integrity shall be activated and which dedicated radio bearers associated with the PDU session will be protected.

Signalling data confidentiality protection is always required to protect information from unauthorized access. These requirements are also mandatory for the gNB (5G Node Base Station) for RRC (Radio Resource Control) signalling and the AMF for nonaccess stratum signalling.

Furthermore, signalling data integrity and replay is required to protect information from unauthorized alteration for the UE, for RRC signalling in the gNB and for non-access stratum signalling in the AMF.

The list of potential ciphering/integrity algorithms is quite extensive and includes:

- NEA0/NIA0 (plain text with no encryption);
- 128-NEA1/128-NIA1 (SNOW 3G cypher/SNOW 3G);
- 128-NEA2/128-NIA2 (AES-128 CTR cypher/AES-128 in CMAC mode);
- 128-NEA3/128-NIA3 (ZUC stream cypher/128-bit ZUC).

The main identified problem is that traffic may be modified during transit.
Our qualifiers:

- User Plane and traffic security policy require confidentiality and integrity;
- Signalling data requires confidentiality protection;
- Signalling data requires integrity and replay protection from unauthorized alteration.

The general outcome is an availability to define Network Access Security access level by defining security attributes, as shown above.

Network Transport Security. N2 and N3 interfaces convey sensitive information between the access network and core. Therefore, both interfaces may be objects of signalling attacks and attacks to the user plane data. According to the 3GPP TS 33.501, the ways to ensure the integrity and replay protection for all traffic over these interfaces include (i) IPSec ESP and IKEv2 certificate-based authentication, (ii) support of security profiles DTLS implementation and (iii) F1 and E1 internal interfaces implementation to support security mechanisms. For both, IPSec is mandated.

For non-SBA interfaces, NDS/IP is used for network layer protection.

Security attributes will be mapped into Network Transport Security as the lowest level enforcing security mechanisms.

The identified problems are:

- Man-in-the-middle (MIM) attacks for intercepting control and user plane traffic;
- DdoS attacks, including IPSec Flood DdoS Attacks;
- Attacks to manipulate slicing components by injection of malicious traffic.

Our qualifier is the integrity and replay protection for all traffic, and the expected outcome is the availability to define Network Transport Security protection levels with attributes describing security protection technics.

5. The Proposed Solution for Security Controls

The security domains presented in the previous section have the scope of defining and implementing the security attributes of the 5G System. On the one hand, the definition of the attributes makes feasible a mapping (of the attributes) among domains. On the other hand, the security attributes should be implemented in all the domains, which are realized through the deployment of security controls. The security controls reduce the chances that a threat will exploit a vulnerability and are a fundamental part of security assessment in mobile networks.

In this section, we present the new security controls that should be introduced in each of the security domains such that the orchestrator may enforce the security requirements at different levels. In order to propose different security controls, we propose to extend the 3GPP SeCurity Assurance Specifications (SCAS) by including the security requirements with non-3GPP security control classification corresponding to the security incidents. The security controls can be classified into different criteria. We take criteria relative to a security breach act:

- Preventive controls, intended to prevent incidents before their appearance;
- Detective controls, intended to identify when an incident takes place;
- Corrective controls, intended to limit the magnitude of the incident.

Table 2 presents the proposed security controls and the security domain, where they should be implemented. Concretely, we propose the introduction of well-known security technologies that act as security controls in different domains. The control technologies are divided into preventive, detective and corrective, as described above. Next, we reason the selection of such technologies.

The reasons for using the exposed security technologies are the following:

The security assurance of the network requires security-specific monitoring tools, such as **Security Incident and Event Management (SIEM)** systems. The SIEM collects sources of relevant information (log and event data) from various infrastructure components, including firewall and IDS. It analyses, aggregates and correlates them, triggers them into alerts and tasks the security team to analyse and remediate the potential threat. It is necessary for all the security domains, except the Application Layer, which is not entirely in the hands of the MNO. **Security Orchestration, Automation and Response (SOAR)** collects information from various sources, whereas SIEM provides alerts. SOAR obtain analysis on various levels, paths to follow on an alert. The SOAR can help with the automation of investigating workflows and proceed with the correction by triggering policy enforcement and changing network policy. It requires predefined correlation rules

for any attacks indicators and vector attacks. If the defined rule is missing, existing rules do not cover all possible cases, and we may have a gap in the detection to corrective process. For example, detecting any zero-day attacks is complicated. It requires predefined correlation rules for any attacks indicators and vector attacks. If the (pre)defined rule is missing, existing rules do not cover all possible cases, and we have a gap in the detection process. The most critical period is when attackers know vulnerability, the fix is ongoing, the patch is not ready and the system is exposed to this vulnerability. A zero-trust approach with preventive security practices may protect from zero-day attacks.

Table 2. Security control type and technology in 5G Network.

	Security Domain	**Technology**	**Preventive**	**Detective**	**Corrective**
User Plane					
	Service-oriented Safeness	Self-aware Network for QoS, Energy Consumption and Security	e.g., ACLs, configuration rules, Intrusion Prevention System (IPS), DdoS Prevention System	e.g., machine learning-based decisions, Intrusion Detection System (IDS), SIEM *	e.g., machine learning-based decisions, SOAR
	Application Security	Firewalls, IDS, TLS	e.g., firewalls, segmentation and zoning, IPS, protection of DNS traffic, secure communication	IDP, Vulnerabilities Management, SIEM	Patching Management
	Secondary Authentication	EAP, PPP, CHAP, AKA, TLS	e.g., multifactor authentication	auditing, logging, reporting, Security Incident and Event Management (SIEM)	control procedures, Security Orchestration Automation and Response (SOAR)
Control Plane					
	Service-Based Architecture Security	PKI System, NRF as Authorization Server, SCP	e.g., mTLS, PKI, Trust Domain	auditing, logging, reporting, SIEM	control procedures, SOAR
	Exposure Security	PKI system, Oauth2.0 Server, FW with DdoS	mTLS, Trust Domain, digital certificates	auditing, logging, reporting, SIEM	control procedures, SOAR
	Authentication and Key Management for Applications	PKI System, NRF as Authorization Server	mTLS, Trust Domain, digital certificates	auditing, logging, reporting, SIEM	control procedures, SOAR
Both (User and Control Planes)					
	Network Access Security	IoT, D2D, V2X dedicated solution	Nationwide PKI system, mutual authentication, privacy protection	auditing, logging, reporting, SIEM	control procedures, SOAR
	Network Transport Security	Security Gateway for aggregation	NDS/IP (IPSec) or TLS, PKI	auditing, logging, reporting, SIEM	control procedures, SOAR

* Please note that SIEM aggregates logs and generates alerts and incidents, and the source of logs may also be preventative systems, e.g., Intrusion Prevention System (IPS).

The **Active Intelligent Network (AIN)** can enhance security by dynamically activating packet filtering or authenticating traffic flows for Service-oriented Safeness. The AIN updates IP networks based on predefined policies with specific network and security conditions [43]. The two primary security concerns with AIN are: (i) AIN can create processing overload caused by the traffic addresses to itself and (ii) AIN introduces packet injection to disrupt or intercept packets, and these packets can create possible security risks.

The AIN makes adaptive decisions in the network nodes by providing controllers at the network level (Software-defined Networking, SDN). The adaptive reactions of the controllers in a path are triggered mainly in the case of QoS degradation due to huge packet forwarding delay and/or security degradation within the trust metric in the path [44]. The SDN controller integrates Artificial Intelligence (AI)-based decision algorithms to optimize energy, QoE/QoS and security. All incidents shall be reported to the Security Operating Center for further analysis.

The network IDS/IPS and DdoS solutions have become additional security mechanisms to security infrastructure. The Intrusion Detection System (IDS) uses different detection methods: anomaly detection by comparing events with predefined rules to detect system deviations, analyzing stateful protocols activities with predefined protocol profiles and comparing signatures against events. The defined policy defines preventive action on traffic for part of the network and application. The firewall with Intrusion Preventive System (IPS) can prevent the instruction one entry at a time. The early detection system with adjusted security architecture can effectively mitigate DdoS attacks for combined behaviours attacks.

The **Application Security Controls** that the network could provide are [45]:

- Firewalls to allow only approved traffic;
- Infrastructure and application placement protection by segmentation and zoning;
- Intrusion Detection Systems (IDS) to detect any abnormalities on the network isolation application in case of compromisation;
- Protection of DNS traffic to ensure that data are forwarded to the correct destination. DNS vulnerabilities have the power to compromise security data. The DNS traffic without embedded digital signatures in data poses a potential threat. An attacker can identify weakness and seize or redirect the domain name for their purposes;
- Secure communication (through Transport Layer Security, TLS) and application data in transit to ensure data confidentiality;
- Patching and Vulnerabilities Management, patching and updating application components and discovering vulnerability assets on the network.

The Extensible Authentication Protocol (EAP) conveyed the protocol between the AAA server and the UE in the **Secondary Authentication** domain. During the Secondary Authentication protocol interaction, the 5G network functions do not parse authentication, and the vertical application can complete it by algorithms and protocols provided by MNOs. The 3GPP defines standard Secondary Authentication protocols, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Point-to-Point Protocol (PPP), Authentication and Key Agreement (AKA) and Transport Layer Security (TLS).

The system logging mechanisms are invaluable for providing security events. It provides information about all states of authentication phases and identifies security incidents. The auditing process examines who conducted what and monitors any policy violations.

The **Service Communication Proxy (SCP)** provides signalling routing controls with resiliency and observability of the network. The SCP decentralizes the service-based architecture and provides end-points for NFs with implemented TLS protocol. The SCP can monitor the state of control data transfers and analyse their contents with the SIEM system. The SIEM can respond to security incidents or any alarms when they occur and implement complicated defence-in-depth capabilities. In the reporting phase, the SIEM sends the audit/logging phase findings to SOAR. It analyses the report, develops corrective action and implements change, if possible.

With a set of digital certificates and policies, the SCP and a Public Key Infrastructure (PKI) can be the foundation for defining a Trust Domains (TDs). They define modularly and independently authentication policies and encryption methods per TDs.

In the **Exposure Security** domain, the protection of the system APIs should be based on several security layers as recommended by standards such as 3GPP, CAS(T) and ISO

27001. Based on these security principles, the leading security concepts that must be followed to secure the orchestration tool are:

- Layering: the deployment of security controls to control all traffic entering or leaving the zones. This protection targets the following threat scenarios:
  - (Distributed) Denial-of-service attacks;
  - Scanning attempts or spoofing attempts;
  - Traffic injection;
  - Unauthorized traffic and communications;
  - All attacks on L4 OSI level and lower.
- Data Hiding/Encryption: secure communications; securing all communications using secure communication protocols (TLS and HTTPS). It is also essential to identify and authenticate the elements that will communicate to/from. This protection targets the following threat scenarios:
  - Rouge API calls and spoofed API calls;
  - Man-in-the-middle attacks;
  - Unauthorized requests from unauthorized resources;
  - Unauthorized requests from authorized resources.
- Public Key Infrastructure with distinguished certificates for different trust domains will provide robust system authentication without username and passwords;
- A mechanism from TLS to protect man-in-the-middle attacks. This mechanism introduces packet sequence numbers in the encrypted packets to prevent packet injection, whereby, in order to detect payload changes, authentication is used. TLS sequencing is required to detect and protect from message replay attacks. TLS uses TCP, so it is vulnerable to TCP SYN floods. Since TCP SYN Flooding is a DDoS attack, a firewall with DDoS rules is needed to protect API calls.

Authentication and Key Management for Applications (AKMA) and the UE should reuse the same credentials for 5G access as for the primary authentication procedure and primary methods [40]. The interfaces between Network Functions participating in the authentication procedure shall be confidentiality-, integrity- and replay-protected.

The **Security in 5G Network Access** may be threatened by the massive number of devices interacting with the network at the same moment. The threats may be posed in scenarios such as ultra-short-time authentication, authorization and seamless security handover. Massive IoT devices require concurrent security access, privacy protection and lightweight security mechanisms. The network may verify the device group at the aggregation level to reduce signalling and communication overhead [46–49]. Moreover, in 5G, Device-to-Device (D2D) communication represents a distributed and centralized communication model introducing several security concerns from mobile and ad hoc networks. Many application scenarios to secure D2D communication need to be considered separately from the network since, regretfully, the current D2D security protocols are not combined with 5G networks and cannot be considered in application scenarios. Secure group communication and uniform, efficient mutual authentication with handover need to be studied [50,51]. Access to the network in other scenarios, such as autonomous cars, also poses security challenges, such as identity authentication, authentication of broadcast messages and privacy protection. In Vehicle-to-Everything (V2X) scenarios, any communication requires different authentications for securing broadcasting messages, one-many V2X communication and privacy protection, etc. The solution studies in literature analyse performance and certificate management schemes for V2X systems [52], DDoS attacks due to a mass of pseudo certificates with puzzle-based authentication schemes [53] and nationwide Public Key Infrastructure for V2X security [54].

At last, **Open-RAN Security** should take security models such as Zero Trust Architecture (ZTA) [55]. ZTA is based on the paradigm that no trust principles are used, and it is designed to prevent data breaches. O-RAN architecture is based on the following

preassumptions: (i) secure communication between all interfaces and (ii) trust-based authentication with Public Key Infrastructure.

Moreover, it is worth remarking that secure communication includes secure interfaces between all components. Therefore, it is required to have NDS/IP (IPSec) or TLS. Mutual authentication with certificates is used while establishing IPSec or TLS protocols [56].

6. Network Slices with Security Constraints: An Example

The attributes mentioned in Section 4 are an abstraction that refers to network slice security characteristics. The attributes can be extended by adding the new reflection security controls described in Section 5. The network slices will have different security requirements based on multiple factors, translated into specific security functions, embedded security features, policies, etc. The slice controller shall support an automation process that considers the security design of the network slice with possible constraints. These constraints mapped from attributes are used to find the optimal solution for implementing such a design in the network. These constraints may be geographical, isolation at the selected level, server capacity and others.

The possible outcomes of the security design of a slice could result in Virtual Security Functions activation, isolation class 'Network services, network functions' (see Section 3), physical or logical selection of the cloud or physical resources, location of the resources and others.

In this section, we provide an example of two types of slices with different security levels—the network slice with a low-security profile and the eMBB network slice with secure internet access.

The default slice can be represented with the diagram in Figure 11. We assume that there are no specific security constraints and all the Network Functions are shared in the network.

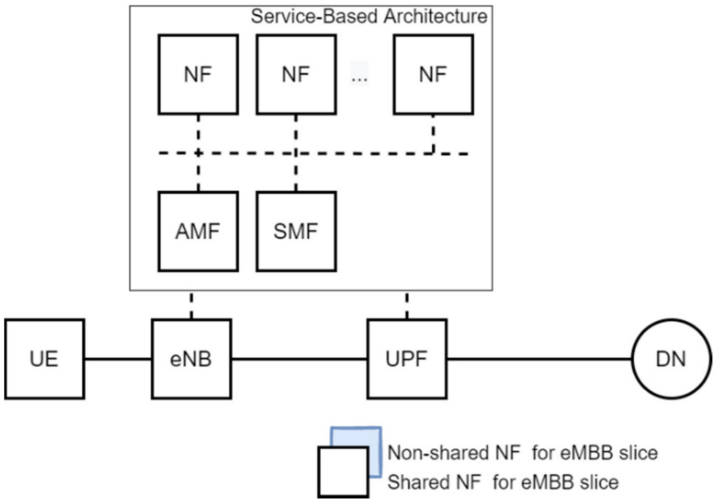

Figure 11. Network Slice with no security. NF: Network Function; AMF: Access and Mobility Management Function; SMF: Session Management Function; UE: User Equipment; gNB: 5G Node Base; UPF: User Plane Function; DN: Data Packet Network.

A network slice for secure internet access shall require:

- Activation of specific security features embedded in UPF, at least High-performance Carrier-Grade NAT (CGNAT), Application Content Filtering (AF) and Firewall Protection (FW) and
- DDoS Protection network function (DDoS).

In addition, there are the following assumed constraints:

- Constraint 1: Specific group or servers and location for the 'Secure' UPF and DDoS protection network functions;

- Constraint 2: SMF and UPF are only intended for this network slice, i.e., they cannot be shared with other slices;
- Constraint 3: AMF is common and may be shared between slices.

In that case, the schema for the eMBB secure slice is presented in Figure 12.

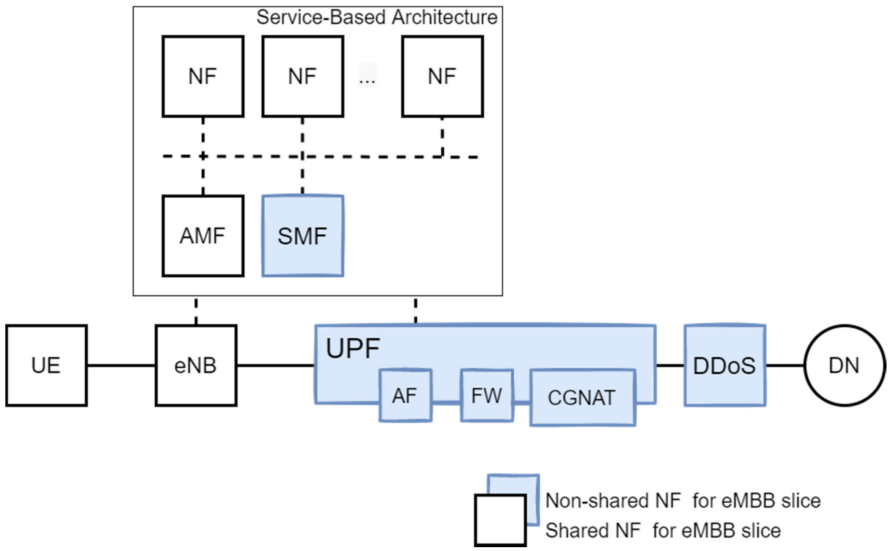

Figure 12. Network Slice with Secure Internet Access.

With such a definition, the slice controller shall optimize the solution for completing the network resources across the available resources all over the security domains.

Figure 13 presents an example of a Network Slice Subnet Instance (NSSI) allocation procedure with the above security attributes. The procedure of creating NSSI is intended to satisfy the network slice requirements (the attributes in the slice profile).

Network Slice Subnet Management Service Consumer (NSSMS Consumer) requests the Network Slice Subnet Management Service Provider (NSSMS Provider) to allocate an NSSI. The NSSMS Provider needs to check the feasibility of the NSSI with related resources and has to decide whether the requested NSSI can be shared with other consumers and whether any existing NSSI can be reused. Figure 11 presents a limited view for a new NSSI allocation with selected security constraints/attributes. Before the NSSI is constituent, the NSSMS Provider needs to check all corresponding network slice subnet capabilities, including the virtualization network part, e.g., VNF/CNF (Virtual Network Function/Containerized Network Function).

If the Network Function Management Service Provider (NFMS Provider) requests to create a Network Function, it checks virtualized-based Network Function requirements with the related parameters, as presented in Section 3. These parameters are part of the 'Specification and enforcement of resource usage policies' isolation class (Figure 5). They must guarantee a minimum number of resources. NFMS Provider also needs to check if the Network Function shall meet all other requirements related to the isolation classes. In our example, the attributes, High-performance Carrier-Grade Network Address Translation (CGNAT), Application Content Filtering (AF) and Firewall Protection (FW) for the UPF, are related to the 'Entity framework and specification for default behaviour with variants' isolation class. The default parameters require the activation of the standard configuration of functionality.

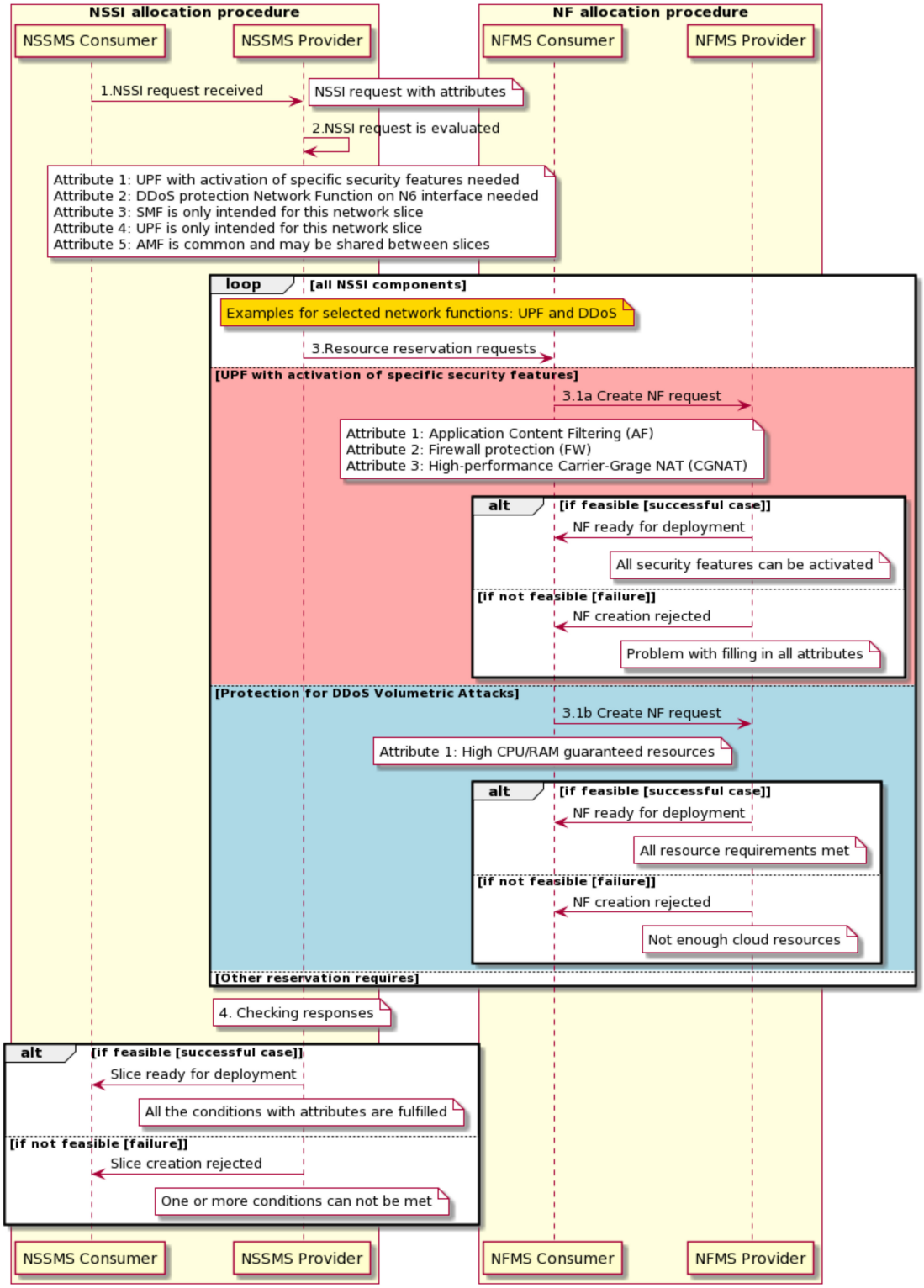

Figure 13. NSSI/NF allocation resources with security attributes.

In this procedure, other isolation class parameters were inherited from the 'Network services, network functions' isolation class. The parameter indicates whether network functions are not shared. The example shows how attributes are mapped at different layers and how the network's elements communicate to establish a network slice with required security attributes.

Step 1. Network Slice Subnet Management Service Provider (NSSMS Provider) receives an NSSI request from Network Slice Subnet Management Service Consumer (NSSMS Consumer) to allocate an NSSI.
Step 2. NSSMS Provider evaluates the request feasibility with requested attributes.
Step 3. NSSMS Provider sends resource reservation requests for UPF and DDoS.
Step 3.1a. NSSMS Consumer receives a request for resource reservation for UPF with three attributes and checks for feasibility; NSSMS Consumer answers if NF can be deployed with all security constraints.
Step 3.1b. NSSMS Consumer receives a request for resource reservation for DDoS with an attribute and checks for feasibility; NSSMS Consumer answers if NF can be deployed with isolation class constraint. Note: NF instance requires virtualization resources, so then the NSSMS Provider needs to see whether the VNF/CNF instance can be scaled out for a new NF instance.
Step 4. Network Slice Subnet Management Service Provider (NSSMS Provider) sends feedback to the NSSI request from Network Slice Subnet Management Service Consumer (NSSMS Consumer) about feasibility of allocating an NSSI.

Figure 14 presents an example of a brute-force attack during a secondary authentication procedure. In this case, the UE is after successful primary authentication and the UE provides the AAA server inside the EAP message in the PDU Session Authentication Complete message. The SMF initiates the authentication procedure with a specific AAA Server via the UPF to grant access. The UPF transparently forwards the messages from the SMF to the selected AAA Server.

The UE cannot authorize the service (network slice) and uses an automatic method to obtain information by breaking a password. SIEM collects failed login attempts and groups them with parameters as frequency attempts. It also aggregates historical data and the actual events and reports the identified anomalies to SOAR. SOAR prepares an automatic response to the incident and temporarily, or until manual intervention, requests to stop forwarding the authentication messages to the AAA server for this UE.

The request to stop forwarding EAP messages is part of the 'Entity framework and specification for default behaviour with variants' isolation class (Figure 5). It is a deviation from the default configuration when all EAP messages are allowed to be forwarded. It requires a particular format of an attribute representing the forwarded/blocked table entries. Moreover, the attribute may represent the type of operation: add, append, delete and update entries, but the final format depends on vendor implementation.

This procedure updates configuration parameters at the 'Entity framework and specification for default behaviour with variants' isolation class. The parameter indicates differentially how the table of forwarding EAP messages is defined.

Steps 1 and 2. SOAR receives an incident message from SIEM and prepares a response.
Steps 3, 4 and 5. Update request is sent to the entity to change the default behaviour.
Step 6a. Update confirmed. EAP message to AAA Server blocked.
Steps 7 and 8. Update request–response.

In the same line, many other examples of Network Slices with other security attributes may be built in the network. This approach responds to our previous studies that require a more comprehensive, even if more complex, response to security in a network with many underlying infrastructures [7,8].

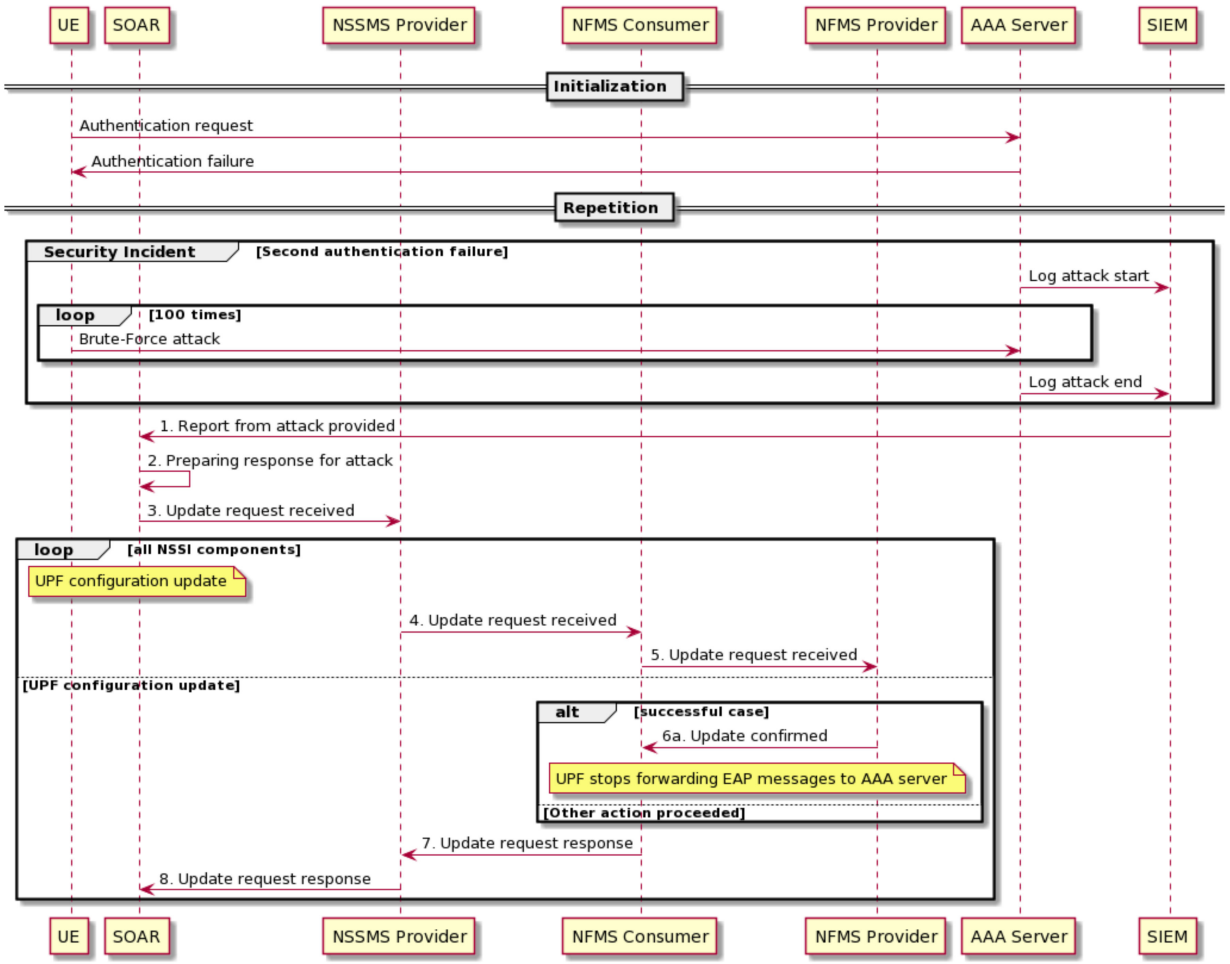

Figure 14. Response procedure to the brute-force secondary authentication attack.

7. Conclusions and Future Directions

This paper presents security controls for network slicing and its security orchestration. The 3GPP defines the Management System, where the Type B Network Resource Model represents the resources and the 5G network functions. The security requirements for procedures, flow and interfaces are specified in 5G Security Assurance Specifications; however, these specifications are limited to 5G NFs, so the 5G Network Resource Model for additional security controls as firewalls is not standardized and needs to be defined by vendors. We presented a model for analysis and classification of the security controls needed to meet the security requirements posed by verticals. This model assumes that verticals open network slices for transmitting their data. The network slice is a set of different resources and security entities at different levels, where all entities need to meet network slice specifications and security constraints (attributes). Based on these assumptions, we proposed a model for security controls in slices for verticals.

Our analysis concludes many open issues that need to be solved when implementing network slices in 5G. We can structure these development areas as follows:

Resources. The resources are critical because of their multifariousness, the different locations for hosting them and their different administrative domains. Moreover, the customer's offered service may come from various entities, complicating resource reservation enforcement. Since the MNO decided to use virtualized technology, the customers can share the resources, including machines and operating systems. Challenges are how to guarantee the performance and security assurance of the services over shared infrastructure with dynamic behaviour. The solutions should be a resource allocation strategy, with fairness in

making network resource usage more efficient, and, on the other hand, dynamic control of resources with security controls to provide secure and stable environments for services.

Isolation. The isolation can be applied to different layers of a network's architecture (see Figure 5) to secure network slice resources. The crucial issue is ensuring interslice isolation to obtain independent control and user planes. The idea is that an attack on a slice will not affect other network slices when affected network functions are not shared. Therefore, we may conclude that the isolation requirements need to be formalized and standardized to be effective and productive. The proper definitions and parametrization with proper values help fulfil its objectives, mainly from avoiding propagation of an attack, known as the cascade effect, in the network and between network slices.

Security. The profiling security network slicing with its characteristics will help avoid specific attacks such as Distributed Denial of Service (DDoS) or access to other slice traffic without authorization. The scheme profile of the network slice behaviour with proper security controls may significantly reduce the risk of attacks. For example, security controls with incident detection and enforcement of security entities help avoid impact when a shared NF or slice under a shared cloud is compromised. The final objective is to build trust domains for a slice with all network slicing components authorized, including (non)service-based architecture. For this scope, the services require separate resources to have different security levels and policies, e.g., secure UPF + DDoS function for secure internet access or integrity and confidentiality protection on user plane traffic.

Author Contributions: Conceptualization, methodology, investigation and writing, T.W.; conceptualization and methodology of security of network slices, writing and supervision, J.M.B.; data curation, C.X.M.; formal analysis, J.Ż.; review and editing, G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work (all the authors except the Corresponding author) was undertaken under the Grant No. CYBERSECIDENT/489818/IV/NCBR/2021 of the CyberSecIdent IV Programme supported by the National Centre of Research and Development in Poland. The work of the Corresponding author has been funded by POB Research Centre Cybersecurity and Data Science of Warsaw University of Technology within the Excellence Initiative Program - Research University (ID-UB), grant No. CyberiADa-1_2020_W24.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Doukoglou, T.; Gezerlis, V.; Trichias, K.; Kostopoulos, N.; Vrakas, N.; Bougioukos, M.; Legouable, R. Vertical Industries Requirements Analysis & Targeted KPIs for Advanced 5G Trials. In Proceedings of the 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019; pp. 95–100.
2. Mekikis, P.-V.; Ramantas, K.; Antonopoulos, A.; Kartsakli, E.; Sanabria-Russo, L.; Serra, J.; Pubill, D.; Verikoukis, C. NFV-Enabled Experimental Platform for 5G Tactile Internet Support in Industrial Environments. *IEEE Trans. Ind. Inform.* **2020**, *16*, 1895–1903. [CrossRef]
3. Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.A.; Al-Rimy, B.A.S. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. *Appl. Sci.* **2021**, *11*, 9005. [CrossRef]
4. Vaquero, L.M.; Cuadrado, F.; Elkhatib, Y.; Bernal-Bernabe, J.; Srirama, S.N.; Zhani, M.F. Research challenges in nextgen service orchestration. *Future Gener. Comput. Syst.* **2019**, *90*, 20–38. [CrossRef]
5. Ma, W.; Li, H.; Witarsyah, D. A cloud computing separation model based on information flow. *Open Phys.* **2019**, *17*, 128–134. [CrossRef]
6. Maule, M.; Vardakas, J.; Verikoukis, C. 5G RAN Slicing: Dynamic Single Tenant Radio Resource Orchestration for eMBB Traffic within a Multi-Slice Scenario. *IEEE Commun. Mag.* **2021**, *59*, 110–116. [CrossRef]
7. Gomez, G.P.; Batalla, J.M.; Miche, Y.; Holtmanns, S.; Mavromoustakis, C.X.; Mastorakis, G.; Haider, N. Security policies definition and enforcement utilizing policy control function framework in 5G. *Comput. Commun.* **2021**, *172*, 226–237. [CrossRef]
8. Batalla, J.M.; Andrukiewicz, E.; Gomez, G.P.; Sapiecha, P.; Mavromoustakis, C.X.; Mastorakis, G.; Zurek, J.; Imran, M. Security Risk Assessment for 5G Networks: National Perspective. *IEEE Wirel. Commun.* **2020**, *27*, 16–22. [CrossRef]
9. 5G White Paper By NGMN Alliance, 17-February-2015. Available online: https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf (accessed on 19 July 2021).
10. 5G Security Recommendations Package #1 by NGMN Alliance, 06-May-2016. Available online: https://www.ngmn.org/wp-content/uploads/Publications/2016/160506_NGMN_5G_Security_Package_1_v1_0.pdf (accessed on 19 July 2021).

11. Famaey, J.; Latre, S.; Strassner, J.; De Turck, F. A hierarchical approach to autonomic network management. In Proceedings of the 2010 IEEE/IFIP Network Operations and Management Symposium Workshops, Osaka, Japan, 19–23 April 2010; pp. 225–232.
12. Harel, R.; Babbage, S. 5G Security Recommendations Package #2: Network Slicing by NGMN Alliance, 27-April-2016. 12. Available online: https://www.ngmn.org/wp-content/uploads/Publications/2016/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf (accessed on 19 July 2021).
13. Racz, N.; Weippl, E.; Seufert, A. Governance, Risk & Compliance (GRC) Software—An Exploratory Study of Software Vendor and Market Research Perspectives. In Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 4–7 January 2011; pp. 1–10.
14. Ekelhart, A.; Fenz, S.; Neubauer, T. AURUM: A Framework for Information Security Risk Management. In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 5–8 January 2009; pp. 1–10.
15. ISO/IEC 27005:2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html (accessed on 13 November 2021).
16. SA2—Architecture. Available online: https://www.3gpp.org/specifications-groups/sa-plenary/sa2-architecture (accessed on 19 July 2021).
17. Ping, J. Network Resource Model for 5G Networkand Network Slice. *J. ICT Stand.* **2019**, *7*, 127–140. [CrossRef]
18. 3GPP TS 28.533: "Management and Orchestration; Architecture Framework". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3416 (accessed on 21 July 2021).
19. 3GPP TS 28.531: "Management and Orchestration; Provisioning". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3274 (accessed on 19 July 2021).
20. 3GPP TS 28.541: "Management and Orchestration; 5G Network Resource Model (NRM); Stage 2 and Stage 3". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3400 (accessed on 5 August 2021).
21. 3GPP TS 28.632: "Telecommunication Management; Inventory Management (IM) Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=480 (accessed on 5 August 2021).
22. 3GPP TS 28.658: "Telecommunication Management; Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=489 (accessed on 5 August 2021).
23. 3GPP TS 23.501: "System Architecture for the 5G System (5GS)". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144 (accessed on 5 August 2021).
24. Thalanany, S.; Hedman, P. Description of Network Slicing Concept. NGMN Alliance. 2016. Available online: https://ngmn.org/wp-content/uploads/160113_NGMN_Network_Slicing_v1_0.pdf (accessed on 6 August 2021).
25. 3GPP TR 28.801: "Telecommunication Management; Study on Management and Orchestration of Network Slicing for Next Generation Network". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091 (accessed on 8 December 2021).
26. Pla, L.F.; Shashidhar, N.; Varol, C. On-Premises Versus SECaaS Security Models. In Proceedings of the 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 1–2 June 2020; pp. 1–6.
27. ITU-T Recommendation Database. Available online: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=1515&lang=en (accessed on 19 July 2021).
28. GSMA. From Vertical Industry Requirements to Network Slice Characteristics—Future Networks. Available online: https://www.gsma.com/futurenetworks/resources/from-vertical-industry-requirements-to-network-slice-characteristics/ (accessed on 6 August 2021).
29. 3GPP TS 23.003: "Numbering, Addressing and Identification". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 6 August 2021).
30. Wong, S. The Fifth Generation (5G) Trust Model. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–5.
31. [Report] Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation. Available online: https://content.fireeye.com/apt-41/rpt-apt41/ (accessed on 6 December 2021).
32. La Rosa, M. Managing Variability in Process-Aware Information Systems. Ph.D. Thesis, Queensland University of Technology, Brisbane City, QLD, Australia, 2009.
33. Chinnasamy, P.; Vinothini, B.; Praveena, V.; Subaira, A.; Ben Sujitha, B. Providing Resilience on Cloud Computing. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 27–29 January 2021; pp. 1–4.
34. Novak, M.; Shirazi, S.N.; Hudic, A.; Hecht, T.; Tauber, M.; Hutchison, D.; Maksuti, S.; Bicaku, A. Towards Resilience Metrics for Future Cloud Applications. In *Proceedings of the 6th International Conference on Cloud Computing and Services Science, Rome, Italy, 23–25 April 2016*; SCITEPRESS—Science and Technology Publications: Rome, Italy, 2016; pp. 295–301.
35. Lycett, M.; Radwan, O. Developing a Quality of Experience (QoE) model for Web Applications. *Inf. Syst. J.* **2019**, *29*, 175–199. [CrossRef]

36. Yang, M.; Li, Y.; Li, B.; Jin, D.; Chen, S. Service-oriented 5G network architecture: An end-to-end software defining approach. *Int. J. Commun. Syst.* **2016**, *29*, 1645–1657. [CrossRef]
37. Fragkos, D.; Makropoulos, G.; Sarantos, P.; Koumaras, H. 5G Vertical Application Enablers Implementation Challenges and Perspectives. 6. Available online: https://evolved-5g.eu/wp-content/uploads/2021/09/fragkos_meditcom2021.pdf (accessed on 12 December 2021).
38. Hardt, D. *The OAuth 2.0 Authorization Framework*; Internet Engineering Task Force: Fremont, CA, USA, 2012.
39. 3GPP TS 33 501: "Security Architecture and Procedures for 5G System". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (accessed on 6 August 2021).
40. 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3345 (accessed on 6 August 2021).
41. Tangudu, N.D.; Gupta, N.; Shah, S.P.; Pattan, B.J.; Chitturi, S. Common Framework for 5G Northbound APIs. In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020; pp. 275–280.
42. 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) Based on 3GPP Credentials in the 5G System (5GS)". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3690 (accessed on 6 August 2021).
43. Galis, A. (Ed.) *Programmable Networks for IP Service Deployment*; Artech House Telecommunications Library, Artech House: Boston, MA, USA, 2004; ISBN 978-1-58053-745-2.
44. Gelenbe, E.; Domanska, J.; Frohlich, P.; Nowak, M.P.; Nowak, S. Self-Aware Networks That Optimize Security, QoS, and Energy. *Proc. IEEE* **2020**, *108*, 1150–1167. [CrossRef]
45. Lenaeus, J.D.; O'Neil, L.R.; Leitch, R.M.; Glantz, C.S.; Landine, G.P.; Bryant, J.L.; Lewis, J.; Mathers, G.; Rodger, R.; Johnson, C. *How to Implement Security Controls for an Information Security Program at CBRN Facilities*; PNNL-25112, 1236337; Pacific Northwest National Lab. (PNNL): Richland, WA, USA, 2015.
46. Haq, I.U.; Wang, J.; Zhu, Y. Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. *J. Netw. Comput. Appl.* **2020**, *161*, 102660. [CrossRef]
47. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
48. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]
49. Cao, J.; Ma, M.; Li, H.; Fu, Y.; Liu, X. EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks. *J. Netw. Comput. Appl.* **2018**, *102*, 1–16. [CrossRef]
50. 3GPP TR 33.888: "Study on Security Issues to Support Group Communication System Enablers (GCSE) for LTE". Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2332 (accessed on 6 August 2021).
51. Xie, P.; Feng, J.; Cao, Z.; Wang, J. GeneWave: Fast Authentication and Key Agreement on Commodity Mobile Devices. *IEEE/ACM Trans. Netw.* **2018**, *26*, 1688–1700. [CrossRef]
52. Villarreal-Vasquez, M.; Bhargava, B.; Angin, P. Adaptable Safety and Security in V2X Systems. In Proceedings of the 2017 IEEE International Congress on Internet of Things (ICIOT), Honolulu, HI, USA, 25–30 June 2017; pp. 17–24.
53. Liu, P.; Liu, B.; Sun, Y.; Zhao, B.; You, I. Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-Based Co-Authentication in 5G-VANET. *IEEE Access* **2018**, *6*, 20795–20806. [CrossRef]
54. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A Security Credential Management System for V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [CrossRef]
55. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2020.
56. O-RAN ALLIANCE. Available online: https://www.o-ran.org/ (accessed on 4 August 2021).