IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2020.DOI

5G Network Slicing: A Security Overview

RUXANDRA F. OLIMID[1] and GIANFRANCO NENCIONI[2]

[1]Department of Computer Science, University of Bucharest, Bucharest, Romania (e-mail: ruxandra.olimid@fmi.unibuc.ro)
[2]Department of Electrical Engineering and Computer Science, University of Stavanger, Stavanger, Norway (email: gianfranco.nencioni@uis.no)

Corresponding author: Gianfranco Nencioni (email: gianfranco.nencioni@uis.no).

ABSTRACT The fifth-generation (5G) of cellular networks is currently under deployment by network operators, and new 5G end-user devices are about to be commercialized by many manufacturers. This is just a first step in the 5G's development, and the true potential of 5G is still far from being reached. Currently, one of the main 5G technologies under the interest of the research community is the network slicing. Network slicing will allow exploiting the 5G infrastructure to flexibly and efficiently provide heterogeneous services (e.g., voice communication, video streaming, e-health, vehicular communication). Like every new technology, one of the critical aspects that need to be considered is the security. In this article, we spotlight the security in 5G network slicing. We highlight threats and recommendations, which are presented in terms of life-cycle security, intra-slice security, and inter-slice security. Furthermore, we identify and discuss open security issues related to network slicing.

INDEX TERMS 5G, Network Slicing, Security.

I. INTRODUCTION

The evolutionary part of 5G, which consists of improvements in the performance compared to 4G, has been already released to the market. But the revolutionary part of 5G is still under the investigation of the research community and in work by the standardization organizations [1], [2]. It aims to provide differentiated services (e.g., voice communication, video streaming, e-health, vehicular communication) by sharing the same 5G infrastructure. This challenging target can be accomplished by using the novel technology of network slicing [3]. Network slicing is one of the topics targeted in the 3rd Generation Partnership Project (3GPP) Release 16 [1], and further addressed in 3GPP Release 17 [2], which are currently in progress with scheduled completion in June 2020 and 2021, respectively. This motivates an investigation of the security aspects of network slicing at this time.

Network slicing belongs to the category of virtualization networking paradigm, together with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). Network slicing can take advantage of SDN and NFV, but it can be seen as an independent technology. It enables the flexible and efficient creation of specialized end-to-end logical networks on top of shared network infrastructure. Each of these logical networks is able to accommodate a specific type of services, with different and heterogeneous requirements that facilitate vertical industries. The International Telecommunication Union (ITU) specified three main 5G use cases (also approved by 3GPP) that are characterized by different requirements: enhanced mobile broadband, ultra-reliable low-latency communication, and massive machine-type communication [4].

Infrastructural and functional sharing brings advantages in terms of cost and resource consumption, but, at the same time, it raises issues that have to be addressed. The security and privacy aspects of network slicing need to be clarified, especially in a multi-tenancy context. Otherwise, the consequences might be severe.

This article elaborates on the security of 5G network slicing. We focus on security issues specific to network slicing and keep general 5G security aspects out of our scope (even if they impact network slicing to some extent). We aim to give a concise and comprehensive tutorial to the non-specialist reader. Nevertheless, more experienced readers will benefit from the classification of information, detailed discussion (including the indication of open problems), and precise references to more advanced reads. We do not directly address the concept of isolation, which implies operation without any direct or indirect influence between slices, or even between entities within the same slice (e.g., resources, operation, management). But we refer to isolation as a technique to achieve security and mention it whenever needed. Slice isolation can be implemented at various levels, depending on the scenario requirements, and in various forms. An in-depth discussion of these aspects is beyond the goal of this article.

The article aims to indicate possible points of attack and investigate security requirements and recommendations. We look into these from three different perspectives: (1) security aspects in different stages of the *life cycle* of a network slice, (2) security aspects of a network slice by itself (*intra-slice security*), and (3) security aspects in relation to other network slices (*inter-slice security*). Within this classification, we present and examine the security challenges that emerge when using network slicing. As network slicing is a young field, there are still open aspects that need to be clarified and discussed. We refer to some of these and indicate further research directions.

The remaining of the article is organized as follows. Section II gives the literature review. Section III introduces the necessary background in network slicing. Section IV presents the main points of attack and security threats. In Section V, further network slice security aspects are discussed. Finally, Section VI presents the conclusions.

II. LITERATURE REVIEW

Our methodological approach for reviewing the literature includes looking into different types of publications such as standards, white papers, and research papers. Since related works are continuously updated or newly published, we consider the last versions of the standards and focus on the very recent academic and industry works. Hence, the criteria to select relevant sources of information includes diversity (standards, academic, and industry papers), novelty (publication date), and relevance to the topic. More precisely, our goal is to give an overview of network slicing security, so we overlook publications that refer to very tight aspects, such as proprietary solutions or specific methods, implementations, or algorithms. Finally, we build our paper around the three perspectives of interest (life-cycle security, inter-slice security, and intra-slice security), a classification that we have not explicitly found in other works.

3GPP standards establish the fundamentals for the current status of 5G network slicing and hence set the basics for our work [1], [2]. From the large set of 3GPP requirements and specifications, TR33.811 [5] and TR33.813 [6] are directly related to network slicing security, and TS33.501 specifies the security architecture and procedures for 5G [7].

Next Generation Mobile Networks (NGMN) investigates the security requirements and network capabilities exposure in 5G [8], identify flaws that might emerge through the use of network slicing, and make recommendations [9]. The European Union Agency for Cybersecurity (ENISA) gives a threat landscape for networks, which is not focused on but refers to network slicing too [10]. Contrary to this, we look into the security of network slicing from the previously-mentioned three perspectives. 5G Americas also gives a white paper overview of the 5G network security architecture in the 3GPP specification, presents the 5G threat surface, and dedicates a section to network slicing threats [11]. An older 5G Americas white paper is fully dedicated to network slicing [12]. On the industry side, ZTE mostly refers to slice security in terms of end-to-end slice isolation [13], and Huawei gives an overview of 5G security architecture with references to network slices [14]. Finally, we refer to the 5G Infrastructure Public Private Partnership (5G PPP) security white paper, which indicates weak slice isolation as a security risk and dedicates a subsection to network slicing security [15]. Other white papers in the field exist, but it is out of our scope to exhaustively present the related works.

In the academic literature, several papers assess 5G security in general and refer to network slicing in this larger context. In [16], the authors give an extensive survey of security and privacy of 5G in general, discussing network slicing as one of the key technologies in 5G, together with SDN, NFV, and Multi-access Edge Computing (MEC). Related security issues are briefly presented. In [17], the authors introduce the 5G architecture and briefly highlight possible security threats, also considering network slicing as one of the 5G technologies. Similarly, in [18] the authors elaborate on the objectives of a 5G security architecture keeping in mind, among others, the concept of network slicing. In [19], the authors present the concept of network slicing, with a focus on 5G systems, and briefly mention some security and privacy-related issues. The author of [20] gives an overview of network slicing and dedicates one section to network slicing security. In [21], the authors give a survey on the security aspects for 3GPP 5G networks and address network slicing security in one section. Unlike these works, in this article, we instead focus on network slicing security and provide a broader analysis. Only a few other papers focus on network slicing security but they address specific aspects or propose particular methods. We mention some of these now, and refer to these and others whenever needed throughout the paper. In [22], the authors define the Network Slice Manager, an element used by telco on top of the NFV orchestration, and present the related security threats by considering the principles of confidentiality, integrity, authentication, authorization, and availability. In [23], the authors propose trust zones as an alternate approach for security consideration in 5G networks, which can also be applied to network slicing.

Several research projects have been conducted or are currently in progress for the development of 5G, including aspects related to network slicing and security. From these, we mention 5G!Pagoda [24] and ANASTACIA [25], which provided results on network slicing and the Internet of Things (IoT). The list of 5G-PPP projects is available at [26]. Within these, some are related to our work, and we will refer to their findings and deliverables throughout the paper (e.g., 5G-MoNArch, 5G-ENSURE).

III. 5G NETWORK SLICING

This section presents the main concepts and terminology in 5G network slicing [27].

Network slicing is a paradigm that allows the sharing of the same infrastructure for providing differentiated 5G services. Differentiation can be seen in terms of functionality (e.g., mobility, security, control) and performance (e.g., latency,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

throughput, error rate, reliability, availability) [28]. The idea is that a service has a small set of requirements specific to the particular use-case it serves. Focusing on satisfying a smaller set of requirements is feasible and more efficient than considering a large set, which is usually difficult (if not impossible), and many times not even necessary [29].

A network slice instance is an end-to-end logical network custom defined to satisfy required networking characteristics and provide specific services to serve particular use cases (e.g., voice communication, video streaming, e-health, vehicular communication) [19], [27], [30], [31]. A logical network is a set of network function instances on top of physical and virtual resources (e.g., storage, network, processing, and access nodes). A network slice subnet instance is a (local) logical network. One or more network slice subnet instances chained together can constitute a network slice instance. For sake of brevity and simplicity, in the rest of the article, we will refer to network slice instance and network slice subnet instance by using *slice* and *sub-slice*, respectively. The 5G architecture is composed of different network domains, such as the Core Network (CN) and the Radio Access Network (RAN). Chaining a RAN sub-slice and a CN sub-slice is an example of sub-slice chaining.

Slices can be created on-demand, are self-contained, have independent control and management and should be properly isolated [19], [32]. Isolation can be regarded from different perspectives (e.g., performance, dependability, management) [33]. We will further refer to isolation in relation to security aspects only.

A. ARCHITECTURE

The network slicing overall architecture consists of three layers (each with its own management functions) [27], as shown in Figure 1.

1) Resource layer

The lower layer consists of network resources and network functions that serve to provide services to an end-user based on a request. Both resources and network functions can be physical or logical/virtual. Examples of resources include storage, processing, and transmission nodes. Examples of network functions include switching and routing functions, slice selection functions, and authentication functions. A resource or a network function can serve one or more network slice instances [27].

2) Network Slice Instance Layer

The middle layer consists of slices, where a slice provides the network capabilities required by the service instances. A slice can run directly over the network resources or over another slice, and it can serve one or multiple service instances. Two distinct slices might or might not run on the same physical architecture, and hence share or not resources and network functions.

3) Service Instance Layer

The upper layer consists of service instances that are consuming the slices and are offered to customers. Again, for simplicity of exposure, we will refer to a service instance by simply *service*.

The resource management functions are related to the underlying resources and network functions (see Figure 1), and each one can be associated with a different administrative domain. The network slice management function(s) (that from now on we will simply refer to as *slice manager*) manages the life cycle of the slices and interacts with the other management functions. If a slice is composed of sub-slices, there is also a management function for the sub-slices. The communication service management function(s) manages the life cycle of the service and interacts with the slice manager [27].

In the 3GPP specifications [27], [34], roles are defined within a business model and are characterized by different operational responsibilities. Contrary to previous generations, 5G opens the possibility for new business roles for 3rd parties, allowing them more control and system capabilities, on each of the three previously mentioned levels [34]. The 3rd parties are entities, others than the Mobile Network Operator (MNO), that might own or manage some of the resources, functions, slices, and services. Hence, at each layer, the ownership and management can be split among the MNO and the 3rd parties. We will further refer to 3rd parties as *tenants* [35].

B. SLICE LIFE CYCLE

The life cycle of a slice consists of four phases [27], [30]:

1) Preparation

The first phase is dedicated to the preparation of the network environment, designing, creation, and modification of network slices templates. A network slice template is a description of components, structure, and configuration of a slice. The slice itself does not exist in this phase, and it will be built from the template in the second phase [27].

2) Instantiation, Configuration, and Activation

During the second phase, the resources and network functions are created, installed, and configured. The slice is built from the template (using specific instance information), installed, configured, and activated.

3) Run Time

The slice is in use, and it can be subject to modifications (e.g., upgrades, change of configuration, associations, or disassociations of resources and network functions). Supervision and reporting take place in this phase.

4) Decommissioning

The last phase of the life-cycle decommissions the slice. The resources and network functions are now freed. The slice does not exist anymore after this phase.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

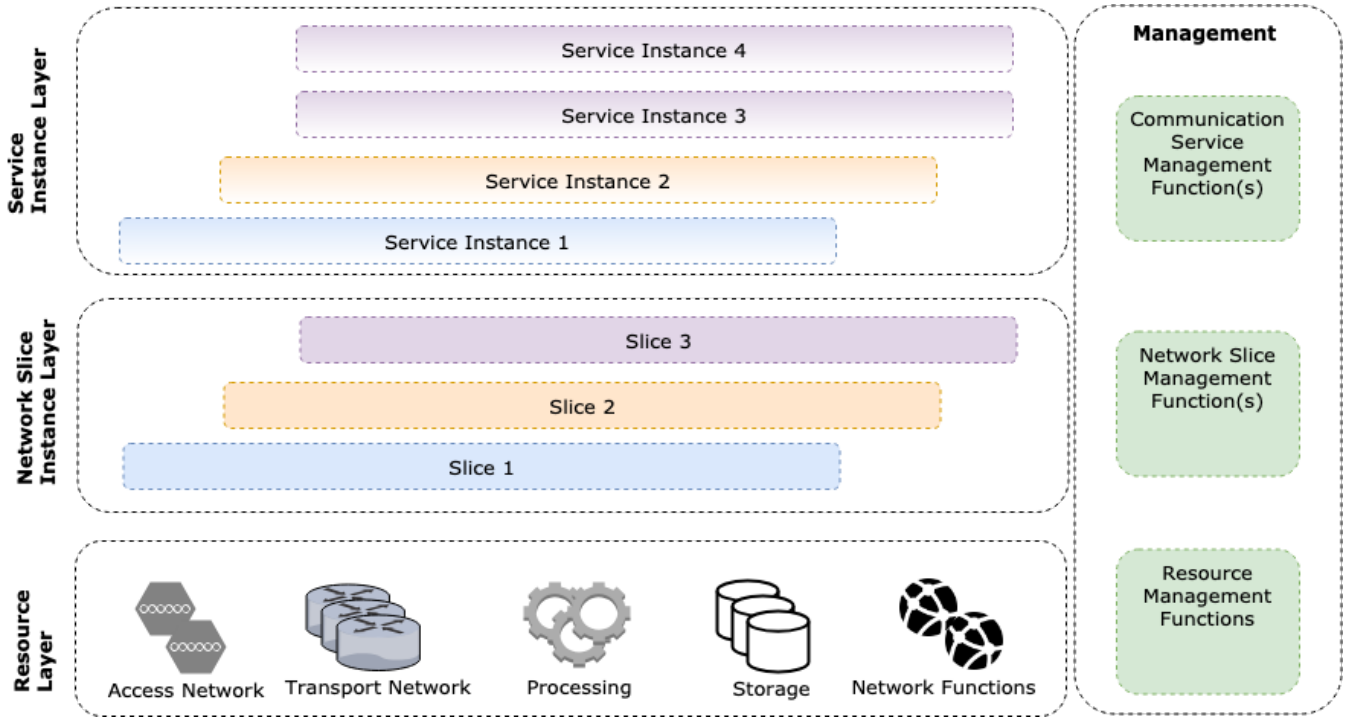

FIGURE 1: Overall architecture in network slicing

The life-cycle management is done via the slice manager, which is responsible for creating and destroying slices, map them to resources and functions, configure the parameters to satisfy services' needs, etc. The slice manager can be accessed by a north-bound standardized Application Program Interface (API) [36]. Depending on the scenario, the operator might allow different actions in the API: create or delete slices, different levels of configuration, report, and monitoring. The security requirements for the APIs, as well as for the phases of a slice in general, will be referred to in Section IV-A.

IV. SECURITY THREATS AND RECOMMENDATIONS

We identify threats and probable points of attack, and we present security recommendations for network slicing in terms of (A) life-cycle security, (B) intra-slice security, and (C) inter-slice security.

A. SLICE LIFE-CYCLE SECURITY

Figure 2 summarizes the representative threats for each phase of the life cycle of a slice.

1) Preparation phase

The main point of attack in the preparation phase is the network slice template. A poorly designed, tampered with or improperly implemented network slice template (e.g., with design flaws, without up-to-date security patches, or injected malware) affects all the slices built from it. In addition to powerful active attacks that might damage the integrity of the template, content exposure might also disclose sensitive information [14], [30].

Specific mitigation techniques include mechanisms to prevent templates from being probed [17]. Cryptographical protocols are used to provide confidentiality (both in transmission and storage), integrity, and authenticity of network slice templates [5]. The correctness of the network slice template must also be verified [5]. Real-time security analysis at the moment of template use can be thought of as a good practice [37].

2) Installation, Configuration, and Activation phase

The main threats in the second phase include creating fake slices or changing the configuration of slices before or during activation. A natural point of attack in this phase is the API, whose compromise would permit an adversary to interfere in the installation, configuration, or activation of a slice [30].

Specific mitigation techniques include mechanisms to secure APIs, such as access and operational rights. Good practices include the usage of TLS (for mutual authentication) or O-Auth (for authorization of service requests) [5], [7]. Moreover, the API should permit auditing, monitoring, and reporting securely (e.g., traffic logs, APIs invocations) [36]. The general cryptographical techniques and real-time security analysis mentioned in the first phase remain useful in the second phase too.

3) Run-time phase

This phase is exposed to the largest variety of threats, which include Denial of Service (DoS), performance attacks, data

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

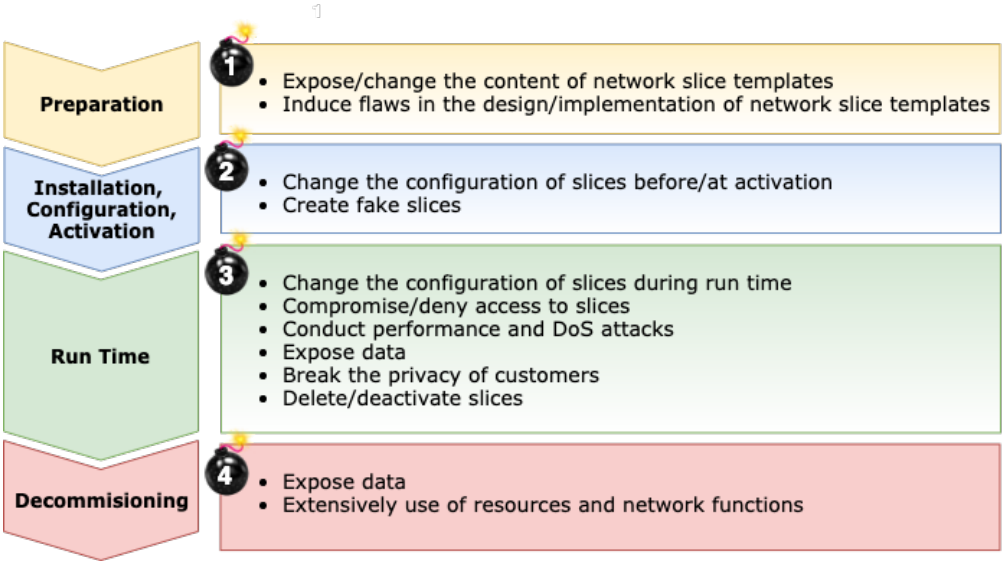

FIGURE 2: Representative threats for each phase of the slice life cycle

exposure, and privacy breaks. Besides, management-related threats, such as unauthorized changes in the configuration, persist also at run time, and new threats, such as the deactivation of a slice, appear. The API remains a main point of attack in this phase, along with the services that consume the slice.

Specific mitigation techniques from the preceding phase remain valid. We highlight here the need for authenticity and integrity verification for the network slice, to prevent fake or modified instances [16]. Specific mitigation techniques against Distributed DoS (DDoS) by slice isolation have been considered [38]. Dynamic NFV that enables on-demand security mechanisms needs still to be studied but is a good candidate for mitigating security issues at run-time [16]. More mitigation techniques will be discussed in Section IV-B.

4) Decommissioning phase

The main threat during and even after deactivation of slices consists of exposing sensitive data that had been improperly handled during decommissioning [30]. A second threat is to consume resources improperly freed to mount a DoS attack.

Specific mitigation techniques include the destruction of sensitive data and the de-allocation of network functions and resources so that they do not remain busy [27].

Throughout the whole lifetime of a slice, the interaction interface used for the slice management must be confidentiality, integrity, and replay protected (e.g., by TLS) [7]. This needs to assure that only authorized parties can create, modify, and delete network slice instances [21]. Moreover, logging and auditing are of extreme importance. Different levels of logging must be implemented in distinct slices, depending on various factors, such as regulations (e.g., lawful interception requirements), the targeted security level for the consuming services, the dedicated type of customer devices (e.g., human vs. machine usage) [30], [39]. Protecting the results of the logs and reports is of extreme importance, as their exposure would leak sensitive information [17]. Usage of dedicated and isolated security zones during the whole life cycle is a good practice to mitigate security risks [23], [37]. General cryptographical primitives, but also more specific 5G physical security technologies (surveyed in [16]) can be used to fulfill data secrecy and privacy.

General security recommendations related to the slice life cycle include [5], [7], [30]:

- Security must be enforced in all four phases because a vulnerability in one phase can introduce vulnerabilities in other phases.
- Appropriate logging and auditing mechanisms should be implemented.
- Network slice templates must be confidentiality and integrity protected in transmission and storage, and their source must be authenticated.
- Isolation should be secured at slice creation, monitored, and, if needed, updated, during the run-time.
- APIs should be secure in terms of access and operational rights and must not expose traffic data; APIs should only allow capabilities and data access as agreed between the parties by legal means.
- At decommissioning, sensitive data must be destructed (or by case, securely stored), and resources and network functions should be freed.

B. INTRA-SLICE SECURITY

Figure 3 summarizes the representative attack points for a slice when we ignore any relation to other slices.

1) 5G customer devices

Outside of organizational protection and mostly used by non-technical users, customer devices are an accessible point

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

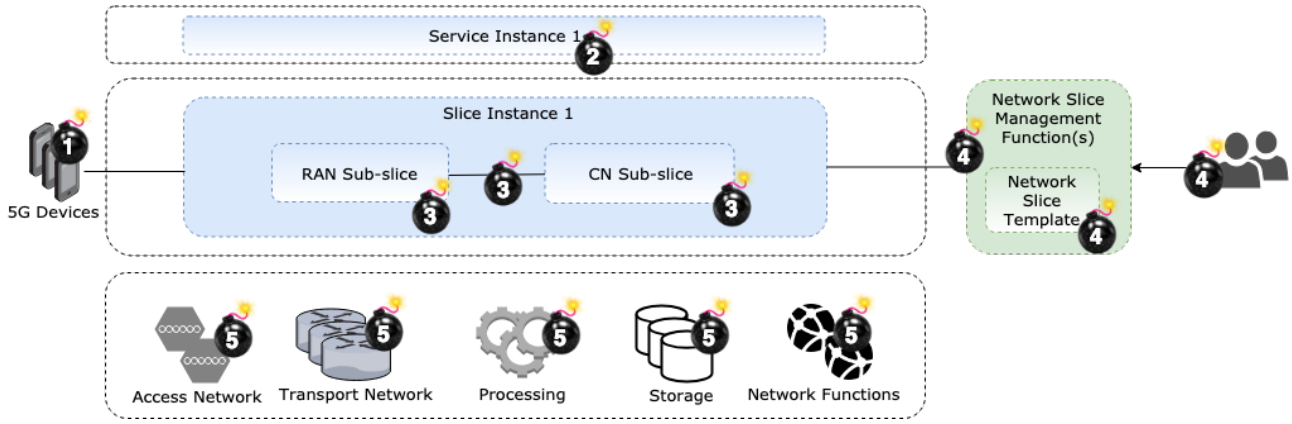

FIGURE 3: Representative points of attack for intra-slice security

of attack. Immediate threats include unauthorized access to slices or services. In addition to economical and privacy and confidentiality problems, unauthorized access impacts the consumption of resources, and hence opens up the possibility for DoS attacks [6]. Moreover, the simple fact of attaching to a slice might by itself introduce customer privacy concerns. For example, slice identification can become a vulnerability in correlation to the permanent identifiers of the customer devices, by delimiting groups of interests composed of subscribers that use the same slice, and hence most probably the same services. The risks associated with the 5G customer devices increase when they access the network slice via non-3GPP networks [30].

Specific mitigation techniques include strong authentication and access control for 5G customer devices. On top of the *primary authentication* that allows devices to access the network, a *secondary authentication* (or *slice specific authentication*) at the slice level is recommended [6], [31], [40]. The primary authentication must be standardized to allow roaming and different technologies interconnection. Secondary authentication should be also standardized, to decrease costs and facilitate integration [6]. The secondary authentication is in the responsibility of the entity that manages the slice. Procedures and candidate solutions for specific access authentication and authorization are given in [6], [40]. In the case of slice tenants, the tenant is directly involved in the access control for the slices it manages, which makes resources allocation more efficient [9]. With respect to slice identification, candidate solutions to protect the privacy of the slice identity are also considered in [6]. Limitations in the number of customer devices that can simultaneously access a network slice, the number of simultaneous active sessions, and the data rate per device, performed at different levels in the network, can mitigate risks associated to DoS [41].

2) Slice-services interface

A possible point of attack is the interface between the slice and the services that consume the slice. More precisely, an adversary might damage the slice by attacking a service. This might result in damaging other services running over the same slice. Moreover, in the case of direct communication between services, this can also be a possible point of attack.

Specific mitigation techniques include the implementation of proper security levels and correct configurations of services (e.g., limitations in rights and resources). A correct level of isolation must be implemented among the services and between the slice and the consuming services.

3) Sub-slices

If the slice is defined as a chain of several sub-slices, both the sub-slices themselves and the interconnection between the sub-slices represent attack points. The overall level of security in a chain of sub-slices is given by the weakest sub-slice.

Specific mitigation techniques include securing the sub-slices and implementing mechanisms to decrease risks at interconnection, especially if the access network is non-3GPP. Investigating security issues at the interconnection of different technologies is still subject to future work and more study needs to be performed with respect to RAN sub-slices [29]. We will discuss more on end-to-end isolation as a possible solution in Section V-A.

4) Slice manager

The slice manager brings in the security issues already discussed in Section IV-A, concerning network slice templates, APIs, access rights, mutual authentication, trust, etc. Increased risks appear when tenants are responsible for the slice management, as they might try to access functionalities that are outside of the legal agreement [9], [36].

Specific mitigation techniques for management issues have already been discussed. Slice life-cycle security can be considered to be a part of intra-slice security, but we discuss it distinctly because of its particularity and importance. Mutual authentication should be set in place between the host platform and the network manager [16]. If more slice managers co-exist, they have to mutually authenticate each other [16]. If tenants are responsible for the slice management, then their capabilities should be restricted in conformity to legal agreements between the parties. More precisely, tenants

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

should be prevented access to any requests, data, resources, and functions other than the ones agreed by legal means [9], [30]. 3GPP also recommends network slice performance and fault monitoring in multiple tenants' environments [35].

5) Resources and network functions

Resources and network functions might be attacked to damage the slices that consume them. A large variety of possible attacks can take place, including physical attacks, software attacks, and more general cyber-attacks.

Specific mitigation techniques include mutual authentication, secure boot, credential access, physical security, and integrity verification. These techniques increase the level of trust but are not strictly specific for network slicing, so they reside outside the scope of this article. Avoid co-hosting for different levels of security or sensitivity [16]. In particular, avoid co-hosting between slices that provide sensitive services and slices that use experimental or test code [8].

General security recommendations related to the intra-slice security include [8], [9], [14], [30], [39]:

- Slices are end-to-end logical networks, so end-to-end security should be considered.
- All communication (e.g., between the slice and the resource layer, the slice and the slice manager, the sub-slices of a slice, the customer device and the access point in the network) should use adequate mechanisms to assure the target security level; minimal requirements should include confidentiality, integrity, authenticity of the data, and mutual authentication between peers.
- 5G customer devices should be strongly authenticated, by primary and preferable secondary authentication too.
- All resources and network functions consumed by a slice should be secured.
- New facilities introduced by tenants (e.g., network functions, configurations, services) and their integration should be adequately secured to prevent weaknesses that can be further exploited.
- Sensitive identifiers should be protected and no correlation between identifiers should be leaked.
- Lawful interception should be accessible at both slice and service layers.
- Tenants access, rights, and configuration capabilities must be conforming to the legal agreements between the parties.
- All the 3GPP general security requirements must be satisfied at the slice level too.

C. INTER-SLICE SECURITY

Figure 4 summarizes the representative attack points for a slice when we consider it in relation to other slices.

1) 5G customer devices

5G customer devices are one of the most vulnerable points of attack. A security threat appears when a customer device authorized to access one slice might try to gain access to another unauthorized slice. The difference with the intra-slice scenario is that now the device is not a complete outsider, and this might be an advantage. Another threat is that the adversarial device might damage the performance of a slice or even succeed a DoS attack by excessively consuming shared resources in the slice it is authorized to access. A performance attack can facilitate other types of attacks by preventing the slice to perform security protocols at the required level because of a lack of resources [8]. Normally, a device should be authorized to attach to a single slice. However, if the device needs diversified access to services, it might be allowed to attach to several slices simultaneously [39]. If so, it appears the risk that the device leaks sensitive data from the more-secured slice to the less-secured slice. Naturally, the risk increases when the access technologies are different (e.g., 3GPP and non-3GPP) [30].

Specific mitigation techniques include proper isolation between slices, in terms of access control, confidentiality, integrity, authenticity, and resource consumption. A particular case here is the *mutually exclusive access* to network slices, when customer devices are restricted to access two (or more) network slices simultaneously [40]. If this is not the case, separate mutual authentication between each slice and the customer device is recommended [16]. The resources should be configured to guarantee their availability for running security mechanisms and also avoid DoS (e.g., by resource capping or ring-fencing) [8], [16].

2) Service-service communication

A possible point of attack is the interface between the services that consume different slices. More precisely, by attacking some services, an adversary might damage other services that run on top of other slices. We consider this to be a low-security risk because usually services running on different slices are independent, and hence there is no necessity of communication.

Specific mitigation techniques include the implementation of proper isolation. Traffic and behavioral analysis, as well as anomaly detection, are general techniques to investigate disallowed communication, within or between the slides and different components [11], [23]. Specific techniques based on traffic capture and defense mechanisms using artificial intelligence might be used to protect against advanced attacks that bypass basic filters [11]. Traffic isolation can also be enforced by network elements by defining flow rules to prevent slice trespassing [10].

3) Intra-slices and intra-sub-slices communication

An adversary might try to attack a less-secured slice (in particular the RAN sub-slice) to attack a more-secured slice [8], [30]. If communication between slices is allowed, possible threats include unauthorized access, leakage of shared parameters (if any), sensitive data transmitted between the slices [10].

Specific mitigation techniques include proper isolation between the slices. More precisely, if one slice is com-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

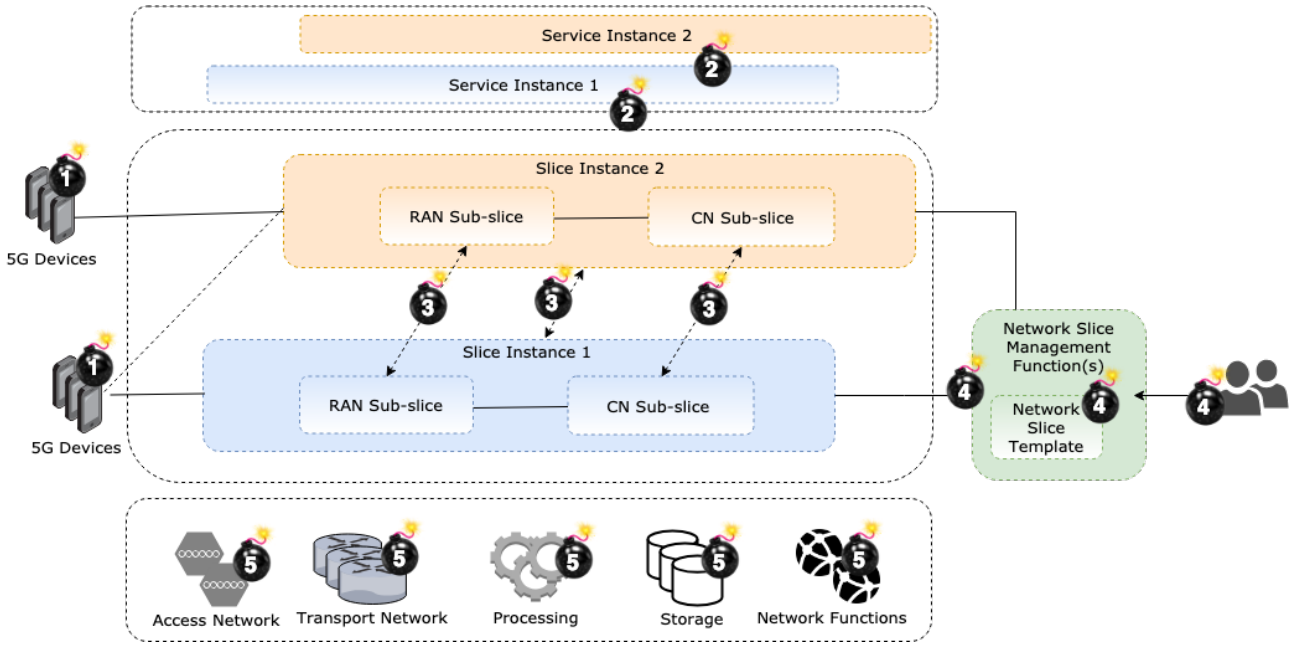

FIGURE 4: Representative points of attack for inter-slice security

promised, this should not affect in any way other slices. The communication between slices has to be controlled and secured [16]. The techniques that we previously referred to for communication between services can be successfully applied here too. To avoid leakage, cryptographic parameters (e.g., cryptographic keys) should never be shared between slices [30]. If the keys from the primary authentication are used within the slices, new and independent keys must be generated for each slice by using a key derivation function [9]. Some solutions for secure keying have been proposed [42], but key management in network slicing must be further investigated. Examples of inter-slice isolation enabling technologies include tag- (using e.g., MPLS), VPN- (using e.g., SSL/TLS), or VLAN-based isolation [29].

4) Management systems

The management system is a point of attack. A tenant might try to access other tenants' slices or change parameters shared among slices belonging to different tenants.

Specific mitigation techniques include proper isolation between distinct slices in the slice manager and restriction to perform changes on parameters shared among slices belonging to different tenants [9]. Strong authentication and access control procedures must be in place.

5) Resource infrastructure

The resource layer is an attack point not only in terms of exhaustive consumption or DoS but also in other terms, such as software attacks. For example, an adversary might access and tamper code in one slice, causing changes in execution in all slices that use the same code [8].

Specific mitigation techniques include code protection techniques and code isolation, which are not strictly specific to network slicing, so they are outside the scope of this paper. We nevertheless refer to some techniques in Section V-B.

General security recommendations related to the inter-slice communication include [8], [14], [29], [30] :

- A minimal security level should be granted for every slice.
- Isolation between the slices should be strong enough to prevent attacks via the less secured slices.
- Communication between slices should be reduced at minimum, defined on strict rules, and implemented via secured channels.
- Cryptographic keys (and other sensitive parameters) should not be shared between slices.
- Allocation of resources should guarantee a minimal level of availability for each slice; in particular, security mechanisms should be able to run regardless of the resource consumption.
- Slices with a significant difference in security levels should not share resources or network functions; in particular, never run slices in test mode together with slices in run time phase.
- Distinct authentication, authorization, and access control mechanisms should be independent for each slice.
- If a 5G customer device is allowed to simultaneously attach to multiple slices, isolation (of data) should be possible at the customer device too.
- Tenants must be disallowed to do configuration changes that impact the slices and services of other tenants.

V. DISCUSSION

Performing a complete analysis of security aspects in network slicing is currently impossible. This is because of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2997702, IEEE Access

on-going security specifications for 5G, which are continuously prone to changes, and lack of implementation of slicing (at large scale). At the moment, the analysis of network slicing security is in an incipient phase, and much is to be learned about the slicing concept itself and the associated security risks. We further discuss some challenges and open problems, identified based on the threats and recommendations presented in the previous section. They all create a basis for future work.

A. END-TO-END SECURITY

Network slices are end-to-end logical networks, so it is natural to aim for end-to-end security. The concept of end-to-end security is closely connected to the concepts of isolation and orchestration. Moreover, it is dependant on the business model and consequentially of the trust model. Therefore, some aspects of the end-to-end security will be discussed in the related following subsections.

In [17], the authors briefly highlight possible security threats after introducing the end-to-end 5G architecture, considering network slicing as one of the 5G enabling technologies. End-to-end isolation can be seen as a prerequisite for end-to-end security, and it is discussed, for each sub-slice, in [13]. End-to-end security in CN is also referred to in [7]. Achieving end-to-end isolation is not a trivial task, as, for example, even the creation of the RAN sub-slices is still problematic [29]. Currently, end-to-end security still remains a challenge in 5G in general and a topic for further research.

B. ISOLATION

Isolation targets no direct or indirect influence between different slices or entities within a slice. Security is one dimension of isolation, together with performance and dependability [33]. Isolation must be considered from different perspectives: isolation between network slices, isolation between network functions, isolation between users, etc. [13]. We remind here isolation in terms of information leaked to the slice environment, as a side-channel attack resistance technique [29]. Each of these isolation types has its own role and the possible flaws bring in security risks. Isolation can be either full or partially [29], and it can be performed by both physical and logical means [13], [33]. The principle of physical separation places an important role in isolation. Examples include resource separation for high secured slices or dedicated spectrum for different network slices [13]. However, physical isolation is sometimes infeasible [20], so strong logical isolation mechanisms must be provided. Technologies such as firewalls, gateways, hypervisors can be used to achieve isolation. Isolation can hence be considered at all levels starting from physical isolation, hardware, operating systems, virtual machines, sandbox based isolation, or even isolation at the network programming language level [29], [43]. Security trust zones were also proposed as an isolation technique [23]. More means for enabling isolation are available in [29], [44].

Slice isolation might also be challenging because of the diversity of technologies used in the network. Isolation should be usually performed at different levels and with heterogeneous environments (e.g., OS kernel, firmware, upper-level software systems) provided by different vendors. Special attention must be given to isolation multi-tenants cloud-based solutions [44], as well as slices belonging to different actors [15], [18]. Complexity in the case of multi-domain infrastructure is a risk for security and raises challenges [21]. In a scenario where the network slices may be created by an organization like a MNO and rented out to 3rd-party organizations like enterprises, network slices relying solely on common infrastructure cannot meet the highest isolation requirements [45]. Isolation within these scenarios is still a hot research topic. Moreover, the measurement of isolation remains an open problem [29], [46].

C. SECURE MANAGEMENT AND ORCHESTRATION

The management and orchestration (MANO) of network slicing is introduced by 3GPP and is composed of three management functions as depicted in Figure 1. The network slice orchestration is directly connected to the NFV orchestration and therefore inherits the related challenges [47].

The architecture of the network slice MANO is challenging from a business model perspective because of the variety of scenarios with different actors, multi-domain environments, and several layers of imbricated tenants, which can play different roles and have different rights. Technically, this means high complexity and flexibility, which bring in higher security risks. The integration of various platforms and technologies (belonging to different tenants) is one of the main concerns. One approach to the problem is the standardization of interconnection interfaces, to assure a minimum security level. Moreover, a MANO instance can be provided to the various tenants by using a MANO-as-a-service paradigm [48]. The orchestration of a network slice spanning across multiple administrative domains is also a challenge that has been tentatively faced by proposing 3GPP-based hierarchical architecture [49]. Many architectures have been suggested, for example, 5G-NORMA proposed a MANO called Software-Defined Mobile Network Orchestrator (SDM-O), which is composed of an inter-slice resource broker for cross-slice resource allocation and slice-specific NFV orchestrators [50].

Another MANO issue is to deploy the correct security mechanisms for each slice in an efficient way. A solution might be a slice security MANO that automatically decides on the security policies and mechanisms based on different parameters (e.g., SLA, technical capabilities of the 5G customer devices) [14]. Artificial intelligence integrated security mechanisms might help in the automated process, especially in the case of dynamic and frequent changes [51]. The development of such security mechanisms is the subject of future work. Models and experimentation to solve the security constraints for automated 5G slice deployment have been proposed [52]. As a network slice can dynamically

change over time, orchestration, and hence orchestration security policies, become mandatory [16]. Finally, securing the slice MANO themselves are a research priority, as a flawed slice manager directly impacts all managed slices. Management rights granted to tenants must be treated with care especially when several tenants share common resources and network functions. For this purpose, the 5G-NORMA architecture includes two main controllers, Software-Defined Mobile Network Coordinator (SDM-X) for the control of common (shared) network functions and Software-Defined Mobile Network Controller (SDM-C) for dedicated network functions [50].

D. TRUST MODEL

The trust model plays an important role in network slicing security. Directly related to the business model and the overall architecture, trust must be considered at different layers between the MNOs and the tenants [30], [34]. The parties must assume a level of trust, which should be expressed by legal agreements. This applies in the relation to tenants and among tenants at any of the three architectural layers: resource, slice, and service layers. Trust must be enforced at a technical level too. For example, a slice manager cannot trust the host platforms by default, and the host platforms cannot trust the slice manager by default, especially when slices use resources from different physical networks [8]. A model for evaluating the overall trust of the network slice has been proposed [53]. The research on technical mechanisms that can help to increase the level of trust in network slicing is of interest.

E. 5G CUSTOMER DEVICES

We have identified 5G customer devices as one of the main attack points. Research priorities should include mitigating risks associated to end devices. Attention should be given to special scenarios such as one device associated to several slices simultaneously, or devices associated to slices running on top of different domains. It is interesting to analyze how security is impacted by roaming. For simplicity, it is assumed that only slices and services that exist in both the home and visiting network will be available [30], [31]. Similarly, security risks that emerge from emergency access must be considered [28]. Over the years, emergency services proved to be a vulnerable point of access, so how are these to be handled at the slice level is to be further discussed. Moreover, it should be analyzed to what extent will slice identification and the correlation to customer devices will expose the privacy of individuals accessing the slices. Mechanisms to provide isolation in the customer devices and best practices for implementing secondary authentication should be further studied.

VI. CONCLUSIONS

We have presented threats and recommendations concerning networks slicing security. We conclude that network slicing security brings in a variety of issues that need to be addressed. Because network slicing itself is at an early development stage, the in-depth security analysis is premature. Many open aspects still need to be clarified and further discussed. We refer to some of these and indicate some possible research directions. Among these, we mention end-to-end security, automated defense mechanisms (using artificial intelligence), rigorous implementation and measurement of isolation, and rigorous security models (for network slicing in general or dynamic network slicing in particular). We anticipate still a considerable time until experimental analysis of network slice security can be conducted (at large scale) to validate theoretical results.

REFERENCES

[1] 3GPP, "Release 16," 2019. [Online]. Available: https://www.3gpp.org/release-16
[2] ——, "Release 17," 2020. [Online]. Available: https://www.3gpp.org/release-17
[3] G. Nencioni, R. G. Garroppo, A. J. Gonzalez, B. E. Helvik, and G. Procissi, "Orchestration and Control in Software-Defined 5G Networks: Research Challenges," Wireless Communications and Mobile Computing, 2018.
[4] ITU-R, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond (Recommendation ITU-R M.2083-0)," 2015.
[5] 3GPP, "TR33.811: Study on security aspects of 5G network slicing management (Release 15) V15.0.0 ," 2018.
[6] ——, "TR33.813: Study on Security Aspects of Enhanced Network Slicing (Release 16) V0.8.0," 2019.
[7] ——, "TS33.501: Security architecture and procedures for 5G system (Release 16) V16.2.0 ," 2020.
[8] NMGN, "NMNG Alliance: NMNG Alliance: 5G security recommendations, Package #2: Network Slicing," 2016.
[9] ——, "NMNG Alliance: Security Aspects of Network Capabilities Exposure in 5G," 2018.
[10] ENISA, "ENISA THREAT LANDSCAPE FOR 5G NETWORKS - Threat assessment for the fifth generation of mobile telecommunications networks (5G)," November 2019.
[11] 5G Americas, "The Evolution of Security in 5G: A "Slice" of Mobile Threats," 2019.
[12] ——, "Network slicing for 5G networks & services," 2016.
[13] ZTE, "5G Security White Paper - Security Makes 5G Go Further," May 2019.
[14] Huawei, "Huawei: Huawei: 5G Security Architecture White Paper," 2017.
[15] 5G-PPP, "5G PPP Phase1 Security Landscape," Last accessed: April 2020. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf
[16] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements and future directions," IEEE Communications Surveys Tutorials, pp. 1–1, 2019.
[17] T.-H. Ting, T.-N. Lin, S.-H. Shen, and Y.-W. Chang, "Guidelines for 5G end to end architecture and security issues," arXiv preprint arXiv:1912.10318, 2019.
[18] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon et al., "A security architecture for 5g networks," IEEE Access, vol. 6, pp. 22 466–22 479, 2018.
[19] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5g with sdn/nfv: Concepts, architectures, and challenges," IEEE Communications Magazine, vol. 55, no. 5, pp. 80–87, 2017.
[20] S. Zhang, "An overview of network slicing for 5g," IEEE Wireless Communications, vol. 26, no. 3, pp. 111–117, June 2019.
[21] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," IEEE Communications Surveys Tutorials, vol. 22, no. 1, pp. 170–195, 2020.
[22] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, "Network slicing security: Challenges and directions," Internet Technology

Letters, vol. 2, no. 5, p. e125, 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.125

[23] D. Schinianakis, R. Trapero, D. S. Michalopoulos, and B. G.-N. Crespo, "Security considerations in 5g networks: A slice-aware trust zone approach," in 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019, pp. 1–8.

[24] 5G!Pagoda, Last accessed: April 2020. [Online]. Available: https://5g-pagoda.aalto.fi/

[25] ANASTACIA, Last accessed: April 2020. [Online]. Available: http://www.anastacia-h2020.eu/

[26] 5G-PPP, Last accessed: April 2020. [Online]. Available: https://5g-ppp.eu/

[27] 3GPP, "TR28.801: Study on management and orchestration of network slicing for next generation network (Release 15) v15.1.0," 2018.

[28] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega et al., "Network slicing to enable scalability and flexibility in 5g mobile networks," IEEE Communications magazine, vol. 55, no. 5, pp. 72–79, 2017.

[29] Z. Kotulski, T. Nowak, M. Sepczuk, M. A. Tunia, R. Artych, K. Bocianiak, T. Osko, and J. Wary, "On end-to-end approach for slice isolation in 5G networks. fundamental challenges," in Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3-6, 2017., 2017, pp. 783–792.

[30] 3GPP, "TR33.899: Study on the security aspects of the next generation system (Release 14) V1.3.0 (withdraw) ," 2017.

[31] ——, "TS23.501: System Architecture for the 5G System; Stage 2 (Release 16) v16.4.0," 2020.

[32] ——, "TR22.891: Feasibility Study on New Services and Markets Technology Enablers; Stage 1; Stage 1 (Release 14) V14.2.0," 2016.

[33] A. J. Gonzalez, J. Ordonez-Lucena, B. E. Helvik, G. Nencioni, M. Xie, D. R. Lopez, and P. Grønsund, "The Isolation Concept in the 5G Network Slicing," in European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, June 2020.

[34] 3GPP, "TR22.830: Feasibility Study on Business Role Models for Network Slicing (Release 16) V16.1.0," 2018.

[35] ——, "TR28.804: Study on tenancy concept in 5G networks and network slicing management (Release 16) V16.0.1," 2019.

[36] ——, "TR23.722: Study on Common API Framework for 3GPP Northbound APIs (Release 15) V15.1.0," 2018.

[37] B. Chatras, U. S. T. Kwong, and N. Bihannic, "Nfv enabling network slicing for 5g," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN). IEEE, 2017, pp. 219–225.

[38] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019, pp. 82–90.

[39] 3GPP, "TR22.864: Feasibility Study on New Services and Markets Technology Enablers - Network Operation; Stage 1 (Release 15) V15.0.0," 2016.

[40] ——, "TR23.740: Study on Enhancement of Network Slicing (Release 16) V16.0.0," 2018.

[41] ——, "TR23.700-40: Study on Enhancement of Network Slicing Phase 2 (Release 17) V0.3.0," 2020.

[42] P. Porambage, Y. Miche, A. Kalliola, M. Liyanage, and M. Ylianttila, "Secure keying scheme for network slicing in 5g architecture," in 2019 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2019, pp. 1–6.

[43] S. Gutz, A. Story, C. Schlesinger, and N. Foster, "Splendid isolation: A slice abstraction for software-defined networks," in Proceedings of the first workshop on Hot topics in software defined networks, 2012, pp. 79–84.

[44] V. Del Piccolo, A. Amamou, K. Haddadou, and G. Pujolle, "A survey of network isolation solutions for multi-tenant data centers," IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2787–2821, 2016.

[45] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5g mobile network slice isolation for highly sensitive third-party services," in 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6.

[46] F. Messaoudi, P. Bertin, and A. Ksentini, "Towards the quest for 5g network slicing," in 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), 2020, pp. 1–7.

[47] A. J. Gonzalez, G. Nencioni, A. Kamisiński, B. E. Helvik, and P. E. Heegaard, "Dependability of the nfv orchestrator: State of the art and research challenges," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 3307–3329, Fourthquarter 2018.

[48] F. Z. Yousaf, V. Sciancalepore, M. Liebsch, and X. Costa-Perez, "Manoaas: A multi-tenant nfv mano for 5g network slices," IEEE Communications Magazine, vol. 57, no. 5, pp. 103–109, 2019.

[49] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," IEEE Network, vol. 33, no. 5, pp. 242–252, 2019.

[50] C. Mannweiler, M. Breitbach, H. Droste, I. L. Pavón, I. Ucar, P. Schneider, M. Doll, and J. R. Sanchez, "5g norma: System architecture for programmable multi-tenant 5g mobile networks," in 2017 European Conference on Networks and Communications (EuCNC), 2017, pp. 1–6.

[51] L. Suárez, D. Espes, P. Le Parc, F. Cuppens, P. Bertin, and C.-T. Phan, "Enhancing network slice security via artificial intelligence: challenges and solutions," 2018.

[52] F. Boutigny, S. Betgé-Brezetz, G. Blanc, A. Lavignotte, H. Debar, and H. Jmila, "Solving security constraints for 5g slice embedding: A proof-of-concept," Computers & Security, vol. 89, p. 101662, 2020.

[53] B. Niu, W. You, H. Tang, and X. Wang, "5g network slice security trust degree calculation model," in 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017, pp. 1150–1157.

RUXANDRA F. OLIMID is Associate Professor at the Department of Computer Science, University of Bucharest and Adjunct Associate Professor at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. She received her Ph.D. in Computer Science from the University of Bucharest in 2013. She has a background in both computer science (BSc and MSc from the University at Bucharest, 2008 and 2010) and telecommunications (BSc from the University Politehnica of Bucharest, 2009). She was a post-doctoral researcher with Norwegian University of Science and Technology, Norway, from 2016 to 2018. Her past experience includes Cisco certifications (CCNA, WLAN/FE) and almost 10 years in Orange Romania. Her research interests include cryptography and privacy, with a current focus on privacy and security in communication networks.

GIANFRANCO NENCIONI received the M.Sc. degree in telecommunication engineering and the Ph.D. degree in information engineering from the University of Pisa, Italy, in 2008 and 2012, respectively. In 2011, he was a visiting Ph.D. student with the Computer Laboratory, University of Cambridge, U.K. He was a Post-Doctoral Fellow with the University of Pisa from 2012 to 2015 and the Norwegian University of Science and Technology, Norway, from 2015 to 2018. He is an Associate Professor with the University of Stavanger, Norway, from 2018. He is currently the leader of the project 5G-MODaNeI funded by the Norwegian Research Council. His research activity regards modelling and optimization in emerging networking technologies (e.g., SDN, NFV, 5G, Network Slicing, Multi-access Edge Computing). His past research activity has been focused on energy-aware routing and design in both wired and wireless networks and on dependability of SDN and NFV.