End-to-End Network Slicing Security across Standards Organizations

Ranganathan Mavureddi Dhanasekaran, Jing Ping, and German Peinado Gomez

Abstract

This article makes a holistic analysis of the security aspects specified for 5G network slicing across the main standards and industry organizations, namely 3GPP, ETSI, and GSMA. A network slice is a logical end-to-end network that provides specific network capabilities and characteristics to serve a defined business purpose of communications service providers' (CSPs') customers. That purpose can be motivated by CSP internal reasons including network operation optimization, services classification, resources optimization, cost savings, support of network automation, or other specific customer demands. Network slicing can be defined as a paradigm where network slices are created with appropriate isolation, set of resources, and optimized topology, becoming a key feature and business driver for 5G. The overall security architecture of the 5G network is being constantly enhanced with new security features available as well in network slices as logical networks created within the 5G network. In contrast, the threat surface is increased with network slicing as new factors such as business models, tenants, functions, interfaces, and signaling flows are introduced, especially when the isolation among network slices is not well designed and effectively enforced. By analyzing the underlying security threats on network slicing, the article derives the corresponding security requirements and studies the specified mechanisms to protect the network slices. The article concludes pointing out several gaps in current standards with respect to 5G network slicing security and depicts possible next steps for further investigation.

Introduction

Network slicing is a key feature and business driver for 5G, with enables enterprises and operators to address specific requirements of different market segments (e.g., industrial, smart cities, healthcare, automotive). Similar to requirements of bandwidth, performance, latency, or mobility, security is a fundamental network requirement in the design of network slices that needs to be optimized for each specific use case, especially for those uses cases where security becomes critical, such as vehicle-to-everything (V2X) platooning, enterprise virtual private networks (VPNs), and electric grids.

Since Release 16, the 3rd Generation Partnership Project (3GPP) has provided specific security requirements and features for network slicing [1], and the work continues in Release 18. Groupe Spéciale Mobile Association (GSMA) members have also contributed to the implementation of security mechanisms [2–4]. Also, the European Telecommunications Standards Institute (ETSI) has addressed this topic within the Zero Touch Network and Service Management (ZSM) group [5].

This article analyzes the security aspects specified for 5G network slicing across the main standards developing organizations (SDOs), with special focus on 3GPP specifications and GSMA recommendations, and some references to ETSI's relevant work.

By analyzing the underlying security threats and requirements on network slicing in standards, the article studies the specified mechanisms to protect the network slices. The article concludes pointing out several gaps in current standards with respect to 5G network slicing security and depicts possible next steps for further investigation.

The structure of this article is as follows. The next section provides an overview of the network slicing architecture, relevant identifiers, and the security landscape. Following that, we capture the main security mechanisms to protect network slices. We then make a brief gap analysis in standards with respect to network slicing security aspects and suggest next steps for further study. Finally, we summarize our main conclusions.

Network Slicing Security: Setting the Scene

Previous mobile network generations already had certain capabilities to partition the network, providing a limited form of isolation based on different network sharing configurations, for example, gateway core network (GWCN), dedicated core network (DECOR), access point name routing (APN), and multi-operator core network (MOCN). A major limitation was the lack of an end-to-end framework to slice up the network and manage the slices, which is now solved in 5G. In 5G, a network slice is defined as a logical network that provides specific network capabilities and network characteristics to serve a defined business purpose of customer(s) [6]. A network slice subnet (NSS) is a representation of a set of managed network functions and required resources (e.g., compute, storage, networking). Each network slice is made up of several NSSs like the

Digital Object Identifier:
10.1109/MCOMSTD.0005.2200055

Ranganathan Mavureddi Dhanasekaran is with Nokia Standards, Germany; Jing Ping is with Nokia Shanghai Bell, China; German Peinado Gomez is with Nokia Standards, Poland..

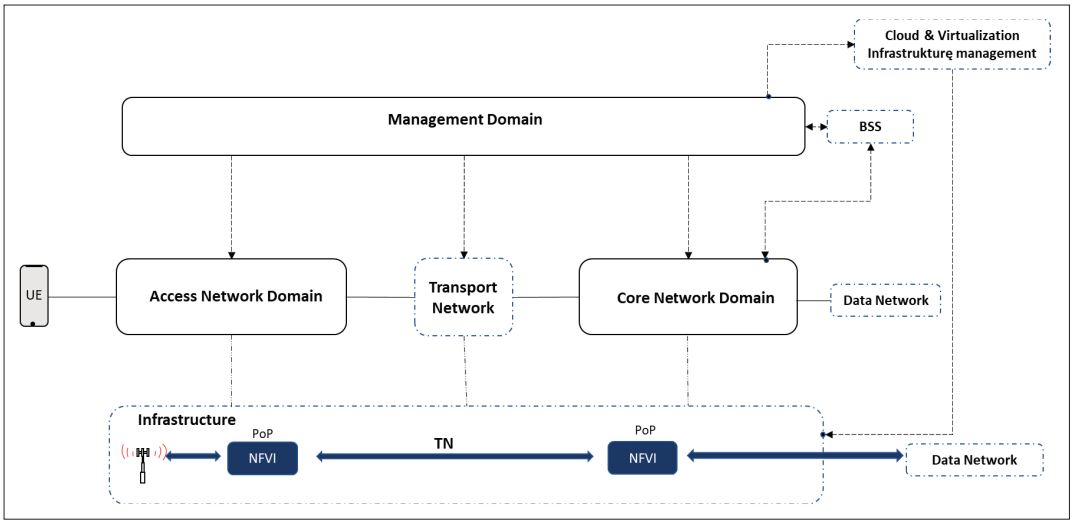

FIGURE 1. Network slice architecture.

radio access network (RAN) subnet, the 5G core network (CN) subnet, and the transport network (TN) subnet. The CSP determines which subnets build a network slice.

Network slicing is a key feature and business driver for 5G, enabling enterprises and operators to address specific requirements of different market segments, including factories, smart cities, automotive, and so on. For more detail about market segments and use cases, please refer to [7].

Network Slice Architecture

Figure 1 shows the overall network slice architecture [2, 5, 8, 9]. It is structured into three main stratums:

- O&M stratum
- Network and application stratum
- Infrastructure stratum

O&M Stratum

The operations and management (O&M) stratum conveys the operation support system (OSS) functionality enabling the deployment and operation of network slices. A network slice management system can be deployed based on a service-based management architecture as defined in 3GPP SA5 [8] and ETSI ZSM [5]. The 3GPP-defined network slice management system includes three management domains: end-to-end (E2E) service Management Domain (MD), RAN MD, and CN MD. TN Management domain is addressed by the Internet Engineering Task Force's (IETF's) Traffic Engineering Architecture and Signaling (TEAS).

Network Stratum

The network stratum provides the user plane and control plane functionalities across different segments of the 5G network, such as RAN and CN. Additionally, to provide E2E communication services, 3GPP's specified 5G network can integrate application servers and non-3GPP entities, such as data networks (DNs) and transport networks (TNs). When preparing a network slice, the 3GPP management system coordinates with non-3GPP management systems to fulfill and assure E2E service requirements from the communication services. An E2E network slice is built as the interlocking of RAN, TN, and CN network slice subnets.

Infrastructure Stratum

The infrastructure stratum accommodates all hardware and software resources building up the operator substrate, which includes user equipment, and compute, storage, and network equipment. The infrastructure stratum has the abilities to manage that infrastructure and orchestrate the allocation of resources needed to provide the required network services. Additionally, it could also map specific requests to an appropriate network service catalog, taking into consideration network service instance requirements, such as bandwidth and/or latency.

The article focuses on the security aspects within the domains of the aforementioned O&M and network strata, that is, the O&M, RAN, TN, and CN domains in the figure. Further, the article mentions the capability of infrastructure to support resource isolation for a slice. Please note that the figure is not exhaustive and provides a simplified view. For further details and stratum internals, please refer to [7].

Network Slice Identifiers

The identifier of a network slice is the single network slice selection assistance information (S-NSSAI), where NSSAI represents a collection of S-NSSAIs. An S-NSSAI comprises a mandatory information named slice service type (SST), which indicates the slice characteristics, and optional information named slice differentiator (SD). SD allows the operator to differentiate among multiple network slices with the same SST [10]. This differentiation can be in terms of slice features (e.g., mobile vs. fixed-wireless access services, charging), customer information (tenancy), and slice priority. Figure 2 shows a list of S-NSSAIs with different standardized SST values corresponding to slices suitable to handle 5G enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), massive IoT (MIoT), V2X services, high-performance machine-type communications (HMTC), and others.

Network Slicing Security Landscape

A service level agreement (SLA) in network slicing represents a commitment of a provisioned network as a service between a network slice provider (NSP) and a network slice consumer (NSC). As part of the SLA, the NSC declares services requirements to the NSP, and those requirements,

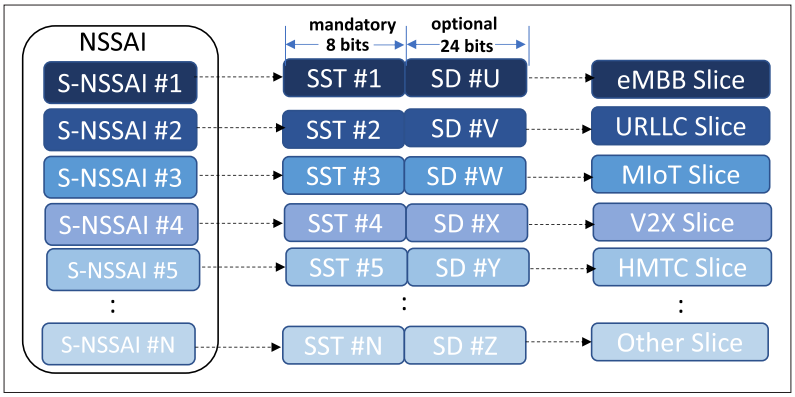

FIGURE 2. S-NSSAIs with different standardized SST values.

including security related requirements, build the service level specification (SLS). To translate the requirements into specific attributes and parameters to be configured in the network slice, two artifacts have been defined in GSMA:

- The generic network slice template (GST): A set of attributes characterizing a type of network slice service and not tied to any specific network deployment.
- The network slice type (NEST): A GST filled with values. It is an input to the network slice preparation performed by the NSP [3].

Figure 3 shows the building blocks involved in the whole process of how GST attribute values are used by 3GPP network slice architecture as inputs to the network slice network resource model (NRM) [11].

5G use cases come with very diverse networking requirements in terms of bandwidth, performance, latency, and mobility. Many of those use cases will be configured in network slices. Security is a fundamental network requirement in the design of the network slices, which, as any other requirement, needs to be optimized for each specific use case, especially for those use cases where security becomes critical (e.g., V2X platooning, enterprise VPNs and electric grids).

When operators of the 5G system aim to provide network slices to their customers (slicing tenants), the following (non-exhaustive) list of security requirements should be satisfied by the 5G system:

- It should allow the operator to authorize a third party to create, modify, and delete network slices.
- It should provide suitable means to allow an authorized third party to create and modify its network slices and apply its own security policies, for example, in terms of user data privacy, slices isolation, or enhanced logging.
- It should provide suitable means to allow the use of a trusted-third-party-provided encryption mechanism for data exchanged between any UE served by a private slice and a CN entity in that private slice.
- It should provide suitable means to allow the use of a trusted-third-party-provided integrity protection mechanism for data exchanged between any UE served by a private slice and a CN entity in that private slice.

Note: The previously mentioned encryption and integrity protection mechanisms assume that both the third party and the UE have been authenticated and authorized before accessing services of the 5G system.

- It should support a mechanism for the operator to authenticate and authorize UEs for access to both a hosted non-public network and private slice(s) of the operator associated with the hosted non-public network [12].

Isolation is a key principle and security requirement in network slicing. A network slice could be fully or partially, logically and/or physically isolated from another network slice(s). Different types of isolation may be implemented in network slicing; for example, network slices may be physically separated by being implemented in different racks, different locations, or different hardware, and/or logically separated via virtual machine (VM) isolation or cluster isolation in the case of virtualized cloud infrastructures.

Standards bodies and industry fora are currently working on network slicing security requirements and appropriate mechanisms, and maintain relationships across them. This landscape is pictured in [13].

Security Threats on Network Slicing

With network slicing, the threat surface of the network is extended due to the introduction of new business models, deployment options, interfaces, and functional blocks, especially when the isolation framework is not well designed and isolation policies are not effectively enforced. Because of that, the overall trust model of a 5G network may be indeed impacted in several circumstances:

- Lack of isolation
  - –When delivering slices with diverse security requirements to different customers by the same operator infrastructure, a compromised low-level security slice may impact a critical highly sensitive slice.
- Multi-tenancy support
  - –Exposing network slices as a service to multiple tenants, allowing them to manage and analyze the performance of those network slices.
  - –Allowing tenants to bring self-developed and managed network functions to build network slices.
- Connectivity of network slices to other external networks
  - –Allowing network slices provided by the operator to connect to tenants' own (private) networks.
  - –Supporting an E2E network slice across multiple operators, or across operators and other service providers.
- And so on.

Some key security threats on network slices are listed and grouped here:

- Theft of services and/or resources
  - –During UE registration or protocol data unit (PDU) session establishment procedures, a malicious network function (NF) that belongs to one slice may get an access token from an NRF for another slice and gain access to unauthorized information and services [4].
- Attacks on slicing-specific procedures, such as the slice selection during UE registration and PDU session establishment, and/or the slicing-specific authentication and authorization.
- Leakage of sensitive information
  - –Information of the NSC (e.g., end users) or the NSP (e.g., operator) in signaling procedures, for example:
    - · If an application function (AF), connected to

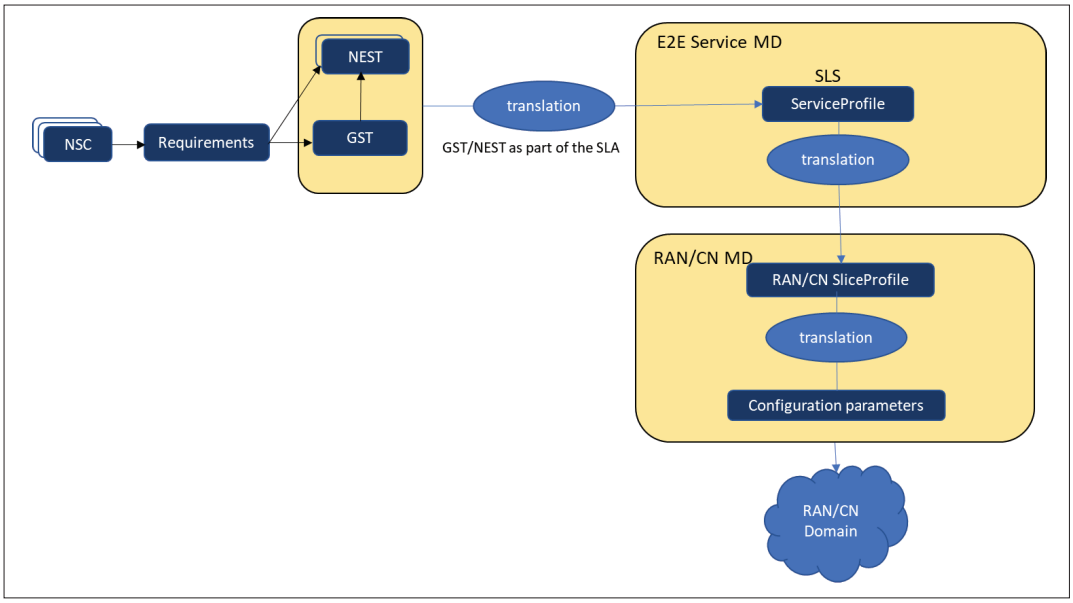

FIGURE 3. SLA requirements translation.

the 5G system, is neither authenticated nor authorized before accessing the network slice information, a malicious AF could collect such sensitive information for other purposes.

· If S-NSSAI is sent in cleartext during the radio resource control (RRC) connection establishment procedure, or in the initial NAS message without security context.

· If NSSAI information is transmitted in the clear.

–Leakage of sensitive information during network-slice-specific access authentication and authorization (NSSAA).

–Leakage of sensitive information of NSCs and/or NSPs through slicing management and/or network function services.

- Denial of service (DoS) attacks on slices
  –When resources are shared by multiple slices, those allocated for one slice may be exhausted by other slices, which could cause a DoS attack, especially under a resource starvation situation.
- Attacks on network-slice-specific functions (e.g., spoofing, DoS, tampering, misconfiguration), such as the network slice selection function (NSSF), the network-slice-specific authentication and authorization function (NSSAAF), or the network slice admission control function (NSACF).
  –For example, faked or spoofing network elements are part of intra and/or internetwork slice communications, causing malicious messages to be routed within a slice or between different slices.
- Compromised operational procedures, for example, tampering with the configuration of the slices on network functions, and tampering with network slice management data (e.g., fault/performance/configuration/accounting/security data).

Security Mechanisms to Protect Network Slices

Several reports and specifications in standardization bodies and industry organizations have defined security mechanisms to protect the confidentiality, integrity, and availability of network slices. This article has grouped them in two main categories:

- Management plane related security mechanisms
- Signaling (control) plane and user plane related security mechanisms

The list of key issues to be addressed by the management plane related security mechanisms are the following:

- Lack of isolation at the management level in multi-tenant network slicing scenarios, where resources (network functions and management) are required to be physically and/or logically isolated and assigned per tenant
- Authentication and authorization procedures on network slice management interfaces
- The potential need (as per customer slice-specific requirements) of provisioning slice-specific authentication and authorization mechanisms
- The potential need (as per customer slice-specific requirements) of provisioning slice specific security service chains

The list of key issues to be addressed by the signaling (control) plane and user plane related security mechanisms are the following:

- Potential leakage of slicing-related sensitive information of both operator and subscriber
- Authentication and authorization of the UE to access the network slice
- Lack of isolation implemented in control and user planes of network slices
- DoS attack, especially when resource is shared between slices and under a resource starvation situation

Security Mechanisms in Management Plane

Isolation Management of Network Slices: The resources of network slices allocated to a certain tenant can be isolated from resources used in other network slices. Further, the network slices of a tenant may be assigned to a so-called isolation group (IG). Network slices in an IG can share resources with each other, and typically have the same isolation policies. The resources of a network slice include managed resources (network

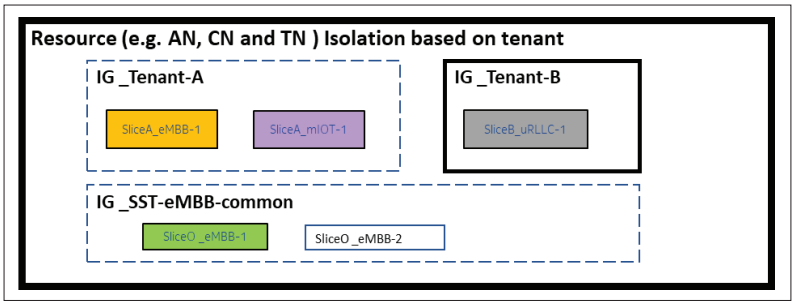

FIGURE 4. Isolated deployment of network slices of two customers.

functions, radio resources, transport network, etc.) and management resources (management data, management functions, etc.).

A practical example of an isolated deployment is shown in Fig. 4. An eMBB slice (SliceA_eMBB-1) and an mIoT slice (SliceA_mIOT-1) of tenant A are assigned to the same IG (i.e., no isolation is required between them). Slices of tenant A are required to be logically isolated from other slices. Another URLLC slice of tenant B (SliceB_uRLLC-1) is physically (solid line square) and logically isolated from other slices. Finally, two eMBB slices of the operator (SliceO_eMBB-1 and SliceO_eMBB-2) share resources, but they are logically isolated from other slices.

Enhancing the 5G NRM of 3GPP-specified architecture to support network slice IGs and isolation policies, as well as solutions to isolate the management data in its collection, storage, transmission, and use, have been studied in 3GPP TR 28.811, and are currently under discussion for their adoption in normative specifications.

Other isolation aspects are currently under study in standardization organizations and industry associations, such as how to isolate the RAN, CN, and TN resources during deployment, or how to enforce isolation policies during runtime (e.g., when the network slice is in service).

Access Control on Network Slice Management Interface: Service-based architecture of the 3GPP management system enables a management service (MnS) consumer to access and utilize capabilities of an MnS producer to provision and/or monitor: logical networks (e.g., network slices), services (e.g., network slice as a service [NSaaS]), or resources (e.g., network functions allocated to the consumer). The 3GPP management system is built on several MDs: E2E service/slice domain, RAN domain, and CN domain. There may be interactions between external entities and the 3GPP management system, between management functions (MnFs) of different MDs , or between MnFs in the same MD.

According to [8], the 3GPP management system provides capabilities of provisioning and supervising network slice and network slice subnet via MnSs. Without proper access control, a tenant of one slice may deliberately or indeliberately damage a slice of other tenants, or steal sensitive information of slices of other tenants, hence breaking the isolation principle for the slices. A benign administrator of the operator may also unintentionally delete a network slice by misoperation, causing unavailability of the slice. Therefore, access control on MnSs to support network slice management is essential to protect confidentiality, integrity, and availability of a slice, as well as to ensure isolation between slices.

Access control in the 3GPP management system represents the set of features and procedures that allow controlling how MnS consumers and MnS producers communicate and interact with each other, hence protecting the 3GPP management system, managed services, and resources from unauthorized access. Access control mechanisms can determine the level of authorization of a consumer after an authentication procedure has been successfully completed. In addition, they can track the access activities of a consumer to enforce accountability for the consumer's actions.

Authentication and authorization services are provided by the 3GPP service-based management framework for access control on 3GPP management services (e.g., create, read, update, and delete network slices/ network slice subnets/ network functions). The MnS consumer interacts with the authentication service producer for identification and authentication. After being authenticated, the MnS consumer calls the authorization service for permissions to access management services provided by the 3GPP management system. After successfully validating the permission of the MnS consumer, the MnS producer provides the requested MnS to the MnS consumer.

The management services provided by the 3GPP management system include provisioning service, performance service, alarm service, management data analytics service (MDAS), as well as authentication and authorization service, and so on.

See the details of authentication and authorization service definitions, as well as authentication and authorization workflow in [9].

With access control features provided by the 3GPP management system, the network slice consumer is granted corresponding permissions based on SLA and operator policies, and will be authenticated and authorized before accessing the slice-related management services. In this way, the NSC can only consume authorized services and resources of limited slices; hence, isolation and CIA of slices can be ensured.

Provisioning of Network-Slice-Specific Authentication and Authorization: Network slice-specific authentication and authorization (NSSAA) requires the access of the UE to the network slice to be authorized and authenticated by an authentication, authorization, and accounting server (AAA-S). It uses specific credentials, which are different from the ones used for UE primary authentication. The access and mobility function (AMF) performs the role of EAP authenticator and communicates with the AAA-S via the network-slice-specific authentication and authorization function (NSSAAF). The NSSAAF undertakes any AAA protocol (e.g., Radius, Diameter) interworking with the one(s) supported by the AAA-S. To support the NSSAA feature, the operator may configure the following information as possible enhancement to the NRM [14]:

- NSSAA related requirements added to the service and slice profiles in the CN
- NSSAA related parameters added to the AMF function information object class (IOC)
- New IOC added to support AAA-P, AAA-S, and NSSAAF

Note: The first enhancement has been implemented in the latest NRM specification [11]. The potential changes to core NFs as described in the second and third bullets are for further study in standardization.

Provisioning of Security Service Chains: Providing secure inter-network slice and intra-network slice communication, and securing the access to DNs (e.g., Internet) are fundamental requirements from mobile network operators and industry verticals (e.g. critical infrastructure providers).

DN access attributes describe how the network slice identified by an S-NSSAI should handle the user data toward that network determined by the data network name (DNN). There are several possible connectivity scenarios to DNs requiring access to the Internet, specific operator-hosted DNs for value-add services, secure tunneling to private networks, and so on. Deploying specific security functions (e.g., firewalls) at the CN edge (N6 interface) could protect the network slice from attacks coming from outside the network slice perimeter. Other security features can be part of a hypothetical security service chain in N6, including application content filtering, DDoS protection, high-performance carrier grade NAT, and so on.

For example, 5G NRM may be enhanced to support the proposed network slice protection on the N6 interface by:

- Adding an N6 interface protection requirement in the service profile, and a slice subnet profile for the CN with a list of security features required by the slice (or the slice subnet) consumer (e.g., antimalware, NAT, DDoS protection function, parental control)
- Network policies implemented in the policy control function (PCF) or session management function (SMF) are enhanced to support the routing of traffic to the new security functions on the N6 interface

See [14] for more details.

Note: The first enhancement has been implemented in the latest NRM specification [11]. The potential changes on PCF/SMF as described in the second bullet are for further study in standardization.

Security Mechanisms in the Control and User Planes

Protection of NSSAI Information During the UE Registration Procedure: The UE is not supposed to send slice specific information before the non-access stratum (NAS) security context has been established; thus, NSSAI information is not included in the registration request if the security context has not been established yet. The NSSAI information will be included in the NAS security mode complete message, which is conveyed by RRC message uplink information transfer. Therefore, NSSAI information is protected to avoid leakage of slicing-related sensitive information of both operator and subscriber.

UE Authentication and Authorization for Network Slice Access: Authorization for network slice access and NSSAA from a serving public land mobile network (PLMN) is required for a UE to gain access to a network slice. An authorized network slice can be granted to a UE only after the UE has completed a successful primary authentication. At the finalization of the primary authentication, the AMF and UE receive a list of allowed S-NSSAIs that the UE is authorized to access based on their subscription data. For certain S-NSSAIs, additional NSSAA is required.

NSSAA requires that the UE primary authentication and authorization of the subscription permanent identifier (SUPI) has been successfully completed. If the SUPI authorization is revoked, the network slice-specific authorization is also revoked. Figure 5 shows the nodes involved during primary authentication and network-slice-specific authentication.

A network-slice-specific AAA server may challenge the authentication and authorization of a UE at any time, and indeed, it may revoke the authorization of a UE. When authorization is revoked for an S-NSSAI that maps to an S-NSSAI in the current allowed NSSAI for an access type, the AMF shall provide a new allowed NSSAI to the UE and trigger the release of all PDU sessions associated with that S-NSSAI for this access type.

Network Slice Isolation Implemented in Signaling and User Planes: The following measures can be applied to support network slice isolation in signaling and user planes:

- Restriction of simultaneous registrations of network slices during UE registration procedure
- S-NSSAI-aware access control on NF services of the 5G Core
- Routing of signaling/control messages to corresponding NF/NF service according to S-NSSAI
- Selection of UPF based on S-NSSAI during PDU session establishment procedure, and routing of user plane messages to corresponding UPF allocated for the network slice

Admission Control and DoS Protection of Network Resources: RRM policies are defined in the 5G radio network for slice volume control in the gNB; these include the admission control and the scheduler on radio resources such as physical resource block (PRB), data radio bearer (DRB), radio resource control (RRC) connected users, and so on. Certain quotas (min, max, dedicated) per slice/slice group are defined:

- The quota rRMPolicyMaxRatio defines the maximum resource usage quota for the associated network slice(s), including at least one of shared resources, prioritized resources, and dedicated resources.
- The quota rRMPolicyMinRatio defines the minimum resource usage quota for the associated network slice(s), including at least one of prioritized resources and dedicated resources, that is, the resources quota that needs to be guaranteed for use of the associated network slice(s).
- The quota rRMPolicyDedicatedRatio defines the dedicated resource usage quota for the network slice(s), including dedicated resources.

The following are the definitions for the above-mentioned three resource categories.

Shared Resources: the resources that are shared with other network slices. The shared resources are not guaranteed for use of the associated network slice(s).

Prioritized Resources: the resources preferentially used by the associated network slice(s). These resources are guaranteed for use of the associated network slice(s) as needed. When not used, these resources may be used by other network slices.

Dedicated Resources: the resources dedicated for use of the associated network slice(s). These resources cannot be shared even if the associated network slice(s) do(es) not use them.

With enforcement of the RRM Policies, DoS attacks on RANs can be prevented to some extent. For example, the flood of access requests

Deploying specific security functions (e.g., firewalls) at the CN edge (N6 interface) could protect the network slice from attacks coming from outside the network slice perimeter. Other security features can be part of a hypothetical security service chain in N6, including application content filtering, DDoS protection, high-performance carrier grade NAT, and so on.

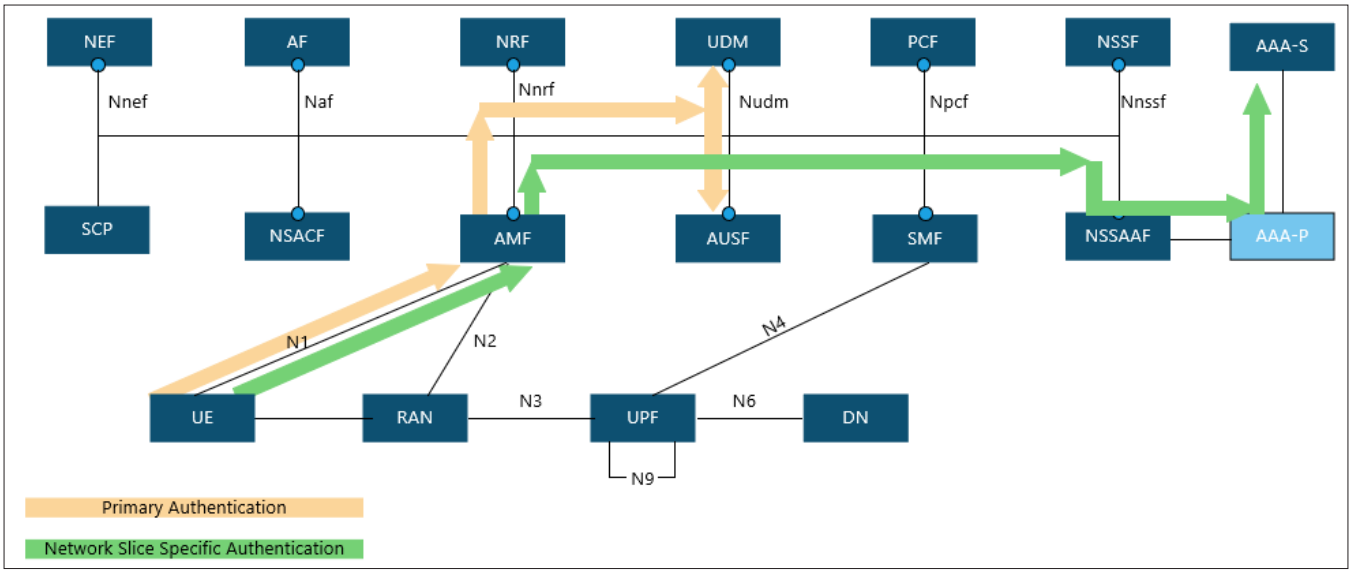

FIGURE 5. Nodes involved during primary authentication and network-slice-specific authentication.

on one network slice will not impact the availability of other network slices, avoiding damage to the network as a whole target. Also, the low capacity/priority slice will not "starve to death" as it can use shared resources in free time.

NSACF also enables the DoS prevention from the E2E network slice perspective. NASCF was introduced in Release 17 to monitor and control the number of registered UEs per network slice and/or the number of PDU sessions per network slice. NSACF is then configured with the maximum number of UEs and/or the maximum number of PDU sessions allowed to be served per S-NSSAI.

NSACF keeps track of the current number of UEs registered for a network slice to ensure that the maximum number of UEs allowed to register with that network slice is not exceeded. NSACF also maintains a list of UE IDs registered with a network slice that is subject to NSAC.

Similarly, NSACF keeps track of the current number of PDU sessions per network slice so that it can ensure it does not exceed the maximum number of PDU sessions allowed to be served by the network slice.

The admission control feature on network slices makes the 5G network more resilient to DoS attacks. Please refer to [7, Fig. 6] for further explanation on admission control and the radio resource scheduler, including impact on quotas.

DoS Protection of UEs: According to the specified AMF re-allocation procedure described in TS 23.502 [11], when an initial AMF receives a UE registration request with network slices, it may need to reroute the registration request to another target AMF, for example, because it does not support some network slices in the Requested NSSAI of the registration request. In that case, the NAS message received from the UE is rerouted to another target AMF either directly over the AMF-to-AMF interface (e.g., N14) or via the RAN.

However, if the initial AMF and UE have established security context but the security context cannot be forwarded to the target AMF via the RAN due to lower trust level of the RAN, the target AMF cannot protect the subsequent NAS message to UE, which will cause UE to reject the NAS message and registration failure. The scenario is shown in Fig. 6.

The UE may try again but may fail again. This constant registration failure threatens the availability of the system.

So far, the solution to transfer security context securely and correctly from initial AMF to target AMF via RAN has not been concluded. Including the requested NSSAI in a secured initial registration message could be one option to solve the problem radically. With requested NSSAI in the NAS initial registration request conveyed by an RRC setup complete message, gNB could direct the registration request to the correct AMF without trigger AMF reallocation, so the aforementioned condition to trigger a UE DoS attack is eliminated.

Gap Analysis and Next Steps for Further Study

Security controls for network slicing have been studied and specified in 3GPP, GSMA, and ETSI ZSM, among other standardization and industry organizations, aiming to mitigate the security threats and risks of network slicing and fulfill the security requirements. Nevertheless, there are still some key issues that have not been addressed in detail so far, at least from the standardization viewpoint, and these will require, in the opinion of the authors of this article, further investigation. Those are, among others:

- Detailed solutions for network slice isolation (inter- and intra-slice) in E2E service, access network, core network, transport network domains, and underlay infrastructure. For example, what isolation requirements and attributes should be added in NRM to enable network slice consumer and producer to isolation management and managed resources for the slice? Which network function should be enhanced to support slice isolation in signaling and user plane? What mechanism could be enforced to avoid data of one slice be accessed by another slice? These are among other isolation issues.
- Security for slices across multiple operators, or across operator and vertical service provider, tenant management, and network slice expo-

sure; for example, how to identify and manage a tenant of a slice in the 3GPP system, how to assign the permissions to a tenant to access the services related to a network slice, and so on.
- Security SLA monitoring and closed-loop security SLA assurance. Example issues are how do we define security SLA for a slice, and what enhancement should be included in NRM? Which measurements need to be collected to evaluate the potential security risk on the slice, and what mitigation plan would be triggered and how?
- Differentiate keys/algorithms for different slices (e.g. instead of using the same key to protect user plane data of all slices of a UE, generating a slice-specific key for each slice and using different security algorithm for integrity and confidentiality protection for different slices of a UE).
- Slice data protection in NWDAF and DCCF.
- Security as a service.
- Protection of slice-related data or report generated by service management and orchestrator or radio intelligence control (RIC) in O-RAN standardized networks.
- Device slicing security (the role of OS mediating between client application and PDU session, and enforcing URSP matching logic).

Conclusion

Network slicing is critical for 5G and upcoming 6G mobile network industry development, as per the connection of the telco infrastructure and services with other vertical sectors, including critical infrastructures. Isolation is a critical factor of the success of network slicing that needs to be investigated further. The allocation and protection of network slices based on security SLAs of operators with industry vertical customers, and the exposure of the network slice capabilities to them, will be a key enabler to commercially deploy and deliver network slicing.

This article compiles the most significant current security challenges, requirements, and solutions described and specified in standards (especially focused on 3GPP) and industry-related organizations (GSMA). It addresses security aspects for end-to-end network slices across access, transport, and core networks, and across management, signaling, and user planes.

The 5G industry, through various standards organizations, is making significant progress in specifying the security mechanisms for network slicing. Those mechanisms are required to provide an acceptable level of security and trust to operators and enterprises. 5G-Advanced and further 6G should continue the work on identified aspects in the present article, such as slice isolation, specific slice trust models, or security SLA assurance, aiming to achieve the trust level demanded by the industry.

References

[1] 3GPP TS 33.501, "Security Architecture and Procedures for 5G System V17.7.0."
[2] GSMA Association NG.127, "E2E Network Slice Architecture version 1.0."
[3] GSMA Association NG.116, "Generic Network Slice Template version 5.0."
[4] GSMA CVD-2021 0047; https://www.gsma.com/security/gsma-mobile-security-research-Acknowledgments/.
[5] ETSI GS ZSM 003, "End-to-End Management and Orchestration of Network Slice V1.1.1."

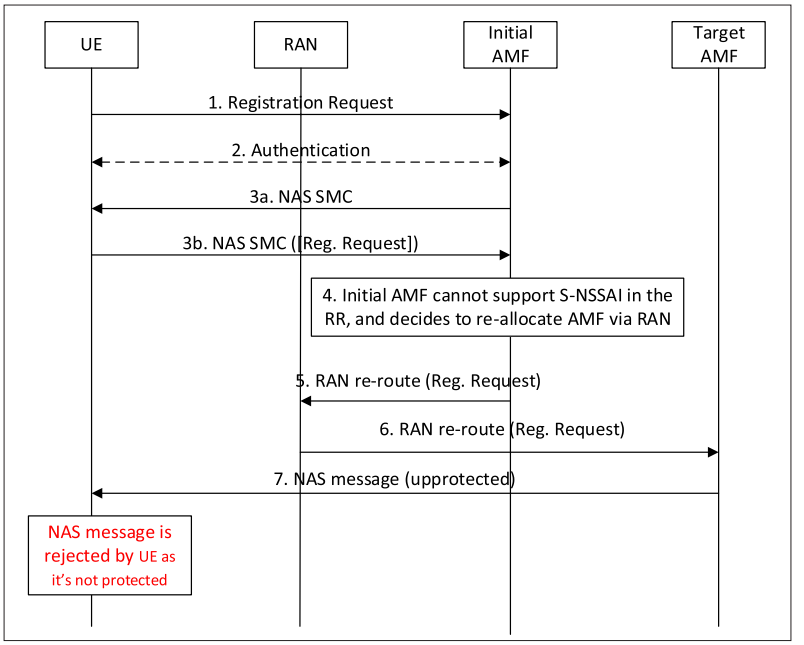

Figure 6. AMF reallocation procedure.

[6] 3GPP TS 23.501: "System Architecture for the 5G System (5GS) V17.6.0."
[7] J. Ordonez-Lucena *et al.*, "On the Rollout of Network Slicing in Carrier Networks: A Technology Radar," *Sensors*, vol. 21, no. 23, Dec. 2021, p. 8094; http://dx.doi.org/10.3390/s21238094. DOI: 10.3390/s21238094.
[8] 3GPP TS 28.530, "Management and Orchestration;Concepts,Use Cases and Requirements V17.3.0."
[9] 3GPP TS 28.533, "Management and Orchestration; Architecture Framework V17.2.0."
[10] 3GPP TS 23.003, "Numbering, Addressing and Identification V17.7.0."
[11] 3GPP TS 28.541, "5G Network Resource Model (NRM); Stage 2 and Stage 3 V18.1.2."
[12] 3GPP TS 22.261, "Service Requirements for the 5G System; Stage 1 V19.0.0."
[13] J. A. Ordonez Lucena, *Management and Orchestration of Network Slicing in Public-Private 5G Networks*, doctoral thesis; https://digibug.ugr.es/bitstream/handle/10481/77685/79489%281%29.pdf?sequence=4&isAllowed=y.
[14] 3GPP TR 28.811: "Network Slice Management Enhancement V17.0.0."

Biographies

Ranganathan Mavureddi Dhanasekaran obtained his B.E degree in electronics and communication engineering from the University of Madras in 2004. He works as a senior research engineer for the Nokia Standards organization. In this role as a researcher, he contributes to security standardization research activities related to international SDOs such as 3GPP SA3. He possesses 17 years of experience in the telecommunications industry, having been involved in multiple projects for operator networks and for user equipment modems. He has worked in India and Germany, and since 2010 he has been based on Germany.

Jing Ping is a senior standardization specialist at Nokia, China, as delegate of to 3GPP and ETSI ZSM. She is currently involved in standardization and research activities spanning different areas such as network security, network and security management, and automation. She received her computer science Bachelor's degree from the University of Electronic Science and Technology of China. She has been working as a product manager, system and software architect, and software engineer in the mobile core network, network management, cloud and security management domains.

German Peinado Gomez holds an M.Sc. degree in telecommunications from Universidad Politecnica de Madrid, a Master's degree in information security from Universidad Pontificia de Salamanca, and is a Ph.D. candidate at Warsaw University of Technology. He also holds security industry certifications including CISSP, CCSP, CISM, and ISO/IEC 27001 Lead Auditor. He is a senior telecommunications and security professional with 20+ years of experience, having assumed different roles and responsibilities in the telco industry including product manager, consultant, security manager, and others. Currently, he works as a security standardization specialist at Nokia, acting as a Head of Delegation in 3GPP SA3.