ESF Potential Threats to 5G Network Slicing

Disclaimer

This document was written for general informational purposes only. It is intended to apply to a variety of factual circumstances and industry stakeholders. The guidance in this document is provided "as is" based on knowledge and recommended practices in existence at the time of publication. Readers should confer with their respective network administrators and information security personnel to obtain advice applicable to their individual circumstances. In no event shall the United States Government be liable for any damages arising in any way out of the use of or reliance on this guidance.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes. All trademarks are the property of their respective owners

Purpose

The National Security Agency (NSA) and The Cybersecurity and Infrastructure Security Agency (CISA) developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / Inquiries: Enduring Security Framework nsaesf@cyber.nsa.gov

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov

Table of Contents

Executive Summary

Building upon the work published in the Enduring Security Framework's *Potential Threat Vectors to 5G Infrastructure,* the Enduring Security Framework[1] (ESF) established a working panel comprised of government and industry experts and conducted an in-depth review of network slicing, a key component of 5G infrastructure. This working panel assessed the security, risks, benefits, design, deployment, operations, and maintenance of a network slice. For this paper, a network slice is defined as an end-to-end logical network that provides specific network capabilities and characteristics for a user.

As with any emerging technology, with increased benefits come increased risks. This paper intends to introduce 5G stakeholders to the benefits associated with network slicing and introduce perceived risks and management strategies that may address those risks.

[1] The ESF is a cross-sector working group that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. national security systems. It is comprised of experts from the U.S. government as well as representatives from the Information Technology, Communications, and the Defense Industrial Base sectors. The ESF is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges.

Network Slicing Overview

Definition

A network slice is an end-to-end logical network that provides specific network capabilities and characteristics to fit a user's needs. Although multiple network slices run on a single physical network, network slice users are authenticated for only one network area, enabling data and security isolation.

Deploying a Network Slice

A network slice spans multiple connected components that form a network. These components include physical computing, storage, and networking infrastructure; with network slicing, they are virtualized, and protocols are in place to create specific network slices for specific users or applications. It is important to note that network slicing components can span multiple operators, so interoperability, security, and robustness become important challenges to address. From a security standpoint, the resources of one network slice should be isolated from other network slices to ensure confidentiality, integrity, and availability.

For example, vehicles in an autonomous fleet can be on different network slices even though they are providing similar services. Graphics-intensive applications like Virtual Reality or Augmented Reality could have a network slice separating them from other applications. Different network slices can also be provisioned for a customer within the same enterprise location that separates different user groups based on their roles.

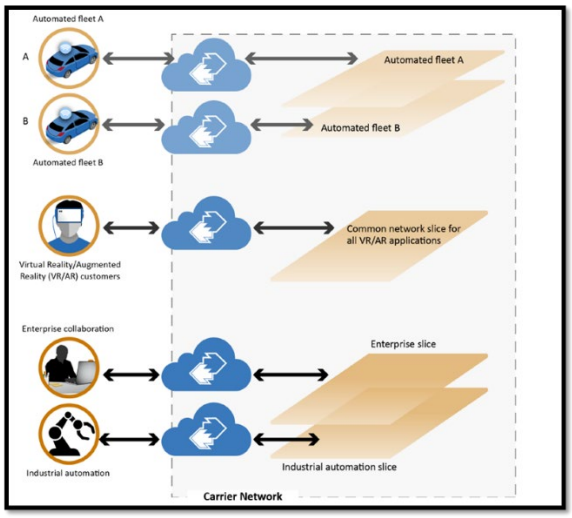

Figure 1 Possible uses for a network slice[2]

[2] U.S. Government Accountability Office. https://www.gao.gov/assets/gao-21-26sp.pdf

This type of architecture heavily relies on a Network-as-a-Service (NaaS) model, combining Infrastructure-as-a-Service with network and security services, which enhances the operational efficiency and resiliency of the 5G infrastructure. Within a 5G architecture, the plan is to deliver the whole NaaS so that different customer segments can be efficiently supported. The 5G network is re-designed based on a service-oriented architecture by breaking everything down into detailed functions and sub-functions.

- Access and Mobility Management Function (AMF) offers registration, reachability, Session Management Function (SMF) to handle session establishment and session management responsibilities.
- Packet routing and forwarding functions are now realized as services rendered through a new network function called the User Plane Function (UPF), and is achieved with technologies such as Software Defined Network (SDN) and 5G Network Function Virtualization (NFV).

In order to design, deploy, manage, and operate a mobile network with the functions previously mentioned, mobile network operators must use a Management and Network Orchestration (MANO) system. MANO systems allow for a mobile network operator to create end-to-end network slices and operate them over their entire lifecycle as they are ordered by a customer. Below is an example of a MANO system that can create, manage, and operate a network slice end-to-end. The MANO system shown supports slice design and creation, activation, deactivation, and termination across the Radio Access Network (RAN), core network, and transport network domains.

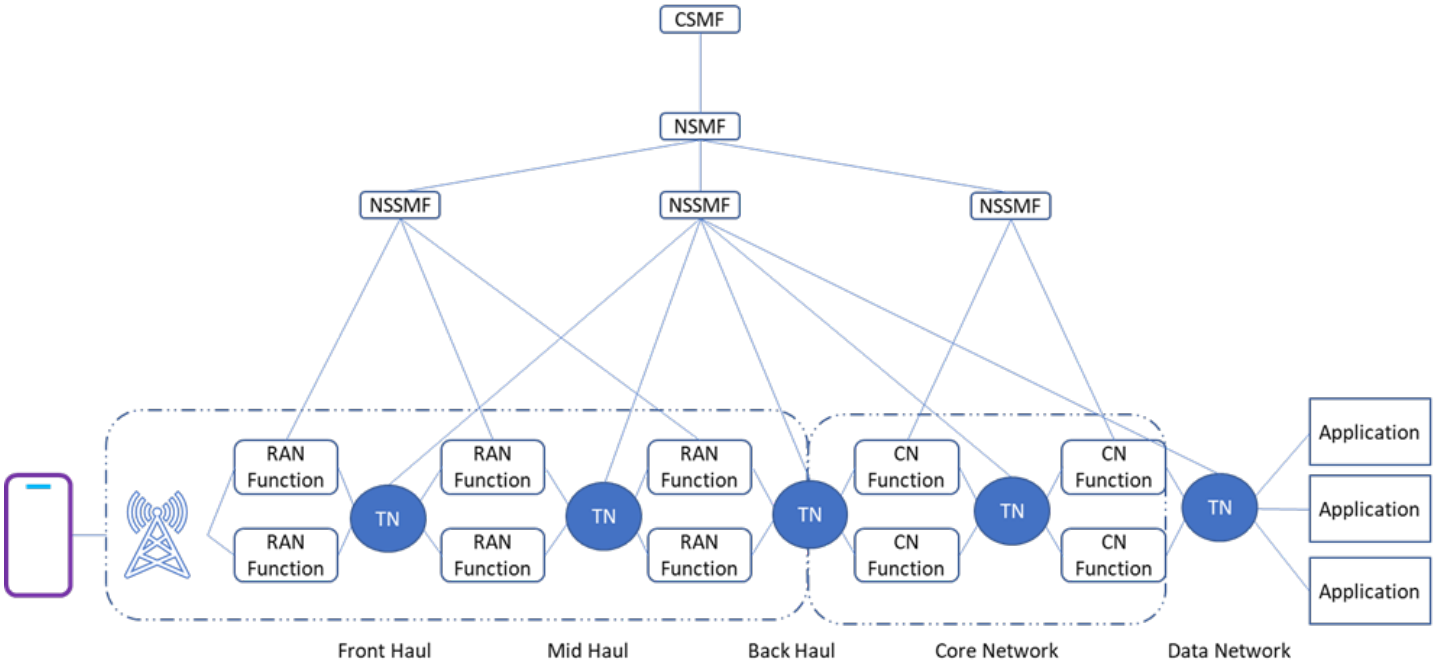

Figure 2 Architecture Diagram for End-to-End Network Slicing

Network Function Virtualization

Network Function Virtualization (NFV) is a core 5G architecture that is fundamental to network slicing. NFV enables the following attributes:

- Eliminates the need for purpose-built hardware and allows carriers to move network functions, such as routers and firewalls, to cloud-based servers.
- Moves network functions nearer to the radio interface or out into the cloud, which enables a flexible and elastic network that is more capable of meeting the demands of network traffic in real time.
- Optimizes performance of multiple applications, even those that require different levels of bandwidth, latency, availability, and security.
- Increases monitoring and logging options; enhancing the visibility into the system and the ability to detect anomalies or prevent vulnerability exploitations.

Network Slicing Threat Vectors

The ESF previously identified potential threat vectors to 5G infrastructure spanning policy and standards, supply chain, and system architecture, as reported in *Potential Threat Vectors to 5G Infrastructure.* Although all are important, for the purposes of assessing threats to network slicing, the primary concern is systems architecture. Within 5G systems architecture, as ascertained by ESF, the following sub-threats were identified.

- Software Configuration
- Network Security
- Network Slicing
- Legacy Communications Infrastructure
- Multi-Access Edge Computing
- Spectrum Sharing
- Software Defined Networking

In *Potential Threat Vectors to 5G Infrastructure,* the threat presented by an improperly developed and implemented network slice is described as:

> *Network Slicing allows users to be authenticated for only one network area, enabling data and security isolation. However, network slicing can be difficult to manage, and the slices add complexity to the network. While there are standards defining specifications for how network operators build their 5G network, there are not clear specifications for how network operators should develop and implement security for network slicing. Improper network slice management may allow malicious actors to access data from different network slices or deny access to prioritized users.*

Further analysis of the relationship between general 5G threat vectors and a network slicing threat, as defined above, was used to develop a high, medium, and low relativity assessment. This information is reflected in Table 1.

Threat Vectors	Descriptions	Network Slicing Relativity
DoS attack on signaling plane	DoS on centralized control elements	H
Hijacking attacks	Attacks on SDN hypervisor controller	L
Unauthorized access	Unauthorized access through low-power access points	L
Configuration attacks	Attacks that take advantage of misconfigured system controls	H
Saturation attacks	Ping-pong behavior in access points and MME due to service saturation	M
Penetration attacks	Malware attack that exposes subscriber info	M
User identity theft	Breaking into user information databases and stealing user credentials	M
Man-in-the-Middle attack	Accessing unencrypted channels or network links and acting as a relay in communications between 2 parties	H
TCP Level attacks	TCP Session or SYN Flooding in gateways, routers	M
Key exposure	Compromise of the authentication and key agreement	L
Session replay attack	Session keys in a non-3GPP access	M
IP spoofing	Control channels	M
Scanning attacks	Radio interface interference	L
IMSI caching attacks	Roaming and User Equipment (UE)	M
Jamming attacks	Wireless channels	L
Channel prediction attacks	Radio interfaces	L
Active eavesdropping	Control channel	L
Passive eavesdropping	Eavesdropping on control channel (i.e., inter-Virtual Network Function (VNF) data) can reveal slice configurations and users, and enable hijacking and other attacks	L
NAS signaling storms	Attack against UE traffic and signaling messages to core network	M
Traffic bursts by IoT	Saturation of GTP endpoints	M

Table 1 Potential 5G threat vectors

Among these threat vectors, three were assessed as having a high level of relativity to network slicing. These threats are denial of service (DoS), Man-in-the-Middle (MitM) attacks, and configuration attacks.

- Denial of Service Attacks
    - DoS attacks primarily impact the availability of a network slice, causing communication services to be severely compromised or unavailable under these types of attacks.
    - DoS attacks will likely target the signaling plane.
- Man-in-the-Middle Attacks
    - MitM attacks can have a broad range of adverse effects on the confidentiality, integrity, and availability of a network slice.
    - MitM attacks imply that the adversary relays and possibly alters the communications between two endpoints. Such an attack could be devastating, as misinformation and disinformation could result from the malicious actor modifying the contents of the messages.
    - Confidentiality can also be violated when information or data is intercepted and exposed to the malicious actor.
- Configuration Attacks
    - Configuration attacks have a broad range of adverse effects on the confidentiality, integrity, and availability of a network slice.
    - These attacks are when malicious actors exploit configured system controls.
    - They may also include security features that are inadvertently turned off or system monitoring services being disabled.

Although not identified in Table 1, Network Function Virtualization (NFV) is another aspect of network slicing that presents increased potential risks. These include but are not limited to:

- The additional microservices and functionalities required by NFV make integration and testing activities more difficult, resulting in new attack surfaces.
- In a virtualized architecture it will be more difficult to detect and recognize the types of traffic crossing these networks and mitigate against any new threats.
- Malicious actors may compromise a network slice by gaining access via the physical components from another slice due to a lack of isolation. This type of compromise may result in data spills.

Network Slicing Threat "In Real Life"

Network slicing will play a pivotal role in emerging technology such as autonomous vehicles. The slice is used to connect to and communicate with the autonomous vehicle which can present the opportunity for a malicious actor to conduct an International Mobile Subscriber Identity (IMSI) caching attack which degrades the performance, reliability, and robustness of the network services.

The actor can use IMSI caching to expose the autonomous vehicle's geolocation, as well as information about the cargo such as sender, destination, and traffic routes. From here, the actor can launch a DoS attack on the network signaling plane to cause disruptions between

the autonomous vehicle and its authorized controller. Assuming the malicious actor has access to the subscriber identity, the actor can also separately launch a configuration attack to tamper with the security features and virtual network function (VNF) policies.

This can compromise authentication and authorization policies, thereby granting illicit access to the network slice. This type of attack can afford the malicious actor an opportunity to expand unauthorized access to other network slices if the security between the slices is not adequate.

Management and Monitoring of a Network Slice

Due to the nature of the threats to network slicing, proper management and continuous monitoring are crucial to the security of a network slice. The management can be applied at four logical layers, as described in Table 2.

Logical Layer	Descriptions
Network Slice Subnet Management Function (NSSMF)	NSSMF decomposes slice subnet instances on its network into virtualized network functions (VNF) instances and related connections; access network (AN), transport network (TN) and core network (CN) have their respective NSSMFs to manage and orchestrate their slice subnets.
Network Slice Management Function (NSMF)	NSMF manages and orchestrates network slice instances and decomposes network slice requirements into network slice subnet requirements.
Communication Service Management Function (CSMF)	CSMF translates service requirements into specific requirements for network slicing, such as the number of users allowed, uplink and downlink transmission rates, latency, and jitter. It also manages service subscription and cancellation.
Capability Exposure Platform	This platform provides standard application programming interfaces and a self-management portal; it also connects to the CSMF, NSMF, business support system (BSS), operations support system (OSS), network exposure function (NEF), multi-access edge computing (MEC) and other such functions and nodes that integrate and orchestrate their network capabilities.

Table 2 Network Slicing Management Plane logical layers

From a network slicing management perspective, monitoring should be performed relative to these four logical layers. This is especially critical due to the dynamic and complex nature of 5G networks. These activities are also critical as a malicious actor attempts to disrupt, deny, or degrade a mobile network operator's 5G infrastructure.

In addition to proper network slice management, continual monitoring is crucial in detecting malicious activity. Mobile network monitoring and security tools often focus on network performance, fraud detection, revenue assurance, or device behavior that impacts network performance and not on detecting adversarial malicious activity. Table 2 lists typical mobile

network monitoring types, as well as recommended network monitoring types to consider when monitoring 5G network security.

Types of Network Monitoring	Explanation
Performance Management	Due to the complex nature of mobile networks and vendors diversity of hosting platforms, a unique overarching performance management technique across different networks and vendors is required.
Quality of Service (QoS)	5G QoS should include network performance metrics (e.g., latency, throughput, etc.) but might also include availability, reliability, accessibility, retainability, etc.
Security Controls	The Risk Management Framework (RMF) process is a cyclical process to ensure security controls and best practices are in place. NIST 1800-33B is an example of security controls for 5G cybersecurity.
Control plane Communication	Control plane communication is not only protected for privacy but also protected against a malicious actor's modifications, performance issues, and anomalous behaviors.
User-plane Communication	This is the communication that connects the actual data coming over the Radio Access Network (RAN) to the Internet, which is helpful to detect acceptable use violations.
Anomaly Detection	Anomaly detection is the capability of identifying unusual activities or behaviors in networks. A variety of sensors, filtering and advanced (e.g., AI/ML-based) security analytics are necessary to detect sophisticated and zero-day threats.

Table 3 Types of Network Monitoring for 5G Networks

Through 5G network monitoring, various types of data can be collected. The collected data can be analyzed and used to gain insight into authorized and unauthorized network activity. This data can then be used to build network analytics, network alerting, network visualization, and network reporting. Table 3 provides a description of these data processing activities.

Data Processing	Description
Analytics	Analytics is about finding patterns in disparate data sources, which requires the ability to collect, process and interpret data.
Alerting	Alerts make data useful. As data is a crucial aspect of network performance and security monitoring. Organization relies on accurate alert notifications so that appropriate resources can be applied to respond to potential system failures and malicious effects.
Visualization	A good dashboard environment should compose of easy-to-understand visualization tool for both technical and non-technical users. The dashboard should display highest-level information (which devices are at risk, aggregate reports, system health, etc.), but also provides the ability to drill down as appropriate.
Reporting	Monitoring performs multiple analyses and provides a reporting summary, for example system status, overview, and open summary.

Table 4 Data Processing in 5G Network Monitoring

Strategies for Network Slicing

As discussed in the previous sections, it is paramount to ensure confidentiality, integrity, and availability for 5G network slicing protection. In addition, more advanced mitigations might include Zero Trust Architecture (ZTA) requirements, Multi-Layer Security (MLS), Cross-Domain Solutions (CDS), Post-Quantum Cryptography (PQC), and Isolation.

Zero Trust Architecture

> *ZTA solutions verify the interactions of the principal user, as well as other inputs such as the trustworthiness of the device used by the principal or its location, against one or more models to detect deviating behavior*

ZTA is based on the principle of "never trust, always verify," which directly relates to the confidentiality and integrity of a given system. It focuses on eliminating implicit trust and continuously validating every stage of a digital interaction through strong authentication and authorization methods. If implemented appropriately, it can drastically reduce the possibility of attacks like MitM and configuration attacks in network slicing.

Upon detecting anomalous behavior, various actions can be triggered, including segregating and isolating the interactions, terminating access credentials, or initiating multi-factor authentication (MFA). The tenets of ZTA aim to reduce the exposure of resources to malicious actors by leveraging network segmentation. This can prevent incidents and minimize lateral movement.

Common ZTA techniques:

- MFA
- Encryption
- Access control

Multi-Layer Security

ZTA is also a prerequisite for enabling Multi-Layered Security (MLS). With the proper access control and authentication, MLS permits access to users with different levels of access while preventing users from obtaining access to information for which they lack authorization. MLS protects itself from subversion and has robust mechanisms to separate information domains based on trustworthiness.

Cross-Domain Solutions

Cross-Domain Solutions (CDS) is defined as a form of controlled interface, a boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems, that provides the ability to manually and/or automatically access and/or transfer information between different security domains[3]. CDS is intended for use in high-value networks where assurance-based security measures, such as firewalls, Security Information and Event Management, and Intrusion Detection Systems, are not sufficient to ensure the security of the trusted domain.

Post-Quantum Cryptography

Another way to further mitigate risks is the use of advanced encryption techniques. A future quantum computer, if built, would be capable of undermining the widely deployed public key algorithms currently used for asymmetric key exchanges and digital signatures. New quantum-safe solutions will eventually need to be adopted in critical infrastructure to mitigate this potential vulnerability. Post-quantum cryptography (PQC) algorithms are under evaluation and will be standardized for the relevant technologies, including 5G. PQC can be seen as a possible solution to enhance data protection when a higher level of security is required. 5G vendors and operators must incorporate updated standards to mitigate potential future risks, as they become available.

Isolation

Isolation is another cyber technique to enhance security in 5G network slicing. The level and strength of isolation may vary depending on slicing requirements and usage. In some network slicing instances, there may be a security requirement for strict slice isolation, but other slicing instances may require the need for communication between slices. Thus, isolation may be perceived in many ways, and it constitutes a set of properties chosen according to implementation needs. Isolation could be based on a sandbox, virtual machine, operating system, or hardware and physical. Some of the enabling technologies might include physical resource block scheduling, slice scheduling, and traffic shaping.

Conclusion

Although network slicing is not solely unique to 5G, it is a critical component because 5G specifications call for network slicing as a fundamental component and therefore require network operators to adopt security practices that can mitigate threats like those described in this paper, DoS, MitM attacks, and configuration attacks.

The monitoring and maintenance of a network slice are crucial to detecting and mitigating potential compromises and forming a basic level of defense. For more robust security, network operators should consider techniques, as referenced in this paper, such as zero trust, multi-layer security, cross-domain solutions, post-quantum cryptography, and isolation.

[3] NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/cross_domain_solution.