# A STRIDE Threat Model for 5G Core Slicing

Authors' Copy - Technical Report - May 31, 2021

Danish Sattar, Alireza Hosseini Vasoukolaei, Pat Crysdale, Ashraf Matrawy
*School of Information Technology*
*Carleton University*
{danish.sattar, alireza.hosseinivasoukolaei, pat.crysdale, ashraf.matrawy}@carleton.ca

***Abstract*—5G networks bring a new paradigm of cellular infrastructure and, therefore, a need to model new types of threats. One of the primary innovations of 5G networks compared to previous generations is the ability to create network slices. This allows network operators to offer a logical section of a network to a client that can be optimized to their individual needs, such as enhanced mobile broadband, massive machine-type communications, ultra-reliable, and low-latency communications. In this paper, we use the STRIDE threat modeling mythology to analyze risks associated with 5G slicing.**

***Index Terms*—5G Threat Model, Network Slicing, 5G Security, Authentication, Authorization**

## I. Introduction

The 5G core is a highly virtualized network that provides, among other things, three areas of improvement compared to previous generations of wireless networks: network slicing, a service-based architecture, and a split between the control & user planes [1]. In this paper, we focus solely on the advent of network slicing. This is the ability to allocate a virtual "slice" of the network to a client and optimize the features of the slice to the specific needs of the client without impact on other slices [1]. For example, a web streaming company may procure a network slice optimized to deliver fast 4k video to clients; however, a municipality may procure an independent slice on the same network optimized for real-time monitoring of police, fire, and ambulance equipment. The needs of these two clients are vastly different. It would be difficult for an earlier generation network to support both clients as it is only with the advent of 5G slicing that such use cases are realistic [1].

Microsoft has created a generalized attack-centric threat model for software developers called STRIDE. It serves as an acronym for 6 categories of threats to security goals Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [2]. This is an attack-centric model that views threats in terms of abstract attack types [2]. **Our main contribution** is a STRIDE threat model that is offered solely in the context of 5G core slicing. Note that the following types of threats are excluded from our model: physical security (e.g., bombings targeting 5G networks [3], vandalism, theft, sabotage), social engineering, bugs [4], natural disasters [5], and insider threats [6]. While we cite examples of these threats causing outages to networks, they are not exclusive to 5G core slicing. While they might be included in any broad organizational threat model, they are not part of our model. **This model is exclusively concerned with identifying threats to 5G slicing and support network infrastructure. Threats from previous generations will be included if they are specifically a threat to slicing.**

**Classifying Threats:** Most real-world attacks will take place using combined exploit/vulnerability pairs from each of the 6 categories. As an example, an attacker that successfully raises their privilege and masquerades as a system administrator on the network is a risk under two categories of STRIDE, Escalation of Privilege (EoP) and Spoofing; however, we would classify this threat as EoP and cite Spoofing as an associated risk. One successful attack can lead to others. Therefore, when considering a STRIDE model, one should consider each of the 6 categories as the first defense against exploits in the other 5 categories. For our model, each threat is categorized by the initial STRIDE category; however, we specify further categories of threats as risks should the threat be realized. We do not assert that our classifications of threats into categories are absolute or immutable. We assume that many groups of competent and qualified security researchers would organize these threats very differently than we chose to. Therefore, we place emphasis on the threats themselves and use the categories of STRIDE as a tool for organizing threats into a understandable format.

**Paper organization:** The rest of this paper is organized as follows: Section II discusses the life cycle of a network slice, Section III explores trust boundaries in network slicing, Section IV is our threat model organized into STRIDE categories, Section V is a discussion of best practices for mitigating threats and finally the paper is concluded in Section VI.

## II. Slice Life Cycle

In this section, we enumerate the 4 phases of the 5G slice life cycle as described by 3GPP in [7] and shown in Fig. 1. Attacks on slicing can take place during any phase of the life cycle. As such, it is important that the reader understands how slices are expected to function to better comprehend how they can be threatened.

1) Preparation: In the initial phase, the needs/priorities of the client are considered. Available hardware infrastructure on the network is procured to meet the individual needs of the client.

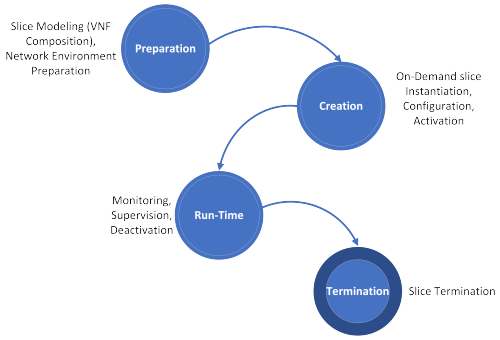


Fig. 1. Simplified Life cycle phases of a Network Slice Instance. Detailed description of the lifecyle can be found in [7]

2) Creation: A virtual network is created on the procured hardware. IP addresses are assigned, slice-specific security controls (defined by the client) are activated, databases are provisioned, all mechanisms necessary to support the needs of the client come online in this phase.
3) Run-time: The services that the client has requested/configured are online and accessible from User Equipment.
4) Termination: The client has shut down their slice, services stop, resources are returned to the available pool for a new slice to procure.

## III. Trust-Boundaries in Network Slicing: A Network Operator Perspective

One of the key advantages of 5G networking compared to previous generations is the ability to optimize and dynamically incorporate resources across many domains and service providers through network slicing [1] [8]. Although a single 5G slice could have some of its Network Functions (NFs) running on its own backbone and the rest on the others, from the Mobile Network Operation (MNO) orchestration standpoint, all the NFs are likely to be part of the same logical administrative domain. Of course, dynamic resource allocation across different providers raises an issue of privacy and confidentiality. It is imperative to define a trust boundary that if crossed, data is presumed to be at higher risk or even compromised [8]. We define trust as whether data rests or travels inside infrastructure controlled by its custodian. Should the data travel to infrastructure under the care of another custodian, it is considered to have traversed a trust boundary [9].

The literature classifies three types of trust boundaries in 5G core networks. Firstly asset providers including anything as a service (XaaS) providers. These providers offer aggregated infrastructure; although, it exists outside trust. Secondly, connectivity providers offer business and wholesale Internet connectivity or Mobile Virtual Network Operation (MVNO) which permit wireless networks to exist outside a trust domain. Lastly, partner service providers such as another 5G network provider offering to share their 5G infrastructure for mutual growth [9]. We assume that in any practical 5G implementation, data will cross at least one of these boundaries.

In Fig. 2, trust boundaries are illustrated for the 4 components of a network slice: radio, transport, core and compute. The boundaries in the figure represent the network (and hence slice) operator's perspective. Note that compute includes both cloud and edge computing nodes. The area in green represents a trusted area where data resides in the custody of its own custodian. The red area is untrusted where data is placed with another custodian. In some cases, an untrusted area exists within a trusted space. These are cases where data is in the custody of its own custodian; however, there is a risk that it might co-exist simultaneously elsewhere.

It is important to emphasize that Fig. 2, is applicable to both the logical domain of the 5G network and the physical allocation of resources across data centers, providers and all other assets involved in network operation. This is because data may exist in the logical administrative control of the MNO but that data can be stored on infrastructure controlled by a partner service provider [10]. In this example, the data would be considered to be untrusted.

## IV. 5G Network Slicing STRIDE Threat Model

In this section, we describe our 5G Slicing STRIDE model. The threats are grouped into subsections by category, and the full threat model is given in Fig. 3. For convenience, we also provide smaller threat models for each category at the start of each subsection in Figs. 4, 5, 6, 7, and 8. For each threat, we offer a description, risks, and mitigations. The description offers a summary of how the threat could be realized. For risks, we provide a list of other STRIDE categories and/or security issues that could subsequently arise if the threat is realized. For example, we classify Man-in-the-Middle attacks as Spoofing but list risks of Information Disclosure, Tampering, and Denial of Service. These are the types of consequences we expect if the attack is successful. Further, there are cases where a Man in the Middle attack could be best transparent and defined as "eavesdropping". Therefore, there's an argument to classify Man in the Middle under Information Disclosure as well as Spoofing. This is because MitM attacks can be passive or active. We chose to focus on active attacks. Therefore it is classified under spoofing; although, we discuss mitigations for both active and passive attacks. Finally, the list of mitigations are not exhaustive or guaranteed to prevent the attack but are based on best practices from the literature.

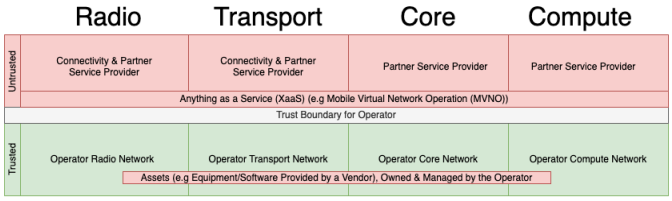


Fig. 2. Illustration of 5G Slicing Trust Boundaries for a Slice Operator

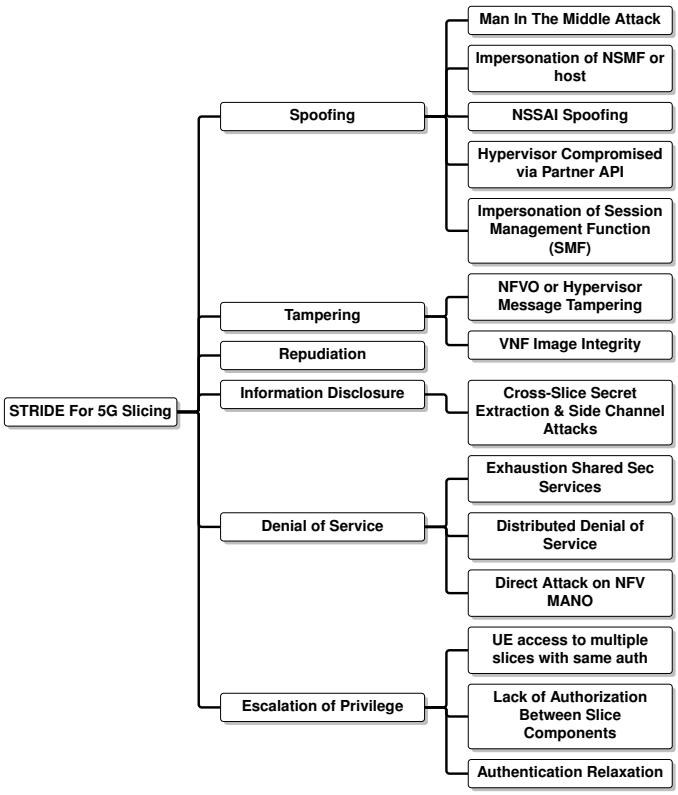


Fig. 3. STRIDE Threat Model

### A. *Spoofing*

Spoofing is a general description for any attack method that impersonates a legitimate user or process [11]. This creates a risk that seemingly legitimate traffic on a system could actually contain malicious traffic. In Fig. 4, we identify Spoofing threats for 5G core slices.

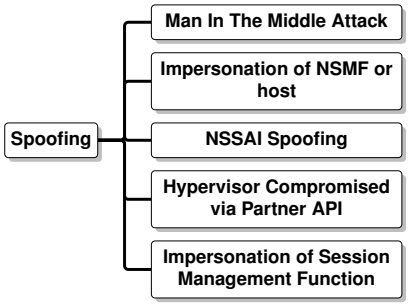


Fig. 4. Identified Spoofing Threats

1) Man-in-the-Middle (MitM) Attack [12]
   - Description: An MitM attack is when a rogue person, piece of equipment, or software is placed as a proxy between two or more authentic nodes and intercepts & repeats the traffic. Typically, both authentic nodes think they are communicating directly with the opposite node(s) [11] [13] [14]. 5G networks allow data to logically exist in trust; however, some nodes may be physically out of trust. A rogue node could be placed physically out of trust and exploit the logical trust of the network. For example, if an adversary places them-self between User Equipment (UE) and a network slice they could manipulate data coming to and from a slice [15]; although, this is only an example, a MitM attack can happen between any two network nodes (even two in trust). The other threats we identify under Spoofing are similar to MitM but discuss specific areas in network slicing where a rogue node could be catastrophic.
   - Risks: Information Disclosure, Tampering, and Denial of Service.
   - Mitigation: It is recommended to use mutual authentication [11] [13] [14]. This can be achieved using digital signatures and certificates [13] to allow each node to authenticate the other. 3GPP recommends using the Transport Layer Security (TLS) protocol, it provides an optional level of mutual authentication [11] known as Mutual TLS (mTLS) [16] to verify the identity of both communicating parties. We also recommend that integrity checking is enabled to ensure data arrives exactly as it was sent and that the data should be encrypted to prevent eavesdropping between two points on the network. If possible, all sensitive network functions should be both physically and logically in trust to minimize risk of compromise for such attacks.
2) Impersonation of Network Slice Management Function (NSMF) or Hypervisor [17]
   - Description: The NSMF is a critical component of 5G. It is the master of all 5G slices and dictates when/how/where a slice is instantiated. If an attacker successfully impersonated the NSMF, they would have control over every slice on the network [17].
   - Risks: Tampering, Repudiation, Information Disclosure, and Escalation of Privilege.
   - Mitigation: Same as MitM.
3) Network Slice Selection Assistance Information (NSSAI) Spoofing [5]
   - Description: The UE uses NSSAI to select a network slice. If we assume that the UE is authenticated with the mobile network, it could send a spoofed NSSAI and potentially gain unauthorized access to the slice.
   - Risks: Information Disclosure and Tampering.
   - Mitigation: UE authentication and authorization should be performed on per slice basis to thwart such attacks [15].
4) Hypervisor Compromised via Partner API
   - Description: As shown in Fig. 2, data can exist logically in trust but simultaneously physically allocated on untrusted hardware. One of the risks associated

with untrusted hardware is the possibility that it is running other network functions or APIs. These could be exploited to attack and control the hypervisor. A hypervisor is responsible for managing the virtualization of many slice components. If the hypervisor were compromised (known as a rogue hypervisor) those in control of the hypervisor would also control the slices and capture traffic from the slices [18].
- Risks: Information Disclosure, Denial of Service and Escalation of Privilege.
- Mitigation: Use protocol and content verification. Ensure hypervisor and virtual machine software are always up to date & patched, isolate the hypervisor behind a firewall, implement intrusion detection systems, and apply an organization-wide defense-in-depth approach to information security [19].

5) Impersonation of Session Management Function (SMF) [20]
   - Description: Successful impersonation of the SMF can give the attacker the ability to establish Packet Forwarding Control Protocol (PCFP) session to the User Plane Function (UPF) (via N4 interface) which is responsible for connecting the subscriber to the public Internet. The UPF and SMF are likely to be logically in the same trusted domain and therefore, the UPF will execute commands sent from the SMF. Potential damaging commands include dropping users from the network, denying service after the drop and redirecting data [20].
   - Risks: Denial of Service.
   - Mitigation: N4 interface should be properly configured and it must not be accessible from outside the operator's network [20].

### B. Tampering

Tampering is any unauthorized modification to a system, user or process. Tampering attacks destroy the integrity of data [11].

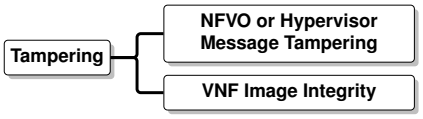


Fig. 5. Identified Tampering Threats

1) Network Functions Virtualization Orchestrator (NFVO) or Hypervisor Message Tampering [21]
   - Description: This is a type of MitM attack where a rogue node sits on the network between the Orchestrator and Host and modifies the exchanged messages.
   - Risks: Information Disclosure, Escalation of Privilege and Repudiation.
   - Mitigation: Mutual Authentication and Integrity Checking

2) Virtual Network Function (VNF) Image Integrity [21]
   - Description: An adversary with access to the network between the VNF image repository and host can alter image data (e.g., incorporate malware) as it is downloaded. There two scenarios for such an attack. Firstly, when the connection between the VNF image repository and host is not encrypted and integrity protected, the attacker can intercept the traffic and modify it before it reaches the host platform. Secondly, when the connection between the VNF image repository and host is encrypted but not integrity protected. If the attacker performed a MitM attack at the beginning of the session, the attacker would be able to capture encryption keys for both parties, and afterward in-transit information can easily be modified/altered.
   - Risks: Information Disclosure, Escalation of Privilege.
   - Mitigation: The host should verify the image signature before running the image. A digital signature should be created for every stored image. We assume that stored image digital signatures can be trusted.

### C. Repudiation

Repudiation is the ability to dismiss responsibility for an action. Actions by users, processes, and attackers that are not logged/audited cannot be traced to an origin [11]. All untraceable actions are threats. In terms of Repudiation, we find no literature on direct threats to 5G core slicing that begin as a Repudiation attack; however, we assert that Repudiation is a major risk to a 5G core network. All attacks identified in this paper may be significantly more damaging to a network if the source cannot be identified. Attacks could persist longer and therefore be more damaging, if they are not traceable due to lack of information. As an example, we cite mTLS or mutual authentication as the mitigation for several threats. This permits actions to be traceable to a verified identity and strengthens non-Repudiation on the network. We recommend that all activity on the slice be authorized, authenticated, and logged for investigation in case of attack.

### D. Information Disclosure

This type of attack occurs when there is any breach of confidentiality on a system [11].

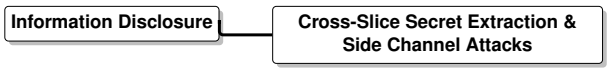


Fig. 6. Identified Information Disclosure Threats

1) Cross-Slice Secret Extraction and Side Channel Attacks [10], [17], [22]–[27]
   - Description: It is well documented in the literature that 5G slices existing on the same hardware

(sometimes called co-residency) introduces an increased risk of information disclosure. Researchers have found a variety of methods for using co-residency to map network topologies, extract secret keys (cross-slice secret extraction), read CPU instructions, buffer contents and cached memory of applications outside the context of a slice. These attacks are known by a variety of names including side channel attacks, cross-privilege boundary data sampling, cross tenant attacks and exploit of placement vulnerability. [10], [17], [22]–[28]. The details of executing these attacks can be found in the preceding references.

- Risks: Tampering, Escalation of Privilege.
- Mitigation: There is no simple mitigation for preventing side channel attacks based on our observations of the literature. The literature recommends increasing background noise with more applications, running program analysis [22], flushing the cache or injecting random data into the cache [23], selective feature deactivation, instruction filtering, removing prefetch gadgets, and flushing buffers [24]. The literature also discourages resource sharing due to the complexity of attacks, resource overhead from the currently know and previously mentioned mitigations and lack of certainty that all attacks will be mitigated [22], [27].

### *E. Denial of Service*

Denial of Service (DoS) attacks occur when resources are too preoccupied with illegitimate requests to efficiently process legitimate requests [11].

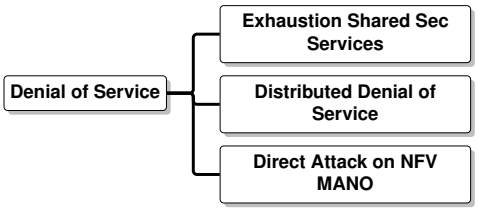


Fig. 7. Identified Denial Of Service Threats

1) Exhaustion of Shared Security Service [17]
   - Description: Assume there are two slices, A and B, protected by the same security mechanism with shared resources. An attacker launches an assault on A; however, the shared security software of A & B is able to thwart the attack. The attacker then launches the same attack on B, now knowing how the system will defend itself. The attack is consistently repeated, depleting the shared security resources to protect B; however, this leaves slice A with a lower level of protection from other attacks as security resources are exhausted [17].
   - Risks: The primary concern with DoS attacks is that services become completely unavailable for everyone, including the attackers. As an example, if security resources are unavailable due to a DoS attack, it is possible for other attacks to occur as the system's defences are lowered.
   - Mitigation: Guarantee each slice a minimum amount of resources and cap each slice at a maximum resource allocation to prevent resources from being exhausted [17].
2) Distributed Denial of Service (DDoS) Attack [28] [29]
   - Description: A DDoS attack is caused by a very large group of automated devices (commonly called a Botnet) which all repeatedly request the same resource until that resource is so overwhelmed no one can access it. The primary risk points for a 5G core network are on the N4 interface, which is the central control point between remote and central data centers, and the N6 interface, which connects to the public Internet [12].
   - Risks: Same as previous.
   - Mitigation: Implement machine learning algorithms to analyze traffic to detect and blacklist bot devices [12]. 3GPP also recommends that slices be isolated from each other to confine cyber attacks to a single slice [29]. Note that these are only examples and not an exhaustive list of mitigations.
3) Direct attack on Network Functions Visualization MANagement and Orchestration (NFV-MANO) [19]
   - Description: The role of the NFVO is to manage virtual network functions. The virtual network cannot exist without the services of the NFVO and hypervisor. If these services were attacked, then service to all slices would be denied.
   - Risks: Same as previous.
   - Mitigation: Regular updates & patches, network isolation & segmentation, implement firewalls & intrusion detection systems and apply organization-wide defense-in-depth strategy [19].

### *F. Escalation of Privilege*

Escalations of Privilege occur when a legitimate or illegitimate user is able to find a way to access more information or services than they have privileges to access [11].

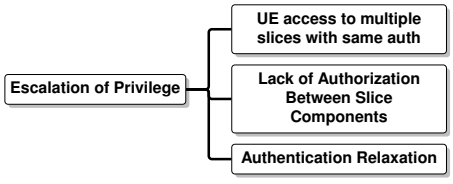


Fig. 8. Identified Privilege Escalation Threats

1) UE accesses multiple slices with same authorization [17]
   - Description: It is expected that many users accessing a 5G network will access content hosted on multiple network slices. If the same credentials (e.g.,

authenticating through the carrier) are used to access multiple slices, there is a risk that if the credentials are compromised (perhaps through a less secure slice), then the attacker will have the credentials to access other slices [17]. Thus escalating the user's privilege in some slices.
- Risks: Information Disclosure and Tampering.
- Mitigation: Repeated and separate re-authentication on each slice [17], or forbid credential reuse across slices.

2) Lack of Authorization between Slice Components [30]
- After a slice's network function is instantiated, it can perform authentication using TLS/mTLS with the NRF (if enabled) and start the registration process. However, there is no mechanism to authorize the NF to check if it belongs to the correct slice. There are several scenarios where an unauthorized NF can register with the NRF. For instance, an attacker could impersonate a valid NF [20], a mis-configured NF could be added during the life cycle of a slice, or a malicious actor is able to modify the configuration of a compromised NF.
- Risks: Information Disclosure, Tampering, DoS [20].
- Mitigation: The NRF must authorize NFs before registration.

3) Authentication Relaxation for services [31]
- Description: Each slice is uniquely setup for the needs of its client. In some cases where the need for availability vastly outweighs the need for confidentiality, authentication may be relaxed to improve latency [31].
- Risks: Spoofing, Tampering, and Information Disclosure
- Mitigation: Demand base level of security across all slices, isolate slices with similar security goals together, have the UE authenticate for each slice individually [17].

## V. Discussion

We remind the reader that no threat model can encapsulate all possible attacks; however, at the time of writing the threats identified are thought to be the most likely and damaging threats. In this section, we discuss general good practices for securing the core 5G network. We recommended 3 general practices to improve 5G core slicing security.

- **Implement mTLS with encryption and integrity** We observe that implementing mTLS is good practice that mitigates against Spoofing attacks, reduces the risk of further damage caused by Repudiation and Tampering attacks. Therefore, our first recommendation is to implement mTLS between all network nodes where applicable.
- **Group slices on hardware by security needs; always authenticate and authorize** A number of threats arise when slices share the same hypervisor or physical hardware. It is recommended that all slices have a base level of security enforced, and slices sharing the same resources have the same security goals. It is not practical in a real-world network implementation to forbid slice co-residency entirely, although it is recommended that slices with high-security needs should be placed on their own as much as possible. It is highly recommended that slices do not share authentication and each slice authenticates individually [19].
- Remember basic IT security hygiene We find that a number of attacks can be mitigated through basic IT security practices such as implementing firewalls, intrusion detection/prevention systems, regularly installing updates/patches and implementing an organization-wide defense-in-depth strategy [19].

## VI. Conclusion and Future Work

5G network Slicing is a new paradigm in communications technology. As it continues to grow and expand towards new use cases, there will be a continued need to maintain and modify its threat model. Therefore, the future work anticipated from this paper is an expanded and more detailed threat model. Such work could be done using a different threat modelling strategy, perhaps an asset-centric model (e.g. PASTA) as opposed to the attack-centric methodology of STRIDE. We anticipate that new threats will continue to be discovered in 5G slicing and that the model should be maintained to reflect these developments.


## Acknowledgement

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and TELUS Communications through the Collaborative Research and Development (CRD). We also thank Wynn Fenwick for his feedback on the use of mTLS and Marc Kneppers for feedback on Repudiation scenarios.


## References


[1] E. Dahlman, S. Parkvall, and J. Skold, *5G NR: the next generation wireless access technology*. Academic Press, 2018.

[2] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of microsoft's threat modeling technique," *Requirements Engineering*, vol. 20, no. 2, pp. 1–18, 2013.

[3] A. Tamburin, "Debunked conspiracy theories quickly circulated amid uncertainty after nashville bombing."

[4] C. Mason, "Software problem cripples at&t long distance network," *Telephony*, vol. 218, p. 73, Jan 22 1990. Copyright - Copyright PRIMEDIA Business Magazines & Media Inc. Jan 22, 1990; Last updated - 2020-09-21; CODEN - TLPNAS.

[5] ENISA, "Threat landscape for 5g networks," tech. rep., November 2019.

[6] M. Mylrea, S. N. G. Gourisetti, C. Larimer, and C. Noonan, "Insider threat cybersecurity framework webtool methodology: Defending against complex cyber-physical threats," in *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 207–216, 2018.

[7] 3GPP, "Telecommunication management;Study on management and orchestration of network slicing for next generation network," TS 28.801 15.1.0, 3GPP, January 2018.

[8] Bin Han, Stan Wong, C. Mannweiler, M. Dohler, and H. D. Schotten, "Security trust zone in 5g networks," in *2017 24th International Conference on Telecommunications (ICT)*, pp. 1–5, 2017.

[9] Stephen C. Phillips, Gianluca Correndo, Mike Surridge, JosManuel Sanchez Vilchez, Ghada Arfaoui, Seppo Heikkinen, Marja Liinasuo, Pekka Ruuska, Christian Schaefer, Mats Naslund, Ravishankar Borgaonkar, Piers O'Hanlon, Gorka Lendrino, Carla Salas, Pier Luigi Zaccone, Luciana Costa, "Trust Model," Tech. Rep. D2.2, 5GPP, August 2016.

[10] V. Varadarajan, Y. Zhang, T. Ristenpart, and M. Swift, "A placement vulnerability study in multi-tenant public clouds," in *24th USENIX Security Symposium (USENIX Security 15)*, (Washington, D.C.), pp. 913–928, USENIX Association, Aug. 2015.

[11] V. O. P. C., *Computer security and the internet: tools and jewels*. Springer, 2020.

[12] "The evolution of security in 5g," *5G Americas*, July 2019.

[13] W. Stallings and L. Brown, *Computer security*. Pearson Education (US), 2017.

[14] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Elsevier/Syngress, Syngress is a imprint of Elsevier, second edition ed., 2014.

[15] "5G Americas White Paper Security Considerations for the 5G era," ts, 5G Americas, July 2020.

[16] J. Forshaw, *Attacking network protocols: a hackers guide to capture, analysis, and exploitation*. No Starch Press, 2018.

[17] S. B. Remy HAREL, "5g security recommendations package #2 : Network slicing," April 2016.

[18] Y. Huang, B. Chen, M.-W. Shih, and C.-Y. Lai, "Security impacts of virtualization on a network testbed," in *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability, SERE 2012*, pp. 71–77, 06 2012.

[19] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "Secmano: Towards network functions virtualization (nfv) based security management and orchestration," in *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 598–605, 2016.

[20] P. Technologies, "5G SA CORE SECURITY RESEARCH," tech. rep., 2020.

[21] S. Lal, S. Ravidas, I. Oliver, and T. Taleb, "Assuring virtual network function image integrity and host sealing in telco cloue," in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2017.

[22] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-tenant side-channel attacks in paas clouds," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, p. 9901003, Association for Computing Machinery, 2014.

[23] S. Wang, P. Wang, X. Liu, D. Zhang, and D. Wu, "Cached: Identifying cache-based timing channels in production software," in *26th USENIX Security Symposium (USENIX Security 17)*, (Vancouver, BC), pp. 235–252, USENIX Association, Aug. 2017.

[24] M. Schwarz, M. Lipp, D. Moghimi, J. Van Bulck, J. Stecklina, T. Prescher, and D. Gruss, "Zombieload: Cross-privilege-boundary data sampling," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, (New York, NY, USA), p. 753768, Association for Computing Machinery, 2019.

[25] D. Sattar and A. Matrawy, "Proactive and dynamic slice allocation in sliced 5g core networks," *IEEE ISNCC*, Oct 2020.

[26] M. S. Inci, B. Gulmezoglu, T. Eisenbarth, and B. Sunar, "Co-location detection on the cloud."

[27] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), p. 199212, Association for Computing Machinery, 2009.

[28] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-vm side channels and their use to extract private keys," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, p. 305316, Association for Computing Machinery, 2012.

[29] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," in *7th IEEE Conference on Comm. and Network Security*, June 2019.

[30] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system," TS 33.501 17.0.0, 3GPP, December 2020.

[31] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.