Threats and Vulnerabilities in 5G Networks

Thesis submitted in partial fulfillment of requirements
For the degree of
Master of Technology in Computer Technology
of
Computer Science and Engineering Department
of
Jadavpur University

by

Satarupa Mal

Registration No.: 154178 of 2020-2021
Examination Roll No.: M6TCT23002B

under the supervision of

Dr. Mridul Sankar Barik
Assistant Professor

Department of Computer Science and Engineering
Jadavpur University
Kolkata, West Bengal, India
2023

Certificate from the Supervisor

This is to certify that the work embodied in this thesis entitled **"Threats and Vulnerabilities in 5G Networks"** has been satisfactorily completed by **Satarupa Mal** (Registration No.: 154178 of $2020-21$; Class Roll No.: 002010504012; Examination Roll No. $M6TCT23002B$). It is a bona-fide piece of work carried out under my supervision and guidance at Jadavpur University, Kolkata for partial fulfilment of the requirements for the awarding of the **Master of Technology in Computer Technology** degree of the Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jadavpur University, during the academic year $2022-23$.

Dr. Mridul Sankar Barik,
Assistant Professor,
Department of Computer Science and Engineering,
Jadavpur University.
(Supervisor)

Forwarded By:

Prof. Nandini Mukherjee,
Head,
Department of Computer Science and Engineering,
Jadavpur University.

Prof. Saswati Mazumdar,
DEAN,
Faculty of Engineering & Technology,
Jadavpur University.

Department of Computer Science and Engineering
Faculty of Engineering And Technology
Jadavpur University, Kolkata - 700 032

Certificate of Approval

This is to certify that the thesis entitled **"Threats and Vulnerabilities in 5G Networks"** is a bonafide record of work carried out by **Satarupa Mal** (Registration Number 154178 of $2020-21$; Class Roll No. 002010504012; Examination Roll No. $M6TCT23002B$) in partial fulfilment of the requirements for the award of the degree of **Master of Technology in Computer Technology** in the **Department of Computer Science and Engineering, Jadavpur University**, during the period of June 2022 to October 2023. It is understood that by this approval, the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the thesis only for the purpose of which it has been submitted.

Examiners:

(Signature of The Examiner)

(Signature of The Supervisor)

Department of Computer Science and Engineering
Faculty of Engineering And Technology
Jadavpur University, Kolkata - 700 032

Declaration of Originality and Compliance of Academic Ethics

I hereby declare that the thesis entitled **"Threats and Vulnerabilities in 5G Networks"** contains literature survey and original research work by the undersigned candidate, as a part of his degree of **Master of Technology in Computer Technology** in the **Department of Computer Science and Engineering, Jadavpur University**. All information have been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

Name: Satarupa Mal

Examination Roll No.: M6TCT23002B

Registration No.: 154178 of $2020 - 21$

Thesis Title: Threats and Vulnerabilities in 5G Networks

Signature of the Candidate:

ACKNOWLEDGEMENT

I am pleased to express my gratitude and regards towards my Project Guide **Dr. Mridul Sankar Barik**, Assistant Professor, Department of Computer Science and Engineering, Jadavpur University, without whose valuable guidance, inspiration and attention towards me, pursuing my project would have been impossible.

Last but not the least, I express my regards towards my friends and family for bearing with me and for being a source of constant motivation during the entire term of the work.

Satarupa Mal
MTCT Final Year
Exam Roll No.: M6TCT23002B
Regn. No.: 154178 of 2020 – 21
Department of Computer Science and Engineering,
Jadavpur University.

Contents

List of Figures

List of Tables

Abstract

The fifth generation mobile communication (5G) is a fascinating technology to everyone, from common man to the industry. In comparison to the the previous generation (4G), it is meant to deliver higher multi-Gpbs peak data speed, ultra-low latency, more reliability, massive network capacity, increased availability and more uniform user experience to more users. It is supposed to design to connect virtually everyone and everything together including machines, objects and devices. Vis-a-vis the security of 5G system is of paramount importance. This thesis elaborates the threats and vulnerabilities in 5G network related to security. It also presents some threat models at the end.

Chapter 1

Introduction

1.1 Background

Mobile networks have undergone a significant change across its generations over the last 40-years. The first two generations supported voice and then text. The 3G transitioned to broadband access, with data rates of the order of hundreds of Kbps. Emerging technologies such as artificial intelligence, Internet of Things (IoT), automation etc. is going to generate massive amount of data which is poised to grow exponentially. The current mobile infrastructure was not designed for such a high information load and requires upgrading. Presently many of the countries have already deployed 5G with the promise of manyfold increase in data rates as compared to current 4G technology which supports data rates in few Mbps.

Among the many features of 5G wireless cellular technology, the notable are: higher upload and download speeds, more consistent connections, much faster and more reliable data service. 5G has the potential to transform the way we use the internet to access applications, social networks, and information. One of the design objectives of the 5G networks is to connect everyone and everything including devices, machines and vehicles. Applications with requirements of very reliable, high-speed data connections, i.e. self-driving cars, advanced gaming applications, live streaming, cloud-connected traffic control, drone delivery, video chatting etc. are going to benefit greatly from 5G connectivity.

At the same time, organizations are facing significant challenges in transitioning from 4G to 5G usage considering the security of such deployments. In some cases lack of standards and guidance, makes it more challenging for 5G network operators and users to know what needs to be done and how it can be accomplished. This calls for systematic analysis of threats and vulnerabilities of 5G technologies and its use cases and also methodologies for selection and deployment of appropriate security solutions.

1.2 Research Objective

The objective of the thesis is: "*To study different threats and vulnerabilities of the 5G network and also methodologies for effective threat modeling*".

1.3 Contribution of the Thesis

The author has concentrated to compile the works of different contributors mentioned in bibliography on 5G and its threats and vulnerabilities. 5G has been introduced in India by Jio and Airtel. It will impact tremendously on various sectors as mentioned below.

- Mobile communication
- Health Sector
- Agriculture Sector
- Security of the country
- Home Automation
- Autonomous Vehicle etc.

This thesis presents a survey on threats and vulnerabilities of the 5G network, different threat modeling techniques and existing threat models of 5G.

1.4 Outline of the Thesis

Following describes the outline of the thesis.

- **Chapter 2:** This chapter describes the contributions made by different authors in last decade on related works in 5G and its threats and vulnerabilities.
- **Chapter 3:** This chapter illustrates the overview of the 5G networks systems.
- **Chapter 4:** Threat modeling is discussed in this chapter
- **Chapter 5:** The threats and vulnerabilities in 5G networks are discussed here.
- **Chapter 6:** This chapter discusses 5G threat modelling.
- **Chapter 7:** This chapter presents the conclusion of 5G threats and vulnerabilities and its future work.

Chapter 2

Related Works

In this paper[19], the results of a comprehensive study on Advanced Persistent Threats(APT), characterizing its distinguishing characteristics and attack model and analyzing techniques seen in the APT attacks are discussed.

The paper [38] discusses potential security requirements for 5G networks. This aims at initiating and spurring the works towards a 5G security architecture. The Software Defined Networking(SDN) and Network Function Virtualization(NFV) for 5G are discussed in this paper[14][15]. This paper also provides an overview of the security challenges in these technologies and the issues of privacy in 5G, its solutions and future directions.

This paper[31] provides a novel scheme used for 5G attack procedure to address the vulnerabilities like leakage of long term key, privacy of subscriber identifier, insecurity of links between mobile network operator and linkability. The recent development and existing schemes for the 5G wireless security[23] are presented here based on the corresponding security services including authentication, availability, data confidentiality, key management and privacy. The new security features involving different technologies applied to 5G such as heterogeneous network, device-to-device communications, massive multiple input multiple output, software defined networks and Internet of Things are discussed.

The paper [22] discusses the security challenges and opportunities applicable to SDN/NFV and cloud to 5G networks and additional security requirements such as SDN controller security, hypervisor security, orchestrator security, cloud security, edge security etc. are proposed. The present security solutions offered by 5G and their impact on the current security standards for vehicular networks[26] are discussed.

The seamless integration of the 5G security with the current security standards used in vehicular networks is also addressed. The authors [40] provide an objective overview of 5G security issues and the existing and newly proposed technologies designed to secure the 5G environment. They categorize security technologies using Open Systems Interconnections (OSI) and for each layer vulnerabilities, threats, security solutions, challenges, gaps and open research issues are presented. The impact and importance of 5G on Internet of Things(IoT)[27] with its applications are presented.

This paper[39] discusses the evolution of wireless communication networks from 1G to 5G and future 6G.

Chapter 3

5G Overview

3.1 Introduction

5G is the 5^{th} generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices [21]. 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries. To offer these capacities, and more generally to improve the user experience, 5G makes use of a set of dedicated technologies [2], such as "Network Function Virtualization" and "Slicing" to increase the modularity, "EDGE computing" for faster response time, Non-Terrestrial Networks (NTN) / Satellite Communications for ubiquitous coverage, etc.

This chapter presents a overview of the 5G architecture and also different technologies that enables realization of 5G design objectives.

3.2 5G Architecture

The mobile cellular network provides wireless connectivity to devices that are usually on the move. These devices are known as User Equipments (UEs) and traditionally take the form of mobile phones and tablets. But increasingly UEs would include cars, drones, industrial and agricultural machines, robots, home appliances, medical devices etc. However, the UEs may also be devices that do not move: for example, a router that uses cellular connectivity to provide broadband access to other remote devices [13].

As shown in figure 3.1, the mobile cellular network consists of two main subsystems: the Radio Access Network (RAN) and the Mobile Core. The RAN manages the radio resources (i.e., spectrum) and makes sure that it is used efficiently and meets the quality of service (QoS) requirements of every user. It consists of a distributed collection of base stations. These base stations are known as eNodeB or eNB (which is short for evolved Node B) in 4G. In 5G, they are known as gNB, where the "g" stands for "next generation".

The Mobile Core is a bundle of functionality (conventionally packaged as one or more devices)

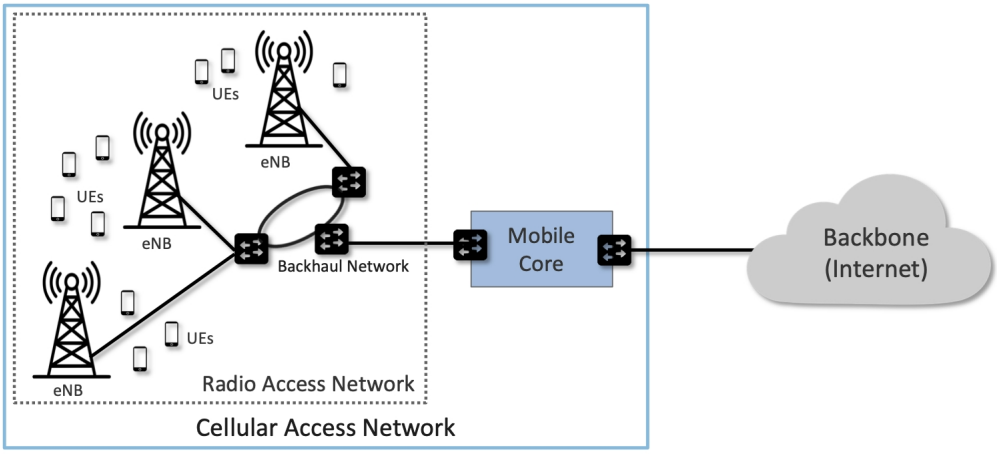

Figure 3.1: Mobile Cellular Network (Source: [1])

that serves several purposes. Mobile Core is a generic term used in 4G and 5G. In 4G it was called the Evolved Packet Core (EPC) and in 5G it is called the 5G Core (5GC). A Backhaul Network interconnects the base stations that implement the RAN with the Mobile Core. This network is typically wired, may or may not have the ring topology.

- Authenticates devices prior to attaching them to the network
- Provides Internet (IP) connectivity for both data and voice services.
- Ensures this connectivity fulfills the promised QoS requirements.
- Tracks user mobility to ensure uninterrupted service.
- Tracks subscriber usage for billing and charging.

The 5GC architecture adopts a "Service-Based Architecture" (SBA) framework, where the components are defined in terms of "Network Functions" (NFs) rather than by traditional "Network Entities". These NFs offer their services via interfaces of a common framework, to all the other authorized NFs and/or to any "consumers". The SBA approach offers modularity and reusability.

The 5GC is here schematically represented by the AMF/UPF entity: the User Plane Function (UPF), handling the user data and, in the signalling plane, the Access and Mobility management Function (AMF) that accesses the UE and the RAN. Further entities of the 5GC are presented below. The reference point between the access and the core networks is called "NG". This reference point is constituted of several interfaces (mostly N2, N3), as shown below in figure 3.2.

The core network must serve devices and applications with varying traffic profiles. As such, it is important to accommodate the needs of applications and allocate network resources based on these diverse requirements. The 5G network core flexibly allocates its resources, based on rules defined in software, for optimal service. This flexibility is achieved with the help of technologies like software defined networking and network function virtualization.

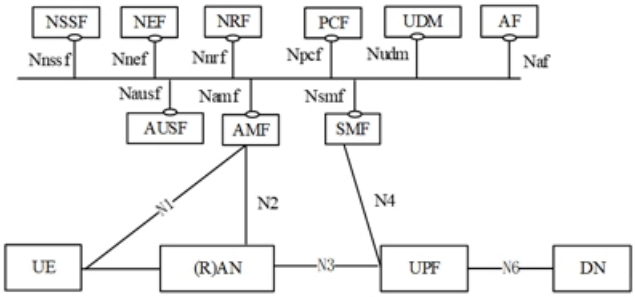

Figure 3.2: 5G Core Architecture (Source: [2])

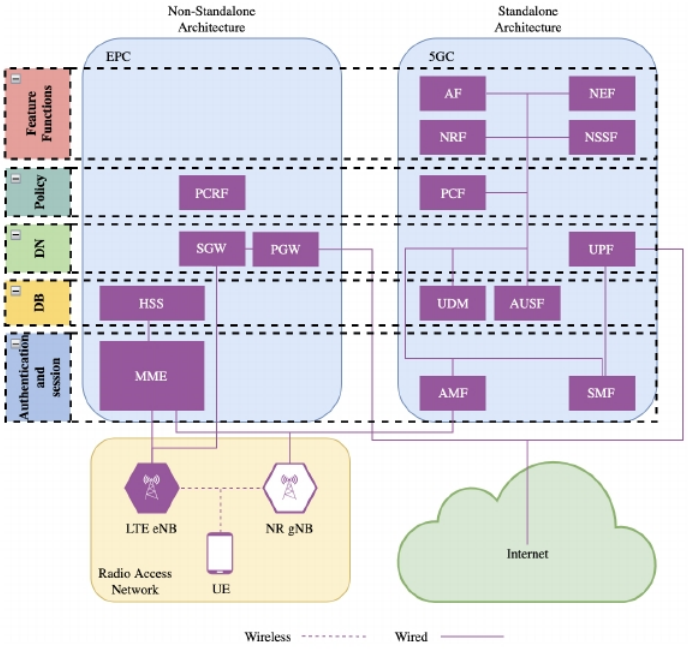

Figure 3.3: 4G Core vs. 5G Core (Source: [18])

3.2.1 Core Network

5G Non Standard Architecture (NSA) utilizes 4G's core also known as Evolved Packet Core (EPC). EPC consists of five components for its Control Plane (CP) and User Plane (UP). 5G Standard Architecture (SA) utilizes new 5G Core (5GC). Figure 3.3 compares EPC and 5GC. Following are the components in EPC:

- **Mobility Management Entity (MME)**: Responsible for tracking and monitoring the UEs throughout the RAN and includes also the recording of not active UEs.
- **Home Subscriber Server (HSS)**: The database that contains subscriber-related data.
- **Policy & Charging Rules Function (PCRF)**: Within this component, tracking and management of policy rules and billing data are held for the subscriber's traffic usage.
- **Serving Gateway (SGW)**: Forwards IP packets to and from RAN, anchoring the UE to the Core Network. Component is also involved in handovers to next base stations.
- **Packet Gateway (PGW)**: This component is in charge of connecting the Core Network to the external data network (more commonly referred to as the Internet). In its rawest form, it is basically an IP router.

The main difference in the design approach of EPC and 5GC lies in the fact that 5GC adopts a micro-service like architecture. It separates the functionality of each component, thereby reducing dependencies between CN and RAN. 5GC consists of ten components:

- **Access and Mobility Management Function (AMF)**: Responsible for user authentication, location, and mobility services and is comparable to EPCs MME service. However, unlike MME, AMF does not concern itself with session management.
- **Session Management Function (SMF)**: As name implies this service is in charge of user sessions and allocates IP addresses much like DHCP. Roughly it corresponds to EPCs MME and PGW (control-related aspect).
- **User Plane Function (UPF)**: Forwards packets between 5GC and Internet. Furthermore, service is also in charge of policy enforcement and traffic usage reporting. Corresponding the equivalency of the EPCs SGW and PGW.
- **Unified Data Management (UDM)**: Generating authentication credentials and managing user identity. To a certain degree resembles EPCs HSS.
- **Authentication Server Function (AUSF)**: Authenticates user by processing credentials generated by UDM. Together, UDM and AUSF form what is the equivariant of the EPCs HSS.
- **Policy Control Function (PCF)**: Manages the policies that every component within the 5GC enforces. Comparable to EPCs PCRF.
- **Application Function (AF)**: Supports traffic routing and interacts with NEF.
- **Network Repository Function (NRF)**: Can be thought of as a "Service discovery" function.

- **Network Exposure Function (NEF)**: Essentially an API exposing capabilities to third-party services.
- **Network Slice Selection Function (NSSF)**: New feature in the world of CSPs, serving UEs with a selected Network Slice.

3.2.2 Radio Access Network

5G networks require a wide band of frequencies. The main difficulty for operators was that available spectrum is very limited. Suitable bands were already allocated for other uses. Ultimately, 5G networks were assigned new millimeter-wave and centimeter-wave bands never used before for mobile communications. But the new frequency bands brought a new problem: short millimeter waves do not travel well through obstacles.

To compensate, a solution was devised with massive MIMO (Multiple Input Multiple Output) antennae comprised of hundreds of elements working in concert. Beamforming creates directional beams to efficiently serve individual subscribers. Each 5G network subscriber receives a spatially and temporally tailored signal from the base station antenna, which provides only the service needed by that particular subscriber. This technology allows using the base station more efficiently and increasing 5G radio bandwidth. And with multi-connectivity, user equipment can connect to multiple base stations simultaneously.

3.2.3 NSA vs. SA Architecture

The first release of 5G by 3GPP introduced two varieties of 5G service implementations: Non-StandAlone (NSA) architecture and StandAlone (SA) architecture. SA introduces lot of new features such as lower latency, increased bandwidth, and reduced power consumption. NSA could be implemented into the existing 4G LTE infrastructure, making it cheaper for CSPs to support subscribers with 5G enabled equipment. While the support for both infrastructures is desirable, the security risks from legacy protocols are also transferable between architectures.

The “Non-Stand Alone” (NSA) architecture, where the 5G Radio Access Network (RAN) and its New Radio (NR) interface is used in conjunction with the existing LTE and EPC infrastructure Core Network (respectively 4G Radio and 4G Core). This makes the NR technology available without network replacement. In this configuration, only the 4G services are supported, but they enjoy the capacities offered by the 5G New Radio (lower latency, etc).

The “Stand-Alone” (SA) architecture, where the NR is connected to the 5G CN. Only in this configuration, the full set of 5G services are supported. The NSA architecture is illustrated in figure 3.5.

The SA architecture is illustrated in figure 3.6. The SA architecture can be seen as the full 5G deployment, not needing any part of a 4G network to operate.

3.3 Enabling Technologies

Several key technologies enable the advanced capabilities of 5G networks [24]. Some of these technologies are discussed in the following section.

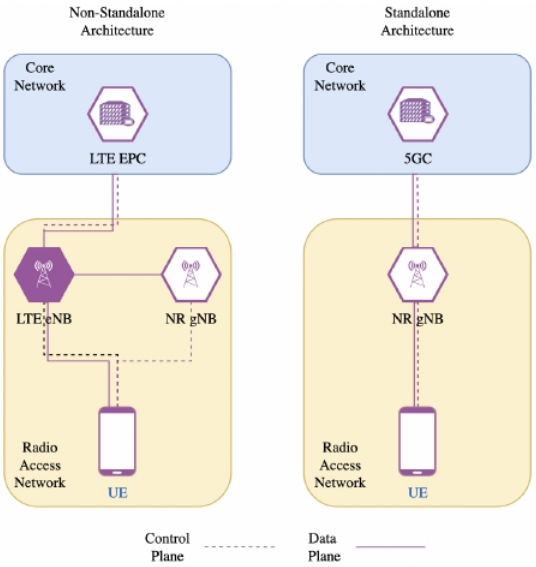

Figure 3.4: 5G NSA and SA Architecture (Source: [18])

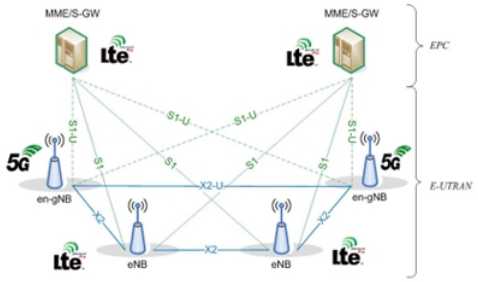

Figure 3.5: 5G NSA Architecture (Source: [2])

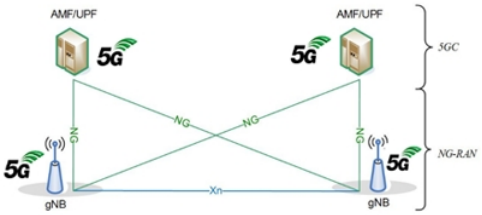

Figure 3.6: 5G SA Architecture (Source: [2])

3.3.1 Software-Defined Networking (SDN)

Software-Defined Networking (SDN) [28] is a relatively new concept in the field of network engineering, and it is changing the way networks are designed and managed. One of the key characteristics of SDN is the separation of the data plane and control plane of network devices. The data plane is responsible for forwarding network traffic, while the control plane decides how to handle that traffic.

With SDN, the control plane is consolidated, allowing a single software program to act as a central control software. This software, known as the SDN controller, can then control the data planes of multiple network devices. This approach provides greater flexibility and control, allowing network administrators to manage the entire network from a central location. There are many popular SDN controllers available, each with its own unique set of features and capabilities.

The main benefit of separating the control and data planes in SDN is abstraction. Similar to how an operating system abstracts the underlying hardware for application developers, SDN allows for the abstraction of the underlying network hardware for networking application developers. This is achieved by separating the control and data forwarding functions of networking devices, making it possible to build a common interface through which a central controller can control the forwarding behavior of multiple switches from different vendors. In traditional networking devices, the control and data planes are tightly coupled, making it difficult for developers to create applications without having to consider the specifics of the different devices. By separating the planes, SDN allows for greater flexibility and ease of development.

To communicate with networking devices in an SDN environment, a secure connection using SSH and APIs is used. One commonly used API is the OpenFlow protocol, which outlines the standards and requirements for communication between an SDN controller and the network device. These network devices are called OpenFlow switches, which can act as switches, routers, NATs, or other networking devices depending on the instructions given by the controller. OpenFlow switches contain one or more flow-tables that store flow rules or entries, which are used to match network traffic and perform actions such as forwarding, dropping, or flooding based on the defined rules.

SDN has become a significant technology in the networking industry as it allows for designing and managing networks in non-traditional ways. Many commercial switches now support OpenFlow, which is a common and well-known API for communication between an SDN controller and the agent network device. The flow entries on OpenFlow switches store information that helps match network traffic and perform actions on the matching traffic. This has allowed network application developers to build load balancers, dynamic access control, and many other useful applications and network features.

SDN has been evolving over a long period and has transformed from the old telephone networks where there was a separation of the control plane and the data plane to simplify the network and manage it better. The SDN controllers give programmers the ability to innovate, which was not possible in the earlier closed networks of telephone services. Today, there are SDN industry consortia like the Open Networking Foundation and the Open Daylight initiative, with many top information-technology companies being a part of them.

3.3.2 Network Function Virtualization (NFV)

The concept of Network Function Virtualisation (NFV) originated from the requirement of telecommunication service providers world wide, to accelerate deployment of new network services and to support their revenue and future growth objectives. NFV tries to decouple the physical network

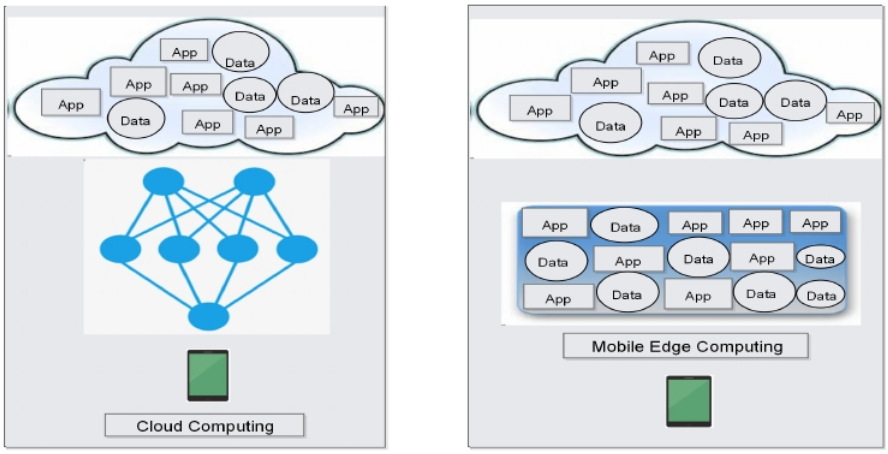

Figure 3.7: Mobile Edge Computing (Source: [21])

equipments from the functions that run on them, thereby replacing hardware centric, dedicated network devices with software running on general-purpose CPUs or virtual machines, operating on common-of-the-shelve (COTS) servers.

By decoupling Network Functions (NFs) from the physical devices on which they run, NFV has the potential to lead to significant reductions in Operating Expenses (OPEX) and Capital Expenses(CAPEX) and will facilitate the deployment of new services with increased agility and faster time-to-value.

For example, network operators may run an software-based firewall in a Virtual Machine (VM). It involves the implementation of network functions in software that can run on a range of industry standard servers and can be moved to or instantiated in various locations in the network as required, without the need for installation of new equipment.

With NFV, it is possible to mix and match network functions on the software level to create unique tel-ecommunication services without making changes at the hardware level.

3.3.3 Mobile Edge Computing (MEC)

Mobile Edge Computing (MEC) is an extension of the cloud computing that tries to bring cloud resources closer to the end-user so as to reduce latency and bandwidth requirements.

Some computational power is introduced as ”physically close” to the end-user as possible. Indeed, some applications such are virtual reality, factories of the future or autonomous driving, are very demanding in terms of the propagation's/network's response time. To reduce this time, some ”local replications” of a main server are introduced closer to the end-user.

3.3.4 Network Slicing

Network slicing splits a physical network into multiple virtual networks or slices [30] [33] [17]. Each slice is allocated its own re-sources (bandwidth, service quality, and so on) and has unique security policies. Each slice is isolated from each other to ensure privacy, security and performance.

One of the key benefits of network slicing is its ability to facilitate the deployment of diverse and specialized services on a single physical infrastructure. For example, a network operator can create a low-latency slice for autonomous vehicles, a high-bandwidth slice for video streaming, and a low-cost slice for Internet of Things (IoT) devices. Network slicing can also enable new business models, where network operators can offer slices to third-party service providers who can then offer their own services on top of the slices.

Network slicing involves of defining an isolated subset of the available virtual resources (computation, networking, storage) together with a set of rules for identifying the traffic that will run on those. A network slice consists of a set of virtual resources and the traffic flows associated with it. A network slice can be defined by slicing the available resources in the forms of:

- Bandwidth: Each slice should have its own fraction of bandwidth on a link.
- Topology: Each slice should have its own view of network nodes (switches, routers) and the connectivity between them.
- Device CPU: Each slice should be assigned proper computational resources.
- Storage: Each slice might have varying levels of storage capacity.
- Traffic: A specific portion of the traffic to one (or more) virtual networks should be associated with a slice in order to be cleanly isolated from the remaining underlying network.

An effective procedure to build and manage network slices is to leverage the principles of NFV and SDN. In brief, the combination of the abstraction possible through SDN with the freedom in deployment of functionalities deriving from NFV allow the proper level of control on the network, computation, and storage resources to build and manage slices.

Figure 3.8 [20] depicts a network topology that deliver three different service through network slicing. It illustrates that these slices are isolated from each other, and the deployment of service slices can be based on demand, allowing for more flexibility beyond the three slices. Fisrt slice fulfill eMBB service, second slice fulfill mMTC/mIoT service and third slice fulfill uRLLC service. To achieve proper packet forwarding for each service, an SDN (Software-Defined Networking) controller is utilized. The SDN controller ensures that packets belonging to each service are directed to the appropriate router for slice deployment. This enables efficient management and routing of network traffic, ensuring that each service receives the necessary resources and maintains its isolation within the network.

3.4 Layered Architecture of 5G

Farooqui et al. [24] presented a threat model for 5G-based systems. Their approach is based on the layered 5G architecture, identifying threat categories and mapping these to corresponding layers. The authors also presented an analysis enabling technologies affected by identified threats along with threat actors, entry points, and the impact of threat categories. In the following, we present different layers in 5G architecture:

- **Device layer:** This layer covers all the devices that may connect to the 5G network. These devices may range from mobile phones to drones, IoT devices to home appliances and autonomous vehicle to a network access point.

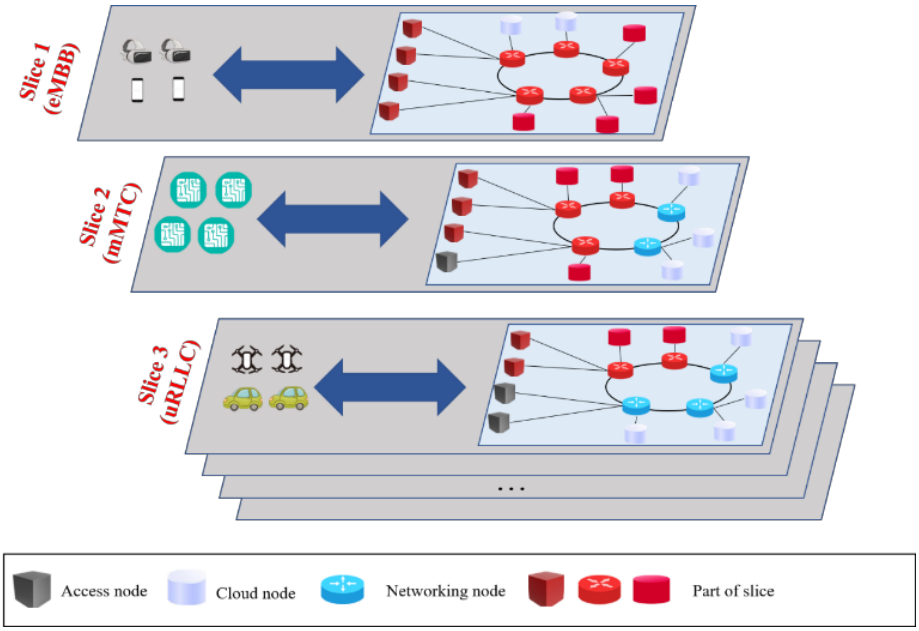

Figure 3.8: Network slicing example (Source: [20])

- **Radio layer:** The Radio Access Network (RAN) provides wireless connectivity to the 5G core network and services over the 5G spectrum.
- **Edge layer:** It facilitates 5G based applications that require ultra low latency, i.e. autonomous vehicle, remote surgery etc. Edge computing can be included in WiFi hotspots, radio towers and network routers.
- **Core layer:** 5G core is typically housed in cloud and is based on emerging technologies such as SDN and NFV. Several interconnected Virtual Network Functions (VNFs) provide 5G core services, i.e. Access andMobility Management Function (AMF), User Plane Functions (UPF), Session Management Functions (SMF), Data Network (DN), Authentication Server Functions (AUSF), Network Slice Selection Function (SMF) and Unified Data Management (UDM).
- **Service layer:** It is an interface which exports APIs to user applications which want to use different 5G network services.

3.5 5G Use Cases

These are also called 5G service classes. The idea is that the same network infrastructure would be able to facilitate or support a diverse set of services.

3.5.1 Enhanced Mobile Broadband(eMBB)

eMBB is an evolution of existing wireless broadband access services, with an emphasis on greater speed and spectral efficiency. Key network requirements: data transmission speed greater than 10 Gbps and network throughput of more than 1 Tbps, latency less than 7 ms, support for high speed mobility upto 500 kmph. Examples include: High-speed Internet access, HD video streaming, AR and VR services, Support for large numbers of subscribers in a single location

3.5.2 Ultra-Reliable and Low-Latency Communications(URLLC)

URLLC services have strict requirements regarding network reliability and quality, prioritizing low latency, reliability, and low probability of error. Key network requirements: probability of error from 10–5 to 10–8 and latency less than 3 ms. Examples include: Self-driving vehicles, Telemedicine, including remote diagnostics and robotic surgery, Remote control of industrial processes.

3.5.3 Massive Machine-Type Communications(mMTC)

This use case centers on high reliability, low power consumption, and support for high device densities in a given area. Key network requirements: density of up to 1 million devices per square kilometer and battery life of up to 10 years without recharging. Examples include: Smart City systems, Transport and logistics, Production and staff monitoring, Other scenarios with exceptionally high concentrations of IoT sensors.

Chapter 4

Threat Modeling

4.1 Introduction

Threat modeling is a process to analyze potential attacks, threats, and risks. It is often used as a structured approach to secure software in the design phase, by focusing on adversary goals when attacking a system. Most of the threat modeling methods can be categorized into manual modeling, automatic modeling, formal modeling, and graphical modeling, where formal modeling is based on mathematical models and graphical modeling can, for instance, be based on attack trees, attack and defense graphs, or tables.

Threat modeling activities are typically performed with the aim of identifying, understanding and making simple descriptions or models of potential threats and attack vectors that the system under study may be exposed to. An effective threat model will help in developing methods for risk analysis, attack detection, deployment of countermeasures and mitigation strategies.

An elaborate threat model produces documents on:

- how data flows through a system to identify where the system might be attacked
- as many potential threats to the system as possible
- security controls that may be put in place to reduce the likelihood or impact of a potential threat

4.2 Threat Modeling Terminology

- A **vulnerability** is a weakness in a system.
- A **threat** exists when there is likelihood that a vulnerability may be exploited.
- An **attack** is the event when a vulnerability is exploited.
- An **attack surface** is the sum of a system's vulnerabilities to cyberattack.
- **Attack vectors** are the methods or pathways that attackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack.

- A **threat agent** is an individual or group that is capable of carrying out a particular threat.
- **Impact** is a measure of the potential damage caused by a particular threat.
- **Likelihood** is a measure of the possibility of a threat being carried out.
- **Controls** are safeguards or countermeasures that you put in place in order to avoid, detect, counteract, or minimize potential threats against your information, systems, or other assets.
- **Preventions** are controls that may completely prevent a particular attack from being possible.
- **Mitigations** are controls that are put in place to reduce either the likelihood or the impact of a threat, while not necessarily completely preventing it.

4.3 Threat Modeling Approaches

There are three basic approaches to threat modeling: software-centric, attacker-centric, and asset-centric.

1. **Software-centric approach**: A risk mitigation focusing on software:
    - Evaluates the application being modeled
    - Determines the risk
    - Identifies controls to mitigate
    - Requires a good understanding of the application and the system it is running on
2. **Attacker-centric approach**: An approach that highlights the attacker:
    - Puts the user into the mindset of an attacker
    - Determines what is most at risk
    - Needs to understand the concept of hacking
    - Must have the skill set of a hacker
3. **Asset-centric approach**: Focusing on assets, this approach:
    - Identifies assets to be protected
    - Classifies assets based on data sensitivity and value potential
    - Determines an "acceptable risk" level
    - Takes a cyber risk–management perspective in satisfying the security auditing process

4.4 Threat Modeling Process

Typically, a threat modeling process includes five steps: threat intelligence, asset identification, mitigation capabilities, risk assessment and threat mapping. Each of these components provide valuable insights into security posture of a system.

4.5 Threat Modeling Methodologies

In general, threat modeling methodologies establish a catalog of potential threats that are relevant to adversary tactics and techniques as well as attack frameworks. When possible, technology specifics are abstracted away. Resolution or mitigation of identified threats with appropriate security controls establish the security posture of the system. Many different methodologies can be used, including:

4.5.1 STRIDE

STRIDE [5] was developed by Loren Kohnfelder and Praerit Garg in 1999 to identify potential vulnerabilities and threats to Microsoft products. This software centric (developer focused) threat model uses the mnemonic STRIDE to categorize threats as follows:

Threat Category	**Property Violated**	**Threat Description**
Spoofing	Authentication	Illegal access and then use of another user's authentication information, such as username and password
Tampering	Integrity	The malicious modification of data
Repudiation	Accountability (Audit)	Associated with users who deny performing an action without other parties having any way to prove otherwise
Information Disclosure	Confidentiality	Exposure of information to individuals who are not authorized to access it
Denial of Service	Availability	Attacks that deny service to valid users
Elevation of Privileges	Authorization	Privileged access gained by an unprivileged user, who then has sufficient access to compromise or destroy the entire system

Table 4.1: STRIDE Threat Model

In the STRIDE methodology, data flow diagrams of the application's use cases are created by decomposing them to identify system entities, events, and boundaries. Threat categories are then used to apply a general set of known threats to the system and assess the system for mitigations to these threats.

4.5.2 PASTA

Process for Attack Simulation and Threat Analysis (PASTA) is a risk-based methodology to threat modeling that takes an attacker-centric approach in identifying threats to an application. This methodology follows the seven-stage process shown in the diagram at left.

As PASTA follows an attacker-centric approach, it uses "attack trees" to depict potential attacks on a system in a tree-form diagram. The tree root symbolizes the goal of the attack, and the leaves show ways to achieve that goal. In order to leverage a threat modeling methodology that uses attack trees, one must be familiar with an attacker mindset and capabilities.

PASTA is seven step methodology of threat modeling with the objective of identifying threat, enumerating them and assigning a score so that organizations can deploy appropriate countermeasures to mitigate risks.

1. Define Objectives
2. Define Technical Scope
3. Decomposition and Analysis of Application
4. Threat Analysis
5. Vulnerability and Weakness Analysis
6. Analyze Modeling and Simulation
7. Risk and Impact Analysis

4.5.3 TRIKE

The TRIKE methodology, which is an open source project that uses threat models as risk-management tools, was originally created to improve the efficiency and effectiveness of existing threat modeling methodologies. It was first implemented as a tool in the programming language Smalltalk and is now implemented through spreadsheets.

4.5.4 VAST

Visual, Agile, Simple Threat Modeling (VAST) is a threat modeling methodology developed by the creators of the ThreatModeler product. Its purpose is to address the enterprise scalability gap by integrating into the full software development lifecycle (SDLC). VAST incorporates three pillars to support a scalable threat modeling solution:

4.5.5 DREAD

The DREAD threat modeling methodology was developed by Microsoft. The DREAD model quantitatively assesses the severity of a cyber threat using a scaled rating system that assigns numerical value to risk categories. It has 5 categories:

- Damage: Understand the potential damage a particular threat is capable of causing.
- Reproducibility: Identify how easy it is to replicate an attack
- Exploitability: Analyze the system's vulnerabilities to ascertain susceptibility to cyber attack.
- Affected Uers: Calculate how many users woould be affected by a cyber attack.
- Discoverability:Determine how easy it is to discover the vulnerable points in the system infrastructure.

The DREAD model enables analysts to rate, compare, and prioritize the severity of threats by assigning a given issue a rating between 0 and 10 in each of the above categories. The final rating, calculated as the average of these category ratings, indicates the overall severity of the risk.

4.5.6 Security Cards

Security Cards is a threat modeling methodology developed by the Security and Privacy Research Lab (CSE) and the Value Sensitive Design Research Lab (iSchool) at the University of Washington, Seattle. Its purpose is to facilitate exploration of potential security threats for a particular system; more broadly, it aims to develop a security mindset. It is based on brainstorming and creative thinking rather than a structured modeling approach.

The Security Cards toolkit provides a deck of 42 cards grouped across four dimensions (or suits):

- Human impact
- Adversary's motivations
- Adversary's resources
- Adversary's methods

Each card contains:

- Card topic
- Card dimension
- Questions to clarify and jump-start thinking
- Illustrative examples

4.5.7 MITRE ATT&CK Framework

The ATT&CK framework (Adversarial Tactics, Techniques, and Common Knowledge) was developed by MITRE Corporation, a private non-profit company in USA [6]. It is a globally accessible database which includes attack tactics, techniques, and mitigation measures for three different domains: enterprise, mobile, and industrial control systems (ICS). This knowledge base may act as a foundation for the development of other threat models, methodologies and tools.

ATT&CK contains 14 categories of adversary tactics and techniques, 12 of which are shared across all matrices. The 14 tactics are:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access

- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

There are two major components, tactics and techniques. Tactics are the objectives of an attacker, and techniques are the method by which the attacker achieves the tactical goals. Tactics and techniques are arranged as rows and columns of MITRE ATT&CK matrix. There are 14 tactics and 218 major techniques listed in MITRE ATT&CK matrix. Primarily, there are three categories of MITRE ATT&CK. ATT&CK for enterprise focuses on adversarial behavior in the enterprise system also covering cloud environments, Windows OS, and Mac OS, ATT&CK for mobile focuses on aggressive conduct, while the ATT&CK for enterprise matrix includes pre-ATT&CK, which focuses on "pre-exploit" hostile behavior.

In the ATT&CK matrix, mitigations are security concepts and a collection of instruments that stop a group of methods or sub- techniques from being effectively applied to a system or in an organization. Analysis of these mitigations, for different techniques, offers deep understanding of attack and help to identify the suitable security controls from NIST security and privacy controls. With deep analysis of the use case, possible attacks are identified in MITRE ATT&CK matrix for smart industrial system of smart firefighting. Mitigations of these attacks are analyzed to find prevention strategies and how attacks are linked with mitigations.

4.5.8 Graph-Based Threat Modeling

A vulnerability is an exploitable weakness in the design, implementation or management of a system. Preconditions are a set of system properties that must exist for an exploit to be successful. An initial precondition is a system property which exists inherently in a system and which did not arise as a consequence of exploitation. The successful perpetration of an exploit results in one or more postconditions. Although the result of an exploit is technically referred to as a postcondition, these can also form the preconditions of further exploits, therefore, most researchers refer to postconditions simply as precondition with the term goal being used to identify the final postcondition. For an exploit to be successful, one or more preconditions must be satisfied. The combination of preconditions can be represented using precondition logic. [29] [32]

Attack graphs are popular modeling tool for multistage attacks. It encodes system security states and attacker actions in form of dyadic relations resulting in a graph. Given the information on system components and their vulnerabilities, network topology and configuration, we can generate attack graphs using open source tools such as MulVAL [7].

Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes.

4.5.9 OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology focuses on organizational risks (as opposed to technical vulnerabilities). It involves building threat profiles, identifying infrastructural weaknesses, and establishing security measures.

4.5.10 NIST

The National Institute of Standards and Technology offers a threat modeling methodology focusing on data security. It includes the following steps:

- Identifying the data assets of interest.
- Identifying attack vectors.
- Characterizing security controls to mitigate the threats.
- Analyzing the model.

4.5.11 Cyber Kill Chain

The Cyber Kill Chain framework [3] was developed at the Lockheed Martin in 2011 for identification and prevention of cyber intrusions activity. There are seven steps in Cyber Kill Chain which enhance knowledge about an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

1. **Reconnaissance**: During the Reconnaissance phase, a malicious actor identifies a target and explores vulnerabilities and weaknesses that can be exploited within the network. As part of this process, the attacker may harvest login credentials or gather other information, such as email addresses, user IDs, physical locations, software applications and operating system details, all of which may be useful in phishing or spoofing attacks. Generally speaking, the more information the attacker is able to gather during the Reconnaissance phase, the more sophisticated and convincing the attack will be and, hence, the higher the likelihood of success.

2. **Weaponization**: During the Weaponization phase, the attacker creates an attack vector, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability. During this phase, the attacker may also set up back doors so that they can continue to access to the system if their original point of entry is identified and closed by network administrators.

3. **Delivery**: In the Delivery step, the intruder launches the attack. The specific steps taken will depend on the type of attack they intend to carry out. For example, the attacker may send email attachments or a malicious link to spur user activity to advance the plan. This activity may be combined with social engineering techniques to increase the effectiveness of the campaign.

4. **Exploitation**: In the Exploitation phase, the malicious code is executed within the victim's system.

5. **Installation**: Immediately following the Exploitation phase, the malware or other attack vector will be installed on the victim's system. This is a turning point in the attack lifecycle, as the threat actor has entered the system and can now assume control.

6. **Command and Control**: In Command and Control, the attacker is able to use the malware to assume remote control of a device or identity within the target network. In this stage, the attacker may also work to move laterally throughout the network, expanding their access and establishing more points of entry for the future.

7. **Actions on Objectives**: In this stage, the attacker takes steps to carry out their intended goals, which may include data theft, destruction, encryption or exfiltration.

   Over time, many information security experts have expanded the kill chain to include an eighth step: Monetization. In this phase, the cybercriminal focuses on deriving income from the attack, be it through some form of ransom to be paid by the victim or selling sensitive information, such as personal data or trade secrets, on the dark web.

   Generally speaking, the earlier the organization can stop the threat within the cyber attack lifecycle, the less risk the organization will assume. Attacks that reach the Command and Control phase typically require far more advanced remediation efforts, including in-depth sweeps of the network and endpoints to determine the scale and depth of the attack. As such, organizations should take steps to identify and neutralize threats as early in the lifecycle as possible in order to minimize both the risk of an attack and the cost of resolving an event.

4.6 Threat Modeling Tools

Many of the threat modeling methodology discussed above involve manual labour intensive activities which are prone to error and do not scale.

4.6.1 Microsoft Threat Modeling Tool

Microsoft Threat Modeling Tool [5] allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve.

4.6.2 Threat Modeler

The Threat Modeler [11] tool depicts how a hacker moves through a system, identifying where they'll attack, and more importantly, what controls are required to mitigate it. Following are some of the key features of this tool.

- **Intelligent Threat Engine (ITE)**: It utilizes functional information from the application, or system's architectural components, to automatically identify all the relevant and applicable threats to each component. As the ITE identifies relevant threats, it also gathers the associated security requirements, test cases, threat agents, code review guidelines and code snippets to provide all the necessary information needed for prioritizing threat mitigation efforts and reducing organizational risk.

- **Automated Threat Intelligence Framework**: It is a central repository for managing, detecting, and alerting users of potential threats.

- **Threat model templates**: Templates correspond to portions of threat models corresponding to frequently used application and system components.
- **Threat model chaining**: It provides the detailed insight into the interactions that occur between the cyber security threat models for each application component, the supporting systems and the infrastructure.

4.6.3 IriusRisk

IriusRisk [4] is a Threat Modeling Solution that helps in designing secure software before even writing a single line of code.

4.6.4 SD Elements

SD Elements [9] automates software threat modeling, delivering relevant countermeasures, compliance best practices, and actionable security requirements directly to developers. It is a developer-centric threat modeling tool that enables secure, compliant software by design.

4.6.5 Tutamen

The Tutamen Threat Model Automator [12] is designed to enable security at the architectural stage, where the cost of fixing flaws is the lowest. It makes a living threat model that changes when the design changes. This tool uses the well-known OWASP Top 10, STRIDE and Common Weakness Enumeration (CWE) for its reference frameworks.

4.6.6 securiCAD

securiCAD [10] is a quantitative threat modelling tool. It uses a domain-specific languages created with Meta Attack Language (MAL) such as coreLang to model IT-infrastructure, so that the user can get an overview of what systems are at risk and what is the likelihood of these systems becoming compromised. One advantage of securiCAD is that it does not require the user to have any knowledge about cyber security. The user only needs knowledge about the IT infrastructure in order to generate insight about possible attack paths.

4.6.7 OWASP Threat Dragon

OWASP Threat Dragon [8] is a modeling tool that can generate threat model diagrams as part of a secure development lifecycle. It can be used to enumerate possible threats and decide on their mitigations, as well as giving a visual indication of the threat model components and threat surfaces. Threat Dragon supports STRIDE / LINDDUN / CIA, provides modeling diagrams and implements a rule engine to auto-generate threats and their mitigations.

4.7 Open Threat Modeling (OTM)

The Open Threat Modeling Format (OTM) defines a platform independent way to define the threat model of any system. OTM allows both humans and computers to understand what are

the components of a system, how are they distributed, the security risks that could be exposed to attackers and the mitigations that could be implemented to avoid those vulnerabilities.

Key use cases for an open threat modeling standard include:

- Easily supporting new sources of application and system design. Anyone can write and share parsers or other tools that take source formats such as CloudFormation, Visio, or Docker Compose files.
- Exchange threat model data within the SDLC and cyber security ecosystem. Having threat models represented in a common format means being able to use that data through integrations.
- Exchange between organisations. It would be a great outcome if open source projects or even commercial vendors were sharing threat models of their systems in a way that could be ingested and used by organisations adopting those systems.

4.8 Summary

Here, the three modeling approaches are discussed i.e. software-centric approach, attacker-centric approach and assset-centric approach. The different threat modeling methodologies discussed here are STRIDE, PASTA, TRIKE, VAST, DREAD, Security cards, MITRE ATT&CK Framework, Graph Based Threat Modeling, OCTAVE, NIST and Cyber Kill Chain. The threat modeling tools discussed here are Microsoft Threat Modeling Tool, Threat Modeler, IriusTisk, SD Elements, Tutamen, securiCAD and OWASP Threat Dragon.

Chapter 5

5G Threats and Vulnerabilities

5.1 Introduction

The 5G mobile cellular network brings enhanced mobile broadband, massive machine type communication (e.g. IoT), critical machine type communication and fixed wireless access and will accommodate new services and applications such as augmented reality, and seamless streaming to all. 5G will boost security with encrypted data, segmented networks (network slices), enhanced privacy, and user authentication, but the 5G success may also attract attackers to look for vulnerabilities, exploits or eavesdropping. The increase in connected devices creates more targets, and larger attack surfaces, hence attacks on vital connected systems could become more chaotic and consequential.

5.2 Threats in 5G Networks

Key 5G design objectives, i.e. realization of network as a service and support of diversity of 5G use cases render security of the network more complex [36]. Availability, confidentiality and integrity of all user data and services, management and control functions need to evolve to support dynamic networks, multiple players involved in service delivery, wide variety of devices (including IoT), users, and applications. Multiple logical networks, i.e. the network slices, will be running on the shared 5G infrastructure. This complexity leads to a large attack surface. Moreover, the huge number of connected devices implies that the network would be exposed to massive attacks by such devices, if they become infected by malware and are abused by an attacker as a botnet for carrying out attacks such as distributed denial of service (DDoS) attacks. The Mirai Botnet[1] attack gives just a preview of such attacks with the potential to cripple ICT infrastructures all over the world. With 5G, vulnerabilities in the network may have more serious consequences than was the case with previous telecom generations due to diversity of use cases. In Addition, the convergence of Telecom and IT infrastructures, services, and operations, require a holistic and broader look at 5G security than before [14] .

[1] https://spectrum.ieee.org/mirai-botnet

5.3 5G Security

5G will connect critical infrastructure that will require more security to ensure safety of not only the critical infrastructure but safety of the society as a whole. Security is the key feature in the telecommunication network industry, which is necessary at various layers, to handle 5G network security in application areas such as IoT, Digital forensics, IDS and many more [22] [18].

5.3.1 5G Virtualization/Softwarization Security

With the advent of virtualization, hypervisors and containers are becoming more prevalent. While these technologies allow multiple tenants and virtual network functions to reside on the same physical hardware, they also increase the systems' attack surface to threats such as data exfiltration, resource starvation, and side channel attacks. Some applicable mitigation techniques that can be applied to such scenarios include hypervisor introspection schemes and hypervisor hardening. These mechanisms can protect a hypervisor's code and data from unauthorized modification and can guard against misconfigurations.

On the other hand, virtualization enables operators to dynamically provide security resources and functions such as DDOS protection, intrusion detection system IDS, intrusion prevention system (IPS), and firewall functionalities. However, successful dynamic provisioning is dependent on other system components such as the orchestrator, SDN controller, network controller, and the NFV security orchestrator. Hence, this dependence extends the risks and vulnerabilities of underlying elements to the security functions themselves. Further risks in security function virtualization stem from relevant integrated automation techniques.

5.3.2 Optimization/Orchestration Security

5G resource allocation and optimization complexity levels have motivated the increased utilization of artificial intelligence (AI)/machine learning (ML) algorithms in the management and orchestration layer. In an SDN/NFV environment, an orchestrator could provide VNFs based on the network condition and intelligence. For example, in case of overload or security attacks,the orchestrator is notified of the condition of the network and communicates with the SDN controller that in turn controls the firewalls and routers to mitigate the attacks. Simultaneously, the orchestrator can instantiate additional VNFs as needed, and scale down as the attack subsides. This built-in orchestration flexibility introduces potential vulnerabilities, where an attacker may use legitimate access to the orchestrator to manipulate its configuration in order to run a compromised VNF.

5.3.3 SDN Security

An SDN controller can enable dynamic security control based on the intelligence gathered through north bound API and then controlling the routers and switches through south bound API. This improves network resilience and enhances the ability to mitigate cyber-attacks quickly. However, an SDN controller can be a target for attacks through its north bound and south bound interfaces. SDN controllers can be targeted by specific threat vectors including denial of service attacks; REST API parameter exploitation; API flood attack; man-in-the-middle attack (MiTM), spoofing; protocol fuzzing, and SDN controller impersonation. Proper mitigation mechanisms need to be put in place to detect these kinds of attacks and take appropriate mitigation techniques to ensure reliable operation of the SDN controller.

5.3.4 5G Network Slicing Security

While network slicing enables sharing resources in the network more efficiently and facilitate the allocation of resources to support different types of applications, these also give rise to security concerns. Proper security controls must be implemented to ensure proper isolation of slices and enabling trusted virtualization infrastructure. Such security controls include slice categorization and adequate provisioning of resources. Further, strong security controls must be implemented to limit and secure information flow between slices. This would prevent and mitigate many threats such as side-channel attacks across slices, DoS attack via virtual resources depletion, etc.

5.3.5 Edge Security

The increasingly critical role of the edge in 5G architecture and use-cases amounts to high adverse impacts if the edge is compromised. When this is combined with the increased threat surface as the edge extends to the end user, the edge becomes an attractive target for cyber attacks. This is further complicated as the edge hosts security controls such as authentication, authorization and real-time attack detection to provide security controls for other 5G use-cases (as it has been illustrated previously). Security controls on the edge should also consider complex and multi-step user handling scenarios, such as in the case of subscriber authentication with a visited network, for a low-latency application. In this case, delay constraints will make authenticating against the HSS infeasible, and alternative solution should be considered. Strong layered security controls must be implemented on the edge to provide adequate protection and availability for the security functions, and any sensitive security contexts that may be stored on the edge, or communicated between the edge and the core. Proper separation of third-party applications and management/network functions would help minimize risks of bi-lateral movement to 5G control plane. Computationally feasible trust platforms could help limiting the attack surface from the user/RAN side.

5.3.6 Supply Chain Security

The continuing increased trend of leveraging commodity modular hardware and software is introducing a multitude of security risks. Example risks include backdoors, dormant malicious code or compromised hardware certificates. Promising solutions will need to address this on multiple levels—computationally feasible trust platforms similar to blockchain will enable establishing some security controls over commodity hardware and integrated software. However, capabilities in security monitoring and anomaly detection in the 5G NFV would need to evolve to enable attacks or malicious incidents detection/prediction.

5.3.7 Open Source / API Security

Currently, there are various open source activities that expedite the deployment of SDN/NFV and 5G. These include the Open Networking Foundation (ONF), OPNFV, Open Day Light, Open Network Operating System (ONOS), Open vSwitch (OVS), and the Linux Foundation among others. Operator community and vendor community are collaborating to develop open source that can be scalable and reliable enough to be deployed. Open source has various opportunities such as flexibility and agility, faster time to market, cost-effectiveness, long-term cost savings, reducing the vendor lock-in, and better information security. However, open source is also challenged with various issues, namely level of support, intellectual property concerns, lack of documentation and

graphical user interfaces (GUIs), extent of customization needed for various use cases. All of these also give rise to security concerns that need to be addressed by the open source community.

5.3.8 Data Security And Privacy

Data will be an integrated part of 5G, where the different types of data (including user data, data about the users, system configurations, system logs and monitoring data) will be used to 1) enable core functions and use-cases, and 2) enable automation of decision-making in applications and system management and orchestration. From a security perspective, several cases should be considered here including classification and proper protection for at-rest and in-transit data. Privacy should be taken into account when designing/configuring the system to ensure only necessary data is collected and stored. Data sharing between subsystems of 5G, and across use-cases and slices should have a structured framework with defined objectives, monitoring and controls.

5.3.9 Predictive Security / Monitoring and Analysis

While it may be effective to detect cyber-attacks quickly and be able to mitigate in a timely manner, stopping the attacks altogether by taking proactive measures is also desirable. This can be achieved by applying AI/ML techniques for anomaly detection, enabling behavior analytics of bad actors through traffic analysis and deep packet inspection, combined with the analysis of past attacks. This approach could improve Zero-Day attack detection and mitigation. Digital forensics solutions have evolved in the last years to address new challenges imposed by contextual change. As 5G enables critical use cases, it should incorporate and enable digital forensic solutions to increase the trustworthiness in the 5G infrastructure from a user-centric perspective. It must be known that, if something happens (malfunction, error or cybercrime), the appropriate technologies will be available to help in the process of identifying the problem and establishing responsibilities.

5.4 Security Threats of 5G Enabled IoT

The use of previous generation networks like 4G was vastly used in the Internet of Things (IoT) devices. The constant need to grow and develop just so the network can fulfill the requirement of IoT devices is still going on. The exponential growth of the data services substantially challenged the security and the networks of IoT because they were run by the mobile internet requiring high bit rate, low latency, high availability, and performances within various networks. The IoT integrates several sensors and data to provide services and a communication standard. Fifth Generation Communication System (5G) enabled IoT devices to allow the seamless connectivity of billions of interconnected devices. Cellular connections have become a central part of the society that powers our daily lives. Numerous security issues have come to light because of the exponential expansion of 5G technologies and the adaptation of the slow counterpart of IoT devices. Network services without security and privacy pose a threat to the infrastructure and sometimes endanger human lives. Analyzing security threats like Eavesdropping, Interception, Traffic Analysis, Contaminating, Spoofing and Jamming, and mitigation is a crucial and fundamental part of the IoT ecosystem. Authorization of data, confidentiality, trust, and privacy of 5G enabled IoT devices are the most challenging parts of the system. This paper[16] includes a comprehensive discussion of 5G, IoT fundamentals, the layered architecture of 5G IoT, security attacks and their mitigation, current research, and future directions for 5G enabled IoT infrastructure.

5.5 Security Threats of Military 5G Systems

The fifth generation of mobile telecommunications (5G) is considered a very interesting solution for military applications. However, characteristics of this technology (open interfaces, cloud-based nature) create additional security threats and generate a very broad threat landscape for the 5G deployments. The different threats to military 5G networks are jamming, Denial-of-Service(DoS), Signaling storms, Eavesdropping and movement analysis, Man in the Middle (MITM), Roaming Security, Attacks on Machine Learning Algorithms and Supply chain attacks. There are specific methods of counteracting the above-mentioned threats. In the article [42], the main security threats related to the Radio Access Network (RAN) are described, taking into account the open version of its implementation – O-RAN. The possible adversarial attacks that can have a significant impact when machine learning algorithms are used e.g. in the RAN Intelligent Controller are emphasized.

5.6 Summary

This chapter describes different threats in 5G networks. It also discusses different 5G securities like 5G Virtualization/Softwarization Security, Optimization/Orchestration Security, SDN Security, 5G network slicing security, Edge Security, Supply Chain Security, Open Source/API Security, Data Security and Privacy, Predictive Security. Security threats of 5G and IoT, and Security threats of Military 5G Systems are elaborated.

Chapter 6

5G Threat Modeling

6.1 Introduction

The 5G networks has enabled deployment of a wide range of applications/services that require high performance and reliability. For this, the 5G network architecture makes use of various enabling technologies, which introduce various new and emerging security threats and attacks. Threat modeling is a proactive approach to identify security requirements, as well as potential threats and vulnerabilities, and prioritize remediation methods.

Due to its architectural characteristics, 5G offers a much wider attack surface and a combination of new attack avenues, including:

- Millions of connected devices with considerably less security features
- Weaker mobile/Wi-Fi/landline connectivity
- Software-based NFVs with a higher number of software vendors and potentially more supply chain issues
- Distributed edge computing
- IoT, which requires updating software on millions of connected devices that are inherently not as secure
- Reliance on cloud vendors for configuration
- Insecure container images, virtual networks for communication between containers, privileged flags, and isolation from hosts

Steps to developing a threat model for 5G:

1. Define the different network and user side assets that are at risk of being attacked.
2. Create a list of potential internal and external threat actors for each individual asset.
3. Identify the actions that the threat actors could take to breach the assets at risk.

4. Analyze the factors and form a list of threats prioritized by likelihood of success and risk to the business.

5. Create an action plan to mitigate the identified threats.

6.2 5G Threat Vectors

Threat vectors or attack vectors are methods used by attacker or cyber criminals to gain unauthorized access to a network or infrastructure. [24] [35]

6.3 Modeling 5G Threats as Graphs

Pell et al. [34] introduced the concept of a threat graph for modeling threat scenarios in 5G infrastructure network. The authors extended the definition of a cyber threat i.e. "possibility of a malicious attempt to damage or disrupt a computer network or system" by including the source and target of a threat. They formally defined a threat scenario as a tuple $T = (src, dst, scenario)$, where *src* is the network component from where the malicious activity originates and *dst* is the network component which is targeted by the attack scenario.

Definition 1 (Threat Graph) *Given a set of threat scenarios $t \in T$, a set of 5G infrastructure components $c \in C$, a threat source $T_s \subseteq C \times T$ and a threat target $T_t \subseteq T \times C$ a threat graph G is a directed graph $G = (C \cup T, T_s \cup T_t)$ where $C \cup T$ is the vertex set and $T_s \cup T_t$ is the edge set.*

Example 1 (Example of a Threat Graph) *The following threat graph shown in Figure 6.1 describes two possible multi stage attack scenarios.*

Threat Scenario 1:

1. *An attacker gains credentials for the MANO component*
2. *The adversary is able to make configuration changes which introduces a malicious NF into the SBA.*
3. *The malicious NF begins to harvest sensitive data by eavesdropping the SBA.*

Threat Scenario 2:

1. *An attacker exploits a vulnerability in the API of the NEF.*
2. *The attacker establishes a remote connection to the NEF of the 5GCN.*
3. *The attacker exploits a vulnerability in the hypervisor and gains access to the PI.*
4. *The adversary is able to access memory storing data for all of the NFs in the SBA.*

Scenario 1, highlighted by the red edges, and Scenario 2, highlighted by the blue edges, show how an adversary can attack the 5GCN through different attack vectors with the same goal of gaining access to sensitive data.

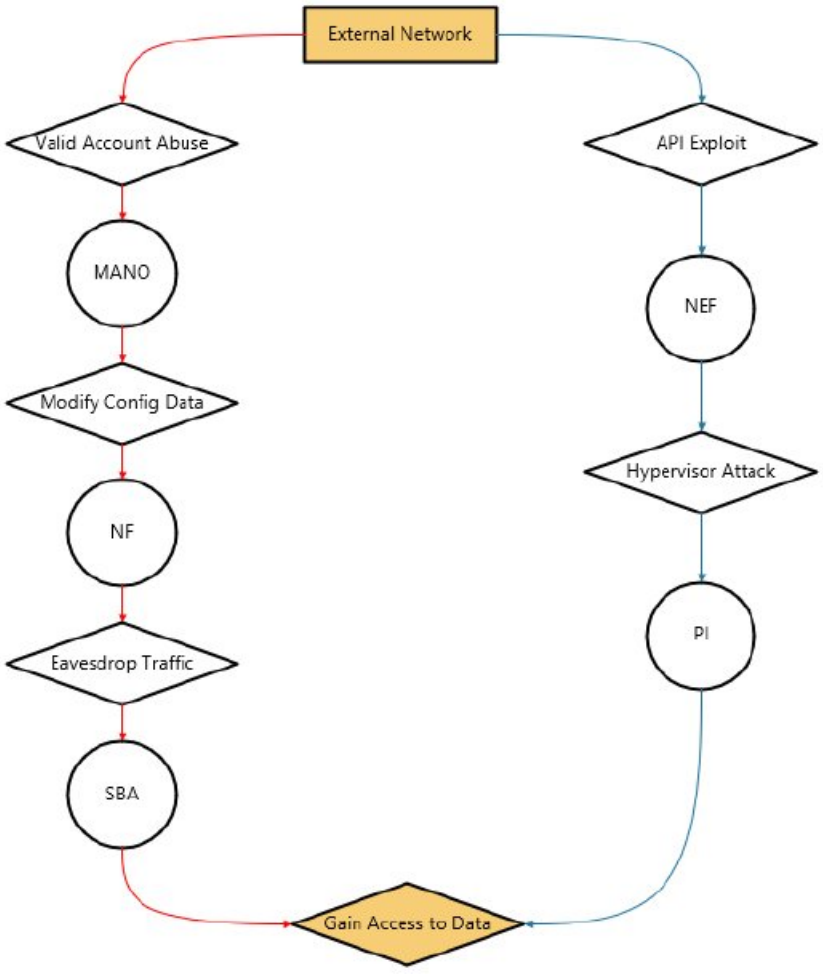

Figure 6.1: Example of Threat Graph (Source: [34])

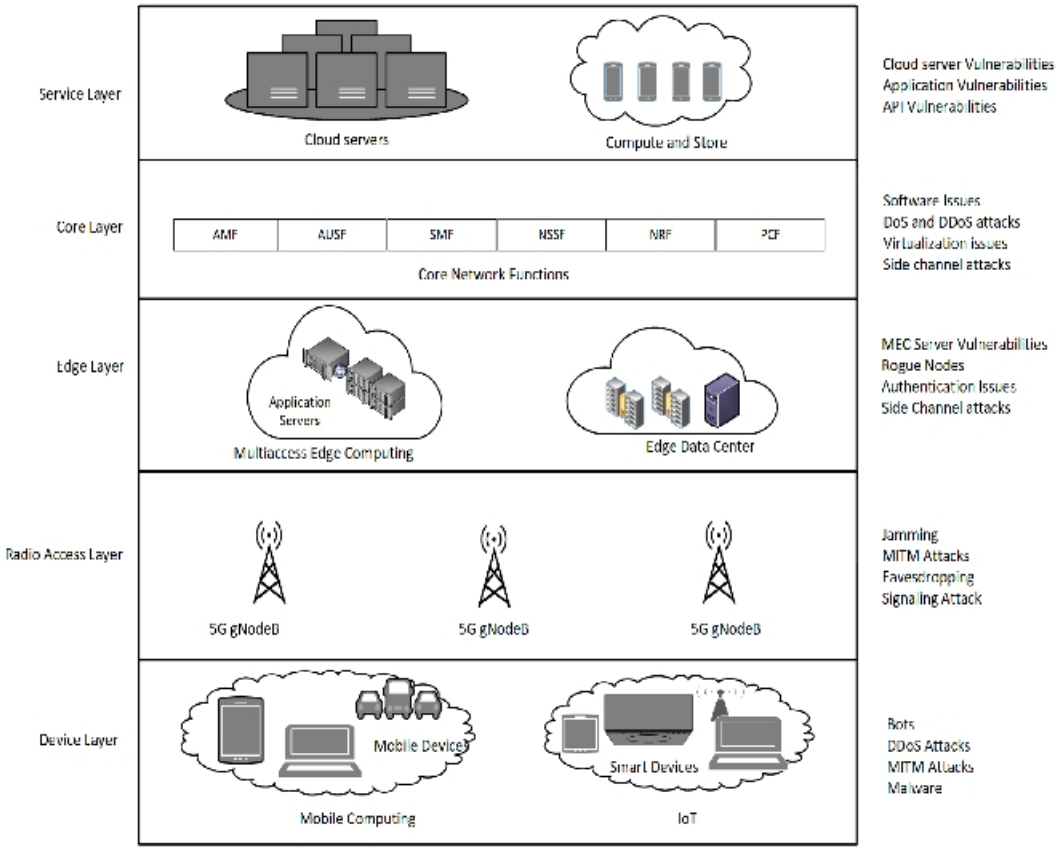

Figure 6.2: Threats in Different Layers of 5G Architecture (Source: [24])

6.4 Extension of MITRE ATT&CK Framework

Santos et al. [36] presented a proposal for extending the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework with adversarial tactics and techniques which are specific to the 5G mobile network infrastructure.

6.5 A Layered Approach to 5G Threat Modeling

The layered architecture of the 5G network includes a device layer, radio layer, edge layer, core layer and service layer. [24]

- **Device layer**: This layer consists of the devices which may connect to the 5G network. These devices can range from mobile phones to drones, IoT devices to home appliances and autonomous vehicle to a network access point. The attack surface of these devices is extremely

volatile with novel threats such as malware, worms, botnets and in some cases advanced persistent threats. The consequence of a successful breach in this case can range from compromise of user privacy to a potential full-scale attack on the network infrastructure and services.

- **Radio layer**: The 5G Radio Access Network (RAN) layer provides wireless connectivity to devices to connect to the 5G core network and services using 5G radio frequencies. Prominent use cases include cloud gaming, AR/VR, autonomous driving, and fixed wireless access. The radio access network consists of transmitters, antennas, base-band (RAN Compute), and RAN software to enable ultra-high speeds and mobility. The 5G network has introduced several improvements in RAN compared to 4G such as multiple antenna arrays, multiple input multiple output (MIMO) and centralized or Cloud RAN (C-RAN). However, these are susceptible to attacks targeting the RAN such as unauthorized access, traffic sniffing, signaling storms, flooding and jamming.

- **Edge layer**: The introduction of an edge layer within 5G architecture is envisaged to facilitate use cases such as autonomous vehicles and remote surgery, which require ultra-low latency (1 ms) and are supported by bringing compute capabilities closer to the end-user. Edge computing can be included in WiFi hotspots, radio towers and network routers. As the edge layer uses NFV and SDN, threats and attacks to these enabling technologies are also applicable on the edge layer in a 5G network.Edge nodes are susceptible to Denial of Service attacks, side-channel attacks and VM-based attacks.

- **Core layer**: The 5G core is designed as a cloud-native service-based architecture that uses NFV and SDN to provide advanced network functionalities. It has defined several interconnected virtual functions which provide services such as authentication, session management, mobility and security. These functions include Access and Mobility Management Function (AMF), User Plane Functions (UPF), Session Management Functions (SMF), Data Network (DN), Authentication Server Functions (AUSF), Network Slice Selection Function (SMF) and Unified Data Management (UDM). These functions are divided into the control and user plane and provide an interface to each other so that any function can request service from any other function. The 5G core design principles include Control and User-Plane Separation (CUPS), modular function design, minimizing dependencies between the RAN and Core network and concurrent access to local and centralized services. Several threats to the 5G core layer functions have been identified which need to be assessed while designing any 5G core network. Both control and user planes may be affected by these attacks, which include DoS and spoofing attacks on AMF, routing attacks on AUSF and UPF and SIP relay attacks on IMS AF.

- **Service layer**: The service layer provides the application interface to the users. Service providers define the programmable interfaces (APIs), and the architecture of this layer is independent of the underlying 5G architecture. Security at this layer is typically the responsibility of the service provider, and the threats faced by the services have a significant overlap with the contemporary Internet-based applications. Proper security features need to be maintained including authentication, authorization, secrecy and non-repudiation.

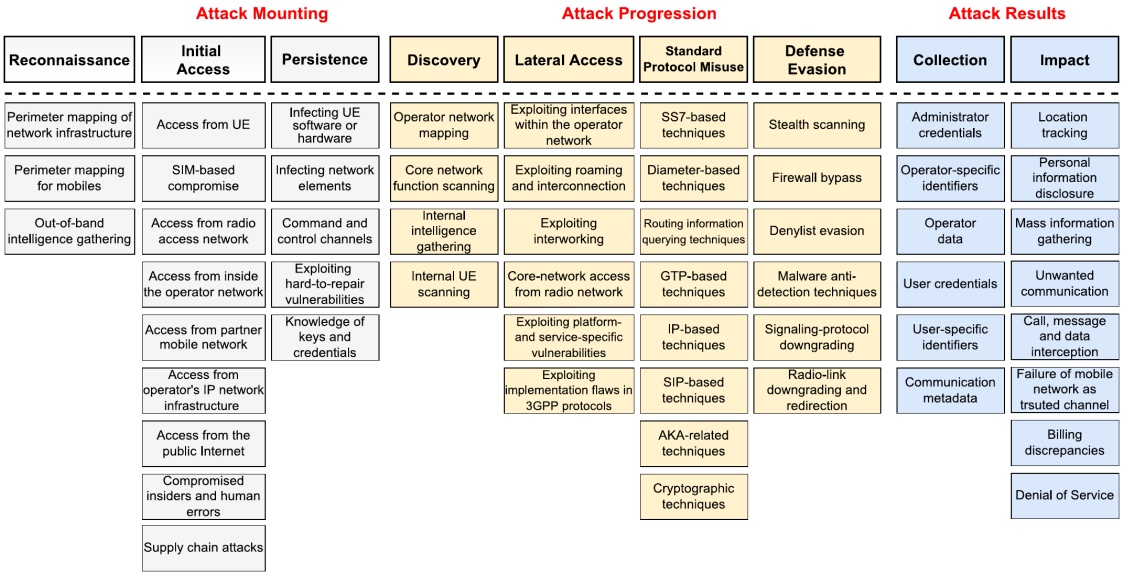

Figure 6.3: BHADRA Threat Modeling Framework (Source: [35])

6.6 The BHADRA Framework

The BHADRA framework [35] is a domain specific threat modeling framework for the telecommunication networks. The key components of the framework are tactics, techniques and assets.

- Tactics represent the adversary's tactical objectives, i.e., the reason ("why") for performing a particular action during an attack. In most of the studied attacks, there are similar phases and intermediate objectives of the adversarial actions during the course of the attack. Thus, the tactics are ordered in the way they represent the natural attack life cycle. Of course, not all attacks include all the tactics.

- Techniques are specific actions or technical means by which the adversary achieves the tactical objectives. They refer to the "how" and "what" aspects of the adversarial strategy. While some techniques may serve multiple tactical objectives, they have been grouped under the tactics which they most commonly serve.

- Assets are things of value that need protection.

The tactics and techniques are described in three phases in the attack life cycle: mounting, progression, and result.

The attack life cycle starts with the attack mounting phase, in which the adversary finds a weak point in the target, gains initial access to the target, and establishes a persistent presence. The adversary may also discover information that will be useful in the following phases of the attack. There are three tactical objectives in the attack mounting phase: reconnaissance, initial access, and persistence.

In the second phase of the attack, which we call attack progression, the adversary exploits vulnerabilities in the system to expand its control from the initial foothold towards its objectives. There are four tactical objectives in this phase: discovery, lateral access, standard protocol misuse, and defense evasion.

In the ultimate phase of the attack life cycle, the adversary hopes to achieve its main goals. The tactical objectives in this phase are thus related to information collection and other attack impact.

6.7 5G Threat Modeling using STRIDE Framework

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. Sattar et al. [37] used the STRIDE threat modeling methodology to analyze risks associated with 5G slicing.

Hasan et al. [25] discussed the security and privacy issues of vehicle-pedestrian communication in 5G technology and analyzes the threat model of such applications using the STRIDE model. The objective of such a model is to help researchers and practitioners build secure V2P systems running over 5G networks.

The 5G network data analytics function (NWDAF) is a crucial 3GPP standard method. It efficiently collects data from user equipment, network functions, operations, administration, and maintenance (OAM) systems within the 5G Core, Cloud, and Edge networks. This wealth of data is then utilized for powerful 5G analytics, enabling better insights and actions to enhance the overall end-user experience. NWDAF promotes the rapid development of artificial intelligence and big data technology in the field of 5G communication. In order to analyze the security challenges faced by NWDAF in the open 5G network operating environment, Wang et al. [41] proposed a threat modeling method for NWDAF using the STRIDE framework.

6.8 Summary

This chapter summarizes 5G threat vectors, Modeling 5G Threats as Graphs, Extension of MITRE ATT&CK Framework, A Layered Approach to 5G threat modeling, the BHADRA Framework and 5G Threat Modeling using the STRIDE Framework.

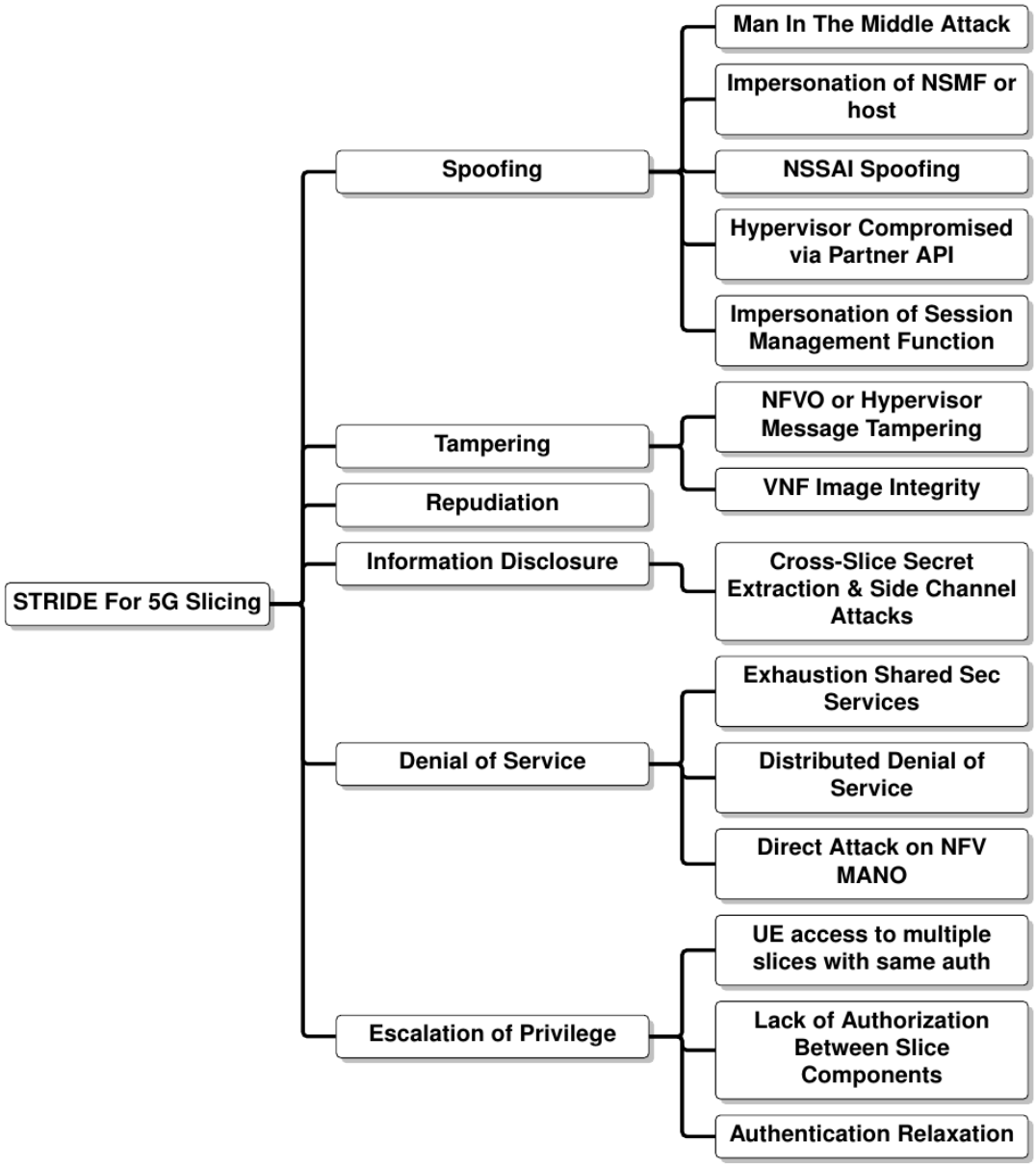

Figure 6.4: STRIDE Threat Model of 5G Network Slicing (Source: [37])

Chapter 7

Conclusion and Future Work

7.1 Conclusion

Adoption of 5G technologies has revolutionized the telecommunication industry with the promise of higher data rate, low latency etc. But it also introduces much wider attack surface - thereby posing significant security concerns. This thesis presents a survey of 5G technologies, 5G threats and vulnerabilities and also different threat modeling approaches specifically engineered for 5G networks. The author has contributed to compiling the works of different contributors mentioned in the bibliography on 5G and its threats and vulnerabilities. This work will benefit future research efforts in designing effective threat models of 5G network.

7.2 Future Work

Future scope of work would include building of a comprehensive attack framework for 5G networks similar in line with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework for enterprise networks.

Bibliography

[1] 5g mobile networks: A systems approach. https://github.com/SystemsApproach/5G. Accessed: 2023-05-20.

[2] 5g system overview. https://www.3gpp.org/technologies/5g-system-overview. Accessed: 2023-05-20.

[3] The cyber kill chain framework. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed: 2023-05-20.

[4] Iriusrisk. https://www.iriusrisk.com/threat-modeling-platform. Accessed: 2023-10-01.

[5] Microsoft threat modeling tool. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool. Accessed: 2023-10-01.

[6] The mitre att&ck framework. https://attack.mitre.org/. Accessed: 2023-05-20.

[7] Mulval: Multi-host, multi-stage vulnerability analysis tool. https://github.com/risksense/mulval. Accessed: 2023-09-10.

[8] Owasp threat dragon. https://owasp.org/www-project-threat-dragon/. Accessed: 2023-10-01.

[9] Sd elements. https://www.securitycompass.com/sdelements/. Accessed: 2023-10-01.

[10] securicad. https://nse.digital/pages/guides/Creating%20threat%20models/securiCAD.html. Accessed: 2023-10-01.

[11] Threat modeler. https://threatmodeler.com/. Accessed: 2023-10-01.

[12] Tutamen threat model automater. https://www.tutamantic.com/. Accessed: 2023-10-01.

[13] K. S. Adu-Manu, G. A. Koranteng, and S. N. A. Brown. Perspective chapter: 5g enabling technologies – revolutionizing transport, environment, and health. In S. Goundar, editor, *Edge Computing*, chapter 8. IntechOpen, Rijeka, 2023.

[14] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. 5g security: Analysis of threats and solutions. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 193–199, 2017.

[15] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, 2018.

[16] A. K. M. Bahalul Haque, T. Nausheen, A. Al Mahfuj Shaan, and S. A. Murad. *Security Attacks and Countermeasures in 5G Enabled Internet of Things*, pages 127–149. Springer Nature Singapore, Singapore, 2023.

[17] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines. 5g network slicing using sdn and nfv: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167:106984, 2020.

[18] S. A. Bjerre, M. W. Klæbel Blomsterberg, and B. Andersen. 5g attacks and countermeasures. In *2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pages 285–290, 2022.

[19] P. Chen, L. Desmet, and C. Huygens. A study on advanced persistent threats. In B. De Decker and A. Zúquete, editors, *Communications and Multimedia Security*, pages 63–72, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[20] S. Chen, C.-N. Lee, and M.-F. Lee. Realization of 5g network slicing using open source softwares. In *Proceedings of the 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pages 1549–1556, Taiwan, 2020. Asia-Pacific Signal and Information Processing Association (APSIPA).

[21] R. Dangi, P. Lalwani, G. Choudhary, I. You, and G. Pau. Study and investigation on 5g technology: A systematic review. *Sensors*, 22(1), 2022.

[22] A. Dutta and E. Hammad. 5g security challenges and opportunities: A system approach. In *2020 IEEE 3rd 5G world forum (5GWF)*, pages 109–114. IEEE, 2020.

[23] D. Fang, Y. Qian, and R. Q. Hu. Security for 5g mobile wireless networks. *IEEE access*, 6:4850–4874, 2017.

[24] M. N. I. Farooqui, J. Arshad, and M. M. Khan. A layered approach to threat modeling for 5g-based systems. *Electronics*, 11(12), 2022.

[25] R. Hasan and R. Hasan. Towards a threat model and privacy analysis for v2p in 5g networks. In *2021 IEEE 4th 5G World Forum (5GWF)*, pages 383–387, 2021.

[26] R. Hussain, F. Hussain, S. Zeadally, and J. Lee. On the adequacy of 5g security for vehicular ad hoc networks. *IEEE Communications Standards Magazine*, 5(1):32–39, 2021.

[27] M. Khuntia, D. Singh, and S. Sahoo. Impact of internet of things (iot) on 5g. In *Intelligent and Cloud Computing: Proceedings of ICICC 2019, Volume 2*, pages 125–136. Springer, 2021.

[28] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, 2015.

[29] H. S. Lallie, K. Debattista, and J. Bal. A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, 35:100219, 2020.

[30] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain. Network slicing for 5g: Challenges and opportunities. *IEEE Internet Computing*, 21(5):20–27, 2017.

[31] F. Liu, J. Peng, and M. Zuo. Toward a secure access to 5g network. In *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, pages 1121–1128. IEEE, 2018.

[32] S. Noel, P. D. Rowe, S. Purdy, M. Limiero, T. Lu, and W. Mathews. Mission-focused cyber situational understanding via graph analytics. In *2018 10th International Conference on Cyber Conflict (CyCon)*, pages 427–448, 2018.

[33] R. F. Olimid and G. Nencioni. 5g network slicing: A security overview. *IEEE Access*, 8:99999–100009, 2020.

[34] R. Pell, S. Moschoyiannis, and E. Panaousis. Multi-stage threat modeling and security monitoring in 5gcn. In L. Maglaras and I. Kantzavelou, editors, *Cybersecurity Issues in Emerging Technologies*, chapter 4. CRC Press, Boca Raton, 2021.

[35] S. P. Rao, H.-Y. Chen, and T. Aura. Threat modeling framework for mobile communication systems. *Computers & Security*, 125:103047, 2023.

[36] B. Santos, L. Barriga, B. Dzogovic, I. Hassan, B. Feng, N. Jacot, V. T. Do, and T. Van Do. Threat modelling for 5g networks. In *2022 International Wireless Communications and Mobile Computing (IWCMC)*, pages 611–616, 2022.

[37] D. Sattar, A. H. Vasoukolaei, P. Crysdale, and A. Matrawy. A stride threat model for 5g core slicing. In *2021 IEEE 4th 5G World Forum (5GWF)*, pages 247–252, 2021.

[38] P. Schneider and G. Horn. Towards 5g security. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1165–1170. IEEE, 2015.

[39] A. A. A. Solyman and K. Yahya. Evolution of wireless communication networks: from 1g to 6g and future perspective. *International Journal of Electrical and Computer Engineering*, 12(4):3943, 2022.

[40] S. Sullivan, A. Brighente, S. A. Kumar, and M. Conti. 5g security challenges and solutions: a review by osi layers. *IEEE Access*, 9:116294–116314, 2021.

[41] H. Wang, Y. Lin, and W. Li. Research on threat modeling for 5g network data analytics function. In *2022 International Conference on Networks, Communications and Information Technology (CNCIT)*, pages 171–178, 2022.

[42] J. Śliwa and M. Suchański. Security threats and countermeasures in military 5g systems. In *2022 24th International Microwave and Radar Conference (MIKON)*, pages 1–6, 2022.