Threat Modelling Framework for 5G Mobile Networks

Thoai Van Do

Master Thesis
Informatics: Programming and System Architecture
60 credits

The Faculty of Mathemathics and Natural Sciences
Department of Informatics

UNIVERSITY OF OSLO

November 2023

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisors, Prof. Carsten Griwodz, Prof. Paal Engelstad and Prof. Boning Feng, for having trust in me and accepting to be my supervisors. I sincerely appreciate the guidance and support you have provided me with during the work with my Master thesis.

Secondly, I would like to thank Dr. Bernardo Flores, Dr. Bruno Dzogovic and van Thuan Do at the Secured 5G4IoT lab at OsloMet, for introducing me to 5G technology and Threat Intelligence and for giving me useful advice and comments which helped me to complete my Master thesis.

Finally, I would like to mention with profound gratitude, the endless support and motivation that my parents, brothers and entire family always provides me with.

Abstract

As 5G gained momentum and became a critical communication infrastructure for a variety of vertical applications, it is exposed to the constantly increasing number of cyber threats. Traditional perimeter defence and signature-based detection using Indicator of Compromise (IoC) is no longer efficient against APT attacks. To combat APT attacks and any other emergent attacks, it is necessary to understand the motivations and behaviors of the attackers, their tactics, techniques, and procedures. To accomplish this, threat modelling and analysis plays a key role. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is an attack-centric threat modelling framework which is most appropriate for 5G networks. Unfortunately, MITRE ATT&CK does not provide sufficient support to model attacks on 5G networks.

This Master thesis work studies, proposes and implements a Threat Modelling Framework for 5G networks by introducing extensions to the current MITRE ATT&CK. The work also includes an analysis of state-of-the art threat modelling framework and is completed with a validation of the implemented framework.

Executive Summary

Due to its low latency, high speed, reliability, consistency and adaptability, 5G has become a critical infrastructure of choice for vertical markets like automotive, industry, agriculture and manufacturing while previous mobile generations just provided voice and data for domestic and business use. 5G is now playing a crucial role in society and any disruption, even very short ones could be fatal. Consequently, it is at utmost importance to protect 5G against cyber-attacks.

As 5G fulfils its commitment of connecting, in addition to smart phones, billions of IoT devices that could be either of Machine Type Communication or Ultra Reliable and low latency type, it exposes itself to a considerably larger surface attack that can be exploited by malicious attackers. Further, attacks are getting more sophisticated and well camouflaged such that each attack is a new zero-day attack capable of bypassing traditional signature-based detection. The use of Indications of Compromise (IoCs) is no longer sufficient to provide protection against zero-day attacks or Advanced Persistent Threats (APTs).

To complement IoCs, it is essential to understand the behaviour of the attacker i.e., the actor responsible for the attack, its tactics, techniques and procedures (TTPs). Consequently, a sound and efficient Threat Modelling Framework is urgently demanded, especially for the virtualized 5G networks. MITRE ATT&CK is currently one of the best threat modelling frameworks to model sophisticated threats such as Advanced Persistent Threats (APT), however it does not sufficiently address mobile networks.

This Master thesis work address the challenges and demands mentioned above and defines its problem statement as *"How to elaborate an efficient Threat Modelling Framework for 5G mobile networks".*

The work starts with a literature review of the background knowledge which ensures readability of this thesis. Next, a thorough study of related works is carried out to identify what has been done such that repetition of the same work can be avoided and usable results can be applied. To build a sound and effective threat modelling platform, an analysis of threats on 5G networks is performed to acquire deep understanding of the threats on 5G networks. The work continues then with the design of a conceptual model of the Threat Modelling Framework. The next chapter of the thesis thoroughly

presents the implementation and realization of the Threat Modelling Framework, which is an extension of the MITRA ATT&CK supporting 5G networks. Finally, a thorough validation is done to complete the work. The thesis is finished with a conclusion and a suggestion for future works.

Table of Contents

Acronyms

5G	Fifth Generation Mobile Network
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
SIM	Subscriber Identity Module
CMTMF	CONCORDIA Mobile Threat Modelling Framework
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
ICS	Industrial Control Systems
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoC	Indicators of Compromise
IoT	Internet of Things
JSON	JavaScript Object Notation
LTE	Long-Term Evolution
MEC	Multi-Access Edge Computing
MTC	Machine Type Communication
NR	5G New Radio
SDN	Software Defined Network
STIX	Structured Threat Information Expression

TAXII	Trusted Automated Exchange of Intelligence Information
TTP	Tactics, techniques and procedures
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications Service
URLLC	Ultra Reliable and low latency Communication
VNF	Virtual Network Function
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

Chapter 1 Introduction

1.1 Motivation

The fifth generation of mobile networks or simply 5G mobile networks have been deployed worldwide at an accelerating high speed, and since 2019 until today 5G is operational in more than 60 countries and the number keeps increasing every day. Due to its low latency, high speed, reliability, consistency and adaptability 5G has become a critical infrastructure of choice for vertical markets like automotive, industry, agriculture and manufacturing while previous mobile generations just provided voice and data for domestic and business use. 5G is now playing a crucial role in society and any disruption, even very short ones could be fatal. Consequently, it is at utmost importance to protect 5G against cyber-attacks.

As 5G fulfils its commitment of connecting, in addition to smart phones, billions of IoT devices that could be either of Machine Type Communication (MTC) or Ultra Reliable and low latency (URLL) type, it exposes itself to a considerably larger surface attack that can be exploited by malicious attackers. Further, attacks are getting more sophisticated and well camouflaged such that each attack is a new zero-day attack capable of bypassing traditional signature-based detection. The use of Indicators of Compromise (IoCs) is no longer sufficient to provide protection against zero-day attacks or Advanced Persistent Threats (APTs). In fact, IoCs are forensic data gathered and shared from systems that have been breached and are hence less useful in the detection of brand new and sophisticated cyber attacks.

To complement IoCs, it is essential to understand the behaviour of the attacker i.e. the actor responsible for the attack, its tactics, techniques and procedures (TTPs). Consequently, a sound and efficient Threat Modelling Framework is urgently demanded, especially for the virtualized 5G networks. MITRE ATT&CK is currently one of the best threat modelling frameworks to model sophisticated threats such as Advanced Persistent Threats (APT), however it does not sufficiently address mobile networks.

Indeed, as software mobile networks, 5G networks are not only subject to the same cyber threats as regular enterprise networks but are also exposed to the ones brought by its capability of providing

connectivity to billions of IoT devices ranging from primitive sensors to advanced medical equipment requiring ultra-reliable and low-latency connections. Potential attackers of 5G networks have different behaviors, tactics and techniques that require extensions to the current MITRE ATT&CK framework. The Bhadra framework [0] is the first attempt to extend the MITRE ATT&CK framework for mobile networks, which emphasizes the need for modelling threats in mobile networks but is unfortunately too simple and incompatible with the mainstream MITRE ATT&CK framework. The second proposal is the CONCORDIA Mobile Threat Modelling Framework (CMTMF) [0], which is a compatible combination of the enterprise, mobile and ICS (Industrial Control Systems) matrices of the MITRE ATT&CK framework. However, the work in CONCORDIA is still at early stages and lacks details about tactics and techniques. Most importantly, it is not yet integrated in the MITRE ATT&CK Framework.

1.2 Problem Statement

To address the challenges and demands mentioned above, this work has defined its problem statement as follow:

"How can an effective Threat Modelling Framework for 5G mobile networks be elaborated?"

The problem stated above can be decomposed into the following sub-problems:

Sub-problem 1: *"Are the existing Threat Modelling Framework suitable for modelling cyber threats in 5G networks?"*

Sub-problem 2: *"How can the MITRE ATT&CK Framework be extended to support the modelling of threats to the 5G mobile networks?"*

Sub-problem 3: *"How can a cyber attack on the 5G mobile network be modelled using the extended MITRE ATT&CK Framework?"*

1.3 Research Method

The scientific research method [4] is used in the Master thesis work and consists of the following steps:

- Identification of research problem
- Literature review
- Specifying the purpose of research
- Determining specific research questions

- Specification of a conceptual framework
- Design and Implementation of the conceptual model solution
- Reporting and evaluating research
- Communicating the research findings and recommendations

1.4. Structure of the dissertation

This dissertation is structured as follows:

- **Chapter 1 Introduction** presents the motivation behind this work, defines the problem and sub-problems statements as well as the followed methodology to achieve the purpose of this work.
- **Chapter 2 Background** provides a background for better understanding of all related topics needed for this work.
- **Chapter 3 Related works** summarises all the works that are related to this current work.
- **Chapter 4 Analysis of threats on 5G networks** identifies and analyses all threats on 5G networks.
- **Chapter 5 Study of state-of-the-art Threat Modelling Frameworks** provides a comprehensive study of existing Threat Modelling Frameworks and identify the most appropriate framework for 5G networks.
- **Chapter 6 Design of a conceptual model** elaborates a conceptual model of the proposed framework.
- **Chapter implementation of the Threat Modelling Framework for 5G Networks** describes thoroughly the implementation of the framework proposed by this work.
- **Chapter 7 Validation** conducts a validation of the work to ensure the quality of the implementation.
- **Chapter 8 Conclusion** concludes the work and suggests future works on threat modelling.

1.5 Scientific contribution

At the end of this Master thesis work a paper has been submitted, accepted and published at the international conference MobiWis 2023 as follows:

- *Thoai van Do et all:* ***MITRE ATT&CK threat modelling extensions for mobile threats****; 19th International Conference, MobiWIS 2023 Marrakech, Morocco, Lecture Notes in Computer Science - ISBN 978-3-031-39763-9 ISBN 978-3-031-39764-6 (eBook), August 14–16, 2023*

Thoai van Do is the main author of the paper and did 80% of both the work described in the paper and also the elaboration of the paper itself. The paper is presented in Scientific contribution, the last part of this thesis.

Chapter 2 Background

In this chapter, we present a brief overview of mobile networks. Next, the 5G network is introduced along with security challenges related to 5G networks. We also present the general objectives and benefits to threat modelling, existing threat modelling approaches and justification for which one is most appropriate for the threat modelling of mobile networks. Additionally, the chapter provides a thorough description of the Structured Threat Information Expression (STIX™) which is a structured language for describing cyber threat information. TAXII (Trusted Automated Exchange of Intelligence Information), an application protocol for exchanging Cyber Threat Intelligence (CTI) over HTTPS is also explained thoroughly together with JSON (JavaScript Object Notation), an open standard file format and data interchange format.

2.1 Briefly about mobile networks

Mobile networks, also known as cellular networks, are telecommunication networks designed to provide wireless communication services to mobile devices. This now includes smartphones, tablets, laptops, and Internet of Things (IoT) devices. Mobile networks enable voice calls, text messages, and data transmissions which enable mobile devices to connect to the internet.

Mobile networks consist of a **network of base stations** or cell towers distributed over geographical areas called ***cells*** as shown in Figure 1. Each base station provides coverage to a specific area, which enables mobile devices to stay connected while moving. As mobile devices move, they connect to different nearby base stations to maintain their connections.

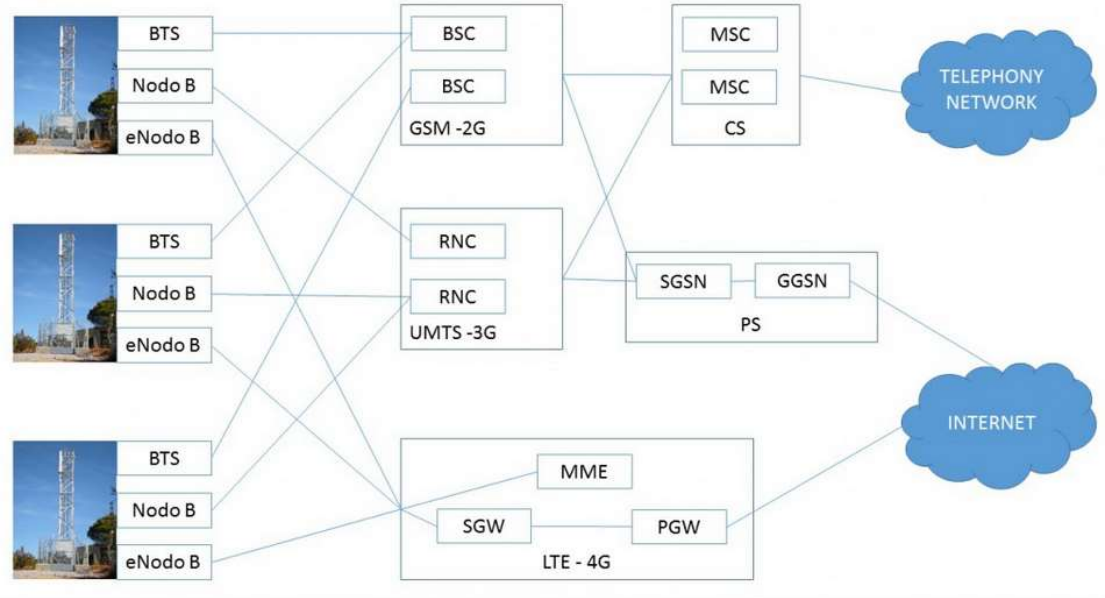

Figure 1 Overall architectures of mobile networks

Mobile networks use specific radio frequencies allocated by regulatory authorities for wireless communication. Frequencies vary by region and are divided into bands for different purposes, including voice and data transmission. Mobile devices, such as smartphones and tablets have built-in radio transceivers that enable communication with nearby base stations. These devices use Subscriber Identity Module (SIM) to identify and authenticate users on the mobile network.

The core network of a mobile operator includes infrastructure for routing calls, handling data traffic and managing user authentication and billing.

Mobile networks use a variety of protocols, including GSM(2G), UMTS(3G), LTE(4G) and NR(5G), to provide different levels of service, speed, and capabilities. Each generation offers improvements in data speed, latency, and network efficiency.

2.2 5G networks

2.2.1 Overall Architecture

5G networks have the common characteristics of a mobile network, however it comes with fundamental differences with its predecessors, 4G, 3G and 2G. The earlier generations of mobile networks were intended merely for mobile phones. On the other hand, the ultimate objective of 5G is to support a wide variety of devices, ranging from data-hungry smart phones to Massive Machine Type Communication (mMTC) e.g., primitive IoT (Internet of Things) or sensors and Ultra-Reliable Low Latency Communications (URLLC) necessary for autonomous driving, remote control in factories, remote surgery, etc. [0]

To be able to meet these requirements, state-of-the-art technology like Cloud-Native, Software Defined Radio, Network Function Virtualization and Multi-Access Edge Computing (MEC) enable 5G to realize its core concept called Network slicing.

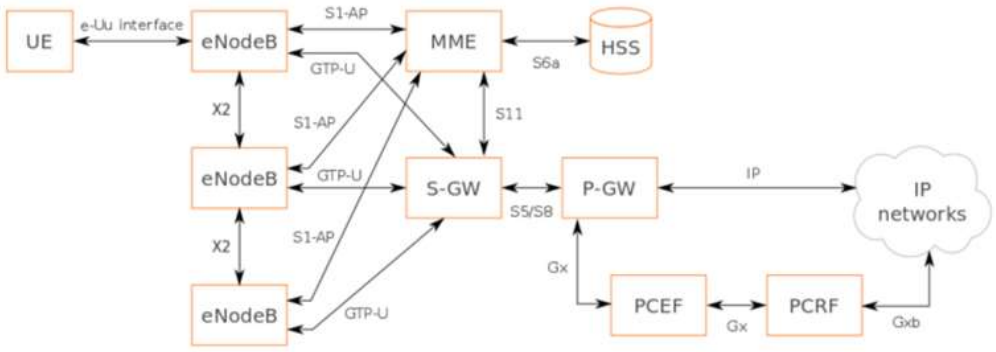

Figure 2 The 4G LTE Network Architecture (courtesy: YateBTS)

The building blocks of 5Gs predecessors are ***network elements***, physical entities which are built upon dedicated hardware devices running specific functional software and executing standardized communication protocols as shown in Figure 2. Mobile operators can reconfigure their networks by adding, moving, and removing network resources to meet the demands, however this could be tedious and time-consuming. The management and operation of traditional mobile networks are complicated and resource demanding.

5G mobile networks fundamentally differs from its predecessors as they are no longer composed of physical network elements, but rather made of ***Virtual Network Functions (vNF)*** which are software components running generic processors. Instantiating and connecting a set of vNFs together using SDN (Software Defined Networking), enables virtual networks to be dynamically created [5]. SDN enables dynamic, programmatically efficient network configuration to improve work performance and monitoring.

The 5G network is a **softwarised network** that can also be cloudified i.e. its vNFs are moved from local servers to datacenters in the cloud. An example of the cloudification of the 5G network is shown in Figure 3. Depending on the needs the vNFs can be dynamically instantiated and executed in the edge cloud, regional cloud, or central cloud.

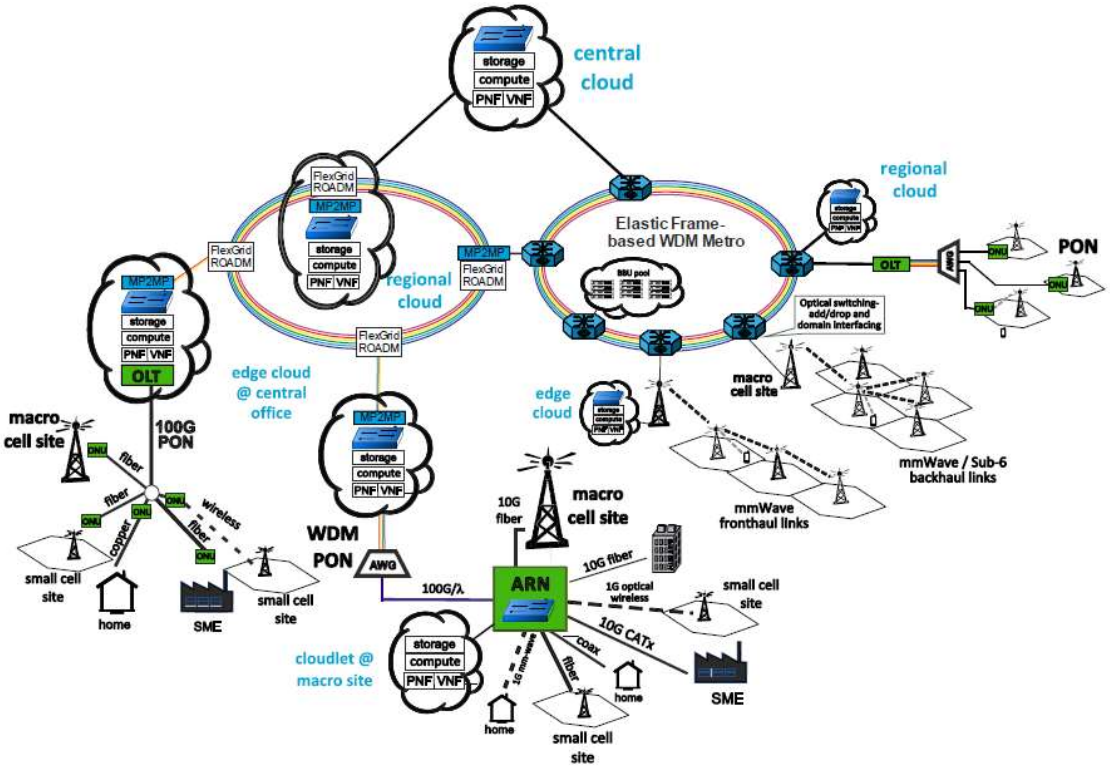

Figure 3 Physical architecture of a converged fixed-mobile network for 5G

2.2.2 Network Slicing

By instantiating and connecting a set of vNFs together using SDN (Software Define Networking) a virtual network can be dynamically created. SDN technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring [0].

Such a virtual network constitutes the fundament of the concept of Network Slicing in 5G network. In fact, as stated in [0] *"to realize network slicing, network slice logically consists of dedicated or shared network functions (NFs) of 5G SA network and resources by utilizing emerging technologies such as virtualization so as to provide required network capability".*

By instantiating several network slices with different QoS characteristics on the same physical infrastructure the 5G network succeeds in supporting the various device and application types with different requirements such as massive Machine Type Communication (mMTC) as shown in Figure 4.

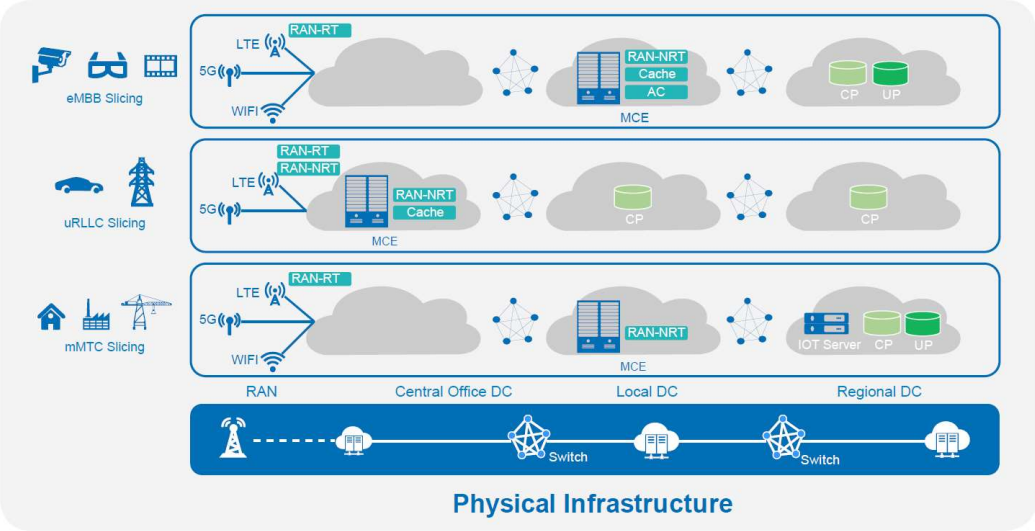

Figure 4 Network slicing in 5G network (Courtesy: Huawei)

2.2.3 Automation and autonomy

Since network slices are composed of software components, they can be created not only dynamically but also automatically without the intervention of human being by a programmable controller offered by a Framework for control, management and orchestration (MANO) of network functions as shown in Figure 4.

As a further advancement 5G networks can evolve from being programmable and automated to autonomous i.e., becoming self-CHOP (Configure, Heal, Optimize, Protect) via the use of Artificial Intelligence (AI)/Machine Learning (ML) as described by ETSI [8].

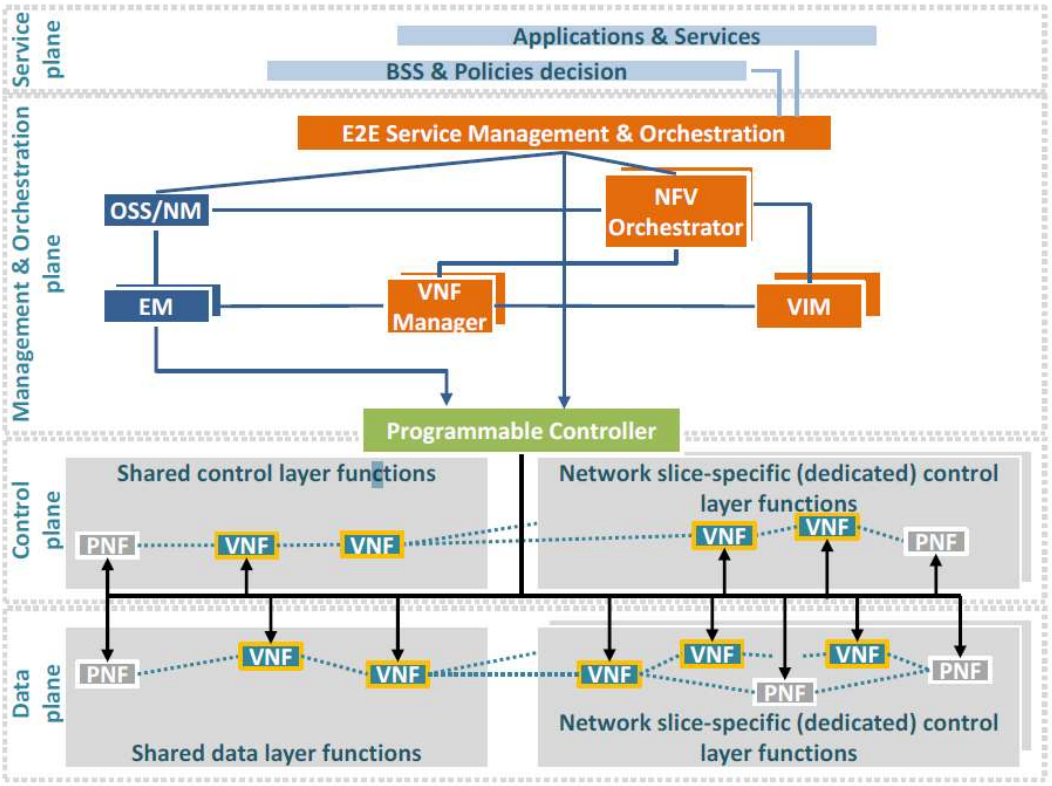

Figure 5 Framework for control, management and orchestration of network functions [9]

2.4 Structured Threat Information eXpression (STIX)

Structured Threat Information eXpression (STIX) is a collaborative and community-driven effort to define and develop a structured language to represent cyber threat information [11][12]. The main goal is to enable organizations to share cyber threat intelligence in a consistent and machine-readable manner. In addition, the STIX language is designed to improve other capabilities such as collaborative threat analysis, automated threat exchange and automated detection and response. The STIX language attempts to convey the full range of cyber threat information by providing structured representations of cyber threat information that is expressive, flexible, extensible, automatable, and readable.

To sufficiently defend against determined cyber adversaries, organizations must maintain a cyber threat intelligence capability as a key part of their defence. Cyber Intelligence includes understanding and characterizing information such as:

- What sort of attack actions have occurred and are likely to occur?
- How can these actions be mitigated?

- Who are relevant threat actors?
- What are they trying to achieve?
- What are their capabilities, in the form of tactics, techniques and procedures (TTP) they have leveraged over time and are likely to leverage in the future?
- What sort of vulnerabilities, misconfigurations, or weaknesses they are likely to target?
- What actions have they taken in the past?

To achieve this capability, information sharing between partners, peers and other trusted parties is a necessity. However, the immense volumes of complex cyber security information organizations face today raises a need for common, structured representations of this information to enable tractability.

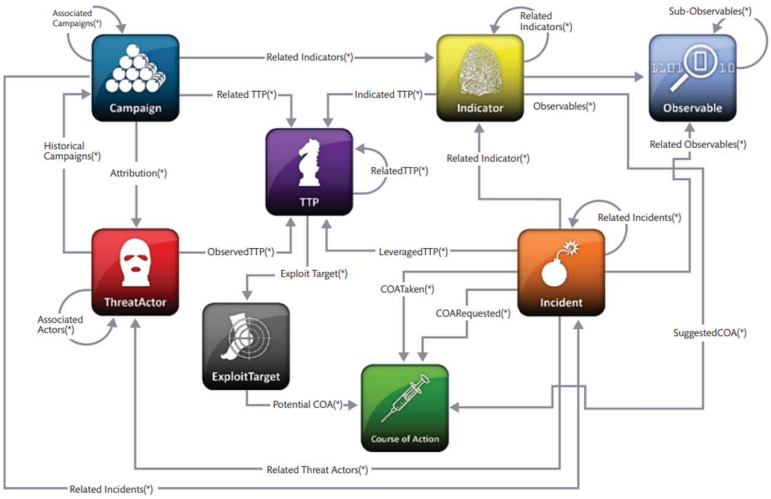

Figure 6 STIX Architecture.

STIX provides a unifying architecture tying together a diverse set of cyber threat information. At a high level, the STIX language consists of the following key constructs:

1. Observables – describing what has or might be seen e.g., network traffic occurs to specific IP addresses or email from a specific address is observed.
2. Indicators – describing potential observables with attached meaning and context.
3. Incidents – describing instances of specific adversary actions.
4. Adversary Tactics, Techniques and Procedures – describing attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, and other methods adversaries may use.
5. Exploit Targets – describing vulnerabilities, weaknesses or configurations that might be exploited.

6. Courses of Action – describing response actions that may be taken in response to an attack or as a preventative measure.
7. Campaigns – describing sets of Incidents and/or TTP with a shared intent.
8. Threat Actors - describing identification and/or characterization of the adversary.

STIX defines 18 STIX Domain Objects (SDOs) and 2 STIX Relationship Objects (SROs) shown in Figure 7 and Figure 8. The STIX Domain Objects categorize each piece of information with specific attributes to be populate. Chaining multiple STIX Domain Objects together through STIX Relationship Objects enables both simple and complex representations of Cyber Threat Intelligence (CTI).

Object	Name	Description
	Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets.
	Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence.
	Grouping	Explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context).
	Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Infrastructure	Represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.).
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
	Location	Represents a geographic location.
	Malware	A type of TTP that represents malicious code.
	Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

	Note	Conveys informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
	Observed Data	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
	Opinion	An assessment of the correctness of the information in a STIX Object produced by a different entity.
	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
	Threat Actor	Actual individuals, groups, or organizations believed to be operating with malicious intent.
	Tool	Legitimate software that can be used by threat actors to perform attacks.
	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

Figure 7 Description of the 18 STIX Domain Objects (SDOs)

Object	Name	Description
	Relationship	Used to link together two SDOs or SCOs in order to describe how they are related to each other.
	Sighting	Denotes the belief that something in CTI (e.g., an indicator, malware, tool, threat actor, etc.) was seen.

Figure 8 Description of the 2 STIX Relationship Objects (SROs)

To ensure that this solution maintains practicality for any single use case, appropriate and numerous flexibility mechanisms are designed into the language, i.e., almost everything in STIX is optional such that any single use case can leverage only the portions of STIX that are relevant for it.

In contrast to STIX 1.0, STIX 2.0 specifies JavaScript Object Notation (JSON) as the “Mandatary To Implement” (MTI) serialization.

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:23.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Figure 9 Example of a STIX 2.1 Campaign object

2.5 TAXII

Trusted Automated Exchange of Intelligence Information (TAXII™) [13] [15] is an application protocol for exchanging CTI over HTTPS. TAXII was specifically designed to support the exchange of CTI represented in STIX, however TAXII can also be used to share data in other formats. TAXII defines a RESTful API and a set of requirements for TAXII Clients and Servers. As shown in the following figure, TAXII defines two primary services, Collections and Channels to support a variety of sharing models.

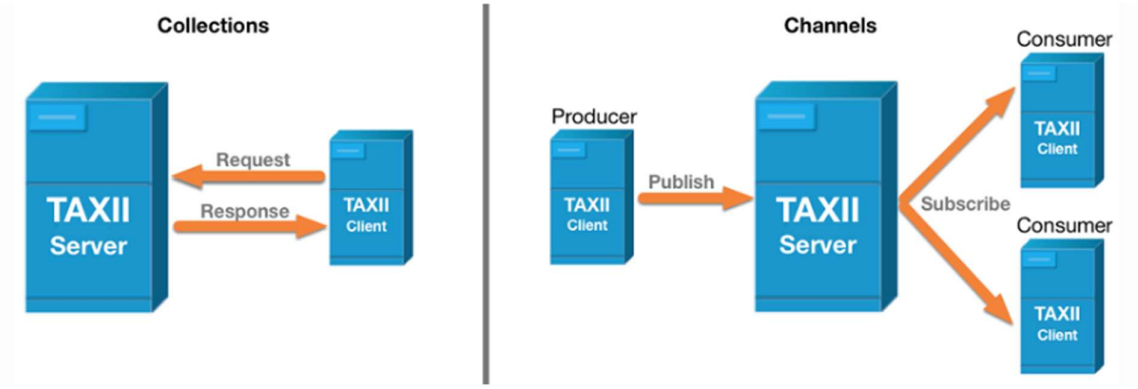

Figure 10 The two sharing models defined by TAXII

A Collection is an interface to a logical repository of CTI objects provided by a TAXII Server, allowing a producer to host a set of CTI data that can be requested by consumers. In Collections, TAXII Clients and Servers use a request-response model to exchange information. A channel allows producers to push data to many consumers who may receive data from many producers. In Channels, TAXII Clients exchange information in a publish-subscribe model.

It is important to note that STIX and TAXII are independent standards: the structures and serializations of STIX do not rely on any specific transport mechanism, and TAXII can be used to transport non-STIX data.

2.6 JSON

JSON (JavaScript Object Notation) is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays (or other serializable values). It is a common data format with diverse uses in electronic data interchange, including that of web applications with servers.

JSON is a language-independent data format. It was derived from JavaScript, but many modern programming languages include code to generate and parse JSON-format data. JSON filenames use the extension .json.

JSON is a lightweight data-interchange format which makes it is easy for humans to read and write and for machines to parse and generate. JSON is built on two structures:

1. A collection of name/value pairs. In various languages, this is realized as an object, record, struct, dictionary, hash table, keyed list, or associative array.
2. An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

In JSON, an object is an unordered set of name/value pairs. An object begins with "{" (left brace), and ends with "}" (right brace). Each name is followed by ":" (colon) and the name/value pairs are separated by "," (comma), as shown in Figure 11.

Figure 11 Example of a JSON representation of a person

The MITRE ATT&CK dataset is available in STIX 2.0 and STIX 2.1, which is required to implement support for JSON for serializations. The MITRE ATT&CK dataset has a flat JSON structure. The types within this JSON are the following (as well as the common wording used for this type):

- attack-pattern (Techniques)
- relationship (This is a unique type that contains relationships between types)
- course-of-action (Mitigations)
- identity (unused)

- intrusion-set (Actors or Groups)
- malware (Malware)
- tool (Tools)
- x-mitre-tactic (Tactics)
- x-mitre-matrix (MITRE ATT&CK MATRIX)(unused)
- marking-definition (unused)

Chapter 3 Related works

This chapter gives an overview of all existing works that are closely related to this thesis work and some of their results are used in the elaboration of a Threat Modelling Framework for 5G networks.

3.1 THE BHADRA THREAT MODELLING FRAMEWORK

The Bhadra Threat Modelling Framework is the first attempt in 2020 to build a threat modelling framework dedicated to mobile communication systems [1]. The framework consists of 8 tactics and 47 techniques that are classified into the three phases **Mounting**, **Execution** and **Results.** The biggest limitation of the framework lies in the fact that is neither aligned with the Mitre Enterprise Matrix nor the Mitre Mobile Matrix, making it difficult to use.

Since the first version presented in 2020 however, there has been one more update to the framework adding 5 more techniques and 1 more tactic, but as presented by the author in [80], the framework only accounts for 4G networks and it is quite difficult to model an attack when considering 5G networks and IoT devices in both the Network and Application layers.

3.2 THE MITRE FIGHT MATRIX

Recognising the differences between a 5G network and an enterprise network, MITRE created a new matrix called FIGHT [14] which is "a globally accessible knowledge base of adversary tactics and techniques used or potentially used against 5G networks. FIGHT adds an addendum to ATT&CK for Enterprise content that has different characteristics in the context of 5G networks, but otherwise remains largely the same. FIGHT contains 15 tactics and 88 technics, which only address the threats on 5G networks and not the ones on the mobile devices. Although FIGHT includes relevant techniques related to 5G networks it is not yet integrated in the MITRE ATT&CK framework and is not accessible from ATT&CK Workbench and ATT&CK Navigator.

3.3 THE CONCORDIA MOBILE THREAT MODELLING FRAMEWORK (CMTMF)

The CONCORDIA Mobile Threat Modelling Framework (CMTMF) [18] is more aligned with the MITRE Enterprise matrix and has 14 tactics. The techniques from the mobile matrix represented by red boxes are merged with the one of the Enterprise matrices in yellow boxes. The CMTMF also includes

the techniques proposed by the Bhadra framework represented by purple boxes. Since it is not sufficient with the current techniques, additional CONCORDIA techniques have been proposed.

Since one tactic can be repeated several times in an attack, CMTMF introduced the notion of **phase** which corresponds to the phases in a kill chain of an APT (Advanced Persistent Threat) attack.

Some phases of an attack in mobile networks can be recursive e.g., they can spread to multiple devices, so CMTMF introduced the notion of **loops** to describe this attack behavior.

The CMTMF is integrated in the open-source threat sharing platform MISP and its current tactics and techniques are incorporated as a MISP galaxy. An attack can easily be translated to IoCs (Indicators of Compromise) and shared in the mobile cyber security community. Unfortunately, the CMTMF is not integrated and adopted in the MITRE environment.

Chapter 4 Analysis of threats on 5G networks

This chapter partially addresses Sub-problem 1: *"Are the existing Threat Modelling Frameworks suitable for modelling cyber threats in 5G networks"*. Indeed, in order to conclude whether a Threat Modelling Framework is usable in the modelling of 5G networks it is essential to have a firm understanding of threats in 5G networks.

We can classify the threats in 5G networks into two dimensions. The first dimension consists of all the threats which are related to the virtualization of the mobile network such as issues related to the hosting of virtual Network Functions (vNFs) in the cloud. The second dimension consists of the threats on the mobile network itself. Let us now consider successively these two dimensions.

4.1 5G Threats on the virtualization dimension

The goal of the fifth generation (5G) mobile cellular network is to meet the requirements of broadband access everywhere, high user and device mobility, and connectivity of massive number of devices (e.g., the Internet of Things) in an ultra-reliable and affordable way [19].

To meet these requirements, technologies such as software defined networking (SDN), network function virtualization (NFV) and mobile edge computing serve as some of the fundamental building blocks of 5G. The convergence to these technologies extends many of the security challenges and opportunities applicable to SDN/NFV and cloud to 5G networks [20].

4.1.1 Network functions virtualization (NFV)

Network functions virtualization (NFV) enables network slicing by replacing network functions on appliances such as routers, load balancers, and firewalls with virtualized software instances that run on commodity hardware. Virtual network functions (VNFs) are utilized to run these functions as packaged software that sits on virtual machines (VMs). Virtualization can lead to vulnerabilities such as denial of service and malware.

Security Challenges introduced by NFV

Although NFV provides 5G with the flexibility to meet all the requirements from a variety of vertical applications, the concept introduces several challenges related to the characteristic of VNF as follows:

Virtualisation: As a software component NFV has potential software vulnerabilities or it can be a malware itself. Since NFVs are hosted in the cloud attackers can make use of the existing vulnerabilities of the hypervisor to get access to the virtual computing and storage to compromise the confidentiality, integrity or availability of VNFs [21].

In virtualised implementations all VNFs are implemented using a common software platform such as OpenStack, Kubernetes and the code core will be largely identical. Consequently, software vulnerability in one VNF may likely exist in other VNFs increasing the risk of cascading security failure [22].

While vendors may produce tweaked variants, the code core will be largely identical. Similarly, host OS, hypervisor and VNFs software will be identical or from a limited set of variants. What this means is that if an attacker is able to identify software vulnerability in one VNF, that vulnerability will likely exist in many other VNFs making the attackers job much easier and increases the risk of a cascading security failure in the network.

Management and Orchestration

The main role of Management and Orchestration (MANO) is to create, configure, operate and monitoring the network slices and their corresponding VNFs. A lack of consistency in the management and orchestration of the network services can create serious security problems. The MANO constitutes hence a single point of failure and an attractive target for attack since any disruption may lead to the failure of the entire mobile network.

Administration and access control

The adaptability of 5G relies on the openness and programmability of the NFVs which are provided by different types of APIs such as internal network functions, internetworking interfaces, roaming interfaces, etc. exposed in different layers of the network. A weak administration and access control to NFVs could incur catastrophic consequences to the 5G mobile network.

4.1.2 Software-defined networking (SDN)

Software-defined networking (SDN) utilizes network management to separate the control plane from the forwarding plane. SDNs enable programmable network controls and abstract the underlying infrastructure from the apps and network services. Centralized and controllable, SDNs provide the

agility required to adapt to the evolving needs of 5G microservices. SDNs are susceptible to attacks such as forwarding device attacks, control plane threats, API vulnerabilities, counterfeit traffic flows, and more.

Security Challenges introduced by SDN [23]

Software-Defined Networking (SDN) uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN differs from traditional networks, which use dedicated hardware devices such as routers and switches to control network traffic. SDN can create and control a virtual network or control traditional hardware via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network or to connect devices on different physical networks to create a single virtual network, SDN enables a new and very practical way of controlling the routing of data packets through a centralized server. Unfortunately, SDN also brings vulnerabilities that could be critical for the mobile network.

Control plane

The centralized control plane server is the brain of SDN ensuring the availability, reliability and security of the network services. Consequently, it is a single point of failure which may be exposed to attacks like network monitoring, IP address spoofing, DDoS attacks, Virus, worms and Trojan attacks.

Application layer

The application layer will provide a variety of complex network application services through application programming and management strategy and is exposed to threats like malicious applications and security rule conflicts between applications.

4.1.3 Expanded attack surface

The arrival of 5G offers a wide range of connectivity supporting various devices. These devices range from data-hungry smartphones to primitive sensors and high precision devices requiring ultra-reliable and low latency connections. According to Statista, “the number of Internet of Things (IoT) devices worldwide is forecast to almost double from 15.1 billion in 2020 to more than 29 billion IoT devices in 2030” [24].

Billions of connected devices with considerably less security features raises concerns regarding security [25], e.g., IoT requires updating software on millions of connected devices that are inherently not as secure. Additionally, 5Gs promise to deliver lightning-fast speeds and ultra-low

latency paves the way for numerous mission-critical use cases such as smart cars, telemedicine, remote surgery, and more. For these use cases a lack of security is simply not an tolerable, as it could lead to grave consequences such as potential loss of human life.

The quickly expanding attack surface through billions of devices, generating huge amounts of data, has dramatically changed the cyber threat landscape. The traditional cyber security perimeter defence based on securing the perimeter of a network from cyber threats is no longer sufficient. This calls for a new cyber security strategy, namely Threat Intelligence and Threat Modelling which is a holistic approach that identifies and analyses the evolving threat landscapes and provides mitigations to cyber threats [26].

4.2 Threats on the 5G mobile network dimension

Although enhancements have been in 5G networks to strengthen security and privacy considerably compared to 4G networks, the new 5G capabilities and features such as the support of a wider variety of devices and applications, virtualization and cloudification, interfacing with multiple vertical sectors, etc. has introduced new threats to the 5G networks.

To get an overview of the threats to 5G networks, it is essential to identify all the entry points to the 5G network. Additionally, it is necessary to derive and analyse all the possible threats at these entry points. The following figure shows these entry points which are the mobile devices, the access network, the core network and the external services and applications.

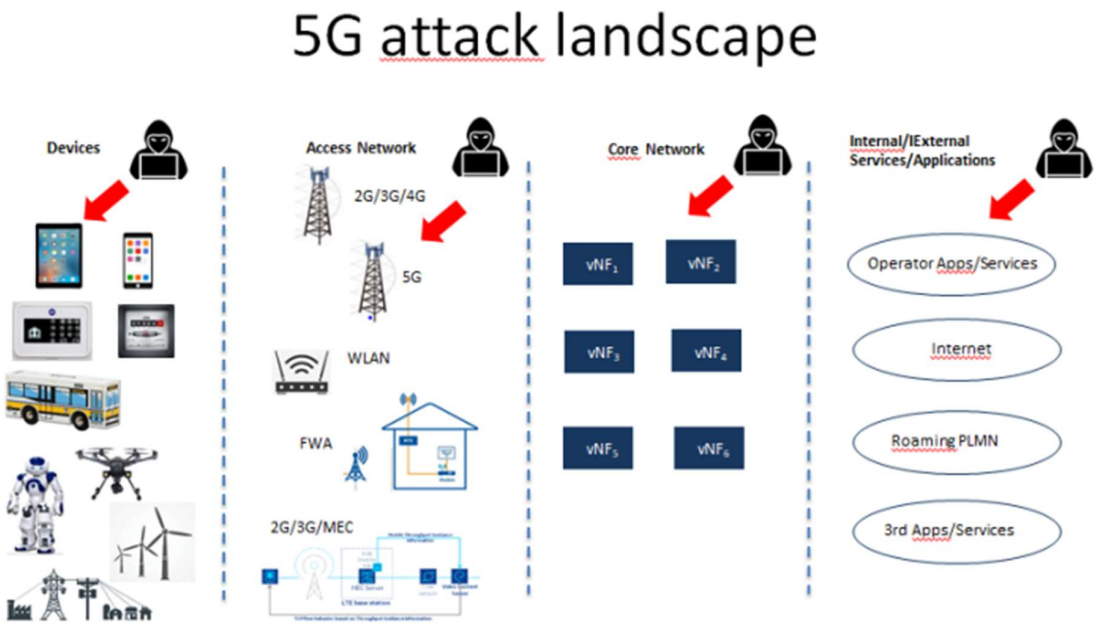

Figure 12 Attack Entry Points to the 5G network

Mobile devices

As previously mentioned, the predecessors of 5G were intended for mobile devices which at the time were smart phones consisting of two main components, the Mobile Equipment (ME) and the Subscriber Identity Module (SIM). A mobile operator can fully identify a smartphone using the IMSI (International Mobile Subscriber Identity) and the IMEI (International Mobile Equipment Identity) which after successful strong authentication is granted access to the mobile network.

On the other hand, 5G supports an open range of devices ranging from primitive sensors to powerful supercomputers, which has dramatically changed the threat landscape. Mobile operators no longer have knowledge of what kind of devices are operating in their networks, as the authentication process only verifies that the device has a legitimate subscription (IMSI) but cannot tell whether the device is benign and trustful or malicious and distrusting. As such, a large number of infected devices have the potential to flood and take the mobile network down. So far there is no countermeasure to stop such a flooding attack because the devices are already inside the network.

In the case that it is not possible to stop a flooding attack once it has been initiated, the only solution may be to detect and prevent it before its initiation. To enable the detection and prevention of such threats it is crucial to understand the behaviours of the devices and most importantly the techniques, tactics and knowledge of the potential attackers.

Access Network

The Access Network of 5G networks is exposed to the same physical threats as its predecessors due to the common characteristic of an access network, which is its huge geographical coverage making their protection quite challenging. Base stations and antenna masts are scattered around and are exposed to physical threats such as theft and vandalism. Furthermore, new threats are introduced with the new 5G capabilities and features such as local breakout allowing IP packets of roaming subscribers to be sent directly to the Internet from the visited network and MEC (Multi-Access Edge Computing). Direct interfacing with third parties at the access network could be a vulnerability that can be exploited by adversaries.

Core Network

The Core Network in 5G networks is composed of software components. Therefore, as other software it is vulnerable to cyber threats such as data confidentiality, data privacy, key security, and encryption application-level authentication. Security measures must be identified and designed meticulously to protect the Core Network. Most mobile operators tend to use private clouds instead of public multi-tenant cloud, however virtualization and cloudification bring other challenges such as

side-channel attacks, flooding attacks, hypervisor hijacking, malware injection, and virtual machine (VM) migration related attacks.

Internal/External Services/Applications

5G networks have interfaces with the Internet and third parties in addition to the traditional interfaces with other mobile networks and interfaces with their own applications and services. Therefore, adequate perimeter defence such as firewalls, border control gateways, secure gateways, etc. must be deployed to protect the mobile network without disrupting legitimate traffic to flow.

Chapter 5 Study of state-of-the-art Threat Modelling Framework

Chapter 5 also addresses Sub-problem 1: "*Are the existing Threat Modelling Frameworks suitable for modelling cyber threats in 5G networks*" since it investigates whether there is state-of-the art Threat Modelling Framework suitable for 5G network.

5.1 Definition of Threat Intelligence

There is uniform definition of the term "intelligence" but in the work intelligence is defined as information about threats and threat actors that provides sufficient understanding to mitigate a harmful event.

CrowdStrike [27] defines threat intelligence as *"data that is collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours"*.

The continuously evolving nature of cyber threats and modern threat landscapes poses a challenge for organizations to quickly adapt and take decisive actions. The threat intelligence lifecycle is a framework to enable teams to optimize resources and effectively respond to deal with this challenge.

5.2 The importance of threat intelligence modelling

To understand why threat intelligence modelling is important, it is necessary to understand the state-of-the art cyber attacks and their evolution compared to a few decades ago.

5.2.1 Increase in number of cyber attacks

According to Embroker [28] *"cyber attacks have been rated the fifth top rated risk in 2020 and become the new norm across public and private sectors. This risky industry continues to grow in 2022 as IoT cyber attacks alone are expected to double by 2025. Plus, the World Economic Forum's 2020 Global Risk Report states that the rate of detection (or prosecution) is as low as 0.05 percent in the U.S."*. It is expected that the number of cyber attacks will be exploding and if nothing is done the damages will be severe and could potentially lead to the loss of lives.

5.2.1 Increase in variants of cyber attacks

Since the appearance of the worm arriving as attachment in email in the late 1990s, cyber attacks have evolved not only in numbers and variants but also in the level of sophistication and severity. The level of severity is defined by the US Cybersecurity & Infrastructure Security Agency (CISA) in which the level severe (Red) is likely to result in significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties [29].

While cyber attacks are growing in numbers, their variability are also increasing enormously and it is necessary to classify them into main types in order to recognize, detect and mitigate them. An attempt to classify cyber attacks is done by Sullivan, M [30] and can be briefly summarized as follows:

1. **Malware:** includes a variety of cyber threats including Trojans, viruses and worms. It is realized by code with malicious intent that typically steals data or incurs damages to computers. Malware is usually introduced to a system through email attachments, software downloads or operating system vulnerabilities.
   The best countermeasure against malware are user awareness and deployment of robust and updated firewalls and deep packet inspection which detect and enable blocking of the penetration of malicious data files to the enterprise network.
2. **Phishing:** is a technique for attempting to acquire sensitive data through a fraudulent solicitation in e-mail, on a website, SMS, or social medias, in which the perpetrator masquerades as a legitimate business or reputable person, NIST [31]. Phishing is getting sophisticated, and it is quite difficult to differentiate legitimate information requests from malicious phishing. For example, phishing emails containing a link that upon clicking will initiate information stealing.
   To prevent phishing, companies recommend users to be careful and not to surrender their personal information. It may be actual to do verification, i.e., telephone verification of messages from the sender.
3. **Password Attacks:** Malicious parties try to gain access to user's system by cracking their password. Attackers try to crack your password by using many methods including brute force attacks built to guess passwords as well as comparing various word combinations against a thesaurus file. Strong passwords or multi-factor authentication are the way to safeguard against password attacks. It is also a good practice to change passwords at regular intervals.
4. **Denial-of-Service (DoS) Attacks:** focuses on blocking services delivered by a system or network by flooding them with a large volume of requests such that they get overloaded and stop functioning. There are a few variants of DoS, but the most common is distributed denial of service (DDoS), in which multiple devices are used to generate a large number of service

requests. DDoS attacks are very difficult to stop once they happen. The only way is probably to detect and block them at an early stage.

5. **“Man in the Middle” (MITM):** By impersonating both parties of an online information exchange, the MITM attackers can obtain and alter the exchanged information for their benefit. The best way to prevent MITM attacks is to conduct mutual authentication of the communicating parties combined with encryption of the communication.
6. **Drive-By Downloads:** Legitimate websites infected by malware can download a small snippet of code to visitor’s computer without requiring any action from the user. After installation on the user’s computer, the malware will communicate with an alien server to download the rest of the program. To prevent this type of attack, users should set up higher levels of security on their browser and remove unused features.
7. **Malvertising:** Malware is distributed to users via an advertising network. When users click on one of these ads, malware will be downloaded to their computers. Any website can be subject to malvertising without knowing. The best way to avoid this kind of attack is common sense and being suspicious of tempting ads.
8. **Rogue Software:** is malware that is disguised as legitimate and necessary security software for the protection of the user’s system. The users are requested to update their security software and by accepting, rogue software is downloaded to their computer. Firewalls and anti-virus software are the tools to prevent rogue software.
9. **Ransomware:** is a type of malware that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them [32].

Before rounding up the description of cyber attack types, it is worth noting that the mentioned classification of attacks is at a very high level and attacks can be quite different even though they belong to the same type. In fact, it is quite seldom that the same attack is replayed without any modification because it will be detected and blocked.

5.2.3 Level of Severity

Cyber attacks can produce from minor operation disruptions to devastating damages to both private consumers and enterprises. These can be categorized in five areas as follows:

- Financial losses

- Loss of productivity
- Reputation damage
- Legal liability
- Business continuity problems

Lately, ransomware attacks are more frequent and by the end of 2016, in average one business became victim to a ransomware attack every 40 seconds. Ransomware attacks rose by 92.7% in 2021 compared to 2020 levels, with 1,389 reported attacks in 2020 and 2,690 in 2021, Security Magazine [33]. The total cost of all cybercrime damages in 2021 is expected to amount to about $6 trillion worldwide, Cybercrime Magazine [34].

5.2.4 Level of sophistication

Current attacks are very sophisticated and consist quite often of more than one single step, in addition to being spread in time and space. They also employ advanced tools to evade detection and blocking. Typical examples of sophisticated attacks are Advanced Persistent Threats (APT) attacks, characterized by using sophisticated and concentrated efforts by coordinated attackers targeting a single victim. APT's objective is to infiltrate a system, remain undetected as long as possible, steal as much data as possible and leave quietly without trace.

APTs are particularly difficult to detect and block. Consequently, it is essential to understand the anatomy of an attack. In 2011, Lockheed Martin [35] stated that APTs are so sophisticated that they manage to circumvent all the conventional network defence tools. Lockheed Martin advocate that it is essential to understand the adversaries and their capabilities and proposes to use a "kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense". There are afterwards a few more kill-chain models and the most popular one is the MITRE ATT&CK® [36][37], which is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Unfortunately, although more efficient than traditional intrusion detection mechanisms, the MITRE ATT&CK framework is still lagging behind the attacker's tools and will need to be improved considerably.

5.2.5 Advanced technologies in cyber attacks

While advanced technologies such as Artificial intelligence (AI) and Machine Learning (ML) are used by the security community to provide better protection for enterprise networks, the same technologies are also used by cyber attackers to generate sophisticated attacks, evade detection, and bypass classic defences. Some examples are as follows:

- CAPTCHA, which has the objective to differentiate human beings from robots is no longer complex enough because ML models are quite efficient in solving the operations challenged by CAPTCHA.

However, models are now remarkably efficient in solving such operations. Even if developers have been trying to make CAPTCHA ever more challenging to recognize and crack, it is now a losing game for defenders, even for big platforms such as Amazon.

- ML automates brute force attacks. Hackers can now generate password lists automatically.
- New kinds of phishing attacks: ML can be used to tailor the target profile on any social platform and initiate phishing automatically.
- Adversaries can fool the machine by injecting contaminated data into the data set. For example, by adding or removing a few details in medical images, attackers can dupe ML programs that check medical images for evidence of cancer, making the correct diagnosis hard and potentially impossible for both machines and humans.

5.2.6 Hostile nations

As illustrated in Figure 13, cyber attacks are no longer carried out by young curious hackers or motivated individuals but mostly by organized crime groups or hostile nations that possess a vast amount of resources. After identifying a target, they can use time and resources to try and retry attacks until they succeed. To combat these hostile actors is currently almost impossible for individuals and small medium enterprises. More efficient and affordable security tools are urgently needed.

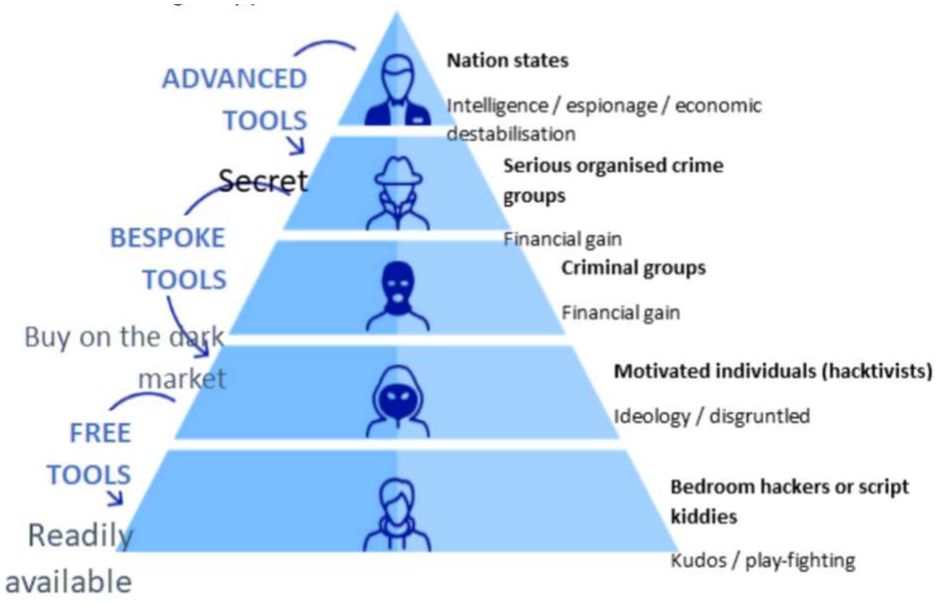

Figure 13 Attackers Pyramid from https://www.e-motec.net/worried-about-foreign-state-actors-hacking-cars

5.3 Threat Modelling

"*Threat modelling is the activity aiming at identifying, understanding and making simple descriptions or models of the potential threats and attack vectors that a system could be exposed for such that risk analyses, detection methods, countermeasures, and mitigation strategies can be developed*" [3].

A threat modelling framework generally includes five components, namely threat intelligence, asset identification, mitigation capabilities, risk assessment and threat mapping. As shown in "A review of threat modelling approaches for APT-style attacks" by Tatam et al. from 2021 [38], there are different approaches to threat modelling. These include:

- Asset-centric threat modelling, which focus on the assets of the target system
- Threat-centric or attacker-centric threat modelling, which focus on the attackers and attacks
- Data-centric threat modelling, which focus on the data of the target system
- System-centric threat modelling, which focus on the target system

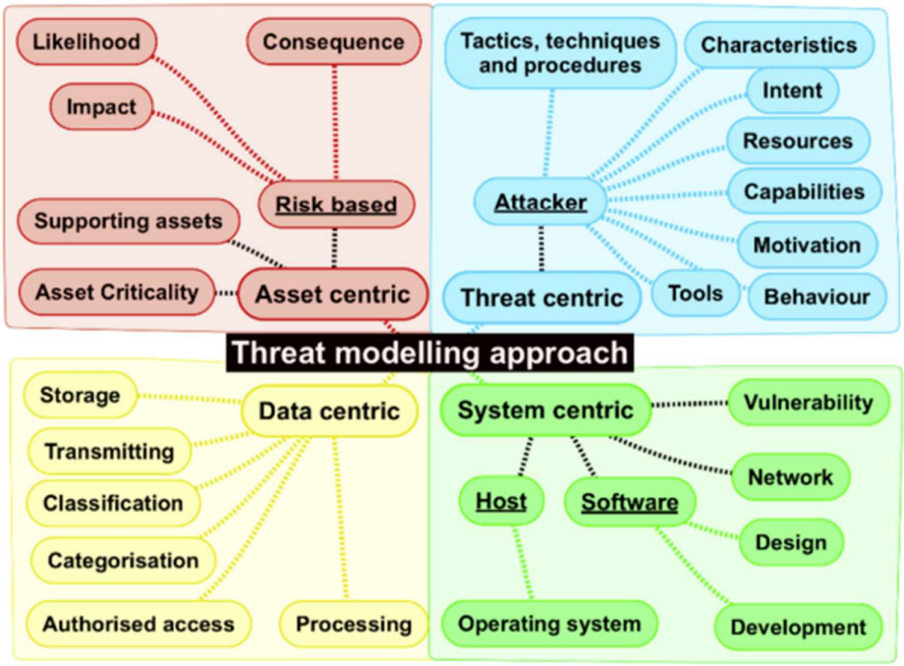

Figure 14 Threat Modelling Approaches

Let us now evaluate the most dominant threat Intelligence Frameworks and determine whether any of them could be used in the modelling of threats in the 5G networks.

5.3.1 STRIDE

STRIDE is a threat modelling framework created by Praerit Garg and Loren Kohnfelde at Microsoft [39] with the intention to guide the discovery of threats in a system. It is hence a system centric threat modelling framework which is used along with a model of the target system. It is most effective for the evaluation of individual systems.

STRIDE provides a mnemonic for security threats in six categories as follows:

- **Spoofing of user identity:** a user or program pretends to be another
- **Tampering with data:** attackers modify components or code
- **Repudiation:** threat events are not logged or monitored
- **Information disclosure (privacy breach):** data is leaked or exposed
- **Denial of Service (DOS):** services or components are overloaded with traffic to prevent legitimate use
- **Elevation of privilege:** attackers grant themselves additional privileges to gain greater control over a system

The threat modelling with STRIDE consists of the following steps:

1. A decomposition of the system into relevant components
2. An analysis of each component related to their exposition to threats and mitigations. This step is repeated for all the components until all the threats are identified and mitigations are provided.

Evaluation: For a 5G Core network with a dynamic set of VNFs connected through an adaptive SDN, it is challenging but still possible to identify all the components and to identify the threats to them.

The problem lies on the access network due to the large number of heterogeneous and unidentified devices. Indeed, seen from the mobile operator a legitimate mobile device connected to the 5G network is merely one equipped with a legitimate Subscriber Identity Module. Nothing can be said whether it is trustable or malicious and ready to attack the network. Consequently, it is not feasible to analyse all the mobile devices.

Further, 5G vertical applications are quite diversified and their ability to protect themselves against cyber attacks could pose cascading problems to the 5G networks. Unfortunately, applications are beyond the knowledge and control of mobile operators and no decomposition nor analysis can be done.

Conclusion: STRIDE or any other system centric threat modelling frameworks are not suitable for 5G networks.

5.3.2 Trike

Trike [40] is a security audit framework for managing risk and defense through threat modelling techniques. Trike is a risk-based threat modelling framework which requires the definition of the system, the enumeration of the system's assets, actors, rules, and actions to build a requirement model. Trike generates a step matrix with columns representing the assets and rows representing the actors. Every matrix cell has four parts to match possible actions (create, read, update, and delete) and a rule tree — the analyst specifies whether an action is allowed, disallowed, or allowed with rules.

Trike builds a data-flow diagram mapping each element to the appropriate assets and actors with the requirements defined. The analyst uses the diagram to identify denial of service (DoS) and privilege escalation threats.

Trike assesses attack risks using a five-point probability scale for each CRUD action and actor. It also evaluates actors based on their permission level for each action i.e., always, sometimes, or never.

Evaluation: Due to the lack of control of mobile devices connected to the access network and the heterogeneous vertical applications, it is not possible to perform a definition of the 5G mobile network system and an enumeration of its components.

Conclusion: Trike or any other asset-centric threat modelling frameworks are not suitable for 5G mobile networks.

5.3.3 NIST threat modelling guide

The U.S. National Institute of Standards and Technology (NIST) in 2016 published its own data-centric threat modelling methodology that focuses on protecting high-value data within systems [41]. It models aspects of attack and defense for selected data. In this model, risk analysis is conducted using the following four significant steps:

1. Identify and characterize the system and data of interest.
2. Identify and select the attack vectors to be included in the model.
3. Characterize the security controls for mitigating the attack vectors.
4. Analyze the threat model.

The guide is targeted at security managers, security engineers/architects, system administrators, auditors, and others responsible for the security of systems and data. According to the authors, "the

intent is not to replace existing methodologies, but rather to define fundamental principles that should be part of any sound data-centric system threat modelling methodology.

Data-centric system threat modelling is needed because of the dynamicity of cyber security. Both the attack and defence sides are constantly changing. To follow general best practices for security is not sufficient to safeguarding high value data which needs to additional security measures.

Evaluation: Data-centric threat modelling framework is only intended as a supplement of other framework in-use in order to enhance the protection of high value confidential data.

Conclusion: Data-centric threat modelling should be used in addition to another threat modelling framework to improve the protection of high-value data.

5.4 MITRE ATT&CK

MITRE ATT&CK, abbreviation for "Adversarial Tactics, Techniques and Common Knowledge" is defined by MITRE as a "curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target" [37].

ATT&CK is a threat or attack centric threat modelling framework. ATT&CK is a behavioral model that consists of core components such as Tactics, Techniques and Sub-techniques, Procedures and Groups.

1) **Tactics, the "Why"**

"Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical objective: the reason for performing an action [36]. Tactics serve as useful contextual categories for individual techniques, which cover standard notations for actions made by adversaries during an operation. These actions include things such as persisting, discovering information, moving laterally, executing files and exfiltrating data. Within ATT&CK, tactics are treated as tags where techniques and sub-techniques are tagged with one or more tactics depending on the different results achieved by their use.

2) **Techniques, the "How"**

"Techniques represent the "how" an adversary achieves a tactical objective by performing an action. Techniques may also represent "what" an adversary gains by performing an action" [1]. For a given tactic, there may be several techniques to achieve the tactical objective. Therefore, multiple techniques may be grouped into each tactic category.

3) **Sub-Techniques**

Techniques may be further broken down into more specific descriptions of how specific behaviour achieves an objective. Given that there are multiple ways to perform a technique, multiple distinct sub-techniques can be grouped under a technique.

4) Procedures

Procedures are specific implementation adversaries have used for techniques or sub-techniques. In ATT&CK, there are two important aspects to note about procedures. First, a procedure is how an adversary uses techniques and sub-techniques. Secondly, a procedure can span multiple techniques and sub-techniques.

5) Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. In other words, mitigations can be considered as a "What to do" when facing a possible threat.

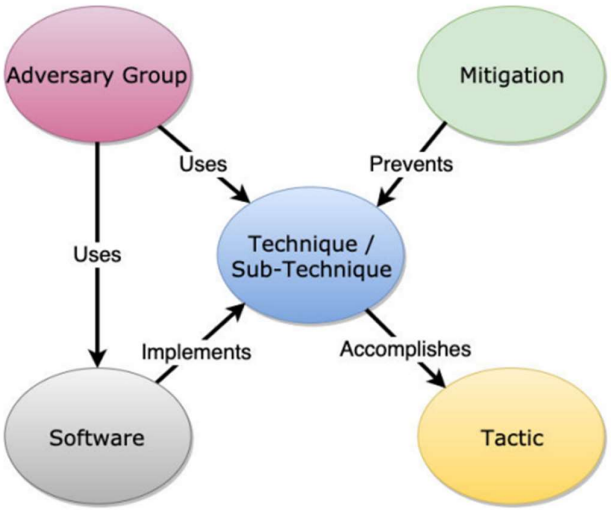

Figure 15 ATT&CK Model Relationships between components

ATT&CK is organized in a set of technology domains, defined as "the ecosystem an adversary operates within that provides a set of constraints the adversary must circumvent or take advantage of to accomplish a set of objectives" [37]. To date there are three technology domains defined:

1. Enterprise, representing traditional enterprise networks and cloud technologies
2. Mobile, for mobile communication devices
3. ICS, for industrial control systems

MITRE ATT&CK includes a set of matrices dedicated to each technology domain. ATT&CK defines multiple platforms within each technology domain, defined as the system the adversary is operating

in, which may be an operating system or application, e.g. Linux, macOS, Android or iOS. Techniques and sub-techniques apply to multiple platforms.

Evaluation: MITRE ATT&CK and any other attack centric threat modelling framework do not require total control of the 5G mobile network system but focus on the attackers, their behaviours, tactics, techniques and procedures, which is feasible for the 5G mobile network.

Unfortunately, MITRE ATT&CK does not fully support the threat modelling for 5G network but only mobile devices. There are currently a few activities on developing new matrices for ATT&CK but they are not yet completed.

Conclusion: MITRE ATT&CK is a promising threat modelling framework for mobile networks, but extensions have to be implemented and integrated in the MITRE ATT&CK environment.

Chapter 6 Conceptual Model of the Threat Modelling Framework for 5G Networks

This chapter addresses Sub-problem 2: “How can the MITRE ATT&CK Framework be extended to support the modelling of threats to the 5G mobile network?”. In the previous chapter the evaluation of threat modelling frameworks has concluded that the MITRE ATT&CK is most appropriate to be adopted and extended to meet the needs from the 5G network. This chapter elaborate a conceptual model of the Threat Modelling for 5G Network. It will also derive the high level functional requirements which will be used later in the validation of the implemented framework.

6.1 Modelling the Threat Modelling Framework for 5G Network

The Threat Modelling Framework for 5G network will be modelled using two UML diagrams, namely use case diagram and class diagram which will be successively presented in the following sections.

6.1.1 Use Case diagram

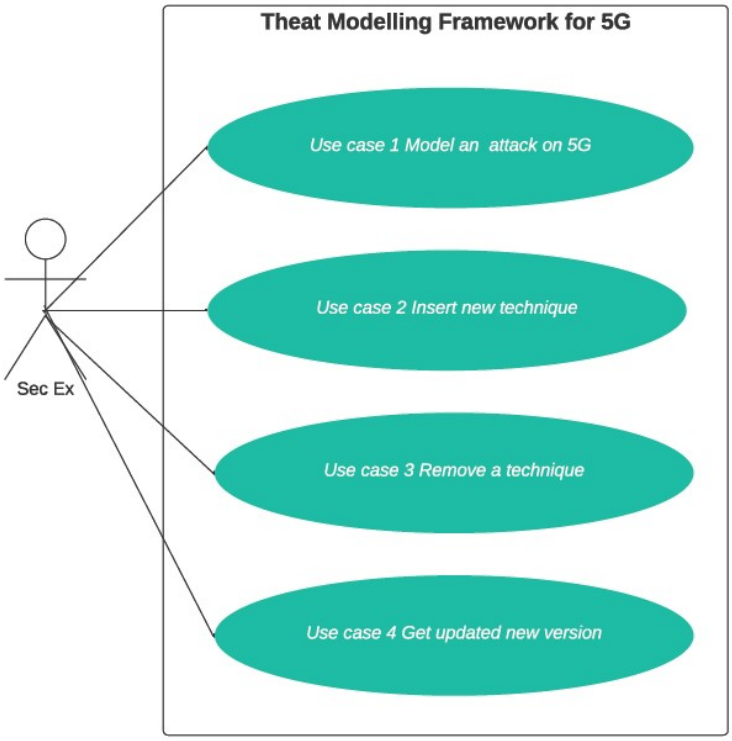

Figure 16 Use case diagram of the Threat Modelling Framework for 5G networks

A use case diagram also referred to as behaviour diagram is used to describe a set of actions i.e., use cases that a system should or can perform in collaboration with one or more external users of the system. The use case diagram can help providing a higher-level view of the Threat modelling Framework and in deriving the high level functional requirements of the framework. It is a graphical depiction of potential user interactions with a system. As shown in Figure 16, use cases are represented by either circles or ellipses.

The Threat Modelling Framework has 6 use cases as shown in Table 1.

Use Case	Requirements
UC1: Design an attack on the 5G network	**R1:** The security expert shall be able to design an attack on the 5G network
UC2: Insert new technique to the threat modelling framework	**R2:** The security expert shall be able to add new technique to the threat modelling framework

UC3: Remove a technique from the threat modelling framework	**R3:** The security expert shall be able to remove a technique from the Threat Modelling Framework
UC4: Get updated a new version	**R4:** The security expert shall be able to initiate an update to get new version of the Threat Modelling Framework

Table 1 Use cases and high level functional requirements of the Threat Modelling Framework

The derived requirements shall be used in the validation phase at the end of the work to verify that the implemented Threat Modelling Framework fulfils the requirements and is hence validated.

6.1.2 Class diagram

A UML Class diagram is static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. The class diagram is the main building block of object-oriented modelling. It is used for general conceptual modelling of the structure of the application, and for detailed modelling, translating the models into programming code.

Class diagram is used in this work to describe the structure of the Threat Modelling Framework. Figure 17 depicts the Class diagram of the matrices and technics of the Threat Modelling Framework. The class 5G Matrix inherits from class ATT&CK Enterprise Matrix. It contains all its tactics and techniques of the ATT&CK Enterprise Matrix but the unused techniques can be removed. Since an attack on the mobile network can be initiated from mobile devices, the 5G Matrix also contains techniques from the ATT&CK Mobile Matrix. Finally, the 5G Matrix shall also include new techniques used in attacks on 5G mobile networks.

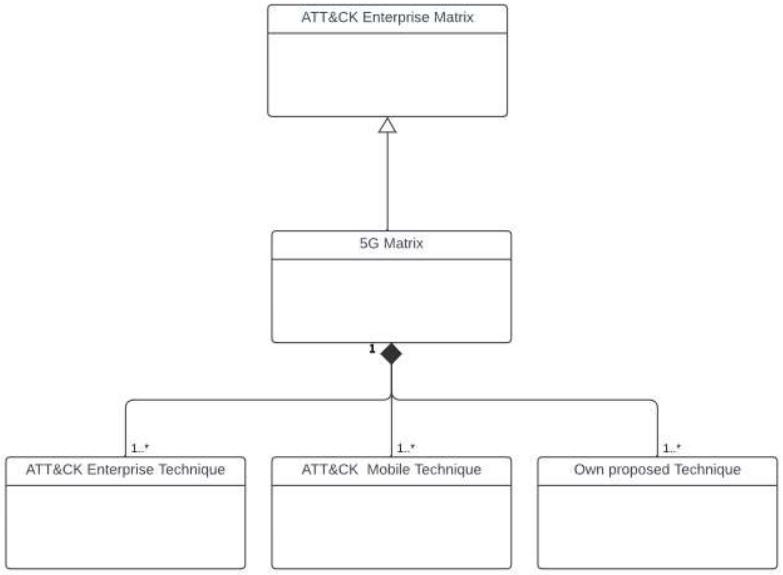

Figure 17 Class diagram of the 5G Matrix

Chapter 7 Implementation of the Threat Modelling Framework for 5G

To carry out the implementation of the conceptual model of the Threat Modelling Framework designed in the previous chapter, a new ATT&CK matrix composed of the ATT&CK Enterprise v13 matrix, the ATT&CK Mobile v13 matrix and also the new techniques that are identified and necessary for the modelling of threat on 5G networks.

The ATT&CK Enterprise v13 matrix is selected to be the fundament of the Threat Modelling Framework for 5G. The techniques from ATT&CK Mobile v13 matrix and new techniques related to 5G will be added to form a new complete matrix suitable for 5G. For this task the ATT&CK Workbench will be used. To perform the modelling of attacks on 5G the ATT&CK Navigator is employed.

This chapter starts with the introduction of the MITRE ATT&CK Enterprise Matrix and ATT&CK Mobile Matrix. The MITRE's tools namely ATT&CK Workbench and ATT&CK Navigator will then be described thoroughly to prepare for the implementation, the main part of the chapter.

7.1 MITRE ATT&CK Enterprise Matrix

The MITRE ATT&CK Matrix for Enterprise contains 14 tactics presented and described in Figure 18. In addition, the relationship between tactics, techniques and sub-techniques are visualized the ATT&CK Matrix in Figure 19.

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Figure 18. Description of ATT&CK Mobile Tactics

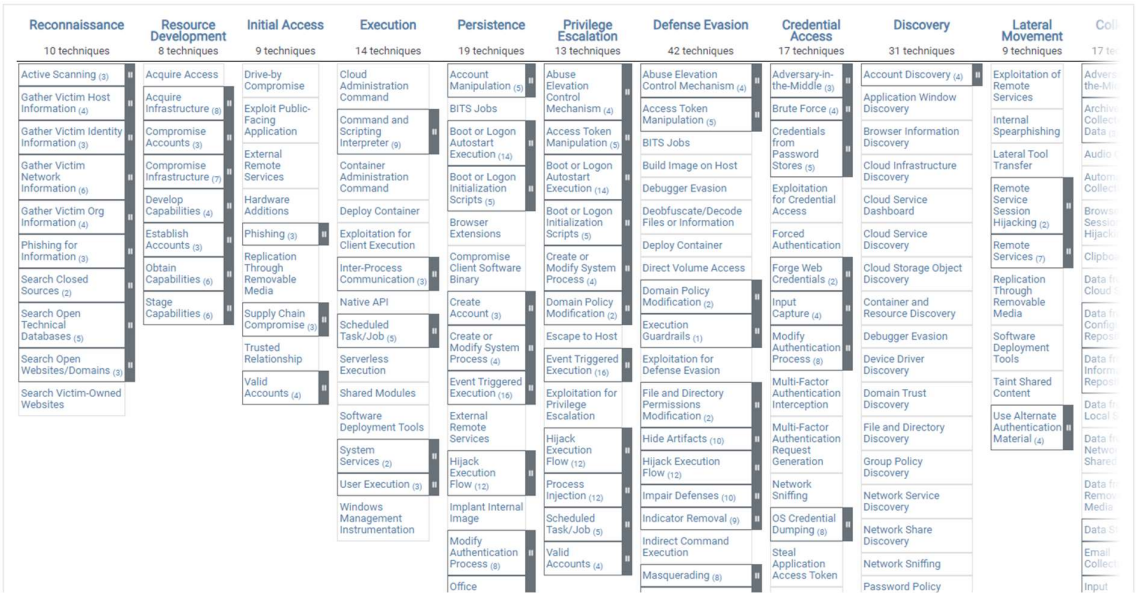

Figure 19. ATT&CK Mobile Tactics and Techniques representing the ATT&CK Matrice for Enterprise

7.2 MITRE ATT&CK Mobile Matrix

The MITRE ATT&CK Matrix for Enterprise contains 12 tactics presented and described in Figure 20. In addition, the relationship between tactics, techniques and sub-techniques are visualized the ATT&CK Matrix in Figure 21.

ID	Name	Description
TA0027	Initial Access	The adversary is trying to get into your device.
TA0041	Execution	The adversary is trying to run malicious code.
TA0028	Persistence	The adversary is trying to maintain their foothold.
TA0029	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0030	Defense Evasion	The adversary is trying to avoid being detected.
TA0031	Credential Access	The adversary is trying to steal account names, passwords, or other secrets that enable access to resources.
TA0032	Discovery	The adversary is trying to figure out your environment.
TA0033	Lateral Movement	The adversary is trying to move through your environment.
TA0035	Collection	The adversary is trying to gather data of interest to their goal.
TA0037	Command and Control	The adversary is trying to communicate with compromised devices to control them.
TA0036	Exfiltration	The adversary is trying to steal data.
TA0034	Impact	The adversary is trying to manipulate, interrupt, or destroy your devices and data.
TA0038	Network Effects	The adversary is trying to intercept or manipulate network traffic to or from a device.
TA0039	Remote Service Effects	The adversary is trying to control or monitor the device using remote services.

Figure 20. Description of ATT&CK Mobile Tactics

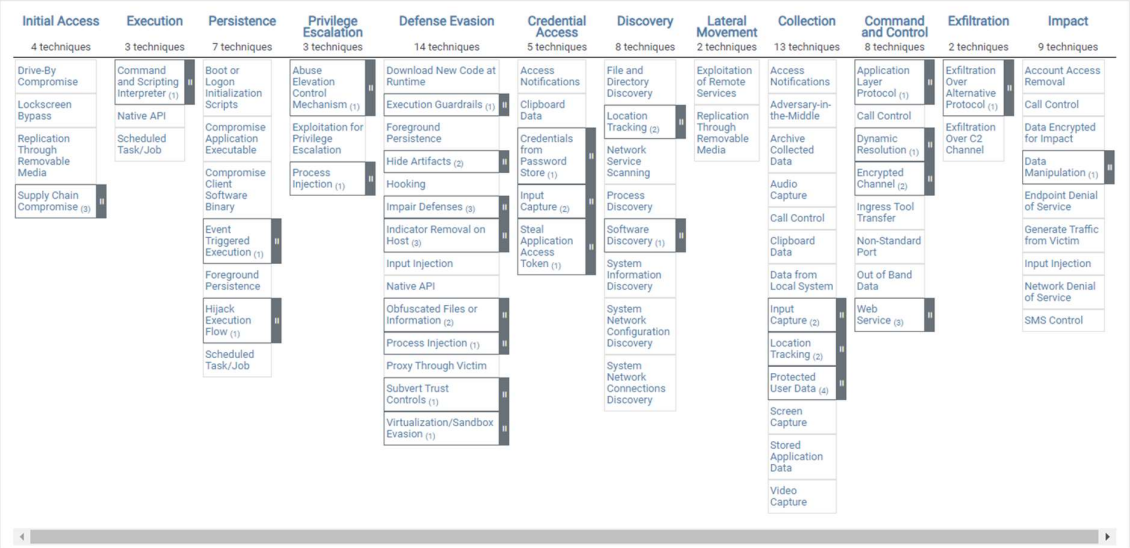

Figure 21. ATT&CK Mobile Tactics and Techniques representing the ATT&CK Matrice for Mobile

7.3 MITRE ATT&CK Workbench

ATT&CK Workbench is an application to explore, create, annotate, and share extensions of the MITRE ATT&CK knowledge base. Users may use ATT&CK Workbench to initialize an instance of the application to serve as the centrepiece to their own customized instance of the ATT&CK knowledge base, attaching related tools and interfaces as desired. ATT&CK Workbench enables extensions of this local knowledge base with new or updated techniques, tactics, mitigation groups and software. In addition, ATT&CK Workbench provides the means to share these extensions with the ATT&CK community [42].

7.3.1 Installation and execution of ATT&CK Workbench

Installing and running ATT&CK Workbench was done in the following steps:

1. Installing prerequisites:
    a. Node.js version 16 or greater from https://nodejs.org/en/blog/release/v16.20.2
    b. Docker Desktop for Windows from https://www.docker.com/products/docker-desktop/ and running it
2. Downloading the required repositories under a common parent directory, which was done with the following commands from the working directory.

```
# download the front-end repository
git clone https://github.com/center-for-threat-informed-defense/attack-workbench-frontend.git
# download the REST API repository
git clone https://github.com/center-for-threat-informed-defense/attack-workbench-rest-api.git
```

3. Navigating to the attack-workbench-frontend directory, which contains the docker-compose.yml file. The command “docker-compose up” builds the necessary Docker images and run the corresponding Docker containers.
4. Accessing the ATT&CK Workbench application is done by visiting the URL “localhost” in a browser with the docker-compose running.

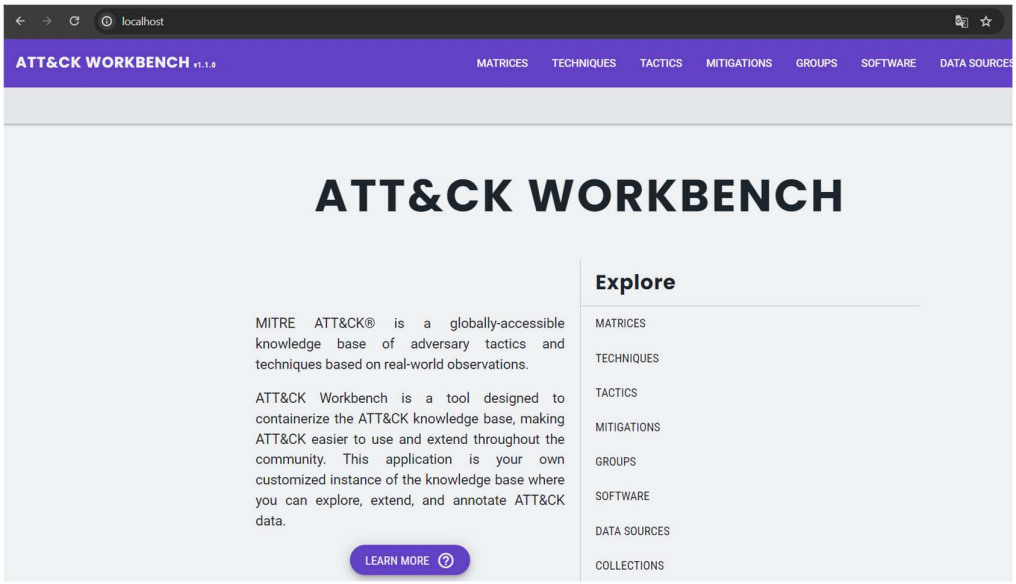

Figure 22 Screenshot of accessing ATT&CK Workbench in browser

7.4 MITRE ATT&CK Navigator

ATT&CK Navigator is a web-based tool designed to provide navigation and annotation of ATT&CK matrices, replacing the need to use tools such as Excel. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more. The principal feature of ATT&CK Navigator is to enable users to define custom views of the ATT&CK knowledge base, called layers. A layer could be used to show techniques for a particular platform or to highlight techniques a specific adversary has been known to use. Layers can be created interactively within the Navigator or generated programmatically and then visualized via the Navigator [43].

7.4.1 Installation and execution of ATT&CK Navigator

Installing and running ATT&CK Navigator was done in the following steps:

1. Installing prerequisites:
    a. Node.js v16 from https://nodejs.org/en/blog/release/v16.20.2
    b. NPM v.8.19.4 with the following command: npm install -g npm@8.19.4
    c. AngularCLI with the following command: npm install -g @angular/cli

2. Downloading the required repository, which was done with the following command: git clone https://github.com/mitre-attack/attack-navigator.git
3. Navigating to attack-navigator\nav-app and running the following command: npm install –legacy-peer-deps
4. To serve the application on local machine, the following command was run within the nav-app directory: ng serve
5. Accessing the ATT&CK Navigator application by visiting the url “localhost:4200” in a browser

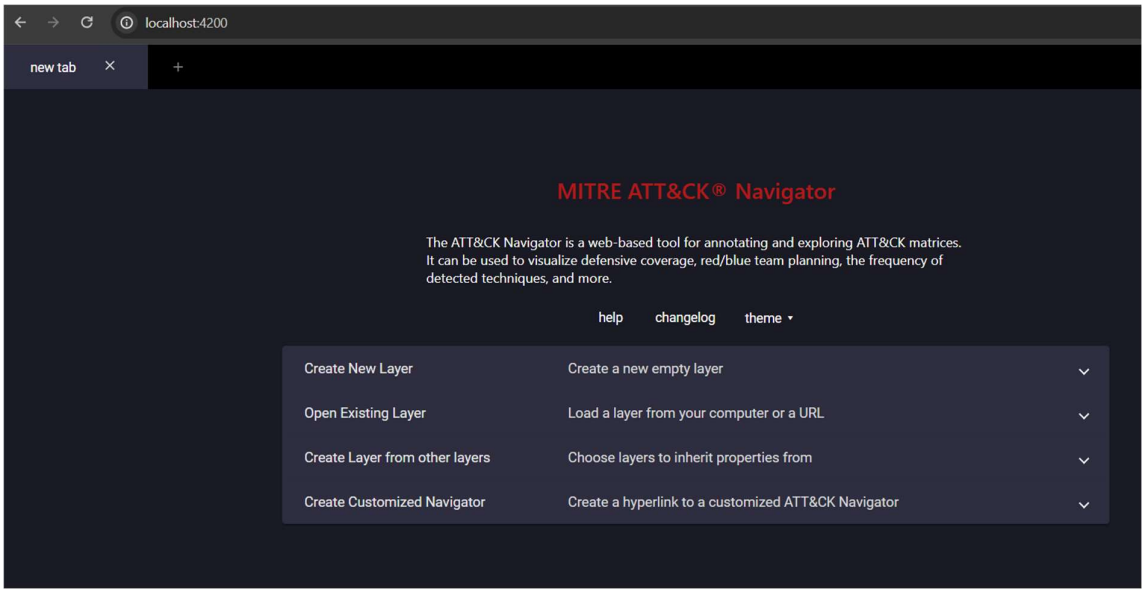

Figure 23 Screenshot of accessing ATT&CK Navigator in browser

7.4.2 Configuring the ATT&CK Navigator to display contents of local knowledge base

ATT&CK Workbench was designed to integrate with a variety of tools, including ATT&CK Navigator. ATT&CK Navigator can display contents of the local knowledge base in ATT&CK Workbench by editing the config.json file located in the directory nav-app\src\assets\config.json. Depending on whether ATT&CK Workbench was installed manually or with docker, the URLs to be set will differ, as shown in the Figure 24 and Figure 25.

Deployment Type	Installation Type	Host (hostname:port)
local	manual	`http://localhost:3000`
local	docker	`http://localhost`
remote	manual	`{remote-hostname}:3000`
remote	docker	`{remote-hostname}`

Figure 24 shows which hostname:port is used for each deployment and installation type

Domain	API Route
Enterprise	`/api/stix-bundles/?domain=enterprise-attack`
Mobile	`/api/stix-bundles/?domain=mobile-attack`
ICS	`/api/stix-bundles/?domain=ics-attack`

Figure 25 The API routes used to access STIX-bundles representing the local knowledge base

In our work, we installed ATT&CK Workbench with docker and deployed it locally. The original config.json file is shown in the following figure.

```
{
    "versions": [
        {
            "name": "ATT&CK v13",
            "version": "13",
            "domains": [
                {
                    "name": "Enterprise",
                    "identifier": "enterprise-attack",
                    "data": ["https://raw.githubusercontent.com/mitre/cti/ATT%26CK-v13.1/enterprise-attack/enterprise-attack.json"]
                },
         {
                    "name": "Mobile",
                    "identifier": "mobile-attack",
                    "data": ["https://raw.githubusercontent.com/mitre/cti/ATT%26CK-v13.1/mobile-attack/mobile-attack.json"]
                },
        {
                    "name": "ICS",
                    "identifier": "ics-attack",
                    "data": ["https://raw.githubusercontent.com/mitre/cti/ATT%26CK-v13.1/enterprise-attack/enterprise-attack.json"]
                }
            ]
        },
        {
            "name": "ATT&CK v12",
            "version": "12",
            "domains": [
```

Figure 26 shows how the config.json file looks before editing.

To display contents of the local knowledge base in ATT&CK Workbench, the following steps were made:

1. Prepending a new object to the versions array, named “ATT&CK Workbench”
2. Using a new, unique version number
3. Changing the data values to URLs corresponding to how we installed and deployed ATT&CK Workbench and the correct STIX-bundle

```
{
    "versions": [
        {
            "name": "ATT&CK Workbench",
            "version": "14",
            "domains": [
                {
                    "name": "Enterprise",
                    "identifier": "enterprise-attack",
                    "data": ["http://localhost/api/stix-bundles/?domain=enterprise-attack"]
                },
                {
                    "name": "Mobile",
                    "identifier": "mobile-attack",
                    "data": ["http://localhost/api/stix-bundles/?domain=mobile-attack"]
                }
            ]
        },
        {
            "name": "ATT&CK v13",
            "version": "13",
            "domains": [
                {
                    "name": "Enterprise",
                    "identifier": "enterprise-attack",
                    "data": ["https://raw.githubusercontent.com/mitre/cti/ATT%26CK-v13.1/enterprise-attack/enterprise-attack.json"]
                },
```


Figure 27 shows how the config.json file looks after editing.

7.5 Creating the 5G Mobile Network Matrix

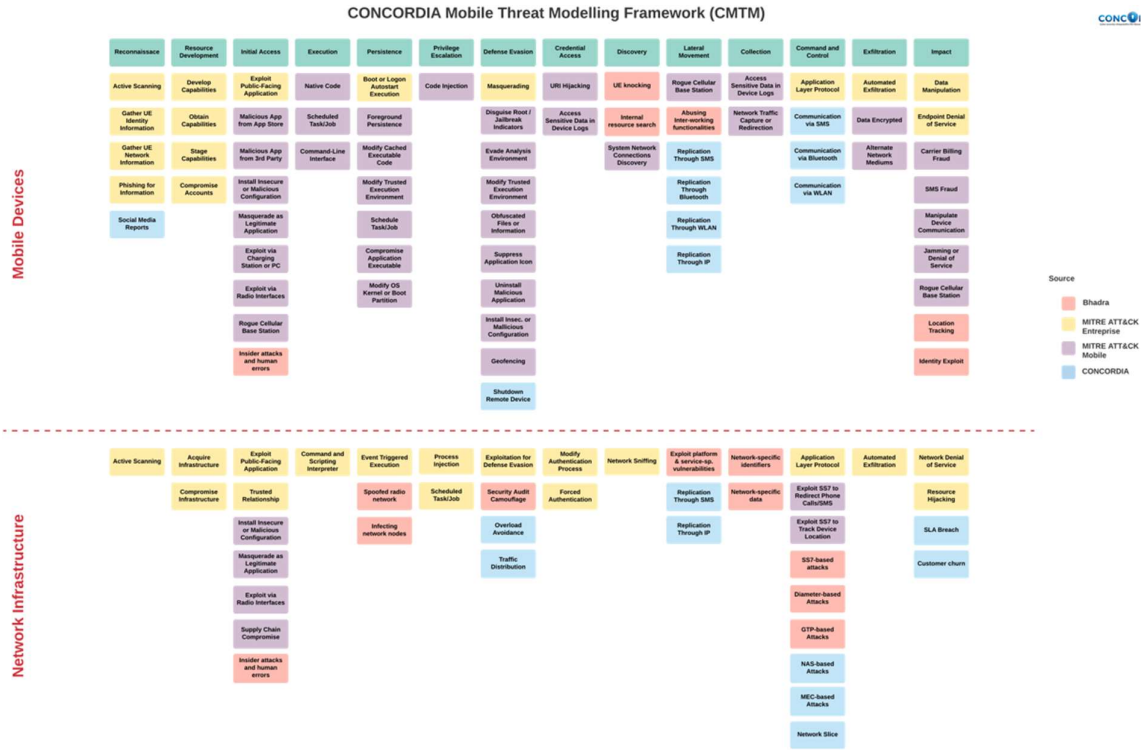

Figure 28. The CONCORDIA Mobile Threat Modelling Framework (CMTMF)

ATT&CK Enterprise v13.1 was selected as the fundament for the 5G Mobile Network Matrix as stated in the beginning of chapter 6. Then, techniques from ATT&CK Mobile presented in Figure 28 was

added. It must be noted that the proposed techniques from ATT&CK Mobile by the CONCORDIA Mobile Threat Modelling Framework (CMTMF) were based on ATT&CK v10, and several techniques have been either deprecated or revoked in ATT&CK v13. Chapter 7.5.1 contains a list showing which techniques were added.

The addition of techniques from ATT&CK Mobile was done by manually modifying each technique in ATT&CK Workbench, modifying the domain-field to include enterprise-attack. In addition, the corresponding tactics in ATT&CK Enterprise were included in the tactics-field. To illustrate with an example, the modifications made to the technique “Supply Chain Compromise” from the Mobile matrix is illustrated in the following figures.

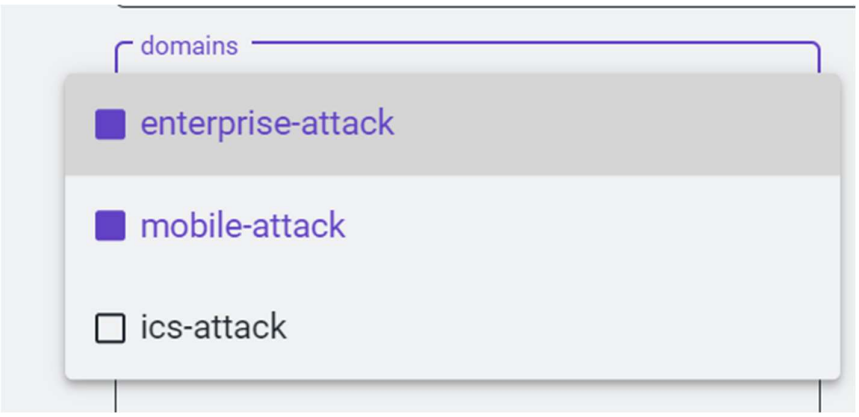

Figure 29. The domain field modified to include enterprise-attack

Figure 30. The tactic field modified to include the tactic Initial Access from enterprise-attack

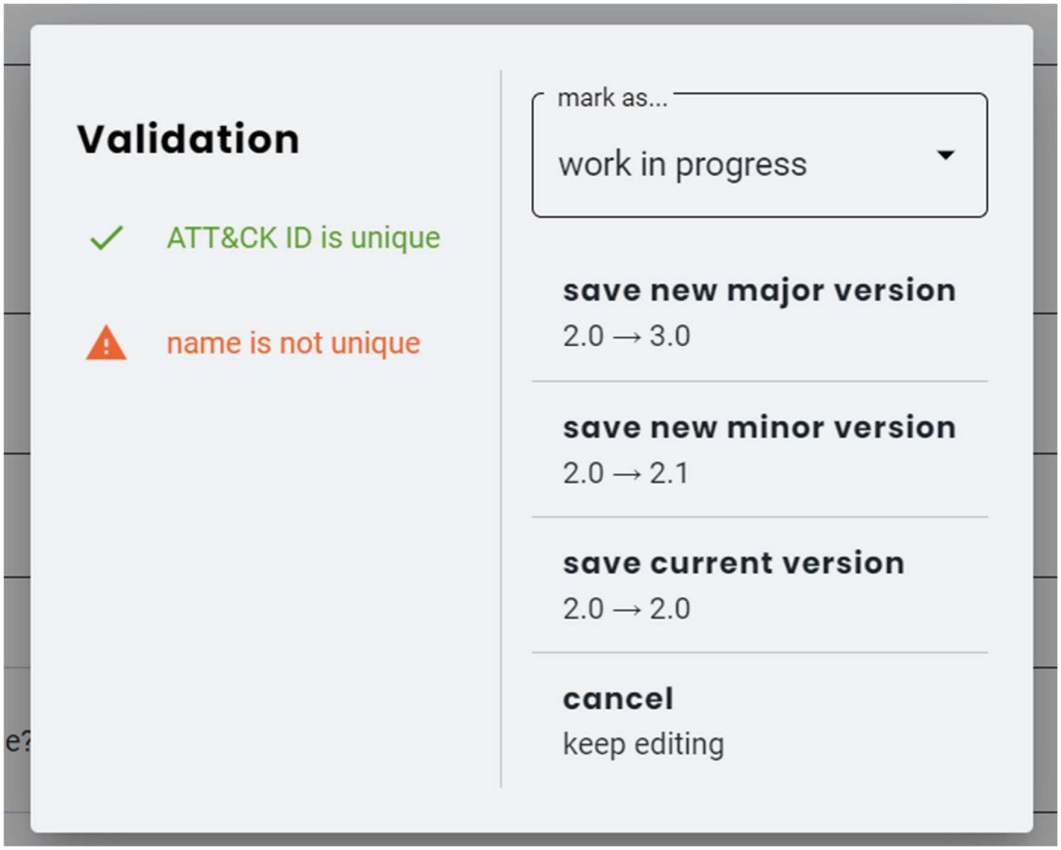

Figure 31. The ATT&CK Enterprise matrix already contained a technique with the name "Supply Chain Compromise"

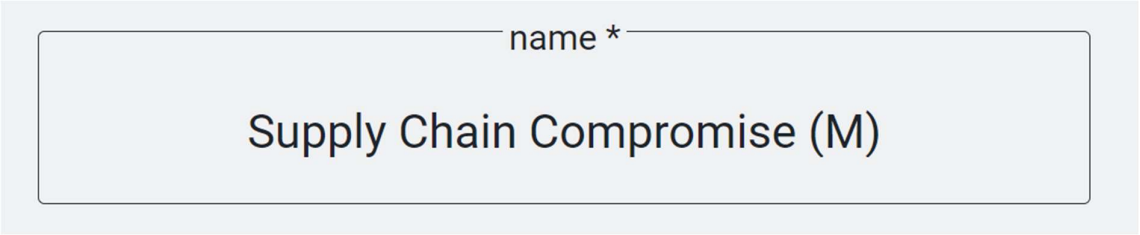

Figure 32. To ensure a unique name for the technique, "(M)" was added at the end of the current name

7.5.1 List of Additions from ATT&CK Mobile

Below is a list containing the techniques from ATT&CK Mobile v10 proposed by the CONCORDIA Threat Modelling Framework (CMTMF) in figure 25. Deprecated techniques were not added to our 5G Mobile Networks Matrix.

Initial Access

"Malicious App From App Store" was deprecated.

"Malicious App from 3rd Party" was deprecated.

“Install Insecure or Malicious Configurations” was revoked by T1632 Subvert Trust Controls: Code Signing Policy Modification. The following technique was added:

- T1632 Subvert Trust Controls (M)
    - T1632.001 Code Signing Policy Modification (M)

“Masquerade as Legitimate Application” was deprecated.

“Exploit via Charging Station or PC” was deprecated.

“Exploit via Radio Interfaces” was deprecated.

“Rogue Cellular Base Station” was revoked by T1638 Adversary-in-the-Middle. The following technique was added:

- T1638 Adversary-in-the-Middle

“Supply Chain Compromise”, the following techniques/sub-techniques were added:

- T1474 Supply Chain Compromise
    - T1474.001 Compromise Software Dependencies And Development Tools
    - T1474.002 Compromise Hardware Supply Chain
    - T1474.003 Compromise Software Supply Chain

Execution

“Native Code” was revoked by T1575 Native API. The following technique was added:

- T1575 Native API

“Scheduled Task/Job”, the following technique was added:

- T1603 Scheduled Task/Job

“Command-Line Interface” was revoked by T1623.001 Command And Scripting Interpreter: Unix Shell. The following techniques/sub-techniques were added:

- T1623 Command And Scripting Interpreter
    - T1623.001 Unix Shell

Persistence

“Foreground Persistence”, the following technique was added:

- T1541 Foreground Persistence

“Modify Cached Executable Code” was deprecated.

“Modify Trusted Execution Environment” was deprecated.

“Schedule Task/Job”, the following technique was added:

- T1603 Scheduled Task/Job

“Compromise Application Executable”, the following technique was added:

- T1577 Compromise Application Executable

“Modify OS Kernal or Boot Partition” was deprecated.

Privilege Escalation

“Code Injection” was revoked by T1631.001 Ptrace System Calls. The following techniques/sub-techniques were added:

- T1631 Process Injection
    - T1631.001 Ptrace System Calls

Defense Evasion

“Disguise Root/Jailbreak Indicators” were revoked by T1630.003 Disguise Root/Jailbreak Indicators. The following techniques/sub-techniques were added:

- T1630 Indicator Removal on Host
    - T1630.001 Uninstall Malicious Application
    - T1630.002 File Deletion
    - T1630.003 Disguise Root/Jailbreak Indicators

“Evade Analysis Environment” was revoked by T1633.001 Virtualization/Sandbox Evasion: System Checks. The following techniques/sub-techniques were added:

- T1633 Virtualization/Sandbox Evasion
    - T1633.001 System Checks

“Modify Trusted Execution Environment” was deprecated.

“Obfuscated Files or Information”, the following techniques/sub-techniques were added:

- T1406 Obfuscated Files or Information
    - T1406.001 Steganography
    - T1406.002 Software Packing

“Suppress Application Icon”, the following techniques/sub-techniques were added:

- T1628 Hide Artifacts
    - T1628.001 Suppress Application Icon
    - T1628.002 User Evasion

“Uninstall Malicious Application”, the following sub-technique was added:

- T1630.001 Uninstall Malicious Application

“Install Insecure or Malicious Configurations” was revoked by T1632 Subvert Trust Controls: Code Signing Policy Modification. The following technique was added:

- T1632 Subvert Trust Controls: Code Signing Policy Modification

“Geofencing” was revoked by T1627.001 Execution Guardrails: Geofencing. The following techniques/sub-techniques were added:

- T1627 Execution Guardrails
    - T1627.001 Geofencing

Credential Access

“URI Hijacking” was revoked by T1635.001 Steal Application Access Token: URI Hijacking. The following techniques/sub-techniques were added:

- T1635 Steal Application Access Token
    - T1635.001 URI Hijacking

“Access Sensitive Data in Device Logs” was deprecated.

Discovery

“System Network Connections Discovery”, the following technique was added:

- T1421 System Network Connections Discovery

Lateral Movement

"Rogue Cellular Base Station" was revoked by T1638 Adversary-in-the-Middle. The following technique was added:

- T1638 Adversary-in-the-Middle

Collection

"Access Sensitive Data in Device Logs" was deprecated.

"Network Traffic Capture or Redirection": was revoked by T1638 Adversary-in-the-Middle. The following technique was added:

- T1638 Adversary-in-the-Middle

Command and Control

"Exploit SS7 to Redirect Phone Calls/SMS"

- T1616 Call Control

"Exploit SS7 to Track Device Location":

- T1430 Location Tracking
    - T1430.001 Remote Device Management Services
    - T1430.002 Impersonate SS7 Nodes (Added to Collection instead)

Exfiltration

"Data encrypted" (Added this to Impact instead):

- T1471 Data Encrypted for Impact (M)

"Alternate Network Mediums":

- T1639 Exfiltration Over Alternative Protocol (M)
    - T.1639.001 Exfiltration Over Unencrypted Non-C2 Protocol
- T1646 Exfiltration Over C2 Channel

Impact

"Carrier Billing Fraud" was revoked by T1643 Generate Traffic from Victim. The following technique was added:

- T1643 Generate Traffic from Victim

“SMS Fraud” was revoked by T1582 SMS Control. The following technique was added:

- T1582 SMS Control

“Manipulate Device Communication” was revoked by T1638 Adversary-in-the-Middle. The following technique was added:

- T1638 Adversary-in-the-Middle

“Jamming or Denial of Service” was revoked by T1464 Network Denial of Service. The following technique was added:

- T1464 Network Denial of Service (M)

“Rogue Cellular Base Station” was revoked by T1638 Adversary-in-the-Middle. The following technique was added:

- T1638 Adversary-in-the-Middle

7.5.2 Additions from Bhadra needed to model SIMBOX Fraud

For each relevant technique proposed to be added from Bhadra v1, a new technique was created in ATT&CK Workbench, starting with ID=T9999 and decrementing the value for each new technique. The tactic was set according to Figure 28.Figure 28. The relevant techniques are listed below.

“SS7-based attacks”

- T9999 SS7-based attacks

“Diameter-based attacks”

- T9998 Diameter-based attacks

“GTP-based Attacks”

- T9997 GTP-based Attacks

“Security Audit Camouflage”

- T9996 Security Audit Camouflage

7.5.3 Additions from CONCORDIA needed to model SIMBOX Fraud

For each relevant technique proposed to be added from CONCORDIA, a new technique was created in ATT&CK Workbench, starting with ID=T9999 and decrementing the value for each new technique. The tactic was set according to Figure 28. The relevant techniques are listed below.

“NAS-based Attacks”

- T9995 NAS-based Attacks

“MEC-based Attacks”

- T9994 MEC-based Attacks

“Network Slice”

- T9993 Network Slice

“Traffic Distribution”

- T9992 Traffic Distribution

“SLA Breach”

- T9991 SLA Breach

“Customer Churn”

- T9990 Customer Churn

7.5.4 The resulting 5G Mobile Network Matrix

Figure 33. The Tactics and Techniques representing the 5G Mobile Network Matrix visualized in ATT&CK Navigator

7.6 Modelling cyber attack examples using ATT&CK Navigator

7.6.1 Modelling the Cherokee Flood Attack

This attack was demonstrated at Black Hat USA 2015 by researchers Charlie Miller and Chris Valasek who first hacked onto and took full control of their own Jeep Cherokee's multimedia system i.e., the head unit through a Wi-Fi connection offered by Chrysler, the manufacturer of the vehicle. All the head units are connected to Sprint cellular network, even if their owners have not purchased a wireless service. The researchers investigated IP address and port allocation by Sprint. They purchased hacked Sprint femtocell and use a rogue base station to attract other Chrysler cars. They could now take control over all of Chrysler's cars equipped with this kind of head unit. When the number of infected is sufficiently large they can launch a flood attack to the 5G network.

Before modelling the Cherokee Flood Attack, two additional techniques were added to the matrix with ATT&CK Workbench:

- T9989 Intrusion via Radio Interfaces, added to Initial Access
- T9988 Access Sensitive Data in Device Logs, added to Credential Access

After the necessary techniques were added, ATT&CK Navigator was used to create a new layer from the modified local version of the Enterprise matrix in ATT&CK Workbench, shown in below Figure 34.

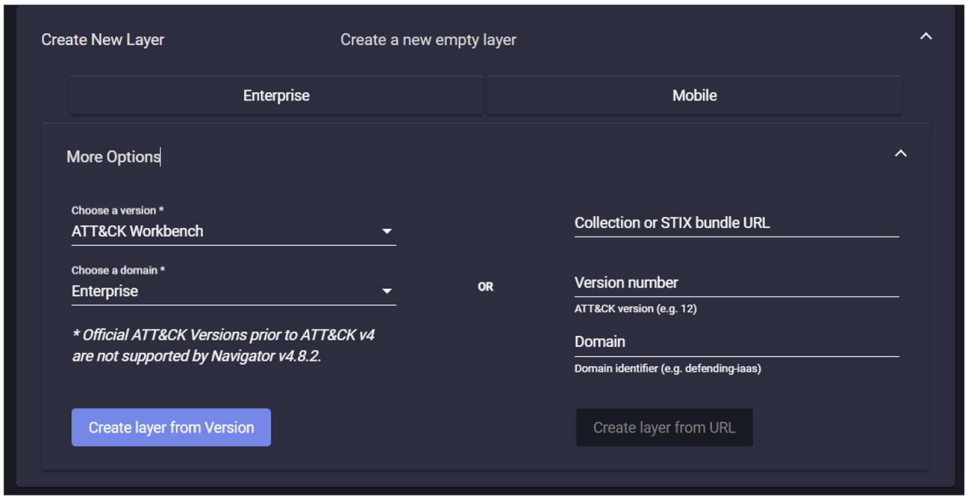

Figure 34. Options set in More Options when creating the new layer

In the new layer, all the techniques related to the Cherokee Flood Attack were selected to be shown, and the rest were toggled off before hiding them with the "show/hide disabled" function in the toolbar. Then, the techniques background colours were changed, producing the model of the Cherokee Flood Attack shown in Figure 35. Finally, the "download layer as json"-function in the

toolbar was used to save a local copy of the layer in JSON-format, enabling us to reopen the model in ATT&CK Navigator whenever needed.

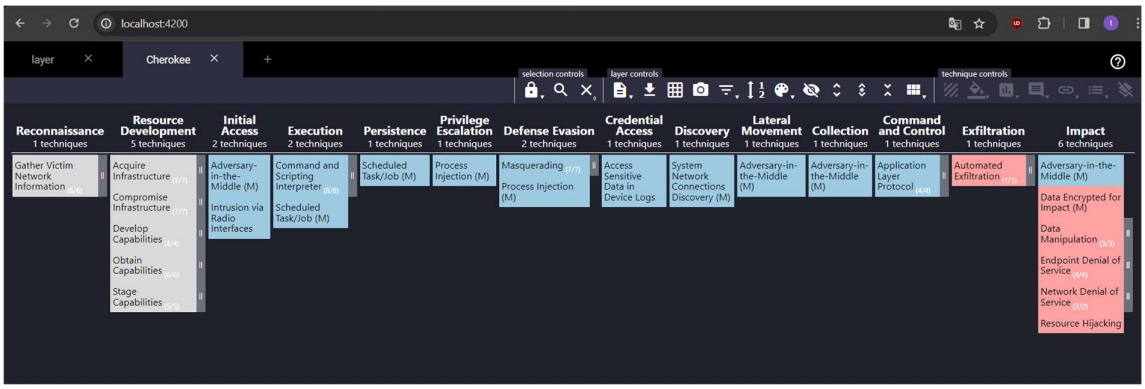

Figure 35. Modelling Cherokee Flood Attack in ATT&CK Navigator

The attack starts with two tactics, Reconnaissance and Resource Development that are done only at the beginning and their techniques are coloured in grey. The next ten tactics, from Initial Access to Command and Control contains techniques which are executed and repeated on every car, coloured in blue. The last two tactics, Exfiltration and Impact are deployed on the network and coloured in pink. It is worth noting that the blue-coloured technique Adversary-in-the-Middle (M) is listed under several tactics because it may be used to achieve more than one tactic. In the Cherokee Flood Attack the technique is not used to achieve Impact, however ATT&CK Navigator does not yet have functionality to disable the technique for a specific tactic, either the technique is shown, or it is not.

7.6.2 Modelling SIMBOX Fraud

Telecom companies are severely damaged by bypass fraud aka SIM Box Fraud. In SIM Box fraud scenarios, international calls are redirected over the Internet to a cellular device that inserts them back into the cellular network through SIM Boxes equipped with multiple low-cost prepaid SIM cards, or even unpaid SIMs acquired with fake identities.

As a result, the calls turn local at the destination network, and fraudsters who set up these boxes pay only local rates or none to mobile operators after charging international rates from the source. While the person making the call will pay the entire call termination fee, it will not be collected by the local operator. The SIM Box bypasses the interconnection.

In the same way as described in the previous section, the SIM BOX Fraud can be modelled in ATT&CK Navigator as shown in Figure 36. This attack is modelled with 6 tactics where the first tactic Resource Development is done just once while the other five are repeated every time an international call is made.

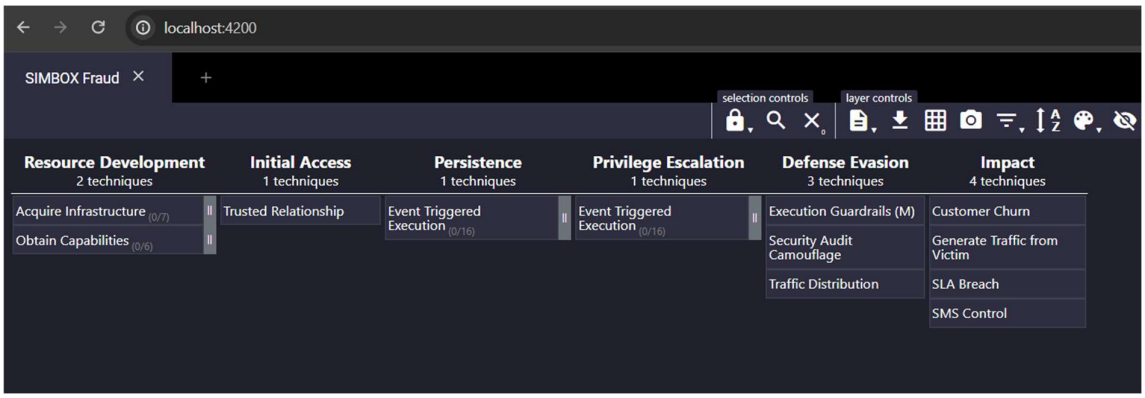

Figure 36. Modelling SIMBOX Fraud in ATT&CK Navigator

Chapter 8 Validation

This chapter performs a validation of the work done in this Master thesis work. A critical review of the work is also done.

8.1 Validation

The validation of the thesis work is done by re-examining the main problem statement and its sub-problems and determining whether they are addressed in a sufficient and adequate manner.

First, the fulfillment of the high level functional requirements defined in Chapter 5 Conceptual Model of the Threat Modelling Framework for 5G Networks is inspected carefully as follows:

Requirements	Fulfilment
R1: The security expert shall be able to design an attack on the 5G network	100% - In Chapter 7 attacks on 5G networks have been modelled and saved for later review or sharing with other security expert
R2: The security expert shall be able to add new technique to the threat modelling framework	100% - Addition of multiple techniques have tested as reported in Chapter 7
R3: The security expert shall be able to remove a technique from the Threat Modelling Framework	100% - Removal of existing but obsolete techniques from the Threat Modelling Framework for 5G is successfully carried out
R4: The security expert shall be able to initiate an update to get new version of the Threat Modelling Framework	100% - It is possible to initiate an update to get new version of the MITRE matrix

Figure 37 Fulfilment of requirements

The sub-problem statements are assessed as follows:

Sub-problem 1: *"Are the existing Threat Modelling Framework suitable for modelling cyber threats in 5G networks"*

Assessment:

- There is currently no Threat Modelling Framework that supports the modelling of cyber attacks on 5G network.
- The most appropriate framework is the MITRE ATT&CK Framework but extensions have to be implemented in order to enable the modelling of cyber attacks on 5G networks.

Sub-problem 2: *"How can the MITRE ATT&CK Framework be extended to support the modelling of threats to the 5G mobile network?"*

Assessment:

- Extensions have been implemented on the MITRE ATT&CK Matrix to include both MITRE ATT&CK techniques and new ones from the mobile domain such that it is sufficient for the modelling of cyber attack on 5G networks

Sub-problem 3: *"How can a cyber attack on the 5G mobile network be modelled using the extended MITRE ATT&CK Framework?"*

Assessment:

- Example of attacks on 5G networks such as Flood attack has been successfully modelled using MITRE ATT&CK Navigator.

Finally, the main problem statement is assessed as follows:

Main problem statement: "How can an effective Threat Modelling Framework for 5G mobile networks be elaborated?"

Assessment:

- An efficient Threat Modelling Framework for 5G mobile networks can be elaborated by extending the MITRE ATT&CK Enterprise Matrix to include the MITRE ATT&CK Mobile techniques and new ones from 5G networks.

CONCLUSION:

The Master Thesis work has achieved its objectives and provides solutions to its main problem statement.

8.2 Critical Review

8.2.1 Yet another extension to MITRE ATT&CK Enterprise

Although we succeeded in elaborating the Threat Modelling Matrix for 5G enabling the modelling of threats on 5G network it is still a variant of ATT&CK which is modified to suit a special enterprise network which is the 5G network. In reality, 5G is a completely distinct technology domain at the same level as Enterprise, Mobile and ICS. Consequently, ATT&CK MITRE should define 5G mobile networks as an independent technology domain.

8.2.2 Support of Dynamic Kill Chain

Quite often, cyber attacks on 5G are first initiated on mobile devices using the same tactics, repeatable on a large range of devices e.g., infection and hi-jacking of a large number of devices before a DDoS attack is launched. Therefore, there is the need to specify a loop in which multiple tactics are repeated until a certain threshold is reached. In some attacks, it may be actual to be able to move backwards to the previous tactics before proceeding to or skipping over some tactics. To model attacks in 5G in an efficient and fully comprehensive it may be necessary to have the support for a dynamic kill chain in which the same tactic or techniques could be repeated. This is not in the case of our implementation.

8.2.3 Composition of other attacks

Cyber attacks can be built by combining multiple existing attacks. It may be actual to be able to perform the composition of attack or more sophistically to do orchestration by combining attack components in a dynamic way. Unfortunately, this feature is not yet provided by MITRE ATT&CK.

Chapter 9 Conclusion

This Master thesis work addresses the need for modelling cyber attacks on 5G networks such that threats can be understood and prevented at earlier stages. An in-depth study of threats on 5G network and an analysis of state-of-the art threat modelling frameworks were carried out to pave the way for the selection of actual threat modelling framework to be extended for 5G networks. The MITRE ATT&CK has proven to be the most appropriate and efforts have been put to complete the design and implementation of 5G extensions enabling the modelling of attacks on 5G networks. Several attacks such as Cherokee Flood Attack and SIM fraud Attack are successfully modelled using the MITRE ATT&CK Navigator.

Although the results from the Master thesis work are promising there are still some limitations mentioned in the critical review as follows:

- The implemented 5G Matrix of our Threat Modelling Framework for 5G is just a variant of the MITRE ATT&CK Enterprise although 5G is not an enterprise network and should have a technology domain 5G defined for it. This can only be done by MITRE.
- The Dynamic Kill Chain is not yet supported allowing the design of cyber attacks having recursive loops, and jumping backs and forth between techniques. Again this can only be implemented by MITRE.
- An attack cannot be modelled as a composition of attacks as the case of advanced campaigns. However, only MITRE can realise that.

As mentioned in Chapter 3 Related works MITRE has initiated the work on elaborating FIGHT (5G Hierarchy of Threats), a knowledge base of adversary Tactics and Techniques for 5G systems when they recognize the need for modelling threats in 5G networks. It will hence be possible to establish liaisons with the MITRE FIGHT Working Group to submit the mentioned needs and requirements such that MITRE can take into consideration in their work.

Bibliography

1. Rao, S. P., Holtmanns, S., & Aura, T. (2020). Threat modelling framework for mobile communication systems. http://arxiv.org/abs/2005.05110
2. Rao, S. "Bhadra framework: Threat Modeling for mobile communication systems by Sid Rao | Nullcon Webinar 2021", YouTube, 29 Oct 2021. [Online]. Available: https://youtu.be/d6iDpHKvX2s?t=1140. [Accessed: 16 August 2022].
3. Santos, B., Barriga, L., Dzogovic, B., Hassan, I., Feng, B., Jacot, N., Do, T. V. (2022). Threat Modeling for 5G networks.
4. Creswell, J.W. (2008). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (3rd). Upper Saddle River, NJ: Prentice Hall. 2008 ISBN 0-13-613550-1
5. 5G America: Becoming 5G advanced: the 3GPP 2025 Roadmap – Dec 2022
6. ETSI: Network Functions Virtualisation (NFV); Architectural Framework ETSI GS NFV 002 V1.2.1 (2014-12)
7. Hakiri, Akram & Gokhale, Aniruddha & Berthou, Pascal & Schmidt, Douglas & Gayraud, Thierry. (2014). Software-Defined Networking: Challenges and research opportunities for Future Internet. Computer Networks. 75. 10.1016/j.comnet.2014.10.015.
8. GSMA: E2E Network Slicing Architecture - Version 1.0 - 03 June 2021
9. ETSI: ETSI TS 103 195-2 V1.1.1 (2018-05) - Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management.
10. 5GPP: 5G PPP Architecture Working Group - View on 5G Architecture, Version 1.0, July 2016
11. https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf
12. Barnum, Sean. (2014). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). https://stixproject.github.io/getting-started/whitepaper/
13. Oasis. (2023) Introduction to TAXII. https://oasis-open.github.io/cti-documentation/taxii/intro.html
14. MITRE FIGHT - https://fight.mitre.org/ - accessed on 10.10.2023
15. Anomali. What are STIX/TAXII? https://www.anomali.com/resources/what-are-stix-taxii
16. ECMA international – Standard ECMA -404 – The JSON Data Interchange Format -1st edition – Oct 2013
17. The MITRE Corporation: MITRE FiGHT™: High-Level Overview, August 2023
18. Do, T. V., Do, T. V., Jacot, N., Flores, B., Feng, B., & Do, T. V. (2023). MITRE ATT&CK threat modeling extensions for mobile threats
19. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018, doi: 10.1109/MCOMSTD.2018.1700063.

20. A. Dutta and E. Hammad, "5G Security Challenges and Opportunities: A System Approach," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 109-114, doi: 10.1109/5GWF49715.2020.9221122.
21. François Reynaud, François-Xavier Aguessy, Olivier Bettan, Mathieu Bouet, Vania Conan. Attacks against Network Functions Virtualization and Software-Defined Networking: State-of-the-art. Workshop on Security in Virtualized Networks (Sec-Virtnet 2016), workshop of 2nd IEEE Conference on Network Softwarization (NetSoft 2016), 2016., Jun 2016, Seoul, South Korea. pp.471-476, 10.1109/NETSOFT.2016.7502487 hal-01393740
22. ENISA; NFV SECURITY IN 5G - Challenges and Best Practices FEBRUARY 2022
23. Technative (2021). The Importance of Threat Modelling for 5G Security https://technative.io/the-importance-of-threat-modeling-for-5g-security/
24. Statista (2023). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
25. Synopsis (2021). Addressing 5G security with threat modelling. https://www.synopsys.com/blogs/software-security/threat-modeling-5g.html#1
26. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018, doi: 10.1109/MCOMSTD.2018.1700063.
27. CrowdStrike Holdings, Inc. is one of the leading American cybersecurity technology company based in Austin, Texas. It provides cloud workload and endpoint security, threat intelligence, and cyberattack response services
28. Embroker. (2022, April 29) 2022 Must-Know Cyber Attack Statistics and Trends. Accessed 31.05.22 from https://www.embroker.com/blog/cyber-attack-statistics/
29. CISA. Accessed from https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System
30. Sullivan, M. (2015, September 14) 8 Types of Cyber Attacks Your Business Needs to Avoid. Accessed 31.05.22 from https://quickbooks.intuit.com/r/article/8-types-of-cyber-attacks-your-business-needs-to-avoid/
31. The National Institute of Standards and Technology (NIST). Accessed from https://csrc.nist.gov/glossary/term/phishing
32. Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.
33. Security Magazine. (2022, February 28). Ransomware attacks nearly doubled in 2021. Accessed 31.05.22 from https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021
34. Cybercrime Magazine. (c2022). Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021. Accessed 31.05.22 from https://cybersecurityventures.com/annual-cybercrime-report-2019-to-2020/
35. Lockheed Martin Corporation, Hutchins, Cloppert and Amin (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Accessed 31.05.22 from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
36. Mitre. (c2015-2022) Accessed 31.05.22 from https://attack.mitre.org/

37. Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2018). MITRE ATT&CK: Design and Philosophy
38. Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks
39. Kohnfelder, Loren; Garg, Praerit (April 1, 1999). "The threats to our products". Microsoft Interface. Retrieved 11 November 2023
40. Eddington, Michael, Brenda Larcom, and Eleanor Saitta (2005). "Trike v1 Methodology Document". Octotrike.org.
41. National Institute of Standards and Technology: Guide to Data-Centric System Threat Modeling - NIST SP 800-154 (Initial Public Draft) - March 2016
42. MITRE. ATT&CK Workbench Frontend. https://github.com/center-for-threat-informed-defense/attack-workbench-frontend/tree/master
43. ATT&CK Navigator. https://github.com/mitre-attack/attack-navigator

Scientific Contribution

At the end of this Master thesis work a paper has been submitted, accepted and published at the international conference MobiWis 2023 as follows:

- *Thoai van Do et all:* ***MITRE ATT&CK threat modelling extensions for mobile threats****; 19th International Conference, MobiWIS 2023 Marrakech, Morocco, Lecture Notes in Computer Science - ISBN 978-3-031-39763-9 ISBN 978-3-031-39764-6 (eBook), August 14–16, 2023*

MITRE ATT&CK threat modelling extensions for mobile threats

Thoai van Do[1], Van Thuan Do[2,3], Niels Jacot[3], Bernardo Flores[2], Boning Feng[2], Thanh van Do[2]

[1] University of Oslo, Gaustadalléen 23B, 0373 Oslo, Norway
[2]Oslo Metropolitan University, Pilestredet 35, 0167 Oslo, Norway
[3] Wolffia AS, Haugerudveien. 40, 0673 Oslo, Norway

thoaivd@ifi.uio.no
{boning.feng,bersan,thanh}@oslomet.no
{vt.do,n.jacot}@wolffia.net

Abstract. With the advent of 5G mobile networks enabling connectivity to billions of devices it is essential to model and analyze threat on mobile threats. To model sophisticated threats such as Advanced Persistent Threats (APT) the MITRE ATT&CK is one of the best threat modelling framework. Unfortunately, it does not address sufficiently mobile networks. This paper provides a brief description of the 5G mobile networks and the potential threats on it. The limitations of the MITRE ATT&CK for mobile networks are clarified before a description of the CONCORDIA Mobile Threat Modelling Framework (CMTMF) is given in details. The main part of the paper is the integration of the CMTMF in the MITRE ATT&CK.

Keywords: 5G mobile networks, 5G security, mobile threat analysis, mobile threat modelling, MITRE ATT&CK

1 Introduction

With the arrival of 5G offering a wide range of connectivity supporting various devices from data-hungry smartphones to primitive sensors and high precision devices requiring ultra-reliable and low latency connections, the number of connected devices has massively increased. According to Statista[1], "the number of Internet of Things (IoT) devices worldwide is forecast to almost triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030". While these devices will provide useful and fancy applications and services which enrich the life of people they also bring with them new cyber security threats.

Indeed, the cyber threat landscape is dramatically changed due to the large and quickly expanding surface through billion devices and due to the huge amount of data generated by these devices. The traditional cyber security perimeter defense based on the filtering of incoming data for potential threats at entry points to the home network Perimeter is no longer sufficient. This calls for a new cyber security strategy namely Threat Intelligence and Threat Modelling which identify, analyze and provide mitigations to cyber threats.

Currently, the MITRE ATT&CK [0] is one of the most efficient threat modelling frameworks which provides solid fundaments for the description and analyses of cyber threats of enterprise networks and mobile devices. Unfortunately, it does address neither the 5G networks nor the mobile networks in general.

Indeed, as software mobile networks, 5G networks are not only subject to the same cyber threats as regular enterprise networks but are also exposed to the ones brought by its capability of providing connectivity to billions of IoT devices ranging from primitive sensors to advanced medical equipment requiring ultra-reliable and low-latency connections. Potential attackers to 5G networks have different behaviours, tactics and techniques that require extensions to the current MITRE ATT&CK framework. The Bhadra framework [0] is the first attempt to extend the MITRE ATT&CK framework for mobile networks which emphasizes the need for modelling threats in mobile networks but is unfortunately too simple and incompatible with the mainstream MITRE ATT&CK framework. The second proposal is the CONCORDIA Mobile Threat Modelling Framework (CMTMF) [0], which is a compatible combination of the enterprise, mobile and ICS (Industrial Control Systems) matrices of the MITRE ATT&CK framework. However, the work in CONCORDIA is still at early stage and lacks details about tactics and techniques. Most importantly, it is not yet integrated in the MITRE ATT&CK Framework. The work in this paper describes the integration of the CMTMF extension in the MITRE ATT&CK and enabling modeling of mobile threats in MITRE ATT&CK.

The paper starts with a brief introduction of the 5G mobile networks. Next, the threat modelling framework will be introduced followed by a concise description of the MITRE ATT&CK framework. The threats in the 5G networks are summarized before the CONCORDIA Mobile Threat Modelling Framework is explained. The main part of the paper is the description of the integration of the CMTMF in the MITRE ATT&CK. A description of a

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

partial proof-of-concept implemented at the Secure 5G4IoT lab at the Oslo Metropolitan University is given to complete the paper which is concluded by some suggestions of further works.

2 Short introduction of 5G mobile networks

Although as the 5th generation mobile network (5G does have the common characteristics of a mobile network it comes with fundamental differences with its predecessors 4G, 3G and 2G. Indeed, while earlier mobile networks are intended merely for mobile phones, the ultimate objective of 5G is to be able to support not only data-hungry smart phones but also Massive Machine Type Communication (mMTC) e.g. primitive IoT (Internet of Things) or sensors and also Ultra-Reliable Low Latency Communications (URLLC) necessary for autonomous driving, remote control in factories, remote surgery, etc. [0].

To be able to achieve its objectives 5G will make use of state-of-the art technology enablers like Cloud-Native, Software Defined Radio, Network Function Virtualization and Multi-Access Edge Computing (MEC) to realize its core concept called **Network slicing**.

The building blocks of the 2G, 3G and 4G mobile networks are network elements, physical entities which are built upon dedicated hardware computers running specific functional software and executing standardized communication protocols. Although mobile operators can reconfigure their networks by adding, moving or removing network resources to meet the demands, such a task could be tedious and time-consuming. The management and operation of traditional mobile networks although fully feasible are complicated and demanding a lot of resources.

The 5G mobile network differs radically from its predecessors because it is no longer composed of physical network elements but is made of virtual Network Functions (vNF) [6] as shown in Figure 1. 5G is softwarised network that can also be cloudified i.e. its vNFs are moved from local servers to datacenters in the cloud.

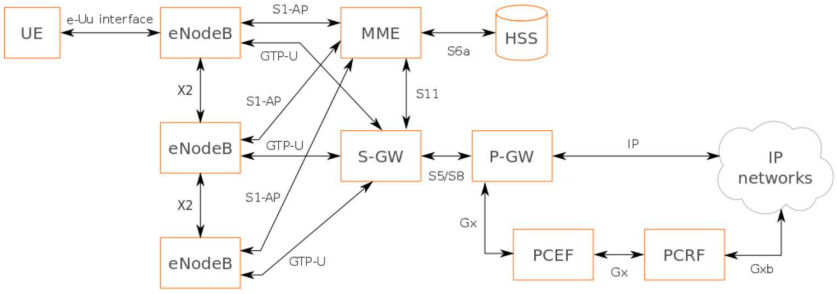

Figure 1 The LTE Network Architecture (courtesy: YateBTS)

By instantiating and connecting a set of vNFs together using SDN (Software Define Networking), a virtual network can be dynamically created. Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring [0].

Such a virtual network constitutes the fundament of the concept of Network Slicing in 5G network. In fact, as stated in [0] "to realize network slicing, network slice logically consists of dedicated or shared network functions (NFs) of 5G SA network and resources by utilizing emerging technologies such as virtualization so as to provide required network capability".

3 Briefly about Threat Modelling Frameworks

Threat Modelling is the activity aiming at identifying, understanding and making simple descriptions or models of the potential threats and attack vectors that a system could be exposed for such that risk analyses, detection methods, countermeasures, and mitigation strategies can be developed. A threat modeling framework usually includes five components, namely threat intelligence, asset identification, mitigation capabilities, risk assessment and threat mapping, but may have different focuses [0] as follows:

- Asset-centric threat modelling frameworks focus on the assets of the target system
- Attack-centric threat modelling framework focus on the attackers and attacks
- System-centric threat modelling framework focus on target system

It will be shown later that the attack-centric approach is most appropriate for the threat modelling of mobile networks and the MITRE ATT&CK is selected as fundament for this work.

4 The MITRE ATT&CK

"*MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.*" [0]

Established in 2010, the Fort Meade Experiment (FMX) research facility allowed researchers to use MITRE's tools with the purpose of how to better detect threats [1]. The type of tests and activities done in that environment where always done under the assumption that a breach in their network or infrastructure has happened and the researchers were to document all the detected threats and come up with possible ways to impede a widespread effect or to protect the infrastructure from the tested exploits.

The MITRE ATT&CK includes a set of matrices which focus on different types of system such as Enterprise, Mobile, ICS (Industrial Control System), Cloud, etc.

The building blocks of MITRE ATT&CK framework consist of tactics and techniques.

Tactic explains the reason why an attacker performs a certain action [0]. An APT Advanced Persistent Threat (APT) can usually be modelled by a series of tactics.

Technique describes in details how an action is performed by an attacker. Multiple techniques can be grouped under the same tactic.

The Tactics and Techniques are classified in a set of matrices which focus on different types of system such as Enterprise, Mobile, ICS (Industrial Control System), Cloud, etc. and shall be used in the modelling of threats in these respective systems.

Last but not least the MITRE ATT&CK includes also procedures describing the implementation of tactics and techniques and mitigations when facing a specific threat.

5 Threats in 5G mobile networks

Although enhancements have been in 5G networks to strengthen security and privacy considerably compared to 4G networks the 5G new capabilities and features such as the support of a wider variety of devices and applications, virtualization and cloudification, interfacing with multiple vertical sectors, etc. introduced new threats to the 5G networks.

To have an overview of the threats to 5G networks, it is essential to identify all the entry points to the 5G network and thereafter to derive and analyze all the possible threats at these entry points. As shown in Figure 6 these entry points are the following:

- Mobile devices
- Access network
- Core network
- External services and applications

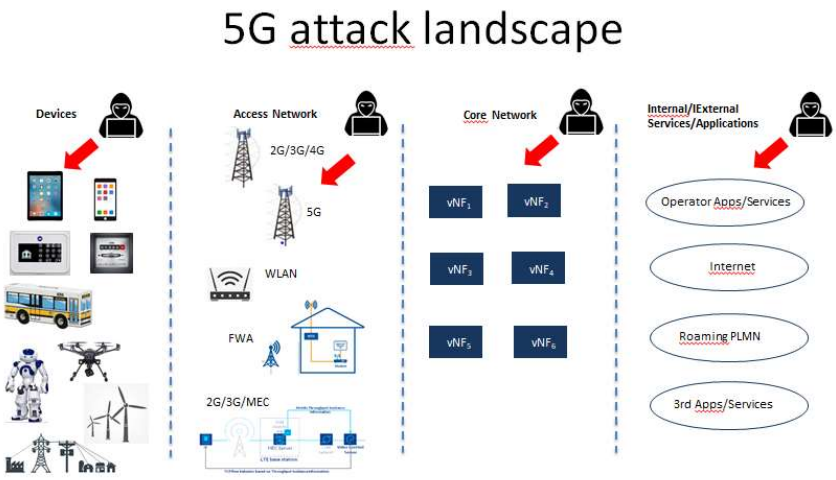

Figure 2 Attack Entry Points to the 5G network

Let us now consider these entry points consecutively.

Mobile devices

In the predecessor 4G, 3G and 2G networks, mobile devices are mostly smart phones that consist of two main components namely the Mobile Equipment (ME) and the Subscriber Identity Module (SIM). A smartphone can be fully identified by the mobile operator using the IMSI (International Mobile Subscriber Identity) and the IMEI (International Mobile Equipment Identity) and get granted access to the mobile network only after successful strong authentication. The landscape has been changed dramatically because 5G is supposed to support not only smartphones but an open range of devices ranging from primitive sensors to powerful supercomputers. Mobile operators do no longer have the knowledge of what kind of devices are operating in their networks because the authentication process only verifies that the device has a legitimate subscription i.e. IMSI, but cannot tell whether the device is benign and trustful or malicious and distrusting. A large number of infected devices can flood and take the mobile network down easily and so far there is no countermeasure to stop such a flooding attack because the devices are already inside the network. This is probably the biggest difference with the fixed networks which are protected by firewalls against unauthorized intrusions and only a limited number of trustful devices are allowed to penetrate the intranet.

If it is not possible to stop a flooding attack once it is started, the only solution may be to detect and prevent it before its initiation. For that, it is crucial to understand the behaviours of the devices and most importantly the techniques, tactics and knowledge of the potential attackers.

Access Network

The 5G Access Network is exposed to the same physical threats as its predecessors due to the common characteristic of an access network which is its huge geographical coverage making their protection quite challenging. Indeed, the base stations and antenna masts are scattered all around the country and are exposed to physical threats such as theft and vandalism. In addition, new threats are introduced with the new 5G capabilities and features such as local breakout allowing IP packets of roaming subscribers to be sent directly to the Internet from the visited network and MEC (Multi-Access Edge Computing). Direct interfacing with 3rd parties at the access network could be a vulnerability that can be exploited by attackers.

Core Network

The 5G Core Network is built up by software components and is hence as vulnerable as other software to cyber threats such as data confidentiality, data privacy, key security and encryption application level authentication [0]. Security measures have to be identified and designed meticulously to protect the Core Network. Although most operators tend to use private cloud instead of public multi-tenant cloud Virtualization and cloudification bring yet other challenges such as side-channel attacks, flooding attacks, hypervisor hijacking, malware injection, and virtual machine (VM) migration related attacks [0].

Interfacing with applications and services

In addition to the traditional interfaces with other mobile networks and interfaces with their own applications and services the 5G network had also interfaces with the Internet and third parties. Adequate perimeter defense such as firewalls, border control gateways secure gateways, etc. must be deployed to protect the mobile network while allowing legitimate traffic to flow normally.

6 The CONCORDIA Mobile Threat Modelling Framework (CMTMF)

Although the MITRE ATT&CK framework is quite efficient to model threats on enterprise networks, mobile devices, Industrial Control System), Cloud, etc. it is not sufficient to model mobile threats.

To illustrate this limitation let us consider the typical example of flood attacks by mobile devices.

This threat consists of two stages:

1. Stage 1 - Infection and hijacking of devices: occurs recursively on devices
2. Stage 2 - Flood attack on the mobile network: happens on the mobile network and will only be initiated when the number of infected devices has reached a certain threshold.

To model the flood attack on the mobile network it is not sufficient to use one matrix but two. First, the Mobile matrix should be used and then the Enterprise matrix. It is not possible to link the two stages together. Further, when the flood attack is launched on the mobile network it is initiated repetitively on numerous devices. This technique should belong to the Enterprise matrix but its performance should belong to the Mobile matrix. Moreover, if the flood attack is launched on the control plane of the mobile network, there is currently no technique to describe it and new techniques specific for mobile networks must be introduced. An extension of the MITRE ATT&CK is required to model threats on mobile network.

The CONCORDIA Mobile Threat Modelling Framework (CMTMF) is an extension which is aligned to the MITRE ATT&CK Enterprise matrix with 14 tactics from Reconnaissance to Impact as shown in Figure 3. Some tactics have both techniques belonging to the mobile network and the ones performed on the devices. Techniques proposed by the Bhadra framework and the newly proposed techniques have been added to enable the modelling of attacks impacting the mobile network. The CMTMF has currently a few new specific mobile techniques but it is “living” framework that will be constantly updated with new techniques.

A mobile threat can be modelled as a chain of phases characterized by tactics which are realised by specific techniques belonging either to Mobile Devices or Network Infrastructure. A tactic in a mobile threat does not have to be unique but can be repeated multiple phases. Several phases can form a loop that is repeated multiple times before the next phase can begin. This is to illustrate the infection and hijacking of devices that is repeated multiple times before the next phase namely the flood attack is initiated. As shown in Figure 4, a Flood attack on mobile network can be modelled with 15 phases in which 11 phases are repetitive on the mobile devices and 3 phases on the network infrastructure.

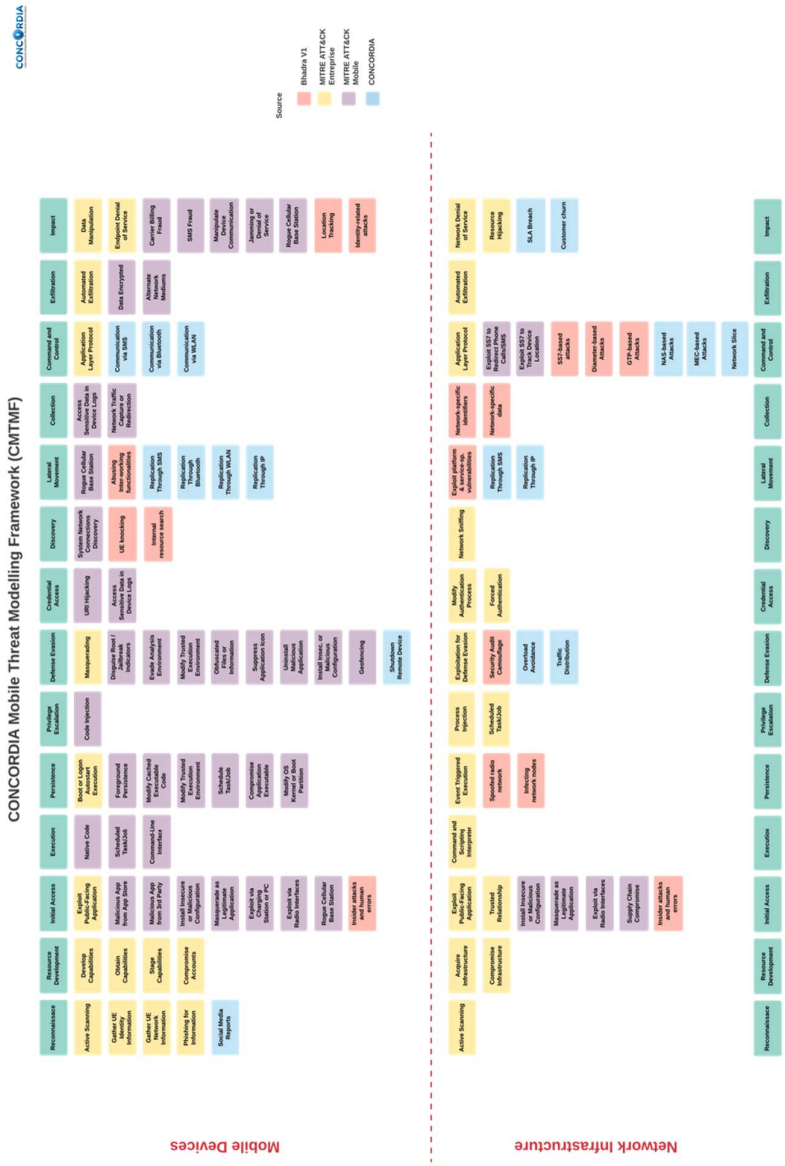

Figure 3 The CONCORDIA Mobile Threat Modelling Framework (CMTMF)

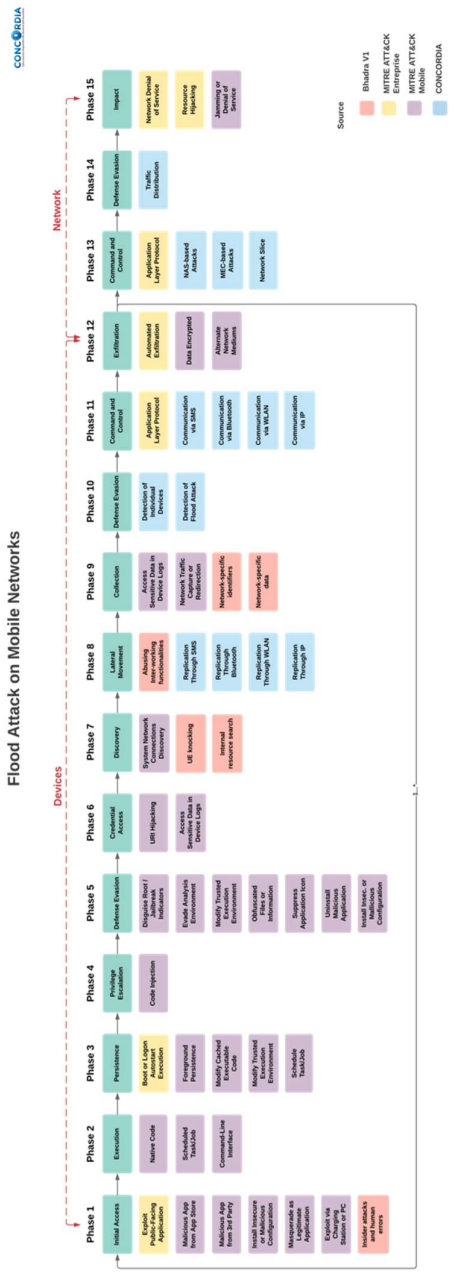

Figure 4 The anatomy of Flood attacks in Mobile Networks

7 The integration of the CMTMF into MITRE ATT&CK

To integrate the CMTMF into MITRE ATT&CK, it is necessary to make a new matrix for mobile domain which includes both the network infrastructure and the mobile device. For that, the ATT&CK Workbench is used. The ATT&CK Workbench [0] is an application allowing users to explore, create, annotate, and share extensions of the MITRE ATT&CK knowledge base.

The ATT&CK Enterprise matrix consisting of 14 tactics is adopted as the fundament as the fundament of the Mobile Network matrix. The next task is to include the Mobile matrix techniques in the Enterprise matrix to form a new extended Mobile Network matrix. The ATT&CK data model is represented in STIX 2.0 format.

The techniques belonging to the Mobile matrix are queried and mapped to the enlarged Enterprise matrix by changing the value of the *kill_chain_phases* property from mitre-mobile-attack to mitre-attack. The *phase_name* shall correspond to the phase_name corresponds to the *x_mitre_shortname* property of an *x-mitre-tactic* object in the Enterprise matrix.

To illustrate this re-mapping, let us consider the technique “Boot or Logon Initialization Scripts” classified in the tactic “Persistence” in the Mobile matrix which is in now re-mapped to the new extended Mobile Network matrix as shown in Figure 5.

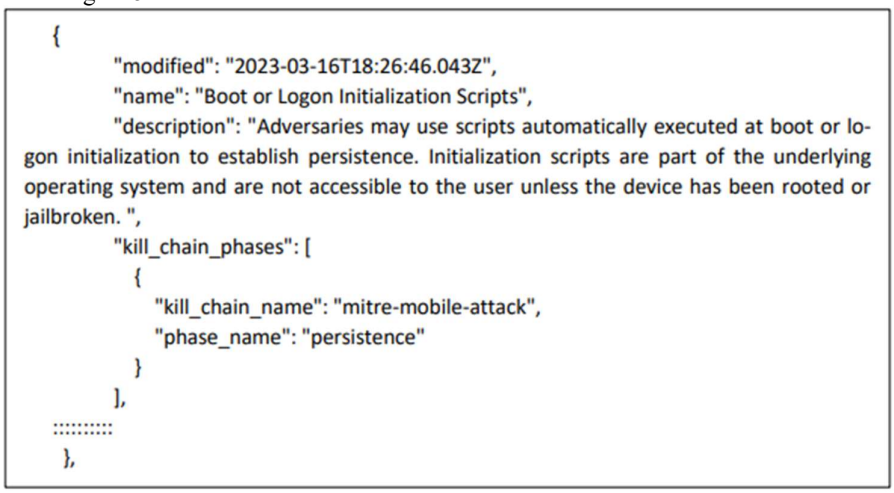

Figure 5 Mapping technique to the new extended Mobile Network matrix

After the inclusion of the techniques of the Mobile matrix, all the techniques proposed by the Bhadra framework [0] for the mobile domain such are also included. Last but not least, the techniques proposed by the CONCORDIA Mobile Threat Modelling Framework (CMTMF) are included. To illustrate the task the JSON STIX description of the proposed *“NAS-based attacks”* technique associated to the tactic *“command-and-control”.* Attacks on the Non-Access Stratum (NAS) [0] on the mobile network are typical threats that may happen only on the 5G mobile networks.

It is worth noting that the inclusion of techniques to the Mobile Network matrix is continuous work in progress and new techniques will be added once they are identified.

To describe an Advanced Persistent Threat (APT) like the flood attack on the mobile network, the ATT&CK Navigator [0] is used. The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more. For the description of an APT attack we propose to create a new layer and to select the tactics and techniques that may be used in this attack.

```
"modified": "2023-05-04T18:06:40.829Z",
"name": "NAS-based attacks",
"description": "By infecting and hijacking mobile phones and IoT devices adversaries may order them to perform simultaneously Non-Access Stratum (NAS) procedure [3GPP TS 24.501 5G;. System architecture for the 5G System (5GS) - 3GPP TS 29.518 5G System, Access and Mobility Management Services] such as Authentication request, UE configuration update, Registration, etc. and hence overloading the control plane of the 5G core network. All the subscriber's access will be blocked resulting to a Denial of Service. In a worst scenario, the 5G Core Access and Mobility Management Function (AMF) may crash and the whole 5G Core will collapse",
"kill_chain_phases": [
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "command-and-control""
  }
],
"x_mitre_contributors": [
  "Thoai van Do",
  "Bernardo Flores",
  "Thuan Do van",
  "Boning Feng",
  "Niels Jacot",
  "Thanh van Do"
],
```


Figure 6 JSON STIX description of NAS-based attacks technique (Part 1)


```
"x_mitre_deprecated": false,
"x_mitre_detection": "",
"x_mitre_domains": [
  "enterprise-attack"
],
"x_mitre_is_subtechnique": false,
"x_mitre_platforms": [
  "Android",
  "iOS",
],
"x_mitre_version": "1.0",
"x_mitre_data_sources": [
  ""Network Traffic: NAS Traffic Flow""
],
"type": "attack-pattern",
"id": "attack-pattern--02c5abff-30bf-4703-ab92-1f6072fae939",
"created": "2023-03-23T19:55:25.546Z",
"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"revoked": false,
"external_references": [
  {
    "source_name": "mitre-attack",
    "url": "https://xxx/T3001",
    "external_id": "T3001"
  }
```


Figure 7 JSON STIX description of NAS-based attacks technique (Part 2)

8 Conclusion

In this paper we have demonstrated the urgent need to model and analyze the cyber threats in the mobile network which did not yet receive sufficient attention due to the misunderstanding about the mobile network. Although 5G mobile networks are softwarised and cloudified the mobile architecture differs considerably from the fixed IP networks and multiple mobile protocols are different and specific to the mobile networks. The MITRE ATT&CK is a very powerful cyber threat modelling framework but is unfortunately not sufficient for the modelling and

analyses of threats on the mobile network. This paper describes the continuation of work in the EU CONCORDIA project that proposes an extension to the MITRE ATT&CK called the CONCORDIA Mobile Threat Modelling Framework (CMTMF). Indeed, the integration of the CMTMF is carried out and although is not yet completed with all the techniques, its feasibility is demonstrated. For further works, more threats on the mobile networks will be modelled and analyzed and more techniques will be added.

9 References

Strom, B. E., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE-ATT&CK: Design-and-Philosophy. https://www.MITRE.org/publications/technical-papers/MITRE-attack-design-and-philosophy

Rao, S. P., Holtmanns, S., & Aura, T. (2020). Threat modelling framework for mobile communication systems. http://arxiv.org/abs/2005.05110

Santos, Bernardo; Barriga, Luis; Dzogovic, Bruno; Hassan, Ismail; Feng, Boning; Jacot, Niels; Do, Thuan Van; Do, van Thanh: Threat Modelling for 5G networks, 2022 International Wireless Communications and Mobile Computing (IWCMC)- ISBN: 9781665467490 - The Printing House; Dubrovnik, Croatia, May 30 - June 3, 2022

5G America: Becoming 5G advanced: the 3GPP 2025 Roadmap – Dec 2022

5GPP: 5G PPP Architecture Working Group - View on 5G Architecture, Version 1.0, July 2016

Hakiri, Akram & Gokhale, Aniruddha & Berthou, Pascal & Schmidt, Douglas & Gayraud, Thierry. (2014). Software-Defined Networking: Challenges and research opportunities for Future Internet. Computer Networks. 75. 10.1016/j.comnet.2014.10.015.

GSMA: E2E Network Slicing Architecture - Version 1.0 - 03 June 2021

Nweke, Livinus & Wolthusen, Stephen. (2020). A Review of Asset-Centric Threat Modelling Approaches. International Journal of Advanced Computer Science and Applications. 11. 1-6. 10.14569/IJACSA.2020.0110201

GSA (Global mobile Suppliers Association): 5G Security Primer: A GSA White Paper; February 2019

Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov: Overview of 5G Security Challenges and Solutions - IEEE Communications Standards Magazine - March 2018

ETSI: 5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (3GPP TS 24.501 version 16.5.1 Release 16) - ETSI TS 124 501 V16.5.1 (2020-08)

MITRE ATT&CK® Workbench - https://attack.mitre.org/resources/working-with-attack/

MITRE ATT&CK® Navigator - https://mitre-attack.github.io/attack-navigator/