A Critical Analysis of Fifth Generation (5G) Mobile Network Security

Jack Grieve (1902470)

BSc Ethical Hacking

Supervised by Laith Al-Jobouri

(l.al-jobouri@abertay.ac.uk)

Word Count: 10,204

+Contents

TABLE OF FIGURES

TABLE OF TABLES

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank several individuals who have helped me through my journey so far. Firstly, I would like to thank my supervisor Laith Al-Jobouri for his continued support and expertise in this field; your patience and guidance were greatly appreciated.

Next, I would like to thank my family for all their hard work and support throughout the years; without them I would have nothing. I would also like to thank my incredible girlfriend for supporting me and putting up with my stress over the last six months.

Additionally, I would also like to thank the Scottish Business Resilience Centre (SBRC) for their continued support and the development of my skills throughout my years at university. I was given countless fantastic opportunities that I'll never forget.

Lastly, I would like to thank my friends for sticking by me over the years and pushing me to be the best version of myself.

ABSTRACT

While the mass deployment of fifth generation (5G) mobile networks continues to be successful, there are still many security concerns and threats to the network. Fifth generation (5G) cellular networks employ innovative and novel technologies to meet the high-level demands of a modern world. Doing so, they leave themselves vulnerable to a wealth of new and old attack vectors commonly used by cyber criminals. Although wonderful, 5G is still susceptible to cyber-attacks. This is partly due to their connectivity to the Internet Protocol (IP) and to a plethora of Internet of Things (IOT) devices.

This paper will focus on building comprehensive threat analysis documentation regarding fifth generation (5G) network security. It will do this by using the PASTA threat methodology, along with the STRIDE threat model, to build the required documentation accurately and efficiently. Information gathered will be correlated from multiple industry and academic sources, allowing the best possible documentation to be completed. The PASTA methodology will include sub-chapters like network overviews, STRIDE classifications, threat agents, threat modelling and threat scenarios.

This paper will be one of the first of its kind due to the severe lack of publicly available information regarding the 5G network. Much of the information found in this document will enable network carriers and users to build the strong foundation, increasing their security posture in the process.

The aim of this project is to research the background and security of the 5G network, analyse the current threat landscape facing the 5G network, and build an appropriate 5G threat analysis document. The completion of these aims will enable the completion of the threat analysis document and allow future work on the network.

ABBREVIATIONS, SYMBOLS AND NOTATION

Abbreviation	Meaning
IP	Internet Protocol
3GPP	Fifth Generation Public Private Partnership
NR	New Radio
MIMO	Multiple Input/Multiple Output
DSS	Dynamic Spectrum Sharing
CA	Carrier Aggregation
DC	Dual Connectivity
MMTC	Massive Machine-Type Communications
URLLC	Ultra-Reliable Low Latency Communications
GSMA	Global System for Mobile Communications
RAN	Radio Access Network
MEC	Multi-Access Edge Computing
NFV	Network function virtualisation
HTTP	Hypertext Transfer Protocol
TLS	Transport Layer Security
SDN	Software Defined Networking
ASIC	Application-Specific Integrated Circuit
PASTA	Process for Attack Simulation and Threat Analysis
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
NSA	Non-Stand Alone
SA	Stand-Alone
EN-DC	E-UTRA-NR Dual Connectivity
ECIES	Elliptic Curve Integrated Encryption Scheme
RRC	Radio Resource Control
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
IMSI	International Mobile Subscriber Identifier
APT	Advanced Persistent Threat
AUSF	Authentication Server Function
UDM	Unified Data Manager
PCF	Policy Control Function
NRF	Network Repository Function
NEF	Network Exposure Function
NSSF	Network Slicing Selection Function

Table 1 - Abbreviations

1 INTRODUCTION

1.1 BACKGROUND

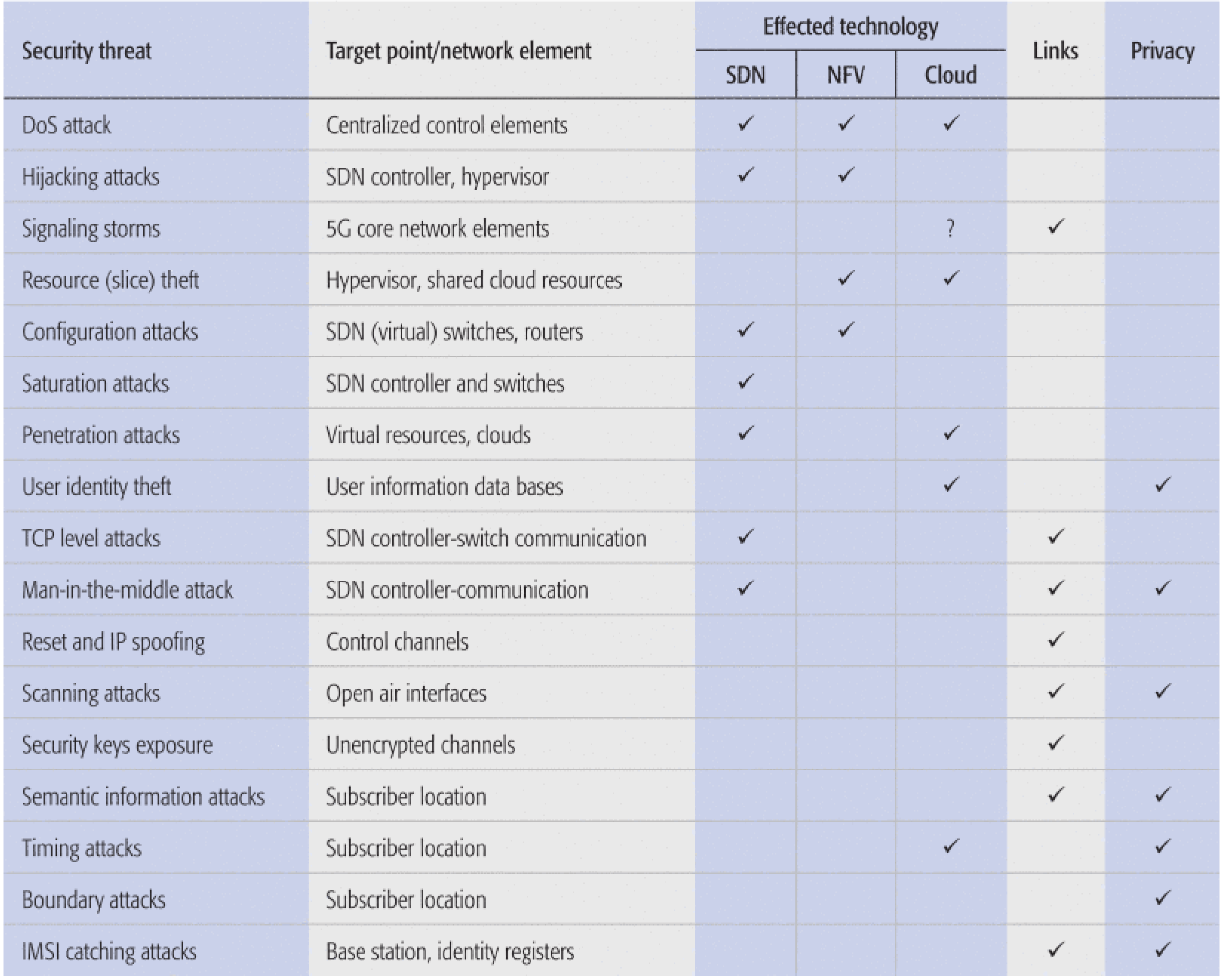
Fifth generation (5G) cellular networks employ innovative and novel technologies to meet the high-level demands of a modern world. Doing so, they leave themselves vulnerable to a plethora of new-found and legacy attack vectors commonly employed by cyber criminals. Although 5G is seen as an advanced and secure communications technology, it is still susceptible to cyber-attacks. This is partly due to its connectivity to the Internet Protocol (IP) and to a plethora of Internet of Things (IOT) devices. The Fifth Generation Public Private Partnership (5G-PPP) clarified that 5G networks will interconnect around seven trillion devices worldwide, reducing creation time and allowing more user-controlled privacy (Ahmad, 2018). The New Radio (NR) standard for wireless communication uses a new and advanced physical layer within the network, supporting millimetre wave communication for massive multiple input/multiple output (MIMO). The 5G network is intended to operate with ubiquitous, rapid-speed, low latency wireless connectivity to user end points. Stating that, it will also improve on matters such as massive machine-type communication and real-time control, which will be the building blocks of a smart, interconnected world of the future (Ahmad, 2018).

The table below displays a brief list of 5G network specifications, with the relevant data attached (Arunachalam, et al., 2018).

Table 2 - 5G Specification (Arunachalam, et al., 2018)

Parameter	**Performance**
Network capacity	One thousand times the capacity of 4G
Peak data rate	20Gbps downlink and 10Gbps uplink
Cell edge data rate	100Mbps
Latency	< 1ms
Bandwidth	1-2 GHz
Connectivity density	One million connected devices per square km
Spectral efficiency	Thirty bits/Hz downlink and fifteen bits/Hz uplink

Numerous security vulnerabilities also stem from this technology and its rapid deployment, with the network supporting many connected devices, and more devices connecting to the network each day. The 5G network brings a much larger threat landscape, much to the difference of previous wireless network protocols like 3G and 4G. As the 5G network develops and becomes more prevalent around the world, new vulnerabilities will be uncovered daily. This is partly due to the 5G network using the Internet Protocol (IP) and having a software-based backbone. Previous networks relied on centralised hardware-based functions, which limited the damage a potential attacker could have. Being software-based makes the network more vulnerable, as the hardware chokepoint fails to exist. 5G is also spectrum dependent, meaning relevant infrastructure needs to be built to ensure user connectivity to the network. The figure below displays the threat landscape facing the 5G network and what services each attack would affect (Ahmad, 2018).



Security threat	Target point/network element	Effected technology			Links	Privacy
		SDN	NFV	Cloud		
DoS attack	Centralized control elements	✓	✓	✓		
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			?	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓	✓		
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds	✓		✓		
User identity theft	User information data bases			✓		✓
TCP level attacks	SDN controller-switch communication	✓			✓	
Man-in-the-middle attack	SDN controller-communication	✓			✓	✓
Reset and IP spoofing	Control channels				✓	
Scanning attacks	Open air interfaces				✓	✓
Security keys exposure	Unencrypted channels				✓	
Semantic information attacks	Subscriber location				✓	✓
Timing attacks	Subscriber location			✓		✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Base station, identity registers				✓	✓

Figure 1 - Security Challenges in 5G Technologies (Ahmad, 2018)

5G security architecture traverses a wide range of locations, from user equipment to the radio access network, to the core network and to the application. The 5G network is split into three layers. The application layer, the serving layer, and the transport layer. These layers together create a more secure system design. Although these methods help safeguard the network, there are still a plethora of vulnerable services on the network that potential cyber criminals could take advantage of (Arunachalam, et al., 2018).

1.2 AIM

This project aims to:

- Research background information and security features of the 5G network.
- Analyse the current threat landscape facing the 5G network.
- Build a comprehensive 5G threat analysis document.

1.3 RESEARCH QUESTION

This project investigated how secure the 5G mobile network was by building a detailed and comprehensive threat analysis document.

Research Question: How secure are fifth generation (5G) mobile networks?

1.4 STRUCTURE

This document will be split into multiple chapters and start with a literature review. This literature review will focus on amassing documentation on topics like 5G standardisation, 5G architecture and any relevant security concerns. The third chapter of the document will be the PASTA methodology used to complete the project. This will start with a network overview, followed by the construction of a STRIDE threat model. Threat agents will then be discussed, followed by threat scenarios and risk identification. The fourth chapter will focus on the gathered results and chapter five will contain an in-depth discussion regarding the subject matter. Finally, chapter six will conclude the paper with a detailed conclusion and any relevant future work.

2 LITERATURE REVIEW

This chapter aims to review and critically evaluate technical literature relevant to the project and is subsequently split into three segments for detailed analysis. The subheadings are as follows: 5G standardisation, 5G architecture and 5G security concerns. Professionals have conducted a vast array of technical research in conjunction with the swift emergence of the fifth generation of mobile networks. This literature review is partial to professional sources, academic papers, and technical documentation. As mentioned previously, this literature review will only cover the three topics listed above. Although more niche research is available on the internet, these three topics will examine the fundamentals of the 5G network and any potential security concerns. This literature review will set the scene for the practical that will take place after the research phase is completed, and aims to answer the question: How secure are fifth generation (5G) mobile networks?

2.1 5G STANDARDISATION

The complex transition from previous generation networks to the 5G network will be slow and gradual, as technology will heavily depend on the assimilation of previous generation networks to operate to its fullest potential. Even today, with the mass deployment of 5G infrastructure around the world, various organisations are still developing standards, establishing potential confusion and security concerns among providers. In September 2015, the initial announcement of the network plans and specifications was detailed at a workshop held by the Third Generation Partnership Project (3GPP). This workshop's purpose was to reveal the first phase of specifications to the public, with an insight into phase two. Phase one detailed the network architecture and how it would correctly meet the service requirements, with Phase two focusing on the protocols for applying the previously mentioned architecture to the standing infrastructure (GSMA, 2019). The mobile giant, Ericsson, published a detailed report regarding 5G New Radio (NR), and the figure below shows the expected timeline for the release of the standardisation documentation (Ericsson, 2020).

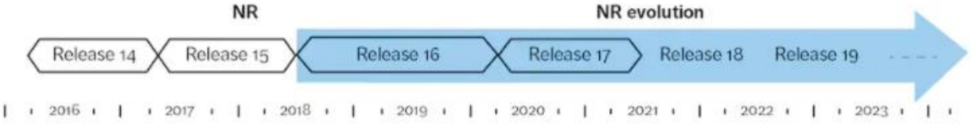
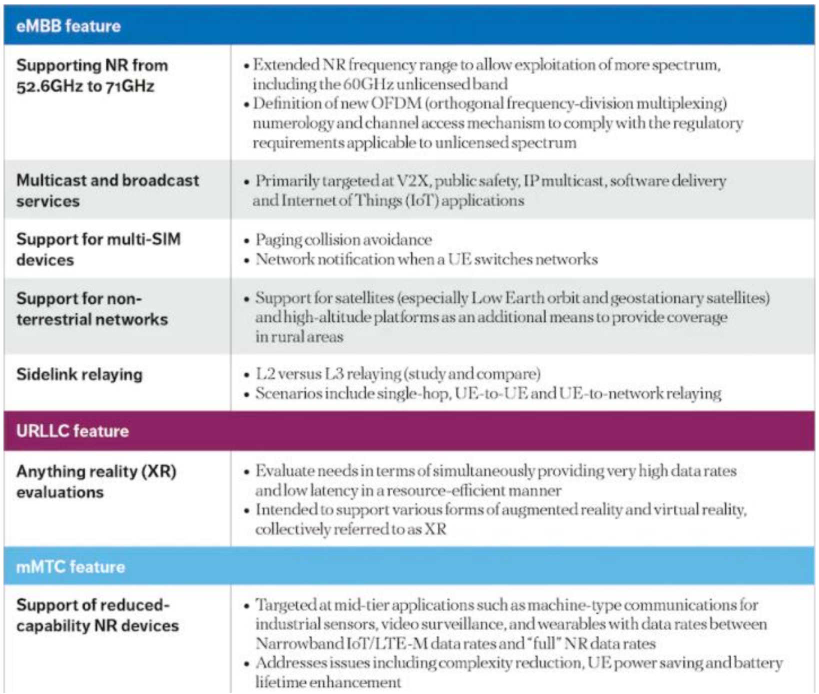


Figure 2 - Standardisation Timeline (Ericsson, 2020)

In July 2018, the initial stage (Phase 1) of 5G standardisation was completed by the 3GPP. The Third Generation Partnership Project (3GPP) released detailed information about the 5G standalone architecture and the relevant technical specifications. This document specified in what way the 5G network would operate with the network core, along with the defined and detailed structure of much of the network core (GSMA, 2019). Phase two (Release 16) standardisation of the 5G network was released in December 2019, with the documentation detailing the notable enhancements in the areas of Multiple-Input, Multiple-Output (MIMO), Dynamic Spectrum Sharing (DSS), Carrier Aggregation (CA), Dual Connectivity (DC) and User Equipment (UE) power saving (Ericsson, 2020).

New Radio (NR) release 17 (Phase 2) was due to be released and published in 2020/2021, but due to the Coronavirus pandemic and other issues, the work was halted, subsequently delayed until 2022, with the intention of having all coding protocols frozen and stable by June 2022 (3GPP, 2020). The documentation was approved in 2019 by 3GPP and will lead to novel features and technologies for three major groups: Massive Machine-Type Communications (MMTC), Enhanced Mobile Broadband (EMBB) and Ultra Reliable Low Latency Communications (URLLC) (Ericsson, 2020). The figure below shows a table composed by Ericsson that displays a list of the new functionalities that release 17 should have when it releases later in 2022.



eMBB feature	
Supporting NR from 52.6GHz to 71GHz	• Extended NR frequency range to allow exploitation of more spectrum, including the 60GHz unlicensed band • Definition of new OFDM (orthogonal frequency-division multiplexing) numerology and channel access mechanism to comply with the regulatory requirements applicable to unlicensed spectrum
Multicast and broadcast services	• Primarily targeted at V2X, public safety, IP multicast, software delivery and Internet of Things (IoT) applications
Support for multi-SIM devices	• Paging collision avoidance • Network notification when a UE switches networks
Support for non-terrestrial networks	• Support for satellites (especially Low Earth orbit and geostationary satellites) and high-altitude platforms as an additional means to provide coverage in rural areas
Sidelink relaying	• L2 versus L3 relaying (study and compare) • Scenarios include single-hop, UE-to-UE and UE-to-network relaying
URLLC feature	
Anything reality (XR) evaluations	• Evaluate needs in terms of simultaneously providing very high data rates and low latency in a resource-efficient manner • Intended to support various forms of augmented reality and virtual reality, collectively referred to as XR
mMTC feature	
Support of reduced-capability NR devices	• Targeted at mid-tier applications such as machine-type communications for industrial sensors, video surveillance, and wearables with data rates between Narrowband IoT/LTE-M data rates and "full" NR data rates • Addresses issues including complexity reduction, UE power saving and battery lifetime enhancement

Figure 3 - Release 17 New Functionality (Ericsson, 2020)

2.1.1 Discussion

Due to the lack of 5G standardisation documentation in academic papers, alternative methods were explored to gather accurate and informative information for this literature review. Three main sources of information were amassed and analysed. They were: The Global System for Mobile Communications (GSMA), Ericsson and the Third Generation Partnership Project (3GPP). The GSMA are a global organisation that specialises in mobile communications. They have more than 750 network providers and four hundred companies under their banner, meaning they were seen as a trustworthy source of accurate information. Ericsson are a multinational networking and telecommunications company. They sell infrastructure employed to provide access to multiple generations of mobile networks, including 5G. They also have experience publishing reports and journals in topics relating to telecommunications and networking, making them experts in this field. The Third Generation Partnership Project (3GPP) is an umbrella term for a vast array of standards organisations that develop mobile communications protocols, including the 5G network and other legacy networks. Due to their standing and knowledge within the subject matter, the work they produce is to be trusted and accurate. All the information gathered from these sources had almost identical documentation, as it all came from the same source, meaning the data is verbatim.

2.2 5G Architecture

To accurately evaluate 5G network architecture as it stands today, a vast array of technical documentation and academic papers were researched and examined for information. This section will examine diverse sources available on the subject matter and discuss the relevant material. This section will be divided into four main headings: 5G Spectrum and Frequency, Multi-Access Edge Computing (MEC), Network Function Virtualisation (NFV) and 5G Radio Access Networks (RAN's). The figure below illustrates an informative example of how the 5G network is commonly set up.

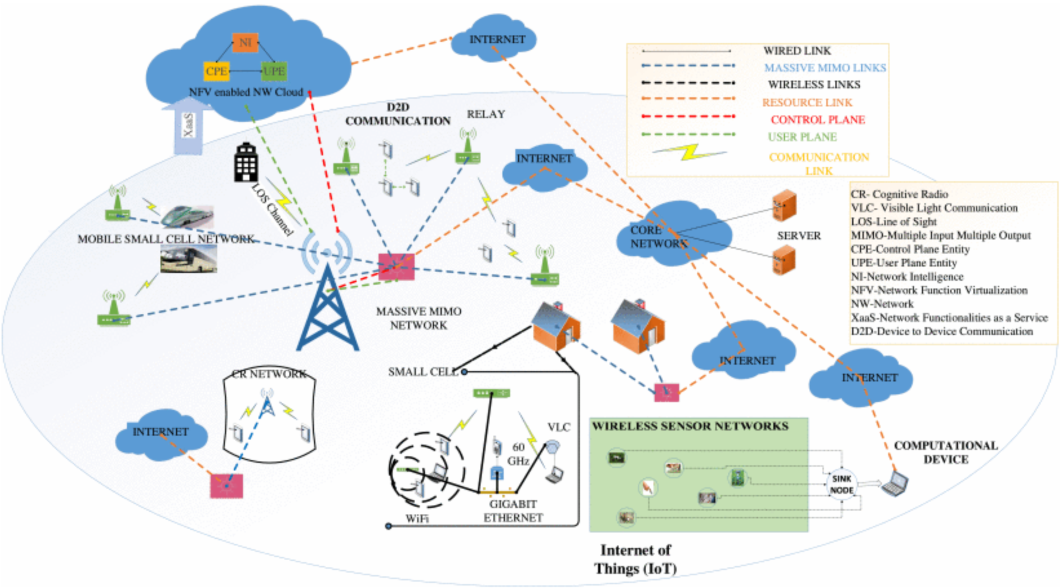


Figure 4 - 5G Architecture (Gupta & Jha, 2015)

A diverse range of frequencies are now being offered to the 5G New Radio (NR) network. Millimetre wave is one of the technologies presented and applied. It operates on an extremely high frequency, which ranges anywhere from 30 GHz to 300 GHz, and is called millimetre wave due to the wavelengths ranging anywhere from 1 to 10mm (al, 2020). In addition to millimetre wave, underused Ultra-High Frequencies (UHF) are also being repurposed and distributed for the 5G network. Some often see UHF frequencies superior to the lower frequencies due to their higher bandwidth, although they have a far shorter range. Millimetre wave frequencies are better for built up and populated areas, making them desirable for high population areas and smart cities of the future (Mumtaz, et al., 2017).

Multi-Access Edge Computing (MEC) is a critical part of the 5G network infrastructure. MEC is a novel cloud solution that pushes traffic and services from the cloud to the edge of the 5G network, subsequently pushing it closer to the user/customer. Contrary to sending the data through the cloud, the network edge analyses and processes the relevant data to increase speed and efficiency (Kekki, et al., 2018). An older paper by the European Telecommunications Standards Institute (ETSI) details and discusses the MEC technology and its place within 5G architecture. Although it is not exclusive to 5G, it talks about the adoption of MEC into the 5G network and how it would be deployed throughout. It explains that MEC will help in the future deployment of IoT devices, as it has lower latency and bandwidth benefits over older technologies (Giust, et al., 2018). The figure below illustrates 5G and MEC architecture together.

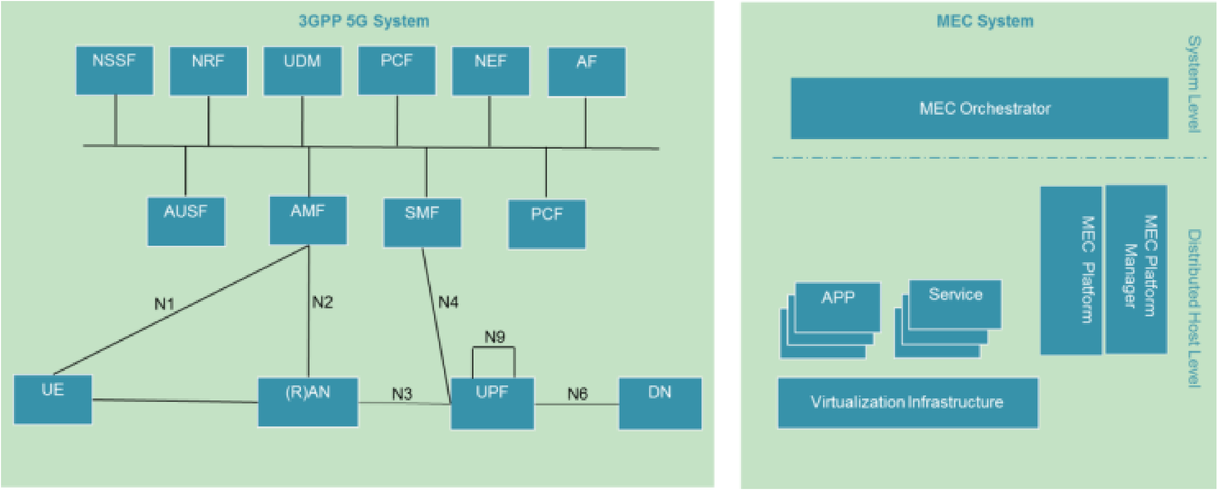


Figure 5 - 5G Architecture and MEC Architecture (Kekki, et al., 2018)

Network function virtualisation (NFV) functions by dissociating software from hardware. This works by changing numerous network functions, such as load balancers, firewalls, and routers, with virtual instances, expelling the need to purchase costly hardware. NFV can also cut costs to the provider by reducing installation times, producing additional profits (Yousaf, et al., 2018). Furthermore, NFV enables the 5G network to virtualize applications with network slicing, allowing multiple virtual networks to run concurrently without the risk of overcrowding. NFV can also help with other challenges commonly found within visualised computing technologies, like storage and network resources (Bouras, et al., 2017). The figure below shows how NFV and network slicing operates.

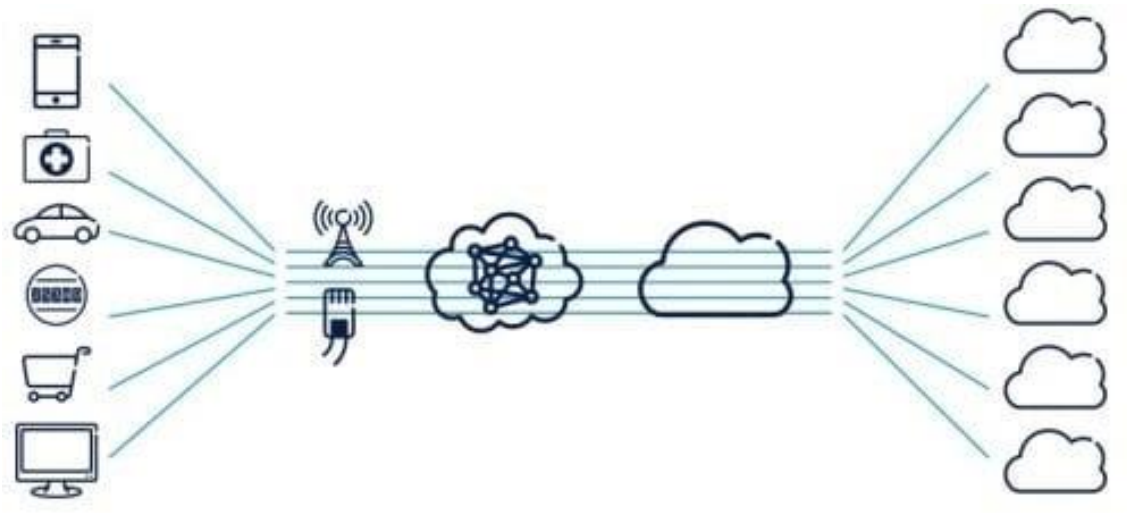


Figure 6 - 5G Network Slicing

Like Network function virtualisation (NFV), 5G expands on previous generational architecture by building a far more intelligent system that operates Radio Access Networks (RAN's), no longer hindered by base station proximity or complicated infrastructure (Gupta & Jha, 2015). Ericsson states the RAN could be used for cloud gaming, AR/VR, autonomous driving, and fixed wireless access (Ericsson, 2022). This will be achieved by using a vast array of antennae, radios, baseband (RAN Compute) and RAN software to facilitate the quickest data transfer speeds and mobility.

2.2.1 Discussion

With the vast number of academic papers and sources detailed previously, there is enough knowledge to successfully create a baseline of understanding regarding 5G architecture, permitting further procurement within the project and its scope. All the sources listed were verified for factual integrity, with minimal argumentation found throughout. As previously mentioned, all data is derived from professional bodies like the Third Generation Partnership Project (3GPP) and the Global System for Mobile Communications (GSMA), meaning there is not much variation in the integrity of the information present.

2.3 5G SECURITY CONCERNS

The 5G network was created to connect every aspect of life with the communication network, further linking the world and bringing people closer together. To achieve this goal, 5G infrastructure and software needs suitable security solutions to avoid potential shortcomings. This section will look at a vast array of literature relating to 5G security concerns and subsequently analyse the findings. Not all the threats below will be discussed, as the word count of this project needs to be adhered to. The table below is from a previously used piece of literature published by the Institute of Electrical and Electronics Engineers (IEEE), highlighting potential security threats to the 5G network (Ahmad, 2018).

Security threat	Target point/network element
DoS attacks	Centralised control elements
Hijacking attacks	SDN controller/hypervisor
Signalling storms	5G core network elements
Resource (slice) theft	Hypervisor, shared cloud resources
Configuration attacks	SDN (virtual) switches, routers
Saturation attacks	SDN controller and switches
Penetration attacks	Virtual resources, cloud
User identity theft	User information databases
TCP level attacks	SDN controller communication
Man in the middle	SDN controller communication
Reset and IP spoofing	Control channels
Scanning attacks	Open air interfaces
Security keys exposure	Unencrypted channels
Semantic information attacks	Subscriber location
Timing attacks	Subscriber location
Boundary attacks	Subscriber location
IMSI (SUPI) attacks	Base station, identity registers

Table 1 – 5G Security Threats

New generation mobile networks will need new communication protocols in the network core, meaning current telecom operators will have to deal with a larger threat landscape. The 5G network core is built on the same protocols that internet devices use, like Hypertext Transfer Protocol (HTTP) and Transport Layer Security (TLS). This will mean that a potential attacker could use a vast array of legacy attack vectors without rigorous research and development models (GSMA, 2019). Another issue faced by providers is network slicing attacks. Although great, network slicing would require the provider to actively monitor multiple networks, not just one, allowing for a higher risk of a successful attack (Olimid & Nencioni, 2020). Splitting up the network into more slices would also increase the chance of further misconfiguration and operator awareness. The figure below illustrates how network slicing could become difficult to manage for the network provider and shows how the infrastructure would commonly be set up.

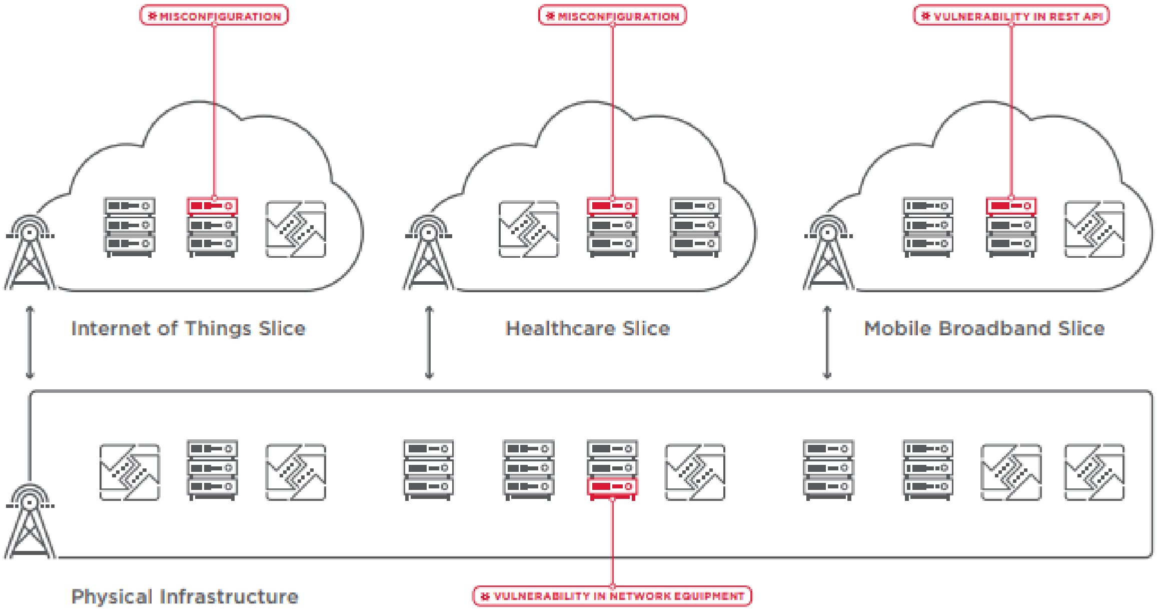


Figure 7 - Increase in Number of Vulnerabilities

Networks built on Software Defined Networking (SDN) and Network Function Virtualisation (NFV) often differ from traditional communication networks. Monitoring network traffic on legacy networks required bespoke hardware like an Application-Specific Integrated Circuit (ASIC), allowing monitoring to take place without hindering network performance (GSMA, 2019). However, on SDN/NFV networks, those tasks will increase CPU and RAM usage, slowing down the virtual network. In conjunction with heightened hardware usage and the need to monitor the network, this could leave blind spots and allow a potential attack vector to reveal itself without the system picking it up.

2.3.1 Discussion

As previously mentioned, all the sources mentioned in this literature review were researched and found trustworthy, as they all take information directly from technical documentation. There was little to no argument between sources, as they all said the same thing.

Between the information previously gathered from the annotated bibliography and sources obtained from the literature review, a solid understanding of 5G network standardisation, architecture and any potential security concerns has been analysed and processed for the practical part of the project to take place.

3 METHODOLOGY

3.1 OVERVIEW

This chapter will walk through the methodology chosen that was subsequently used as a backbone for this paper. To achieve this project's aim and correctly answer the research questions, a vast array of research was conducted beforehand. This was required to fully understand this innovative technology, as academic documentation was difficult to obtain on the subject matter. The project was originally intended to be used in accordance with the 5G test bed that Abertay University had acquired from Nokia. However, due to unforeseen circumstances, there was an issue with the product keys, and that part of the project had to be halted. Instead of using the 5G test bed, another method was implemented. As an alternative to focusing on the test bed, it was decided that more research should be conducted to help develop a vulnerability and threat analysis document. This analysis would be one of the first of its kind and focus on the 5G network and its security measures, along with any threats involved. It would consist of a vast array of collected research to build a comprehensive paper that could be used to help others when the 5G test bed is finally set up.

3.1.1 Research

The research stage was the first step in the chosen methodology. It was used to correlate available data and research, allowing the practical part of the project to take place. A lot of effort and time was put into the research phase, as there was severe lack of publicly available information on the 5G network. The research focused on the 5G network with its use cases, its importance, its relevance, a deep dive into the system architecture, and review of any security concerns relating to the network and its users. Using this information would mean an accurate vulnerability and threat analysis paper could be constructed.

3.1.2 Development

The data gathered in the research phase was used to build a threat/vulnerability analysis paper. The methodology for this paper will be expanded upon and will commence in chapter 3.2.

3.2 THREAT ANALYSIS METHODOLOGY

The development stage of the project focused on building a vulnerability and threat document that aims to analyse and evaluate the 5G mobile network, allowing further work to be built upon it. As the 5G network is a new technology, there was not much publicly available information regarding the vulnerability and threat analysis of the network. This section will focus on the development of the document, with the relevant stages of the methodology listed in the chart below. The methodology is drawn from the Process for Attack Simulation and Threat Analysis (PASTA) and is slightly modified to suit the needs of this project (SHEVCHENKO, 2018). PASTA is a threat-centric modelling framework developed by Heo Zweers, MSc Business Economics, Erasmus University, Rotterdam, and aims to align business needs with threats within technology. Please note that the risk identification section will be added to the results section, and the mitigations will be added to the discussion section of the paper.

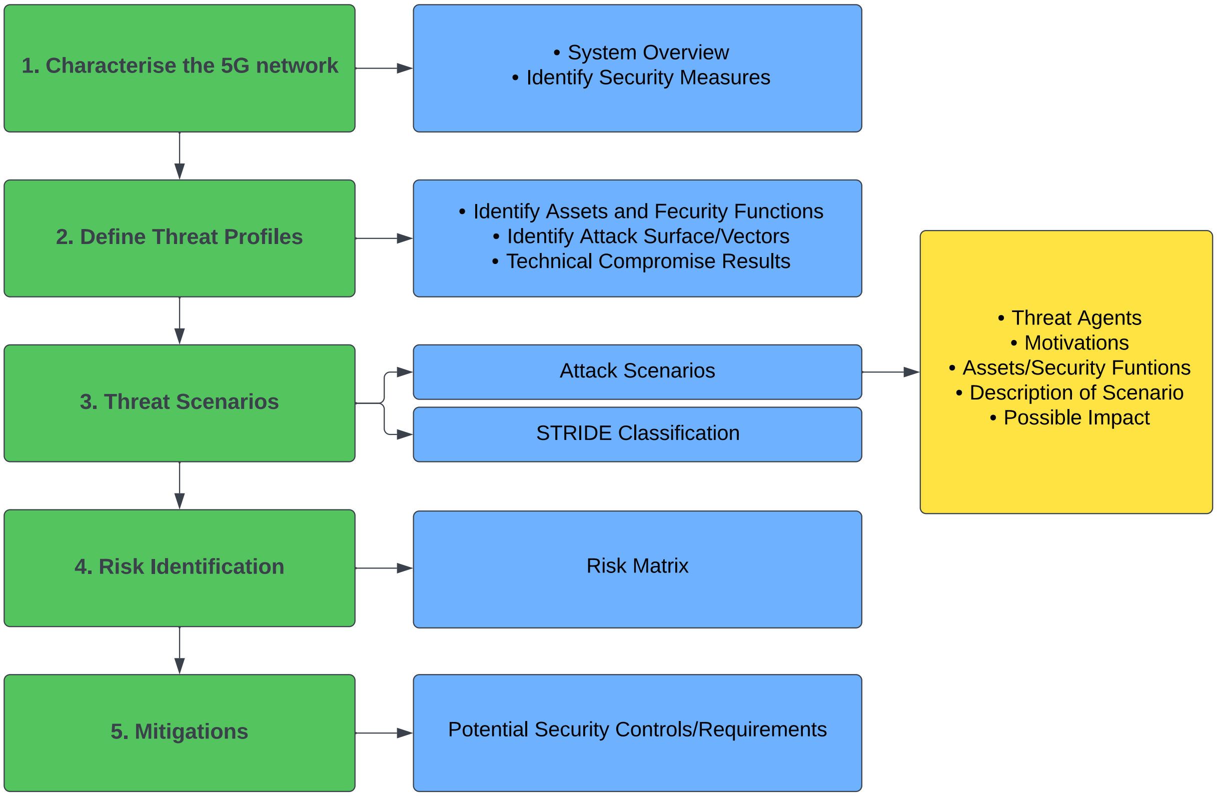

1. Characterise the 5G network
• System Overview
• Identify Security Measures
2. Define Threat Profiles
• Identify Assets and Fecurity Functions
• Identify Attack Surface/Vectors
• Technical Compromise Results
3. Threat Scenarios
Attack Scenarios
STRIDE Classification
• Threat Agents
• Motivations
• Assets/Security Funtions
• Description of Scenario
• Possible Impact
4. Risk Identification
Risk Matrix
5. Mitigations
Potential Security Controls/Requirements

Figure 8 - Vulnerability/Threat Assessment Methodology

3.2.1 The STRIDE Threat Model

To accurately analyse potential threats to the 5G network, the STRIDE methodology was selected for this project, as it is one of the most accurate forms of threat analysis. The methodology was created by Microsoft in the 1990's and aims to model any potential threats to a system or product and calculates the likelihood of a threat in relation to the threat agent's motive (Hewko, 2021). Using this methodology at the start of a development cycle could eliminate any vulnerability in the system that will be secure by design. The STRIDE Threat Model is used in software development and networking, although it will analyse the 5G network for this project.

The STRIDE threat model is divided into six categories for easier recognition:

1. Spoofing identity
2. Tampering
3. Repudiation
4. Information disclosure
5. Denial of service
6. Elevation of privilege

The identified threats are further broken down in the table below:

Table 3 - STRIDE Threat Model (Hewko, 2021)

	Threat Identified	Security Controls	Definition of Threat
S	Spoofing identity	Authentication	Impersonating someone other than yourself.
T	Tampering	Integrity	Modifying data stored on disk, network, memory or elsewhere.
R	Repudiation	Non-repudiation	Claiming that you did not do something or were not responsible; can be true or false.
I	Information Disclosure	Confidentiality	Providing information to someone not authorised to access it.
D	Denial of Service	Availability	Exhausting resources needed to provide a service.
E	Elevation of Privileges	Authorisation	Allowing someone to do something they are not authorised to do.

3.3 5G NETWORK OVERVIEW

This section of the methodology will cover multiple 5G technologies and detail information regarding their hardware, software, and security measures. To fully understand the 5G network, the architecture must be detailed to help with an accurate and reliable threat analysis. The Fifth Generation of mobile networks builds upon previous generations by delivering faster connections with much larger capacity and lower latency. Numerous network providers guarantee maximum speeds are ten times faster than the previous generations (Ahmad, 2018). There are various major changes in the 5G architecture compared to previous generations. This overview will detail the software/hardware, use cases, and any relevant security controls.

3.3.1 5G Non-Stand-Alone Architecture

The Non-Stand Alone (NSA) or E-UTRA-NR Dual Connectivity (EN-DC) architecture integrates the 5G Radio Access Network (RAN) and the New Radio architecture with existing LTE technologies like the 4G Core network. Doing so allows the technology to work without any network replacement, saving time and money in the process (3GPP, 2019). In this configuration, users can only receive 4G signals, but still benefit from the same low latency as the 5G network. The NSA architecture is seen as an interim step towards complete 5G distribution, with the RAN connecting to the 4G core network. In the NSA architecture, the 5G New Radio (NR) base station or the logical node "en-gNB" attaches to the 4G LTE base station via the X2 interface (3GPP, 2019). The X2 interface was designed to work as a node connecting the 4G and 5G base stations, allowing dual connectivity. This means the 4G AN (E-UTRA) and the 5G AN (NR) attach. The figure below was taken from the 3GPP release 15 technical report and shows how the architecture is commonly setup.

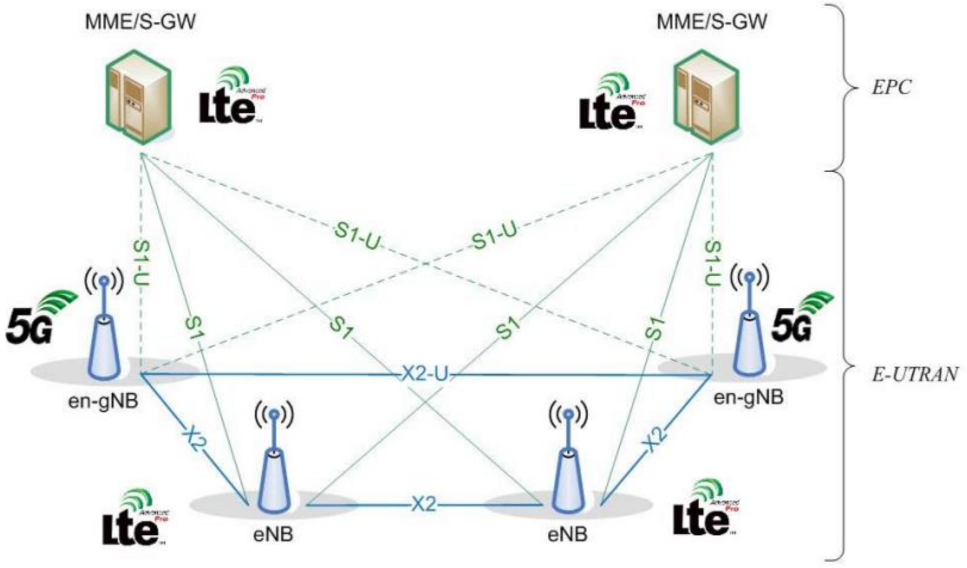


Figure 9 - The NSA Architecture (3GPP, 2019)

3.3.2 5G Stand-Alone Architecture

The Stand-Alone (SA) architecture can be seen as full 5G implementation and does not require any part of the previous generation’s hardware to work. The 5G New Radio (NR) base station or logical node “gNB” connects via the “Xn” interface, and the 5G RAN links with the 5GC network using the NG interface (3GPP, 2019). The core network has also been completely overhauled, using a service-based design. This means the network can be virtualised easier and split into smaller slices for increased efficiency and speed. The figure below was taken from the 3GPP release 15 technical report and shows how the architecture is commonly setup.

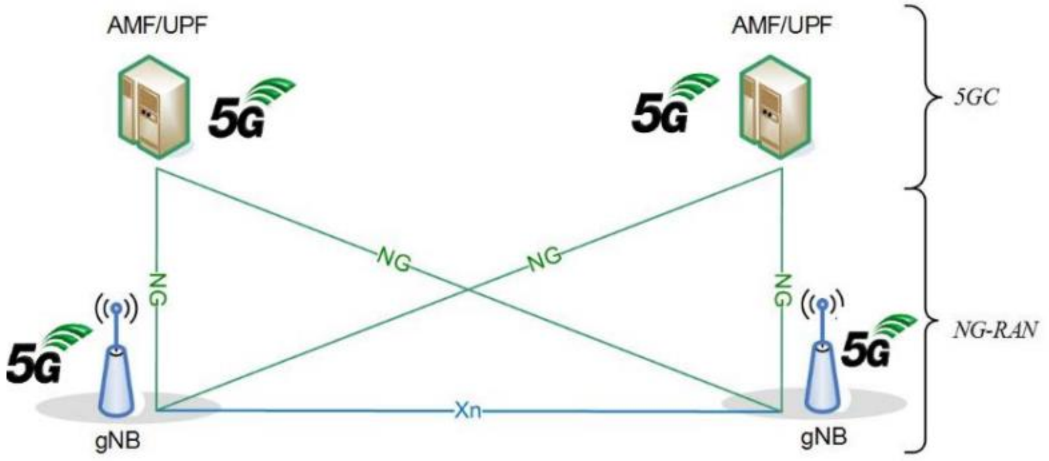


Figure 10 - The SA Architecture (3GPP, 2019)

3.3.3 Comparison of 4G and 5G Security Features

Although the 5G network attempts to patch the many vulnerabilities found in previous generation protocols, there are still many legacy attack vectors that a cybercriminal could use that remain unchanged. Contrary to 4G security features, 5G employs the Elliptic Curve Integrated Encryption Scheme (ECIES). Elliptic curve cryptographic methods are public key processes that provide encryption, digital signature, and key exchange capabilities (Martínez, et al., 2010). This scheme works to encrypt transmissions between the core network and the device, mitigating the risk of IMSI interception. More information regarding these security features will be shown and discussed in chapter five.

The table below lists the differences between generations of networks and states what security features are in place. The security features below were derived from 3GPP documentation (3GPP, 2019).

Security Feature	4G	5G
User Plane Encryption	Yes (Operator Choice)	Yes (Operator Choice)
International Mobile Subscriber Identifier (IMSI) Obfuscation	No	Yes (Uses Elliptic Curve Integrated Encryption Scheme (ECIES))
User Plane Integrity Protection	No	Yes (Operator Choice)
Radio Resource Control (RRC) message integrity protection	Yes	Yes
Radio Resource Control (RRC) message encryption	Yes (Operator Choice)	Yes (Operator Choice)
Non-Access Stratum (NAS) message integrity protection	Yes	Yes
Non-Access Stratum (NAS) message encryption	Yes (Operator Choice)	Yes (Operator Choice)
Authentication of User Equipment (UE) to serving network	Yes	Yes
Authentication of User Equipment (UE) to home network	No	Yes
Network slicing to provide segregated usage	No	Yes

Table 4 - Security Comparison

3.3.4 Network Assets to be Protected

This section of the methodology was used to measure where the threat to the network could come from and what the implications could be. The table below details the network assets that need to be protected and any relevant information regarding them.

Table 5 - Network Assets to be Protected

Network Asset	Information
User Identity and Locational Data	5G networks transmit an obfuscated Subscription Permanent Identifier (SUCI) instead of an insecure International Mobile Subscriber Identity (IMSI) number. This provides a certain level of privacy protection, as the visiting network is only informed of the SUCI number at the end of the authentication procedure (On, 2019). The 5G Global Unique Temporary Identifier (GUTI) aims to mask the user identity and locational data, but if a cyber-criminal can still obtain the SUPI or IMEI of the user, it would still be possible to track them.
Availability of Service	Service availability is paramount to the successful integration of 5G into the telecommunications infrastructure. Not having service could mean a user would have to use an older communications protocol, increasing the chances of certain attacks. It could also endanger human life if certain networks slices are used for emergency services and military assets.
Integrity of Data	Data integrity is important to any communication technology. If there is no data at rest and data in transit encryption, the data would become unreliable. Cyber-criminals could use IMSI/SUPI interception techniques to capture user data, making the network vulnerable.
Confidentiality of Data	Data confidentiality is crucial to the 5G network. Depending on the data source, the information could be valuable to a cyber-criminal and must be appropriately protected. The keys involved in the protection of the integrity and confidentiality of data within the network must also be protected, as they could be used to gain access to critical data.
Performance of the Network	5G has promised high network performance since its inception and relies on being fast with low latency. If the network performance is downgraded with a downgrade attack, the network could become unusable for certain users (Khan, et al., 2018).

3.3.5 Cryptographic Algorithms

This section of the methodology will detail information amassed on the cryptographic algorithms used throughout the 5G network and display any relevant information. The table below displays the information found.

Table 6 - Cryptographic Algorithms

Cryptographic Algorithm	Information
NEA0 / NIA0	NEA0 and NIA0 are commonly referred to as null algorithms. They do not provide any form of protection and are not used frequently throughout the network (3GPP, 2019).
128-NEA1 / 128-NIA1	The 128-NEA1 and 128-NIA1 algorithms are almost identical to a previously used cryptographic algorithm called 'SNOW 3G' and were used for technologies like GPRS, UMTS, LTE and NR. They use 128-bit keys for encryption and authentication (Mattsson, et al., 2021).
128-NEA2 / 128-NIA2	These algorithms are built upon the famous AES block cypher algorithm and are commonly seen as one of the best cryptographic algorithms available (Fabrico, 2019).
128-NEA3 / 128-NIA3	128-NEA3 / 128-NIA3 are based on the ZUC stream cipher and are the newest forms of encryption and authentication methods found on the 5G network. It is to be noted that the algorithm was made by the Chinese Academy of Sciences, potentially meaning it will not be used in the western world due to security concerns.
Elliptic curve integrated encryption scheme (ECIES)	As mentioned previously, the Elliptic curve integrated encryption scheme (ECIES) is an encryption method used for SUPI and SUCI data.
(D)TLS	Datagram Transport Layer Security (DTLS) is a communications protocol aiming to provide security to service-based interfaces. It is based on the famous Transport Layer Security (TLS) protocol and provides transport encryption to 5G assets (Modadugu, 2006).

3.4 5G NETWORK THREATS (STRIDE)

This section of the methodology will focus on current threats to the 5G network, while following the STRIDE threat model to correctly classify them. Doing so will allow the most ground to be covered while conducting the threat analysis and building a detailed model. All the information presented in this section will be a correlation of data gathered throughout the research phase and will be used to build the most accurate threat model possible. Please note that some attack vectors will be left out due to a word count limitation and will be triaged accordingly to display the most critical attacks.

3.4.1 SPOOFING

3.4.1.1 Base Station (gNB) Spoofing (Man in the Middle Attack)

One of the original intentions of this dissertation was to attempt to spoof the 5G network using a Software Defined Radio (SDR) device called a BladeRF. Using an SDR is relatively cheap and easy to do with the correct operating system/software and could allow a cyber-criminal to set up a fake base station. If the fake base station could be introduced into the network core, user plane data would be exposed, as there is often a lack of encryption between the user and the last data sink. Although there are occasionally mitigations to prevent this type of attack, some 5G network arrangements could be misconfigured due to lack of knowledge on the matter. The figure below illustrates how this type of attack could take place.

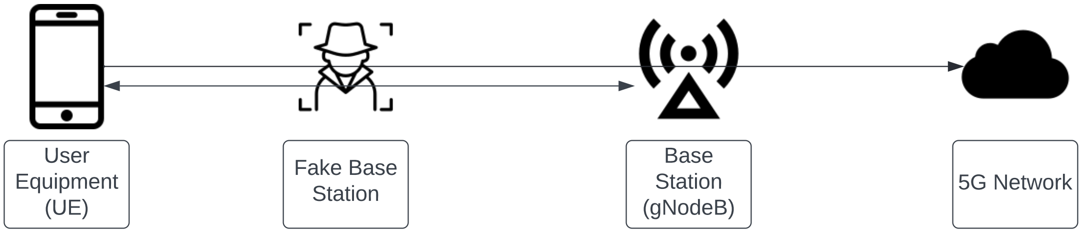


Figure 11 - Man in the Middle (MitM) Attack

3.4.2 TAMPERING

3.4.2.1 Base Station Tampering

A base station (gNB) could be the target of a cyber-attack due to its ability to store and transmit user data. Base stations work by using hardware and software to project the 5G signal, with the software being the expected attack vector for spoofing. Running software of any kind risks a cyber-criminal gaining access to the system and installing malware or a backdoor. This could potentially allow the attacker to view sensitive user information, intercept calls, texts, and even view internet history/network packets. Although this attack vector would be difficult to execute, it would still be possible, and if carried out correctly, it could inflict serious damage to the network provider and any affected customers.

3.4.2.2 Device Tampering

It could be possible that a cyber-criminal could gain access to a 5G enabled device and clone said device, imitating a legitimate user. Although not impossible, this attack would be difficult to execute, as the cyber-criminal would need to physically obtain the device and clone it from a kernel level to fully assimilate the device with the required data. There has been no research into this attack vector by the academic community, thus making this attack purely theoretical as it stands.

3.4.3 REPUDIATION

3.4.3.1 Rogue Base Stations

Since its inception, the 5G network specifications have stated it has moved away from the inherent trust of base stations compared to older generational technologies like 4G. This is because the 5G network aims to be more secure, with user data split between different parts of the network and user devices. This would mean it would be difficult to get as much information as previous technologies like 4G and 3G.

3.4.4 INFORMATION DISCLOSURE

3.4.4.1 Data Interception

As mentioned previously, a cyber-criminal could potentially set up a rogue base station and use it to intercept user communications. Although this attack vector has not been researched in detail, it could still be possible and should be considered a threat to the 5G network until further research has been conducted. Information gathered from this attack would likely include user and manufacturer data, along with any potential device details.

3.4.4.2 Cryptographic Key Disclosure

As discussed previously in the report, the Subscription Permanent Identifier (SUPI) is obfuscated using an asymmetric cryptographic algorithm. It uses the Elliptic curve integrated encryption scheme (ECIES) to encrypt the data and protect the relevant assets. As it stands, this method employs a vast array of mitigations to prevent brute-force attacks, making them nearly impossible. However, these mitigations are not resistant to quantum powered attack vectors, and in theory, nation state actors could have the technology available to crack these algorithms.

3.4.5 DENIAL OF SERVICE

3.4.5.1 Jamming Attacks

Jamming attacks are still achievable on the 5G network. A jamming attack is where a cyber-criminal tunes into the same frequencies that the network produces and injects radio signals into it without any gaps in between. This would prevent any devices in the area from picking up the signal, hindering the network. One of the original experiments planned for this project aimed to use a BladeRF to jam 5G signals, forcing the device to use another network protocol like 4G or 3G. This would allow an attacker to utilise legacy attacks on the network and bring further harm to the user.

3.4.5.2 Physical Interruption of Connection

If a cyber-criminal or other threat actor positively identifies a 5G base station, they could physically interrupt the connection by cutting or removing wires and other hardware within the unit. This would be an easy way to achieve the same goal as software jamming and would be easily achieved if the attacker knew where the signal was coming from.

3.4.5.3 Overloading Network Slices

As previously mentioned, network slices are used within the 5G network to divide the network into smaller portions. Slices are often used to reserve network bandwidth for a certain job, i.e., medical, law enforcement and military communications. This would take the strain off the network and increase security. Attackers employing some sort of DDoS attack could potentially hinder another network slice from doing its job.

3.4.6 ELEVATION OF PRIVILEGES

3.4.6.1 Component Manipulation

If an advanced threat actor somehow got into the network, they could potentially modify the software of the base station to escalate their privileges. Although there is no research regarding this attack vector, it is likely possible with the correct experience/tools. An attack like this would allow the attacker to have a persistent back door to the network and could cause further harm down the line.

3.5 THREAT ACTORS

This section of the methodology will talk about the vast array of threat agents that could potentially harm the 5G network, its users, and display their motivations. This information was essential to form an accurate and informative threat model for the network and its users. Knowing the backgrounds and motivations of the threat actors will be valuable if an incident occurs. The figure below illustrates the tier system of threats to any part of cyber-security infrastructure and uses a tier system to classify them (TelnorGroup, 2020).

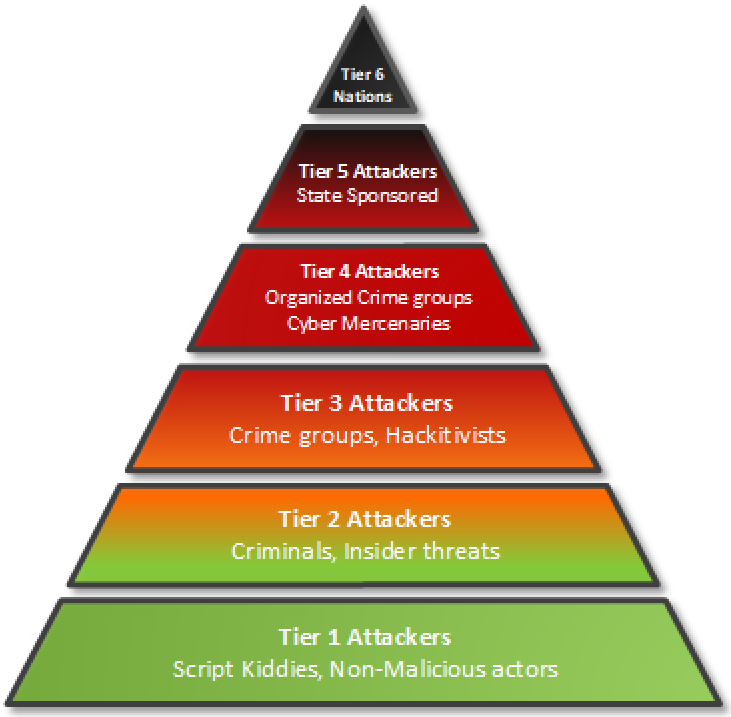


Figure 12 - Threat Actor Classification (TelnorGroup, 2020)

3.5.1 Organised Criminal Gangs

Organised crime groups are the most common threat vector and typically behind cyber-crimes like ransomware and phishing. Although there is no record of cyber-crime gangs attacking the 5G network and its users, they could still be a potential threat in the future.

Their motivations include:

- Financial gain
- Influence
- The funding of other criminal activities

3.5.2 Advanced Persistent Threats (APTs)

APT actors have become busy over the last few years, with most technologically advanced states conducting cyber-attacks on enemy or friendly countries. Their governments heavily fund APT's, and usually conduct highly advanced attacks, sometimes in zero days (Ahmada, et al., 2019). As it stands today, these threat actors present the biggest threat to the 5G network, as they have access to unknown technologies.

Their motivations include:

- Geopolitics
- Financial gain
- Espionage

3.5.3 Insider Threats

Occasionally, disgruntled employees turn against their place of work and conduct illegal activities like corporate espionage or sabotage (Spitzner, 2003). This could cause a lot of damage to the 5G network, as carriers know a lot about how the network works and how to disrupt it. This would also be a highly likely threat actor, as similar things happen all the time.

Their motivations include:

- Financial gain
- Mistreatment by organisation

3.5.4 Lone Wolf Hackers

Unfortunately, the cyber world contains many individuals who enjoy hacking because they can. Their demographic is usually younger people who learned to hack on YouTube or other applications. Working alone, these threat actors display the most unpredictable behaviour patterns, making them dangerous. The threat to the 5G network should be minimal, as most threat actors lack the technical knowledge to carry out such advanced attacks.

Their motivations include:

- Financial gain
- Influence
- Boredom

3.5.5 Hacktivists

Hacktivists are groups of anonymous individuals that hack for a purpose. These purposes are often political and involve large-scale attacks. Over the last year, hacktivist groups have targeted multiple organisations to get their point across. This could be an issue for the 5G network, as they often attack large organisations.

Their motivations include:

- Political motives
- Influence
- Attention

3.6 Threat Modelling

The next component of the methodology was to develop a threat diagram and scenarios for the 5G network. It would also include a breakdown of the network in the form and a diagram and detailed table that listed possible threat scenarios. A professional threat modelling tool was not suitable due to the lack of budget for the project. Therefore, Lucid Chart (LucidChart, 2022) was used to manually enter the details. The figure below shows the threat model for the 5G network as it stands and illustrates what parts of the 5G network communicate and where possible threats may lie.

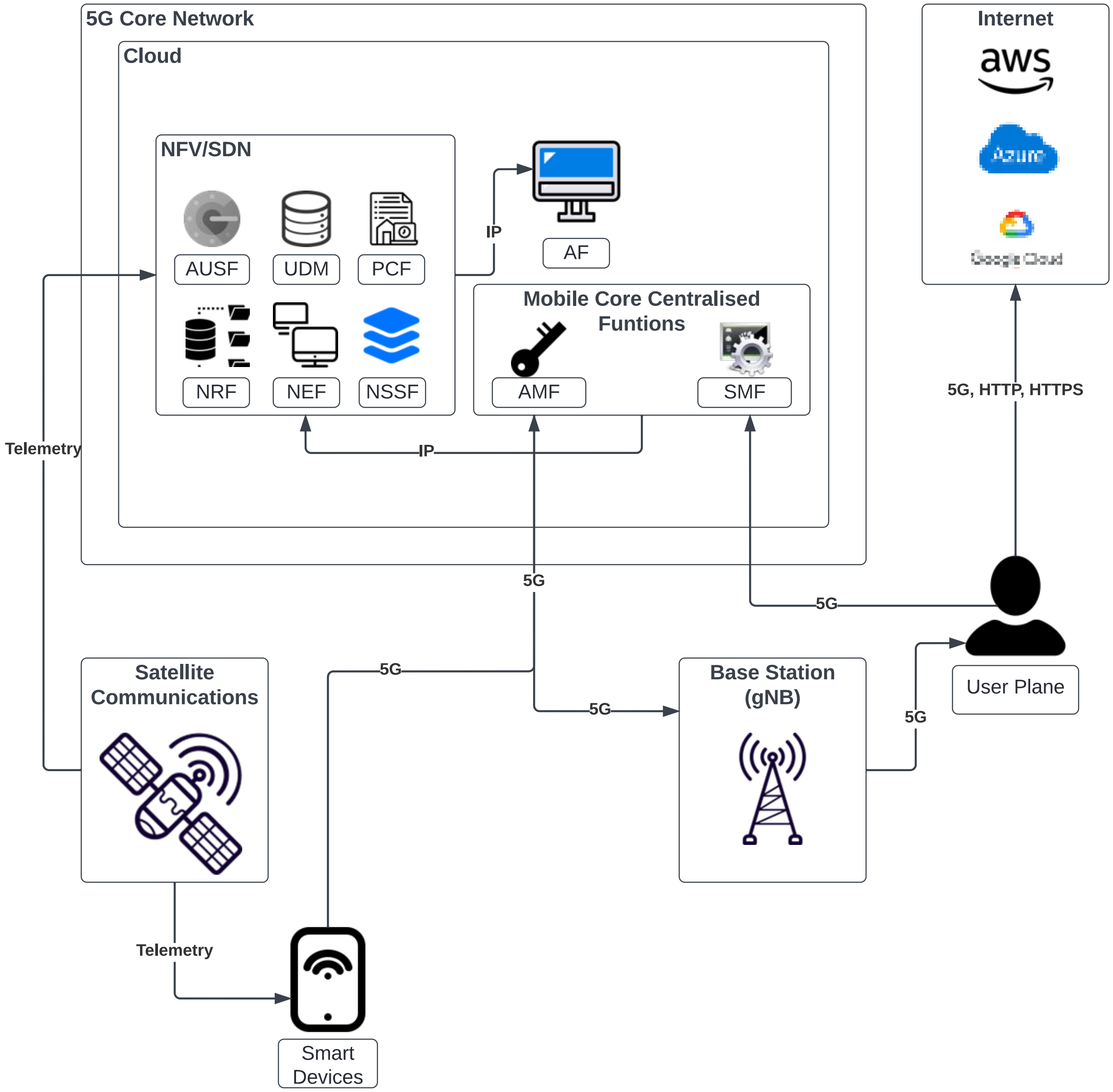


Figure 13 - 5G Threat Model

3.7 THREAT SCENARIOS

ID	STRIDE	Resource	Scenario	Impacts	Likelihood
1	STRIDE	Open Standards	An advanced threat actor from an enemy state could potentially be involved in the creation of technical documentation and standards for the network. This could allow them to put a backdoor in the system and cause issues down the line.	Critical	Very Probable
2	TRIDE	Optional Controls	Standardisation develops certain protocols for the network, some of which are optional. Protocols like User Plane Encryption, User Plane Integrity Protection, Radio Resource Control (RRC) message encryption and Non-Access Stratum (NAS) message encryption are all optional. This could cause problems if not standardised.	Very High	Very Probable
3	STRIE	Counterfeit Components	Counterfeit Components are not as reliable as official ones and could be more susceptible to cyber-attacks. This could allow an attacker to gain access to critical parts of the network.	Critical	Probable
4	STRIE	Inherited Components	Some internal components are inherited from third-party external suppliers. This could mean potentially vulnerable hardware is being brought into circulation.	Very High	Probable
5	TRIE	Software Configuration	A threat actor could potentially access software with the intention of reducing security countermeasures. This would provide them with access to the network and persistent access.	Critical	Unlikely
6	RI	Network Slicing	There are still no standards for the development of network slicing security mitigations. If an attacker took advantage of the miscommunication, the outcomes could be severe.	High	Unlikely
7	STRIDE	Legacy Infrastructure	The 5G network infrastructure still uses legacy hardware to power the network. Older networks will have a vast array of vulnerabilities present and an attacker could exploit them.	High	Probable

8	STRIDE	MEC	As previously mentioned in this paper, Multi-Access-Edge Computing (MEC) works by moving core functions closer to the user end point. A hacker could expose the core functions to a wealth of potential vulnerabilities and damage the network.	Moderate	Unlikely
9	STRD	Spectrum Sharing	The 5G network shares the spectrum to enhance speed and efficiency. An attacker could use this to jam spectrum signals and bring harm to the network and its users.	Critical	Unlikely
10	STRIDE	SDN	Software Defined Networking (SDN) is a method of configuring a network with software, rather than hardware. A potential attacker could use their knowledge of software to construct attack vectors.	High	Probable

4 Results

4.1 Introduction

This section of the paper will talk about the results gathered from the threat analysis document methodology, with the intention of correlating the correct information and data. It will also go through each of the main aspects of the threat model and display any notable findings. The use of the PASTA methodology was a wonderful move in the right direction, as it enabled the successful completion of the project, with all the set goals achieved. As previously mentioned, PASTA is a threat-centric modelling framework developed by Heo Zweers, MSc Business Economics, Erasmus University, Rotterdam, and aims to align business needs with threats found within technology. This paper would allow others to look at it for reference when aiming to put together a vulnerability analysis paper/document. The PASTA methodology previously discussed and used in this paper is shown below.

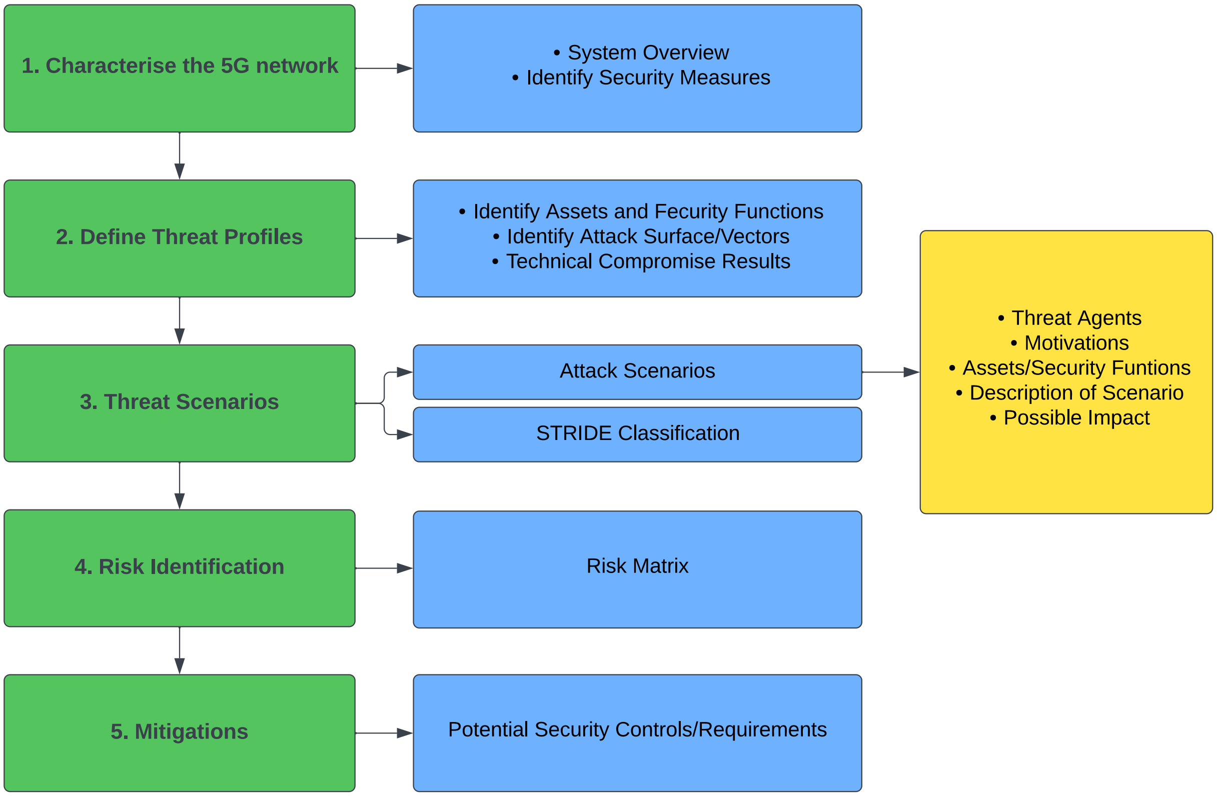

1. Characterise the 5G network
• System Overview
• Identify Security Measures
2. Define Threat Profiles
• Identify Assets and Fecurity Functions
• Identify Attack Surface/Vectors
• Technical Compromise Results
3. Threat Scenarios
Attack Scenarios
STRIDE Classification
• Threat Agents
• Motivations
• Assets/Security Funtions
• Description of Scenario
• Possible Impact
4. Risk Identification
Risk Matrix
5. Mitigations
Potential Security Controls/Requirements

Figure 14 - PASTA Methodology

4.2 CHARACTERISATION OF THE 5G NETWORK

The first part of the methodology involved analysing the system and documenting an overview of the network. The results produced a vast array of information regarding the architecture, cryptographic algorithms, and a comparison between the 4G and 5G networks. Data from this section showed the 5G network has many similarities to the 4G network in terms of security, with many legacy attack vectors still viable. However, the use of cryptographic algorithms has increased drastically, meaning it would be much harder to use brute-force attacks as an effective attack vector. This would considerably decrease the chance of IMSI/SUPI interception, as these cryptographic algorithms mitigate this.

4.3 DEFINING THREAT PROFILES

The second part of the methodology involved using the STRIDE threat model. The STRIDE Threat model was selected for this project, as it is one of the most accurate forms of threat analysis. The methodology was created by Microsoft in the 1990's and aims to model any potential threats to a system or product and calculates the likelihood of a threat in relation to the threat agent's motive (Hewko, 2021). Threats were classified under six headings for easier analysis. The headings were Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privileges. This would allow

The results produced a wide range of data and included multiple threat vectors to the 5G network. It showed the 5G network was vulnerable to attacks from multiple fronts. Although it was not as vulnerable as previous generational networks, it still proved exposed to a vast array of potential cyber-attacks.

Threat actors were also discussed in this section of the paper. Each individual threat actor was listed and discussed, with their motivations included. It was found that Advanced Persistent Threats (APT's) and insider threats were the biggest concern when talking about threat actors, as they would have the most knowledge regarding the 5G network and its assets.

4.4 THREAT DIAGRAM AND SCENARIOS

The third part of the methodology constructed a threat diagram and discussed possible threat scenarios to the 5G network. The threat diagram was built on Lucid Chart (LucidChart, 2022), as the project budget was too low to pay for a professional threat modeller. The diagram displayed a broken-down view of the 5G network and showing where each part fit in. This would allow the reader to get an idea of where an attack could originate and what it would affect.

The next sub-chapter discussed possible realistic threat scenarios that the 5G network could be exposed to. Each scenario contained a resource and description, and was given an ID, a STRIDE classification, an impact classification, and a chance of likelihood. This helped with the construction of the risk matrix and allowed the classified threats to be viewed in an easy-to-read format. Open Standards, Optional Controls, Counterfeit Components, Software Configuration and Spectrum Sharing were the most critical resources found in the 5G network, as they were classified as the most critical and most probable attack vectors.

4.5 RISK IDENTIFICATION

The table below shows the constructed risk matrix with the previously discussed threat scenarios and classifications, showing that many of the scenarios lie in the high, very high and critical categories.

5G Risk Matrix	Likelihood of Risk		
Severity of Risk	Unlikely	Probable	Very Probable
Low			
Moderate	8		
High	6	7 10	
Very High		4	2
Critical	5 9	3	1

5 DISCUSSION

This chapter will focus on the discussion, providing an in-depth analysis of the previous chapters, with all the information correlated and detailed accordingly. This chapter will also describe the importance of the project, its findings, and look back to the original research question: “How secure are fifth generation (5G) mobile networks?” This chapter will be divided into multiple sections and includes discussions on a network overview, network threats, threat agents, threat modelling, threat scenarios, risk identification and any potential mitigations to the network as it stands.

5.1 NETWORK OVERVIEW

5.1.1 5G Non-Stand-Alone Architecture

As previously mentioned, the Non-Stand Alone (NSA) or E-UTRA-NR Dual Connectivity (EN-DC) architecture integrates the 5G Radio Access Network (RAN) and the New Radio architecture with existing LTE technologies like the 4G Core network. Doing so allows the technology to work without any network replacement, saving time and money in the process (3GPP, 2019). In this configuration, users can only receive 4G signals, but still benefit from the same low latency as the 5G network.

Due to the use of the 4G network core, this method of deployment could still encounter several security concerns, including the disconnection of subscribers, traffic interception, SMS interception, and carrying out illegitimate actions on the network. This is partly due to the lack of certain security countermeasures found on the network. The lack of International Mobile Subscriber Identifier (IMSI) Obfuscation makes it easy for an attacker to set up a fake base station and exfiltrate valuable data, as the technology does not use mitigations like the Elliptic Curve Integrated Encryption Scheme (ECIES).

To overcome this security issue, all optional security features should be enabled, and operators must deploy the 5G stand-alone network further. This would prevent many of the most used attacks from taking place.

5.1.2 5G Stand-Alone Architecture

The 5G Stand-Alone (SA) architecture can be seen as full 5G implementation and does not require any part of the previous generation’s hardware to work. This technology allows users to use the full power and speed of the 5G network, along with the vast array of security countermeasures in place. This is partly due to the network not relying on the 4G network core to operate, helping speed and security in the process.

5.1.3 Comparison of 4G and 5G Security Features

Although the 5G network attempts to patch the many vulnerabilities found in previous generation protocols, there are still many legacy attack vectors that a cybercriminal could use that remain unchanged. Contrary to 4G security features, 5G employs the Elliptic Curve Integrated Encryption Scheme (ECIES). Elliptic curve cryptographic methods are public key processes that provide encryption, digital signature, and key exchange capabilities (Martínez, et al., 2010). This scheme works to encrypt transmissions between the core network and the device, mitigating the risk of IMSI interception.

The main dilemma when discussing the differences in security mitigations between 4G and 5G is the large abundance of operator choice allowed on the network. The network operator could make the network as secure or insecure as they want, meaning a new or negligent operator could unintentionally put the network and users at risk by making easily rectified mistakes.

The choices the operator could enable or disable are as follows:

- International Mobile Subscriber Identifier (IMSI) Obfuscation
- User Plane Encryption
- User Plane Integrity Protection
- Radio Resource Control (RRC) message encryption
- Non-Access Stratum (NAS) message encryption

Disabling even one of the security features above could allow an attacker to gain access to the network, putting the carrier and network users at risk. This could be mitigated by standardising network operating procedures among operators, enabling security features as default.

5.1.4 Network Assets to be Protected

This section will cover the main assets found on the network that need to be protected the most from potential cyber-attacks.

They are as follows:

- User Identity and Locational Data
- Availability of Service
- Integrity of Data
- Confidentiality of Data
- Performance of the Network

A successful attack on the 5G network could lead to catastrophic outcomes and affect any of the assets above. The network assets listed above should always be considered first when building a threat model/vulnerability analysis document. This would allow the reader to fully appreciate and understand the value of the network assets. A loss of any of these assets could lead to a severe lack of trust between users and providers, potentially hindering the mass deployment of the 5G network in the process.

5.1.5 Cryptographic Algorithms

It was previously detailed that the 5G network uses many cryptographic algorithms to secure valuable data stored within the network. Please see chapter 3.3.5 for a description of these algorithms.

These algorithms are as follows:

- NEA0 / NIA0
- 128-NEA1 / 128-NIA1
- 128-NEA2 / 128-NIA2
- 128-NEA3 / 128-NIA3
- Elliptic curve integrated encryption scheme (ECIES)
- (D)TLS

It is recommended that network providers force the network to use as much encryption as possible to prevent potential breaches. The prominent use of NEA0/NIA0 means that some parts of the network remain unencrypted and susceptible to a potential cyber-attack. Every part of the network that could use secure algorithms like 128-NEA1/128-NIA1. This would mitigate the risk of a successful cyber-attack further and protect the network.

5.2 NETWORK THREATS (STRIDE)

To accurately analyse potential threats to the 5G network, the STRIDE methodology was used for this project, as it is one of the most accurate forms of threat analysis. The methodology was created by Microsoft in the 1990's and aims to model any potential threats to a system or product and calculates the likelihood of a threat in relation to the threat agent's motive (Hewko, 2021).

5.2.1 Spoofing

It was discovered that a fake base station could be set up to intercept user and carrier data. Although there are mitigations to prevent this type of attack, the device could be used in conjunction with the network core in theory to enable this attack. The network uses International Mobile Subscriber Identifier (IMSI) Obfuscation techniques to hide SUPI and SUCI data. It does this by using the Elliptic Curve Integrated Encryption Scheme (ECIES). Mitigations for this attack vector could include further deployment of cryptographic algorithms to alleviate the risk of successful exfiltration of data.

5.2.2 Tampering

Research discovered that base station and device tampering could occur and be a viable attack vector for a cyber-criminal. Base stations store and transmit user data, and they work by using hardware and software to push the 5G signal, with the software being the expected attack vector for spoofing. Running software of any kind risks a cyber-criminal gaining access to the system and installing malware or a backdoor. This is always a risk, as cyber-criminals could potentially physically access the base station/device, install malicious code, remove security features, etc. Mitigations for this attack vector would include physical security, like locks on doors/devices, and increased cyber culture among stakeholders.

5.2.3 Repudiation

As previously mentioned, the use of rogue base stations was extensively researched to help complete the threat analysis document. Tying back into chapter 5.2.2, the concerns and mitigations remain the same throughout.

5.2.4 Information Disclosure

Data interception was highly triaged and found to be one of the most likely types of attack vectors to take place on the network. This chapter discussed the setup of a rogue base station within the 5G network infrastructure and discussed the type of data that could be extracted. Like the previous chapters, the security concerns and mitigations remain verbatim. As discussed previously in the report, the Subscription Permanent Identifier (SUPI) is obfuscated using an asymmetric cryptographic algorithm. It uses the Elliptic curve integrated encryption scheme (ECIES) to encrypt the data and protect the relevant assets. As it stands, this method employs a vast array of mitigations to prevent brute-force attacks, making them nearly impossible. However, these mitigations are not resistant to quantum powered attack vectors, and in theory, nation state actors could have the technology available to crack these algorithms. Recommended mitigations include increased use of cryptographic algorithms, along with a more aggressive emphasis on cyber culture.

5.2.5 Denial of Service

Denial of service is one of the most popular techniques used by cyber-criminals worldwide. A vast array of research was conducted within denial of service prior to the development of the threat analysis document, with the focus of this chapter being jamming attacks, a physical interruption of connection and network slice overload.

Jamming attacks are still achievable on the 5G network. A jamming attack is where a cyber-criminal tunes into the same frequencies that the network produces and injects radio signals into it without any gaps in between wavelengths. This would prevent any devices in the area from picking up the signal, hindering the network and putting the users at risk. One of the original experiments planned for this project aimed to use a BladeRF to jam 5G signals, forcing the device to use another network protocol like 4G or 3G. This would allow an attacker to utilise legacy attacks on the network and bring further harm to the user. As it stands, there are not many publicly available mitigations available to prevent the jamming of radio frequencies, as that is often kept a closely guarded secret.

If a cyber-criminal or other threat actor positively identifies a 5G base station, they could physically interrupt the connection by cutting or removing wires and other hardware within the unit. This would be an easy way to achieve the same goal as software jamming and would be easily achieved if the attacker knew where the signal was coming from. Mitigations could include an increased attempt to secure the network through physical means. This could mean locks on doors and hardware protection.

As previously mentioned, network slices are used within the 5G network to divide the network into smaller portions. Slices are often used to reserve network bandwidth for a certain job, i.e., medical, law enforcement and military communications. This would take the strain off the network and increase security. Attackers employing some sort of DDoS attack could potentially hinder another network slice from doing its job and potentially putting human life at risk. Mitigations could include a method of locking down certain network slices to reduce the risk of a successful attack on something like Critical National Infrastructure (CNI).

5.2.6 Elevation of Privileges

Research conducted showed that the manipulation of hardware could be a viable attack vector. If an advanced threat actor somehow got into the network, they could potentially modify the software of the base station to escalate their privileges. Although there is no research regarding this attack vector, it is likely possible with the correct experience/tools. An attack like this would allow the attacker to have a persistent back door to the network and could cause further harm down the line. As mentioned previously, physical security would be ideal mitigation for a situation like this, as it would prevent the attacker from accessing the hardware, but if the threat actor was involved in the development of the technology, that could further complicate the situation.

5.3 THREAT AGENTS

As previously discussed in chapter 3.5, threat actors play a large role in properly identifying the threats and risks to the 5G network. A large array of potential threat actors was discussed, with their motivations included. From the research accumulated, it was decided that Advanced Persistent Threats (APT's) and insider threats were the most likely threat actors to attack the 5G network. APT groups have access to cutting-edge technology and resources to attack an advanced piece of technology like 5G, allowing them to conduct clandestine operations domestically and overseas. Insider threats were also listed due to their potential work with the carrier. This would allow them to freely access technical documentation and other resources not found outside the organisation to conduct a successful cyber-attack on the network.

5.4 THREAT SCENARIOS AND RISK IDENTIFICATION

Chapter 3.7 detailed a vast array of threat scenario data, including the ID, the STRIDE classification, affected resource, the scenario, and the likelihood of attack. The correlation of this dataset would allow for an accurate threat model. Please see chapter 3.7 for the output of the data. The method made it easier to triage the threats to the 5G network with data gathered from the vast amount of research conducted beforehand. Resources included open standards, optional controls, counterfeit components, inherited components, software configuration, network slicing, legacy infrastructure, MEC, spectrum sharing and SDN. It was apparent that the 5G network is still extremely susceptible to cyber-attacks, as it uses legacy systems and security mitigations to safeguard it. Recorded were four critical, two very high, three high and one moderate attack scenarios. This showed that even though the network seems secure, it still needs a lot of work to increase its current security posture. With this data, a risk matrix was created to visualise the vast array of data. This would help when presenting this information to a non-technical audience, i.e., to a board of directors of a telecom's organisation.

6 CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSION

This report answered the question: “How secure are fifth generation (5G) mobile networks?” The work carried out during this project effectively demonstrated the importance of mobile network security by constructing a comprehensive threat analysis paper. Given the severe lack of documentation relating to 5G security, this paper met its aims by assembling a vast array of publicly available research and using that information to write the paper. As it stands, this is one of the first threat analysis papers relating to the 5G network, hoping to stand up against academic scrutiny within the information security community, and allow the paper to be used as a starting point for future work on the network.

As previously mentioned, due to unforeseen circumstances, the project had to be moved from a practical evaluation to a more theory-based threat analysis paper. The original plan was to use a device called a BladeRF to physically evaluate the network by sending packets and intercepting radio waves from Abertay’s 5G test bed. This original plan had to be discarded and changed due to an issue with the hardware/software product keys supposed to be supplied by Nokia. Even though this was a setback, next year another student could pick up from where this project left off and use the correlated information to further analyse and attack the 5G network. Upon conclusion of the work, it was found that the 5G network was far more secure than previous generation mobile networks, as it uses various security mitigations to prevent intrusion. However, it is still not completely safe from cyber-attacks. This is partly due to the network using the Internet Protocol (IP) for communications, along with its connections to a vast array of Internet of Things (IoT) devices. The network was also analysed for potential threats by assigning them to the STRIDE threat model. This threat model showed a large abundance of security concerns relating to the network and allowed them to be divided into separated categories, then triaged accordingly. The many threat actors were also discussed in detail. It was found that Advanced Persistent Threats (APT’s) and insider threats were the most likely threat actors facing the 5G network. This was due to the abundance of knowledge needed to successfully attack a new communications technology. Threat scenarios were also listed to enhance the paper’s reliability, and it listed multiple scenarios that the 5G network could face in the real world.

The 5G network still has long ways to go in terms of security and safe mass deployment around the world. It is advised that network providers/carriers enable all possible security features, as seen in chapter 5.1.3. Carrier choice will hinder the networks security, as many providers will fail to meet the requirements if they are not enforced, e.g., user plane encryption and integrity protection. Doing so will mitigate the chance of a successful cyber-attack on the network and prevent customer and carrier data from being stolen. Additionally, an emphasis on network slice security should also be considered. This will enable the network to operate as intended, without the risk of a certain slice being targeted by cyber-criminals. An attack on a network slice dedicated to the medical sector for example could lead to catastrophic results, as human life could be put at risk, subsequently escalating the situation.

This paper has achieved all the objectives set at the start of the project and has been extremely stimulating to produce such an exciting piece of work.

6.2 Future Work

As mentioned before, the project could be expanded by using the BladeRF to enable the physical analysis of the 5G network. Unfortunately, this was cut from the project due to unforeseen circumstances and would be a great addition to the already large amount of gathered research. The BladeRF is a Software Defined Radio (SDR) that allows a user to capture and analyse radio waves of any form and could even allow the transmission of radio waves. This could allow the device to act as a man in the middle, enabling further attack vectors. With the vast array of research conducted in this paper, a good base point could be worked upon to further study this novel technology and protect it from cyber-criminals. The 5G test bed at Abertay is a Stand-Alone (SA) system. However, if the university could acquire a Non-Stand-Alone (NSA) system, the project scope could be drastically increased.

7 REFERENCES

3GPP (2019a) *Digital cellular telecommunications system (Phase 2+) (GSM)*, *3GPP*. ETSI. Available at: https://www.etsi.org/deliver/etsi_gts/03/0338/05.02.00_60/gsmts_0338v050200p.pdf (Accessed: 1 March 2022).

3GPP (2019b) *Release 15*, *3GPP*. 3GPP. Available at: https://www.3gpp.org/release-15 (Accessed: 1 March 2022).

3GPP (2020) *Firm decision on Rel-17 delay in December*, *3GPP*. 3GPP. Available at: https://www.3gpp.org/news-events/2136-r17_delay (Accessed: 1 March 2022).

Ahmad, I. (2018) *Overview of 5G Security Challenges and Solutions*, *IEEE Explore*. IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/8334918 (Accessed: 1 March 2022).

Ahmada, A., Desouza, C. and Boorman, J. (2019) 'Strategically-motivated Advanced Persistent threat: Definition, process, Tactics and a Disinformation Model of Counterattack', *Elsevier*, 86, pp. 402–418. Available at: sciencedirect.com/science/article/pii/S0167404818310988 (Accessed: 5 March 2022).

Arunachalam, S. *et al.* (2018) 'Analysing 5G: Prospects of Future Technological Advancements in Mobile', in *IOSRJEN*. Mubai: IOSRJEN, pp. 06-11. Available at: https://www.researchgate.net/publication/324941597_Analyzing_5G_Prospects_of_Future_Technological_Advancements_in_Mobile (Accessed: 13 March 2022).

Christos, B., Anastasia, K. and Andreas, P. (2017) 'SDN & NFV in 5G: Advancements and challenges', in *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*. Paris, France: IEEE, pp. 107–111. Available at: https://ieeexplore.ieee.org/document/7899398 (Accessed: 12 March 2022).

Ericsson (2020) *Sony Ericsson: Technology Review*, *Ericsson*. Ericsson. Available at:

https://www.ericsson.com/49bdd9/assets/local/reports-papers/ericsson-technology-review/docs/2020/5g-nr-evolution.pdf (Accessed: 22 February 2022).

Ericsson (2022) *5G RAN*, *Ericsson*. Ericsson. Available at: https://www.ericsson.com/en/ran (Accessed: 27 February 2022).

Fabio, G. *et al.* (2018) 'MEC Deployments in 4G and Evolution Towards 5G', *ETSI*, 24(979-10-92620-18-4), pp. 1–8. Available at: https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp24_mec_deployment_in_4g_5g_final.pdf (Accessed: 4 May 2022).

Fabrico (2019) *5G Security*, *Fabrico's Apps*. Fabrico. Available at: https://fabricioapps.blogspot.com/2019/02/5g-security.html (Accessed: 11 April 2022).

GSMA (2019) *5G Security Issues*, *GMSA*. GMSA. Available at: https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf (Accessed: 21 February 2022).

Gupta, A. and Jha, R.K. (2015) 'A Survey of 5G Network: Architecture and Emerging Technologies', *IEEE*, 3(2169-3536), pp. 1206–1232. doi:10.1109/ACCESS.2015.2461602.

Hewko, A. (2021) *STRIDE Threat Modeling: What You Need to Know*, *Software Secured*. Available at: https://www.softwaresecured.com/stride-threat-modeling/ (Accessed: 5 April 2022).

Khan, M. *et al.* (2018) 'Defeating the Downgrade Attack on Identity Privacy in 5G', *arXiv*, 11322, pp. 95–119. doi:10.1007/978-3-030-04762-7_6.

LucidChart (2022) *LucidChart*. Available at: https://www.lucidchart.com (Accessed: 15 April 2022).

Martínez, G., Hernández, E. and Sánchez, Á. (2010) 'A Survey of the Elliptic Curve Integrated', *Journal of Computer Science and Engineering*, 2(2), pp. 7–13. Available at:

http://hdl.handle.net/10261/32671 (Accessed: 15 April 2022).

Mattsson, J.P., Comak, P. and Karakoç, F. (2021) *The Evolution of Cryptography in Mobile Networks and How to Secure Them in the Future*, *Ericsson*. Available at: https://www.ericsson.com/en/blog/2021/6/evolution-of-cryptographic-algorithms (Accessed: 16 April 2022).

Modadugu, N. (2006) *Datagram Transport Layer Security*, *Data Tracker*. Available at: https://datatracker.ietf.org/doc/html/rfc4347 (Accessed: 11 April 2022).

Mumtaz, S., Rodriguez, J. and Dai, L. (2017) *Chapter 1 - Introduction to mmWave massive MIMO*, *Ebook Reading*. Available at: https://ebookreading.net/view/book/EB9780128044780_9.html (Accessed: 16 April 2022).

Naqvi, S. *et al.* (2020) 'Ntegrated LTE and Millimeter-Wave 5G MIMO Antenna System for 4G/5G Wireless Terminals', *Sensors*, 20(14). doi:10.3390/s20143926.

Olimid, R. and Nencioni, G. (2020) '5G Network Slicing: A Security Overview', *IEEE*, 8, pp. 99999–100009. doi:10.1109/ACCESS.2020.2997702.

Shevchenko, N. (2018) *Threat Modelling: 12 Available Methods*, *Insights*. Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (Accessed: 6 April 2022).

Spitzner, L. (2003) 'Honeypots: catching the insider threat', in *IEEE*. 9th Annual Computer Security Applications Conference, 2003, pp. 170–179. doi:10.1109/CSAC.2003.1254322.

Tech Play On (2019) *5G Identifiers SUPI and SUCI*, *Tech Play On*. Available at: https://www.techplayon.com/5g-identifiers-supi-and-suci/ (Accessed: 11 April 2022).

TelnorGroup (2020) *Security Architecture Design Phase: The concept of a threat intelligence driven defendable architecture*, *Telnor*. Available at: https://www.telenor.com/security-architecture-design-phase-the-concept-of-a-threat-intelligence-driven-defendable-architecture/ (Accessed: 16 April 2022).

Yousaf, F.Z. *et al.* (2018) ‘NFV and SDN—Key Technology Enablers for 5G Networks’, *IEEE Journal on Selected Areas in Communications*, 35(11), pp. 2468–2478. doi:10.1109/JSAC.2017.2760418.