UNIVERSITY OF TURKU

Zero Trust Threat Modeling: STRIDE-ZTA

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Amy Nymalm

Supervisors:

Antti Hakkala (University of Turku)

Petri Sainio (University of Turku)

Sonika Ujjwal (Ericsson)

Zakaria Laaroussi (Ericsson)

June 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Amy Nymalm
Title: Zero Trust Threat Modeling: STRIDE-ZTA
Number of pages: 62 pages
Date: June 2025

The concept of perimeterless security has gained popularity, today known as zero trust. Zero trust architecture is complicated, consisting of complex logical components that change the security posture of a system. This change is driven by the need for better security, but with such a change in architecture, it is possible that new threats arise, or old threats are not mitigated after all. To determine the threats present in a system, threat modelling can be used. However, with the changes zero trust architecture brings, traditional threat modelling methods might not be sufficient in locating all possible threats.

This thesis aims to find answers to the questions of what threat modeling framework is sufficient for performing threat modeling on zero trust systems and how zero trust affects the threat modeling process. In addition, this thesis will focus on an interface in the 5G radio access network, the Xn-interface, and examine if zero trust affects the threat modeling process on the interface. Relevant research is found though a literature review.

Based on the research done in this thesis, zero trust does not severely change the way threat modeling is performed, but benefits from certain additions compared to more traditional threat models. These additions include possible new threats to consider, as well as a shift in perspective so that insider threats and compromised assets are better accounted for during the threat modeling process. A threat modeling methodology that takes these concerns into consideration is proposed: STRIDE-ZTA. STRIDE-ZTA is a threat model designed for zero trust systems that also takes zero trust maturity into account. A proof of concept is performed on the proposed model using the Xn-interface to examine the usability of the model, as well as to examine the effects of zero trust on threat modeling the Xn-interface. Based on the proof of concept, STRIDE-ZTA is usable, and zero trust affects the threat modeling of the Xn-interface in the same way as threat modeling in general. Future research of STRIDE-ZTA and zero trust maturity can further polish the model to maximize its usability.

Keywords: Zero trust maturity, threat modeling, 5G, Xn-interface.

Table of contents

Table of Figures

Table of Tables

Acknowledgements

I would like to thank Antti Hakkala and Petri Sainio for supervision and support during my work. I would also like to thank the entire Ericsson team, with a special thanks to my company supervisors Sonika Ujjwal and Zakaria Laaroussi, as well as Kristian Slavov and Vesa Lehtovirta for providing valuable feedback and always being there to answer questions. Lastly, I would like to thank my friends and family for supporting me through my studies and during the process of writing this thesis.

1 Introduction

Cyber threats are becoming increasingly sophisticated and widespread. As organizations tackle both new and old cybersecurity challenges, the need to rethink traditional security approaches has gained traction. Traditional perimeter-based security models have proven inadequate in sufficiently safeguarding sensitive information [1], which has led to the re-emergence of perimeter-less security, today known as zero trust. Zero trust emphasizes the principle of "never trust, always verify", highlighting the idea that access requests should be verified and authorized, even if the request is coming from inside the network [2].

By following zero trust principles, the assets in a network should be safe from attacks, be it from outside the network or from the inside. However, a perfect zero trust system is still only a concept and is yet to be fully implemented in real-life scenarios [3]. This also means that there is little knowledge on the actual security of zero trust systems. Since zero trust will change the security architecture of a system to combat certain threats, there is a possibility of it introducing other security flaws instead. The possible security flaws and threats need to be studied to better secure future zero trust implementations.

A typical way to find threats in a system is through threat modeling. A threat model is a way to identify and understand potential risks or vulnerabilities in a system by locating possible threats [4]. Threat models often utilize sets of threats that are relevant for specific systems. Since zero trust systems are still mostly concepts, they have not been threat modeled much specifically as zero trust architecture. Because of this, and the fact that zero trust brings changes to a system's security architecture, there is a possibility that existing threat models do not sufficiently map the threats relevant for zero trust systems.

This thesis will explore zero trust threat modeling, examining the existing zero trust threat models that exists, as well as analyzing the sufficiency of the general threat model STRIDE. The rest of this introduction chapter is organized as follows: Subsection 1.1 introduces the research objective and scope of the thesis, while also defining the research questions and research challenges. Subsection 1.2 clarifies the contributions by this thesis and subsection 1.3 goes through the research methods used. Subsection 1.4 covers related work and finally, subsection 1.5 explains the structure of the following chapters.

1.1 Research Objectives and Scope

This section presents the objectives and scope of the thesis, outlines the research questions, and identifies the challenges inherent in the research process.

The focus of this thesis is to study threat modeling in a zero trust context. The objectives are to find out how zero trust affects the threat modeling process, as well as examining how suitable existing popular threat models are for performing threat modeling on zero trust compliant systems, and if a new model is needed. This step will also need to consider different zero trust maturities, so the model must perform well on different maturity stages of zero trust.

The objectives in this thesis stem from an interest in zero trust principles in 5G networks. However, given the widespread application and possibilities of zero trust across various areas, focusing exclusively on its role within the 5G context would be limiting. Thus, narrowing the scope down to only 5G is not preferable, and the main scope will not be on 5G but on zero trust in general. Still, 5G is to be included as a suitable context for the developed zero trust threat model and will be used to test the model in a proof-of-concept scenario.

1.1.1 Research Questions

This thesis aims to find answers to the following research questions:

- How will zero trust affect the threat modeling process?
- What is a suitable threat modeling framework for performing threat modeling on a zero trust compliant system?
- Will adding zero trust to mobile networks affect the threat modeling and analysis process of the network?

With these research questions we want to highlight the essence of this thesis, which is finding a threat modeling process that suits zero trust and highlights the different maturities a zero trust system might have. However, before finding a suitable model, we will need to examine if zero trust even necessitates a change in traditional threat modeling, and in the case of this thesis, the widely used threat model STRIDE.

1.1.2 Research Challenges

There are some open questions and possible issues with the research objectives. Threat modeling and analysis are not completely objective, and it might be hard to decide what counts as a sufficient threat model. How do we measure if the threat model is suitable? Are the criteria an easy-to-follow simple model or a model that can determine all threats in the best way possible? Easy-to-follow can be subjective and depend on who is performing the threat analysis. On the other hand, it is practically impossible to know if all possible threats have been found in a system. To determine if the model is good, there are no tests that can be performed outside using the model and in that way determining if it works. This requires multiple iterations of testing the model and possibly making modifications along the way.

To objectively evaluate a threat model we would need measurable metrics that we could determine the reliability of the framework with. Coming up with these metrics is difficult, so a challenge will be determining a good model without being able to objectively test it. Because of this, this thesis will determine the success of the model by doing a proof of concept of it. This way we can determine that the model works in a test case and can be further improved over time when used in future works.

Researching zero trust threat modeling is also challenging. There is very little research already done, and new research is published all the time. Relevant research might be published during the writing of this thesis, which will make finding it more difficult, and keeping up with the latest research might not be possible.

1.2 Contributions

The main contribution of this thesis is the creation of a STRIDE based threat model specifically designed for zero trust systems, STRIDE-ZTA. STRIDE-ZTA does not only consist of the threat model itself, but comprises of an entire process flow, from implementing zero trust to the threat modeling, analysis and possible improvements. STRIDE-ZTA is explained in section 3.

In addition to the main contribution STRIDE-ZTA, this thesis contributes to zero trust maturity, zero trust threat model research, and to mobile network specific maturity functions. The zero trust maturity contribution is in the form of created maturity tables that can be used together with STRIDE-ZTA. The thesis also compares zero trust specific threat models to traditional

ones and examines what kind of threat model is suitable for zero trust systems. Finally, the thesis suggests future research directions related to the work done.

1.3 Research Methods

The research for this thesis has been done through a literature review and the proof of concept has been done through performing a threat analysis.

Relevant literature was found through Google Scholar, Google search and through references in already found sources. In addition, already known government sources and 5G standards were used, such as the NIST zero trust documents and 3GPP specifications.

Since the original scope revolved heavily around the 5G aspects, “5G”, “RAN”, and also “Xn-interface” were used to find relevant zero trust research. The first search for general background material included the keywords "threat modeling" OR "threat modelling", "threat analysis", "5G", "RAN", and "zero trust". This search was done with Google Scholar and yielded 31 results on 26.11.2025 that were released later than the year 2020. By removing “RAN”, the number of results grew to 78. Out of the original 31 results, 26 were deemed at least a little relevant, and 5 not relevant at all. To find the papers including the Xn-interface, “5G” and “RAN” were replaced with “Xn-interface”. This yielded only 3 results, which were all included in the previous search.

Most papers related to zero trust and threat analysis/threat modeling found, revolved around open RAN (O-RAN), which is slightly different from the original RAN specified by 3GPP. The results had little research about basic 3GPP specified RAN. Especially zero trust and threat modeling on the Xn-interface was not researched in any of the papers.

The next major topic was zero trust maturity threat modeling. This search was done on 1.4.2025 using Google Scholar, and included the keywords “threat model” and “zero trust maturity”. This search gave 21 results, including duplicates and inaccessible sources. Out of the 21 results, one paper was already cited, 5 papers were relevant, 11 papers were not relevant, and the rest were either inaccessible or duplicates.

The relevant sources included a study on zero trust architecture for multiaccess edge computing [5], including a 2-stage maturity framework with a minimal viable security level and a fully implemented security level. A. Porrier writes on zero trust security in their doctoral thesis, *Formal Security of Zero Trust Architectures* (2024) [1], and develops an evaluation framework

for identifying gaps in zero trust research. B. Karabacak and T. Whittaker study zero trust as a prevention mechanism for advanced persistent threats in *Zero Trust and Advanced Persistent Threats: Who Will Win the War?* [6]. H. Kim et al. perform threat modeling on cloud service providers to find security requirements for building zero-trust-based remote work environments in *a Study on the Security Requirements Analysis to build a Zero Trust-based Remote Work Environment* [7]. The goal of their work is to propose more detailed security requirements for zero trust architectures compared to NIST and Department of Defense (DoD) guidelines. Finally, an insider threat detection system is introduced by A. Kantchelian et al. in *Facade: High-Precision Insider Threat Detection Using Deep Contextual Anomaly Detection* [8].

1.4 Related Work

There is little research and papers to find on zero trust threat modeling and maturity, especially in a 5G context. There are studies on implementing zero trust architecture into 5G, like [9]. Another study on zero trust in mobile networks is done by [10], where they present intelligent zero trust architecture (i-ZTA) as a security framework for 5G/6G networks with untrusted components. The Alliance for Telecommunications Industry Solutions (ATIS) study the applicability of zero trust in 5G [11].

Few 5G zero trust studies cover zero trust maturity. The number of studies about zero trust maturity in the RAN is nonexistent. O-RAN zero trust studies exist, but they cannot be compared directly with traditional RAN, since differences exist in for example interfaces. One of the few studies covering zero trust security pillars in a 5G context is a study done at Siemens Technology US, where the focus was to implement the zero trust pillars by CISA into the 5G core network [9]. The authors in [12] thoroughly research zero trust and even recommend zero trust maturity as future research direction.

Zero trust specific threat modeling is discussed in one blog [3], and an article discussing that blog [13]. Based on the related work, zero trust threat modeling, especially when focusing on zero trust maturity and zero trust in the 5G RAN, is a research gap that has not been studied much. The zero trust threat modeling research done in this thesis fits perfectly in that gap.

1.5 Structure of Thesis

This thesis is structured as follows: Section 2 covers the background needed to understand the work in sections 3 and 4. It will explore the concepts of 5G, zero trust and threat analysis. The

5G background is needed to better understand the proof of concept and zero trust maturity contributions in section 4. The zero trust section will introduce necessary zero trust topics like zero trust components, zero trust controls, and zero trust tenets and maturity. The threat modeling section will go through the threat modeling process and introduce some common threat modeling frameworks and techniques. It will also explain the benefits of threat modeling and provide motivations for why to do threat modeling in the first place.

Section 3 is the main focus of this thesis. It will merge the background topics through exploring zero trust threat modeling and dives deeper into the related work that exist on the matter. Afterwards, the new STRIDE-ZTA threat modeling framework will be introduced with the motivation behind it. This section will also do a thorough walkthrough of the proposed threat modeling process from the beginning to the end. Finally, use cases and usage scenarios will be explored; to find out in which cases the model is suitable for use and where it might be beneficial.

Section 4 will perform a proof of concept of the proposed STRIDE-ZTA model. This section starts with a study on zero trust in mobile networks, including zero trust maturity. Afterwards, the STRIDE-ZTA model is followed.

Section 5 is an analysis section, that analyzes the methodology of the proposed model. This section also discusses possible future research directions, where the proposed model could be used or how it could be improved and developed further.

Finally, section 6 contains the conclusion for this work.

1.6 Use of Artificial Intelligence

This thesis has been written with the help of OpenAI's GPT-4 Omni generative AI. The AI has been used for the following purposes:

- Finding better suited words for specific contexts.
- Rephrasing complicated sentences.
- Checking the correctness of reference list.

2 Background

This section will introduce the concepts relevant to understand the work in sections 3 and 4. Since 5G will be the environment for the proof of concept in section 4, 5G concepts will be introduced first, including relevant components, interfaces and procedures. Afterwards, zero trust will be discussed, including zero trust components, tenets and zero trust maturity. This section will also cover zero trust in mobile networks. Finally, threat modeling will be presented, introducing common threat modeling approaches and the benefits of threat modeling.

2.1 5G

The fifth generation of cellular networks (5G) have been developed to deliver better data rates, wider bandwidth, and lower latency to users compared to the previous generations. In addition, support for high data volumes has made large deployments of internet of things (IoT) devices possible, even in areas with heavy traffic. [14]

5G is specified by the 3rd Generation Partnership Project (3GPP) [15], a unity of telecommunications standard development organizations. 3GPP has produced technical specifications for mobile systems since the beginning of 3G in 1998 [16] and had fully specified 5G functionality in 2019 [15].

This section introduces 5G, emphasizing aspects critical for the proof of concept in section 4. It begins by examining the 5G radio access network (RAN), focusing on key components and interfaces. Subsequently, additional focus is placed on the Xn-interface and its associated procedures. Finally, the section explores 5G security to understand the security measures implemented in the 5G network, particularly in the 5G RAN.

2.1.1 5G Radio Access Network

The 5G system can be divided into 3 main elements as seen in Figure 1: the User Equipment (UE), the RAN (or NG-RAN for Next Generation Radio Access Network) and the 5G Core Network (5GC). As the name suggests, the UE is the user device, or the client of the network that wants access to the services the network provides. The UE can be any end device used by users for communication, like a laptop, cell phone, or even IoT device. The RAN provides 5G radio access to the UE through base stations, the main components in the RAN. The base stations, called 5G Node Bs, or gNBs for short, forward data from the UE to the 5GC, and vice versa. [11]

The 5GC is the component that delivers the actual telecommunication services to the user, like data connections, voice calls, and connections with other network operators [17]. The 5GC is a complex system of diverse network functions and interfaces. To simplify the 5GC in an NG-RAN context, it can be represented by two network functions: the Access and Mobility management Function (AMF) and the User Plane Function (UPF) as depicted in Figure 1. The AMF and UPF are the only network functions in the 5GC that are in direct contact with the gNBs in the RAN, which make them more relevant than the rest. [15] The AMF manages control information, like the access authentication and authorization of the connected UE, while the UPF hosts actual packet routing and forwarding of user plane data between the RAN and 5GC [18].

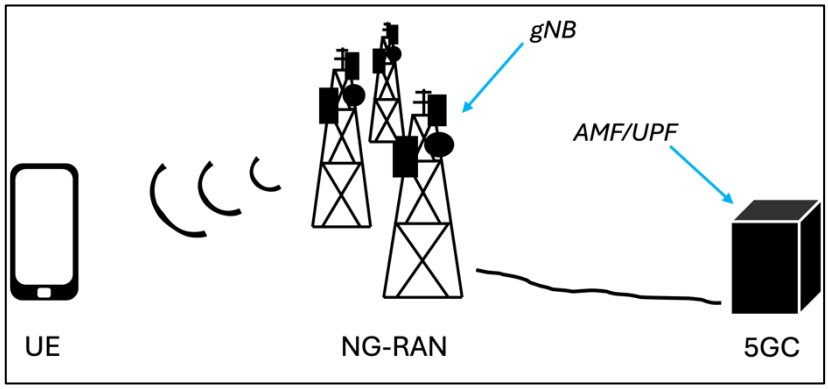

Figure 1. The 5G System [15].

Components and network functions in 5G communicate over interfaces. There are multiple interfaces involved with the RAN. Relevant interfaces include interfaces between the gNBs and the 5GC, between the gNBs and the UEs, and between gNBs themselves. The gNBs are connected to the 5GC via the NG interface, [18] or more specifically, to the AMF via the N2 interface, and to the UPF via the N3 interface [19]. The interface used for communication and data transfer between the gNB and the UE, is called the NR-Uu interface (referred to as Uu going forward) [15]. Lastly, the interface connecting gNBs to each other is called the Xn-interface [18]. In addition to previously mentioned interfaces, the UE also has a connection to the AMF over the N1 interface [19]. However, since the UE does not have a direct communication path to the 5GC, the base stations in the RAN forward these messages.

2.1.2 Xn-Interface

The Xn-interface is a logical interface that allows gNBs to interconnect. The Xn-interface is composed of both user and control plane interfaces, specifically referred to as Xn User Plane (Xn-U) and Xn Control Plane (Xn-C). The dual nature of the interface means that gNBs can efficiently exchange both essential control information and user plane data with each other. While the Xn-C is necessary for the communication between the gNBs, the purpose of the Xn-U is to forward user data during the procedures involving the Xn-interface, like during movement of UE. [20]

The Xn-interface is primarily utilized for two purposes. The first purpose is intra-NG-RAN mobility, which refers to the mobility of the UE from one gNB to another within the same NG-RAN. [20] In intra-NG-RAN mobility, a UE is moved from one serving gNB to another. This process is called a handover and is done to preserve service continuity of the UE. [18] A handover is critical for maintaining uninterrupted service and enhancing user experience as UEs physically move through different areas [21].

In the Xn handover a UE is directly handed over from a source gNB to a target gNB. The handover can be triggered by a need for load balancing, due to new radio conditions, or due to some other service requirement. In addition to the Xn-interface, a handover can also happen over the N2 interface through the core network. The Xn handover is only supported for intra-AMF mobility, meaning mobility where the AMF remains the same. In the case of inter-AMF mobility, where the AMF also changes, an Xn handover is unsuitable and an N2 based handover is used. [21]

The Xn handover is a process that can roughly be divided into three phases: the preparation, execution and completion phases. All these phases are always present in a successful handover. [18]

In the preparation phase, the source gNB makes a handover decision and sends a handover request to a potential target gNB. If the target gNB accepts the handover, it replies with an acknowledgement message. [18]

The execution phase is the main phase of the handover. The UE detaches from the source gNB and synchronizes itself to the target gNB. After the source gNB receives the handover acknowledgement message from the target gNB in the preparation phase, it can start forwarding received user data from the UPF to the target gNB. This means there might be a bit of a delay

in the data stream from when the UE disconnects from the source until it connects to the target. This delay can be circumvented with a dual active protocol stack (DAPS) handover, where the UE is simultaneously connected to both the target and the source gNBs until the handover is complete. [18]

After the execution phase, when the UE has successfully connected to the target gNB, the handover completion phase begins. Up until this point, the Xn handover has been performed without involvement from the 5GC. However, the user data is still flowing from the UPF to the source gNB, since the UPF does not yet know of the handover. The target gNB must make a path switch request to the 5GC. The 5GC switches the downlink data target from the source to the target gNB and acknowledges the change. Lastly, the target gNB informs the source gNB of the completed handover process and the source gNB can drop the information related to the handed over UE. [18]

The second purpose of the Xn-interface is to enable dual connectivity between gNBs. Dual connectivity allows a single UE to maintain simultaneous connections with multiple gNBs. This capability can lead to improved service performance by maximizing data throughput and providing a better network coverage. [20]

2.1.3 5G Security and Security Challenges

5G is counted as critical infrastructure [22]. In addition, 5G networks are complex systems used by an increasingly larger number of users which makes them more attractive targets [12]. This makes the security and resilience of mobile networks important. Robust security measures are needed to safeguard the integrity, confidentiality, and availability of 5G networks. To achieve a reliable security across different networks and vendors, 3GPP have dedicated a big part of 5G specifications and development work for security purposes. 3GPP has specified five security goals for security 5G systems [23]. These security goals include confidentiality, integrity, authentication, replay protection and privacy.

3GPP specified 5G security features include many traits that are familiar in other IT contexts as well, such as authentication, authorization, and encryption requirements. The encryption requirements contain using specific security protocols, like IPsec encapsulating security payload (IPsec ESP) on interfaces between gNBs and the core which provides replay protection and data encryption, integrity, and source authentication in addition to optional confidentiality. In addition, 5G security requirements include more specific security aspects, like protection

from physical attacks and bidding down attack prevention. A bidding down attack is an attack where an attacker makes the network believe that the UE, or vice versa, does not support a security feature and a less secure method must be used for the communication, even though both entities would have supported a more secure method. This is an example of an attack that according to 3GPP specifications shall be prevented. [24]

Even if mobile network generations add new security measures to tackle vulnerabilities present in previous generations, the characteristics of 5G also introduce more security challenges. The new technologies present in 5G architecture have increased the attack surface of 5G. 5G's ability to connect a wide range of devices, including internet of things (IoT) devices opens many possible entry points for cyber threats. In addition, 5G uses technologies like virtualization and network slicing, which increase the number of potential access points into the network, thus increasing the attack surface compared to previous mobile network generations. [12]

Other security challenges present in 5G networks include threat detection challenges and supply chain vulnerabilities. Analyzing the massive amounts of data generated due to the growing number of connected devices and high-speed connections can be challenging. What doesn't help is that the analysis should be done in near real-time to efficiently be able to detect threats. Additionally, the diversity of vendors, protocols and configurations in 5G make threat detection complex, as the security systems must be capable of understanding the diverse types of data across the various environments. [12]

2.2 Zero Trust

Zero trust is a cyber security model that has primarily been developed for better data and service protection in enterprise networks. Before the term "zero trust" was known, the concept existed in cybersecurity as a more secure network strategy, focusing on the security of individual transactions instead of perimeter-based security. After the idea of deperimeterization went public in 2004, it gradually evolved into zero trust. [2] Even if the objectives and ideas behind zero trust are not new, the emergence of modern zero trust architecture tools and new ideas could help institutions become more aware of their security situation and make achieving better security more convenient for them [25].

Zero trust frameworks are built on three fundamental principles: explicit verification at all times, access based on least privilege principles, and the assumption of breach [26]. The concept of zero trust is to never implicitly trust any subject or actor, but to always verify clients for

every request and action in a network before accepting it. Subjects within a security perimeter cannot be trusted just because they are inside the perimeter but should be authenticated and authorized whenever they perform an action or try to access data. The idea behind this is that even if an attacker has access to a resource inside a perimeter, the concept of zero trust should make lateral movement more demanding and lessen the impact and size of a breach. [2] Employing these principles allows zero trust to make fewer assumptions, which helps in eliminating the gaps often seen in traditional security practices [26].

Even if zero trust is getting more and more popular as a concept, actual implementations are still hard to come by [25]. No complete real-world public zero trust architecture exists yet. The only reference architectures that do exist are based on the original NIST zero trust architecture. [3] One possible reason for this is that zero trust is only a security concept with philosophies and controls, but it is not a defined architecture with clearcut implementations, making it ambiguous for potential applications. [25]

The rest of this section will cover the basics of zero trust, discussing what kind of components are part of zero trust architecture, and what controls and policies are used for safeguarding assets. The zero trust tenets developed by the National Institute of Standards and Technology (NIST) will be introduced [2], in addition to the Zero Trust Maturity Model created by the Cybersecurity and Infrastructure Security Agency (CISA) [27]. Finally, the focus will be on how zero trust is implemented in mobile networks.

2.2.1 Zero Trust Components

The focus in zero trust is on continuous authentication and authorization [2]. By authenticating, authorizing and evaluating every access request, legitimate clients should have the privileges to access what they need, while non legitimate subjects are denied access at all. By shrinking trust zones as much as possible, so that the trust zones are as small as singular components, access rules can be made granular, and access can be granted very specifically with least privileges in mind [2]. These small trust zones are called micro perimeters [2].

Zero trust architecture consists of several services and logical components that can be operated onsite or in a cloud. Of the various components three are the most relevant: the policy enforcement point, the policy administrator, and the policy engine. [28] Access in zero trust is granted by the policy enforcement point, which is controlled by a policy decision point. The

policy decision point consists of the policy engine and the policy administrator. [2] The core logical components are illustrated in Figure 2.

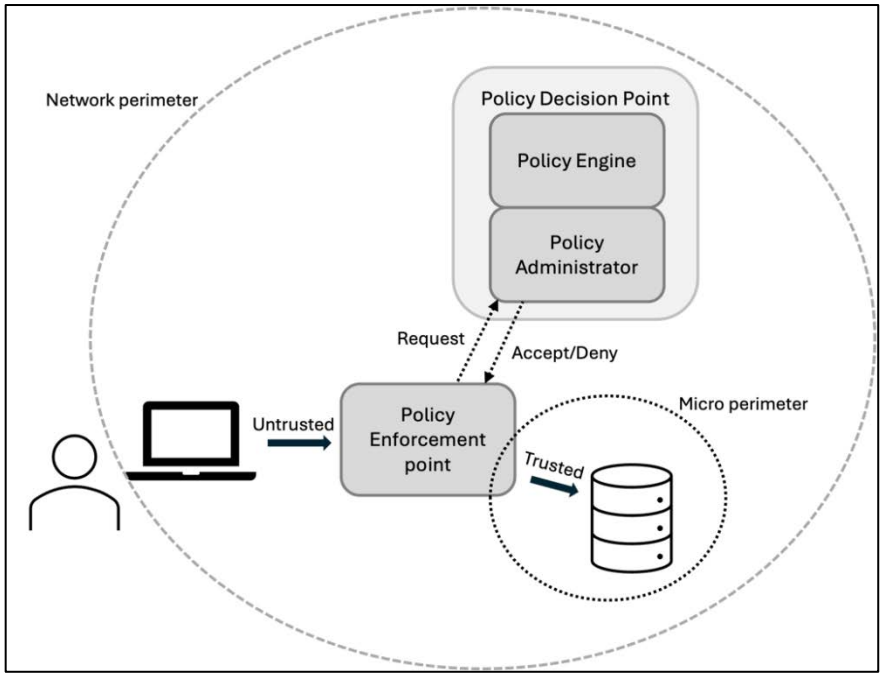

Figure 2: Zero trust policy decision [2].

The policy engine is responsible for making the decision of whether to grant a client access to a resource. The policy engine deploys a trust algorithm to decide whether the access should be granted, denied or revoked. This decision can be made based on a combination of device characteristics, observed behavior, and environmental attributes of the requesting entity. [2] The trust algorithm puts different weights on different attributes depending on their importance and the needs of the system. The decision threshold for granting or not granting access can be determined based on certain criteria or an overall score. The criteria-based access requires that a set of attributes be fulfilled before an action can be permitted, while the score-based access is granted based on a confidence level calculated from the values of input data and compared against a threshold value. [28]

The policy administrator is responsible for handling communication paths between clients and resources. It relies on the decisions of the policy engine to allow or deny a session. In the case of an allowed or denied session, the policy administrator configures the policy enforcement point to either allow the session or deny the connection. [2]

The policy enforcement point is positioned between the client and the resource, acting as a gatekeeper that is told by the policy administrator what to do [2]. The policy decision point provides a dynamically changing confidence score based on various attributes of the subject to

the policy enforcement point, which the policy enforcement point uses to either let the subject connect to the requested resource or not [29]. The trust zone in zero trust is whatever is beyond the policy enforcement point. It can be a bigger trust zone, with multiple components, or it can be a single piece of data or application. Even if it is recommendable to make the trust zones as small as possible, zero trust principles can still be followed with larger trust zones that contain more than one piece of data or functionality. [2]

The number of policy enforcement points in the system corresponds to the number of micro perimeters or trust zones. If the system is large, consisting of many components segregated into their own micro perimeters, also the number of policy enforcement points needed in the system is significant. [29]

2.2.2 Zero Trust Controls

Zero trust architecture encompasses a variety of controls deployed by the zero trust components for safeguarding an organization's digital assets. Relevant controls include a variety of things from access control to logging and monitoring. [30] This subsection will introduce the controls.

The first control is identity and access management [30]. It ensures that only authorized individuals can access specific resources and is done through checking the validity of user accounts and using cryptographic certificates [28]. Closely tied to this is the principle of least privilege, as it limits users' access rights to the bare minimum necessary for completing their tasks. In addition to users being limited to what's necessary for their tasks, they should authenticate using multi-factor authentication. This adds an additional layer of security by requiring users to provide multiple forms of verification, making it more difficult for attackers to breach accounts. Mutual authentication should also be used, to make sure both parties can be trusted. [30]

In addition to access and authentication controls, zero trust architecture controls include network segmentation and micro-perimeters. These divide networks into isolated sections, that can only be accessed through authentication and authorization, limiting lateral movement of attackers and access by unauthorized users. [30] Lastly, zero trust architecture includes logging and monitoring with threat intelligence and continuous diagnostics and mitigation, enabling fast detection and response to suspicious activity [28].

2.2.3 Zero Trust Tenets

Zero trust tenets are principles that guide the implementation of zero trust. Different organizations define these principles a bit differently, while still covering the same core concepts [28]. NIST outline seven tenets in their special publication 'Zero Trust Architecture' [2], providing a framework for designing a zero trust architecture that enhances security posture and resilience against threats. These tenets are not exclusive, as they only specify what should be included in zero trust architecture, not what should be excluded. For example, even if there is assumed “no trust” and micro-perimeters exist in a network, zero trust does not stipulate whether there should still be a wide-area perimeter defense, like a firewall, in the system. [2] In that sense zero trust is flexible, and there isn’t just a single right implementation.

Below are the 7 zero trust tenets as defined by NIST [2]:

1. “All data sources and computing services are considered resources.” Small devices and personally owned devices that can access enterprise resources may be classified as resources.

2. “All communication is secured regardless of network location.” Trust should not be solely granted based on the location of a device, whether it be inside or outside a network. All communication should be confidentiality and integrity protected and be done with source authentication.

3. “Access to individual enterprise resources is granted on a per-session basis.” Requesters are evaluated before being granted access to a resource. Access is granted with least privileges, and authorization to one resource does not automatically grant access to another.

4. “Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.” Based on an organization’s needs and acceptable risk level, the security state of a requesting asset can be based upon device characteristics, observed behavior and environmental attributes.

5. “The enterprise monitors and measures the integrity and security posture of all owned and associated assets.” Since no asset is inherently trusted, the security posture for it must be evaluated when evaluating a resource request. By monitoring the state of

applications and devices, assets that are deemed vulnerable or otherwise don't fulfill the security criteria, may be treated differently or isolated from the rest of the system.

6. "All resource authentication and authorization are dynamic and strictly enforced before access is allowed." Asset management and identity, credential, and access management (ICAM) systems, including multifactor authentication are expected to be implemented in a zero trust architecture. Reauthentication and reauthorization enforced by policies can occur during transactions in a way that a balance of availability, usability, cost-efficiency and security is achieved.

7. "The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture." By collecting data about the network, access requests, and asset security, and then analyzing that data, policy creation and enforcement can be improved.

These tenets defined by NIST are the ideal zero trust goal, but not every security strategy needs a fully implemented zero trust architecture. For some solutions a partial implementation might be enough [2].

2.2.4 Zero Trust Maturity

Making a traditional network zero trust compliant usually does not happen overnight and requires effort, resources and possibly years to fully implement [11]. It might be hard to know what to strive for, and what is enough. CISA have developed a Zero Trust Maturity Model [27] that provides an approach for organizations to design and implement a suitable zero trust architecture for themselves. The maturity model provides detailed guidance and is also supported by Microsoft [31]. It incorporates NIST's zero trust tenets and is explained in this subsection [27].

CISA's Zero Trust Maturity Model consists of five pillars, representing identity, devices, networks, applications and workloads, and data [27]. The pillars have been divided into 4 maturity levels: traditional, initial, advanced, and optimal as depicted in Figure 3. Based on CISA's model, higher maturity levels include more automation, with fully functioning dynamic policies and continuous monitoring with automated triggers at the most optimal level, while the

initial level is more about manual processes. [27] The pillars are explained below, with descriptions of what the different maturity levels might entail.

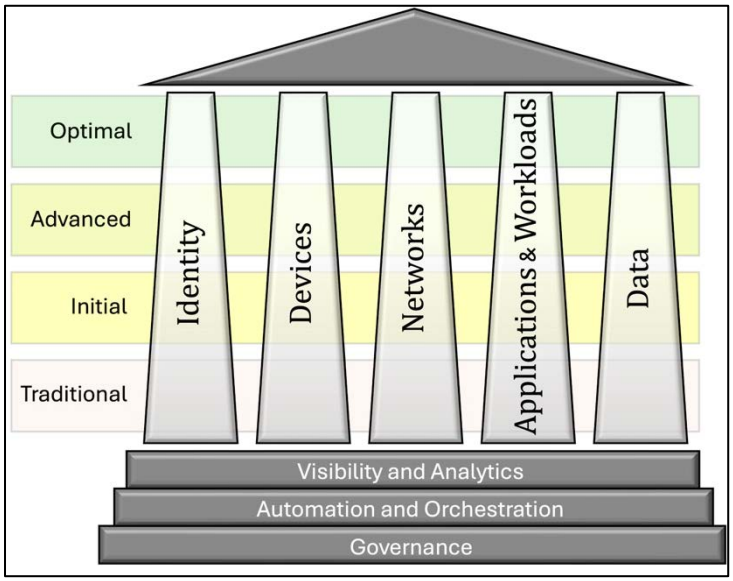

Figure 3: CISA pillars with maturity levels and cross-cutting capabilities [27].

The identity pillar concerns user and entity access. For example, a traditional approach on authentication grants static access on authentication and does not require multi-factor authentication (MFA). The optimal level requires MFA always and continuously, not just on initial request. [27]

The devices pillar concerns assets in the network. A traditional approach to the devices pillar implies manual configuration, maintenance, and deployment of threat protection for devices and virtual assets. Threat protection might only be done for some devices, and lifecycles of devices are manually maintained. A system striving for the optimal approach should instead have centralized threat protection and automated monitoring and lifecycle policies for devices and other virtual assets. [27]

A traditional approach to the networks pillar involves for example large trust perimeters, static network rules and policies, minimal traffic encryption, and a lot of manual processes. Adapting an optimal level of the pillar entails features such as micro-perimeters with dynamic policies and local controls, dynamic network rules and encryption where appropriate. [27]

The fourth pillar, applications and workloads, concerns systems, programs, and services. For the traditional approach, security procedures involve access granting based on static attributes and local authorization, general purpose protection against known threats, security testing only before deployment, and manual policies for accessing applications. Advancing to the optimal

level requires qualities such as continuous authorization for application access, dynamic monitoring across applications, automated application configurations, and security testing throughout a software's development cycle including testing of already deployed applications. [27]

The last pillar, Data, involves all data including metadata across systems, networks and devices. Similarly to the earlier pillars, the traditional approach to the data pillar involves a lot of manual procedures, while the initial, advanced and optimal levels gradually increase automated and dynamic processes. In the case of the data pillar, for example data inventory management and categorization is done manually and in a limited manner in the traditional approach, while the optimal level involves continuous and automated inventory and categorization procedures. The data pillar also includes functions for data availability, access, and encryption, which are primitive on the traditional level and refined on the optimal. [27]

In addition to the five pillars, the CISA Zero Trust Maturity Model has defined three cross-cutting capabilities for integrating advancements across the pillars as depicted in Figure 3. These functions are Visibility and Analytics, Automation and Orchestration, and Governance. [27]

Visibility and Analytics involves collecting logs and analyzing them. On the traditional level this is done manually and in a limited manner, while the optimal level entails comprehensive visibility and dynamic monitoring and analysis of logs and events. [27]

The Automation and Orchestration function is about how operations are orchestrated and how security incidents are responded to. Again, the traditional level relies on manual processes with limited automation, while the optimal level includes dynamic orchestration and response activities to security incidents and changing requirements. [27]

Governance is about policies, how they are implemented and enforced. The traditional approach relies on manual or static processes done in an ad hoc manner. On the optimal level, fully automated policies are in place which allow tailored local controls to be made for specific systems. These controls can then be continuously and dynamically updated. [27]

Zero trust pillars can be modelled in different ways. The forementioned pillars are part of CISA's Zero Trust Maturity Model. DoD have defined their own zero trust pillars. The pillars are similar to those by CISA, also including the crosscutting capabilities automation & orchestration and visibility & analytics as pillars. The setup however is different. In DoD's

model the data pillar is protected by all the other pillars. This is justified by data being a part of all the other resources, and protecting it is one of the foremost goals of zero trust. [29]

2.2.5 Zero Trust in Mobile Networks

Mobile networks are considered critical infrastructure, necessitating higher security measures than enterprise networks in general. However, zero trust architecture can be complex to implement in a mobile network context, partly due to the presence of different data planes and interfaces. The user, control, and management data planes all have their specific standards and protocols. 3GPP specifications outline capabilities related to NIST tenets 1, 2, 3 and 6, and these capabilities are defined differently for each of the data planes. In addition, while implementing security controls across the planes, the mobile network service should be preserved and remain operational. [30]

Zero trust in a 5G environment can be defined as "any access request made to a 5G network function is to be authenticated, authorized and accounted." In addition, all activities in the network should be constantly monitored. [32] Ericsson have summarized the seven NIST tenets as four principles fitting mobile networks [30]:

1. "Network functions and architectural elements are resources secured as micro-perimeters."
2. "Trust is not assumed for any subject, whether human user or network asset, attempting to access a resource. Authentication and authorization are enforced on a per-session basis for external and internal subjects."
3. "Confidentiality and Integrity protection is provided for data in transit on external and internal interfaces, data at rest, and data in use."
4. "Continuous monitoring, logging, and alerting are implemented to detect security events and enforce dynamic security policies."

The principles, although very similar to the NIST tenets provide a more customized guidance on implementation strategies in a mobile network context.

Micro segmentation in 5G has many advantages related to zero trust. Application specific policies for the smaller micro segments become often less error prone and simpler than policies for large heterogenous networks. In addition, developing sophisticated control functions becomes easier when centralized controllers are aware of the state of the whole network. Micro-segments can enforce different access control policies, isolating the perimeters in case of

compromise and restricting lateral movement. Attacks can be more easily tied to a specific location in the network, and the spread of the attack can be minimized. [33]

Even though zero trust is complicated to implement into mobile networks, they are getting more zero trust compliant. One step mobile networks have taken towards better zero trust compliance is the migration to cloud-native network functions [30], as they make the system more open and distributed, instead of it being centralized and tightly coupled. 5G specifications already align with some zero trust principles, like NIST tenet 2, but areas such as policy frameworks, security monitoring, and trust evaluation need further development and standardization [34]. Zero trust tenets in mobile networks are further discussed in subsection 4.2.

One reason zero trust implementations in mobile networks are complicated is the reason that the notion of "trust" in zero trust can be a complex matter. The NIST tenets for instance urge to evaluate the security posture of assets to determine if they can be trusted or not [2], but determining how that trust should be measured is not straight forward. If the trust is based on a score that must reach a certain value, deciding the cut-off value needs to be done with precision. Going off in either direction causes issues, be it restricting service availability to legitimate users and entities or allowing access to malicious ones. One trust modeling approach is suggested by S. Elmadani et al. [35], where they have developed trust evaluation strategies for 5G network slicing.

3GPP started studying a possible alignment of 5G architecture with the NIST zero trust architecture in 2022. This study regarded mostly the 5GC, without consideration for the RAN or UE domains. There have been recommendations of also including the RAN and UE into these studies. [11]

2.3 Threat Modeling

This section introduces threat modeling and its key concepts. Common threat modeling approaches will be discussed as well as the possible benefits and challenges of threat modeling.

Threat modeling plays an important part in designing a secure system. The purpose of threat modeling is to develop a systematic approach to identify and evaluate potential threats in a system with the goal of mitigating them. The process is usually very systematic, involving defining security requirements, identifying assets and threats, drawing data flow diagrams to identify the information flow in the system, evaluating risks, and suggesting mitigations to the identified threats and risks. [17] An essential part of threat modeling is to look for the things

that can go wrong. To achieve this, it is important that the threat modeler knows the system well and can determine the potential attack surfaces. [36]

The Threat Modeling Manifesto [37] introduces four key questions to ask when doing threat modeling:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

These questions explain threat modeling in a nutshell. They are easily understandable by almost anyone and the Threat Modeling Manifesto does emphasize that anyone concerned about security should threat model their systems. [37]

2.3.1 Common Threat Modeling Approaches

Even if the goal of threat modeling frameworks is ultimately the same, threat modeling can be performed in different ways. First, the modeling process itself can differ, since it can be performed manually, automatically, or through a combination of both. In addition, the methods for performing the modeling can differ, with some models using formal mathematical models while others use graphical models, like attack trees or tables. [36]

Threat models can be made for different domains and environments to suit different threat landscapes. Threat models can, for example, be developed for enterprise information systems, as exemplified by the well-known threat modeling framework, MITRE ATT&CK [38].

The situation for mobile networks is less favorable, as a significant domain-specific threat modeling framework has been lacking. Despite mobile networks being around for a long time, in addition to having a lot of threats, no wide-spread threat modeling frameworks dedicated to them exists [17]. A proposal for a mobile network threat modeling framework is the *Bhadra framework* developed by Rao et al. [17], however, it is based on MITRE ATT&CK but can be seen as too simple and incompatible with the original MITRE ATT&CK framework [39]. Instead, a popular and widely used threat model for 5G threat modeling is the STRIDE model [23].

Numerous threat modeling frameworks and methodologies exist, including STRIDE, MITRE, DREAD, OCTAVE and PASTA to name a few, each offering its own set of advantages and disadvantages [23]. STRIDE is a highly structured approach to threat modeling developed by Microsoft to be used in the system design and development process [40]. STRIDE is a mnemonic and stands for the threats spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [4]. The threats are explained in Table 1.

Table 1: STRIDE threats explained [4].

STRIDE	
Spoofing	Spoofing happens when an adversary disguises itself as a legitimate entity. It can also involve using another user's credentials without permission.
Tampering	Tampering equals the unauthorized or malicious modification of data. Tampering can happen to both, data at rest and data in transit, for example data sent over the internet.
Repudiation	Repudiation involves a user or an adversary denying doing something and sufficient evidence of the action is lacking.
Information disclosure	Any information that falls in the hands of an unauthorized entity is an information disclosure threat.
Denial of service	A denial of service attack aims at making a system or service unavailable to its intended users. A typical example is an attack towards a web server, making it temporarily unusable.
Elevation of privilege	Elevation of privilege happens when an unprivileged user gains more permissions in a system. In the worst case an adversary is able to gain administrator access, thereafter being able to perform any actions in a system.

STRIDE aligns its threat categories with the corresponding security properties, establishing a clear connection between identified threats and the appropriate security measures [23]. The threats correspond to the following security properties:

1. Spoofing – authentication
2. Tampering – integrity

3. Repudiation – non-repudiation
4. Information disclosure – confidentiality
5. Denial of service – availability
6. Elevation of privilege – authorization

These six security properties are part of the CIA – R hexagon, which is an extension of the original CIA triad, encompassing confidentiality, integrity and availability [41]. Each letter in the CIA triad symbolizes a fundamental property in cybersecurity. The significance of this security model is evident, since confidentiality, integrity and availability are regarded as the three most critical properties in information security. [42]

2.3.2 Benefits of Threat Modeling

Threat modeling is often done at the design and development phase of a system. This is beneficial for the motivation and support of system design decisions [40]. Threat modeling allows developers to identify and mitigate potential security issues early on before resolving them becomes complex and expensive. As a result, not only is threat modeling beneficial for the security of the system, but it also greatly reduces the cost of development. [4]

Threat modeling helps in recognizing things that could go wrong in a system and allows the developer to pinpoint issues that need to be mitigated [37]. Without design and development phase threat modeling, threats might be overlooked and released systems might have many problems which must be fixed afterwards, making the fixes more expensive compared to if the fix was already added before the launch of the system, or even better, before the development of the system. Threat modeling at the design phase enables Secure by Design, as major security controls are embedded in the system from the beginning [43].

Regular threat modeling sessions not only provide better security systems before launch, but they also encourage continuous evaluation and improvement of security measures as new threats and vulnerabilities emerge.

3 STRIDE-ZTA – Proposal for Zero Trust Threat Modeling

Threat modeling has been around for a long time. Different threat modeling solutions have been developed for different environments and usage purposes [23]. As zero trust gains popularity, it is essential to assess its compatibility with existing threat modeling approaches, determining whether these traditional methods remain effective or if a customized threat modeling strategy is required specifically for zero trust environments.

The introduction of zero trust architecture redefines the understanding of trust requirements within traditional networks and systems. By enforcing more strict criteria for trust, zero trust can potentially impact the effectiveness of threat modeling frameworks created for traditional security systems. Introducing zero trust components changes the attack surface, therefore possibly introducing new vulnerabilities that would not have existed in a non-zero-trust-compliant system [1]. This entails that the shift towards zero trust architecture necessitates a re-evaluation of traditional threat modeling and threat analysis methods. This re-evaluation is crucial in adapting to the dynamic nature of modern threats, ensuring that no possible attack surfaces are overlooked.

In this section we will analyze zero trust threat modeling. We will look at the only existing zero trust specified threat model CAPITALS and weigh the pros and cons of it compared to the traditional threat modeling approach STRIDE. Afterwards, we will propose a new methodology flow for implementing zero trust architecture in a system and performing threat modeling on it. The goal of the proposed model is to break down the zero trust architecture creation and threat modeling process into easy-to-follow steps, with a threat modeling framework fit for zero trust compliant systems.

3.1 Zero Trust Threat Modeling

Zero trust threat modeling is a challenging topic. The only sources found discussing specifically zero trust threat modeling in detail are a conference presentation and blog post by threat modeler Chris Romeo [3] and another short blog by freelance technology writer John P. Mello Jr. [13]. Romeo has developed a threat model designed specifically for zero trust, CAPITALS [3]. However, Romeo's proposed model has not yet been used in any public research, which makes it essential to evaluate the model and consider whether alternative approaches need to be explored. Mello's blog brings together views of multiple different threat modelers, including

Romeo's, but no hard conclusions are drawn in the blog about how zero trust threat modeling is done [13].

Mello's blog highlights the following things to keep in mind when applying zero trust to general threat models: [13]

1. Assumed trust is to be thrown out the window. In threat modeling this means the threat modeler should question existing assumptions and boundaries in the network, including trust relationships between components.

2. Define trust boundaries. The threat modeler should create smaller trust zones in the network by implementing micro perimeters.

3. Identify risks and mitigations. Potential threats like insider threats and compromised devices should be considered.

When zero trust is introduced into a system, old threats might become obsolete, while new threats emerge as the result of new components and functions in the system. For example, continuous authentication and authorization brings the possibility of a new set of threats to be considered, that might not have been relevant in a non-zero trust context [3]. In this case, continuous authentication and authorization could be abusable and launching a denial-of-service attack might be more effective since the system needs to run verifications constantly. In addition, the absence of a larger trust boundary in zero trust architecture presents the risk of an attacker being able to launch an attack closer to critical resources than they would otherwise [3]. These possible new threats mean that we might have to change the threat models and processes used to evaluate threats.

In a zero trust environment we don't necessarily have larger trust boundaries anymore [3], which greatly changes the environment we threat model in. Data sources and computing services might exist only behind a micro perimeter, and classic threat modeling approaches that considers data sources protected from the outside behind a larger trust boundary are not necessarily covering the new micro perimeters. Even if NIST does not explicitly state micro perimeters should completely replace the traditional larger trust boundaries [2], organizations are already implementing zero trust principles that minimize or eliminate these larger boundaries in favor of more granular security controls [44], and this trend is likely to continue. In addition, zero trust assumes an attacker is already in the network, which makes the traditional trust boundary partly redundant for the threat modeling process even if it exists in the system.

The question becomes; how do we determine a good threat model for zero trust? One aspect that has been overlooked in the zero trust threat modeling blogs is zero trust maturity. Zero trust maturity research is difficult to find in papers as well; there are even studies that emphasize the need for further research on zero trust maturity [9].

Since zero trust implementations are complicated and can be overwhelming for organizations [9], we can assume the implementation does not happen overnight. As the process takes time and resources, a good approach could be designing and building the zero trust system incrementally, adding a level of zero trust that fits the current budget and need. In other words, the system would implement a suitable level of zero trust maturity. We would need to take this maturity into account when performing threat modeling and threat analysis on the system. The threat modeling of a zero trust system should not only focus on ideal zero trust implementation, but should take different zero trust maturities into account as well.

Threat modeling and analysis should be effective regardless of the level of maturity of the system. This gives us one criteria in how to determine a successful threat model; it needs to take zero trust maturity into account.

Good threat modeling should be able to identify threats effectively, but this is very hard to measure. Another criterion we could use is the usability and flexibility of the model, but that also brings problems with performance evaluation, since usability is very subjective. These attributes can only be fully achieved through repeated testing, which, in the context of a thesis, can only be superficially addressed. Any thorough testing must be conducted in later research and use.

3.2 Comparing STRIDE and CAPITALS

This subsection will analyze how CAPITALS is tailored for zero trust. We will compare CAPITALS with STRIDE to see what kind of differences there are between the two, and how CAPITALS takes the zero trust aspect into account. We do this comparison, because CAPITALS is based on STRIDE, and we want to evaluate if CAPITALS is better fit as a zero trust threat model compared to a traditional and widely used model such as STRIDE. Like STRIDE, CAPITALS is also a mnemonic, with the correspondence of the letters explained in Table 2.

Table 2: CAPITALS letters explained [3].

C	Compromise & exploit. Happens when an attacker gains unauthorized access or control of an element and/or exploiting its vulnerabilities.
A	Authentication and session management failure: Compromise or failure of the authentication and identification process or mechanism.
P	Poisoning: Introducing misleading or deceptive data.
I	Information disclosure: Exposure of confidential information.
T	Tampering: Unauthorized modification of data or procedures.
A	Authorization bypass: Bypassing any access control procedures in any way.
L	Lack of logging: Neglection of log creation.
S	Segmentation, visibility breakdown and DoS: Disruption of control/data plane, compromise of network visibility, and disruption of service availability.

The CAPITALS blog evaluates the suitability of STRIDE for zero trust systems and builds CAPITALS partly based on the conclusions [3]. Some STRIDE threats are used in CAPITALS, as they are deemed relevant for zero trust threat analysis by the author. The STRIDE threats included in CAPITALS are information disclosure, tampering, and denial of service. As a conclusion to their STRIDE analysis, STRIDE is dismissed as a suitable threat model, because zero trust automatically mitigates the other threats making them irrelevant. One example of this is the dismissal of possible elevation of privilege happening in a zero trust system. Since the core values of zero trust are built around preventing lateral movement and elevation of privilege, the STRIDE threat elevation of privilege is not possible anymore [3].

The arguments used to make STRIDE unsuitable are not used the same way in the creation of CAPITALS. The creation of CAPITALS contradicts itself, since it consists of threats that can be mitigated using zero trust principles. For example, the authorization bypass threat is mitigated by limiting user access with just-in-time and just-enough-access, which is a zero trust principle [2].

Considering threats that are mitigated with zero trust principles is not wrong, since threats should be inspected from different maturity standpoints and a weaker maturity might mean zero trust mitigated threats are still relevant to some degree. However, this is not considered in the STRIDE analysis, but instead STRIDE is dismissed right away based on perfect zero trust

implementations. Considering weaker maturity and flawed zero trust systems, the STRIDE threats might still be just as relevant as the CAPITALS threats.

When looking for a suitable threat model we must consider the possibility of flawed zero trust systems. Just because zero trust in theory automatically mitigates certain threats or threat models, we cannot completely forget about the threats yet. When choosing a threat model, we must make sure that the model is able to cover threats that arise from the zero-trust implementation, like if the new components can be poisoned. However, we must also consider threats that cover an insufficient zero trust implementation. After all, even if we theoretically will be able to make a perfect zero trust system, real-life scenarios might be different.

So, the first flaw of the CAPITALS model is the early dismissal of STRIDE while using the same arguments to support itself. The second flaw are the 'threats' themselves. While STRIDE is composed of actual threats that can be carried out by adversaries, CAPITALS is better explained as a mix of threats and vulnerabilities.

The difference between a threat and a vulnerability is that a vulnerability is a weakness or a flaw in a system, while a threat is an external force that exploits the vulnerability. If we are interested in modeling threats, we should not focus on modeling vulnerabilities. For example, CAPITALS has mapped lack of logging in its model [3], but lack of logging is a vulnerability, and not a threat in itself. Threats can exploit the lack of logging, but the threat is something else, like in the case of lack of logging, repudiation. A lack of sufficient logs can cause a repudiation threat, because the proof of an action might not get logged.

Another interesting aspect to the vulnerabilities mapped in CAPITALS is the correlation with STRIDE. When it comes to the threats, both STRIDE and CAPITALS include tampering, information disclosure and DoS threats. However, the rest of the STRIDE threats: spoofing, repudiation, and elevation of privilege can also be found in CAPITALS, but as vulnerabilities. Spoofing does not exist in CAPITALS as spoofing, but the A in CAPITALS, authentication and session management failure is a vulnerability that can result in a spoofing threat. The STRIDE threat repudiation can be caused by a lack of proper activity logs, which ties to the L in CAPITALS, lack of logging. The CAPITALS C, compromise and exploit is a combination of tampering, elevation of privilege, and possibly other STRIDE threats. Also, CAPITALS letter A, authorization bypass, is technically elevation of privilege. The last CAPITALS threats under the letter S, visibility breakdown and segmentation breakdown can also be mapped to

STRIDE. Visibility breakdown is usually a tampering threat, and segmentation breakdown could be classified as an elevation of privilege threat.

This analysis leaves one CAPITALS threat that is not overlapping with STRIDE, which is poisoning as illustrated in Figure 4. Poisoning is a valid threat not considered in the STRIDE model, that becomes relevant with zero trust components. Poisoning threats become relevant in a system that measures the state of assets and devices, possibly evaluating the secure state with the help of AI. Highly automated systems that rely on behavior attributes and other analytics could possibly be poisoned and "manipulated" to make incorrect security evaluations and even disregard an attack. What makes the poisoning threat special compared to the other threats of STRIDE and CAPITALS, is that it is not usually relevant in a traditional system but becomes relevant in a zero trust system that introduces policy decision points and other AI components.

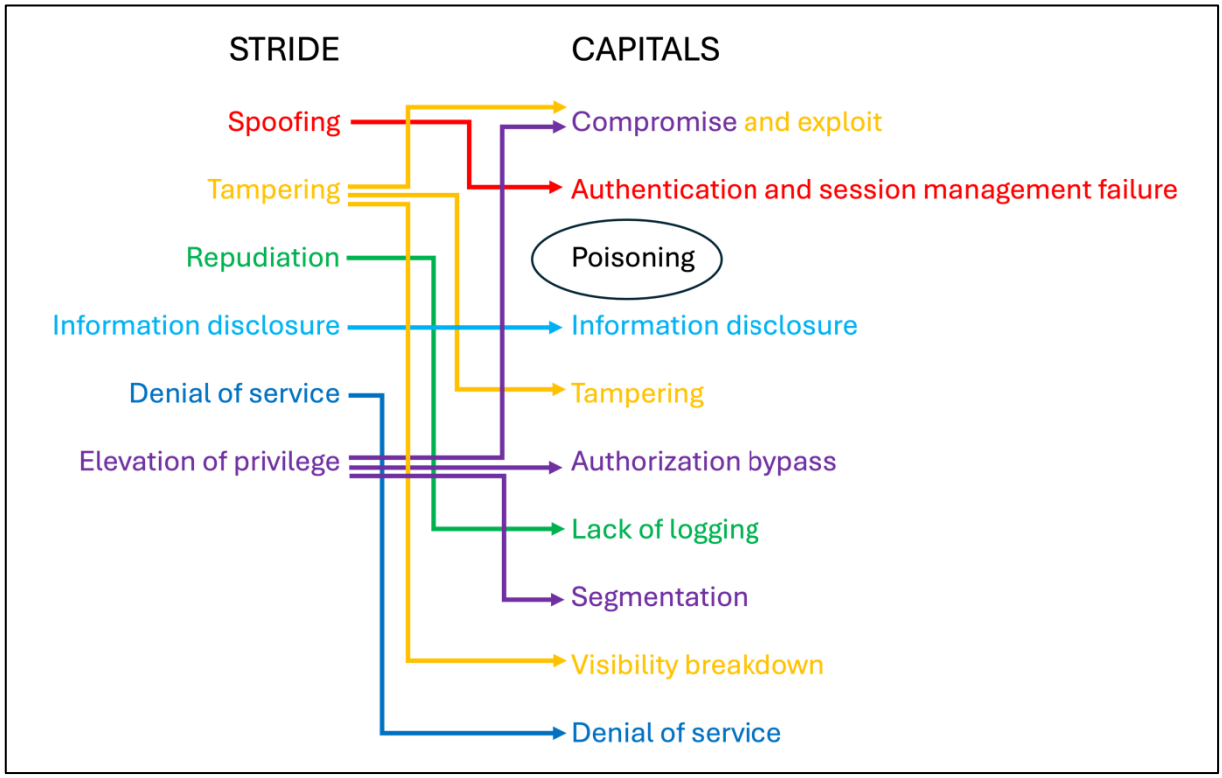

Figure 4: Correlation between STRIDE and CAPITALS threats. Poisoning is the only CAPITALS threat that has no representation in STRIDE.

To conclude, CAPITALS and STRIDE are overlapping quite heavily, and the STRIDE threats are still relevant in a zero trust context. Also, since CAPITALS is not composed of only threats but also vulnerabilities, STRIDE might be a better base for a zero trust threat model. By adding additional threats to STRIDE that consider the particular features of zero trust architecture, we could build a threat model suitable for zero trust systems. As a start, we would need to add

poisoning from CAPITALS as an additional threat. In the next subsection we will further explore the STRIDE-based zero trust threat model.

3.3 STRIDE-ZTA: Proposed Workflow for Zero Trust Threat Modeling Process

To tackle the challenges of zero trust threat modeling while keeping the process as simple and easy to follow as possible, we propose the solution of STRIDE-ZTA. STRIDE-ZTA is not only a threat model, but an entire process that involves the steps necessary to perform a successful zero trust threat analysis.

The reasons for choosing STRIDE as a base for the proposed solution are several. The biggest is that STRIDE is widely used and known [45], so understanding STRIDE-ZTA would not require much extra work if STRIDE is already familiar. In addition, if this threat model is to be used in future works, the popularity of the original model is helpful. There are other threat modeling approaches that have developed niche models based on STRIDE, like STRIDE-AI [41], a threat modeling methodology for machine learning, so STRIDE_ZTA would not be too unusual STRIDE is also easy to follow and is very environment neutral [40], meaning it can be used flexibly across different environments from software systems to 5G networks. This is beneficial, since zero trust systems could exist almost anywhere in the future, so it feels unnecessary to choose a too restrictive approach. Lastly, CAPITALS is the only zero trust threat model we found that already exists and it is based on STRIDE. However, since STRIDE is a widely used and more known threat modeling framework compared to CAPITALS, we decided the best course of action is to design a zero trust threat model based on STRIDE.

In this subsection we will do a walkthrough of the STRIDE-ZTA flow and its steps. Figure 5 illustrates the entire STRIDE-ZTA process and its steps in a flow chart format. The STRIDE-ZTA process consists of a methodology for implementing zero trust into a system, as well as performing threat modeling and analysis on it. The entire process consists of three main phases: the ‘defining scope’ phase, the ‘mapping functionalities’ phase, and the ‘threat analysis and mitigation’ phase. These phases have been color-coded in Figure 5 to be easily distinguishable from each other as the orange, green, and blue phases respectively. We will begin with explaining the first phase, ‘defining scope’ step by step and afterwards move on to the later phases.

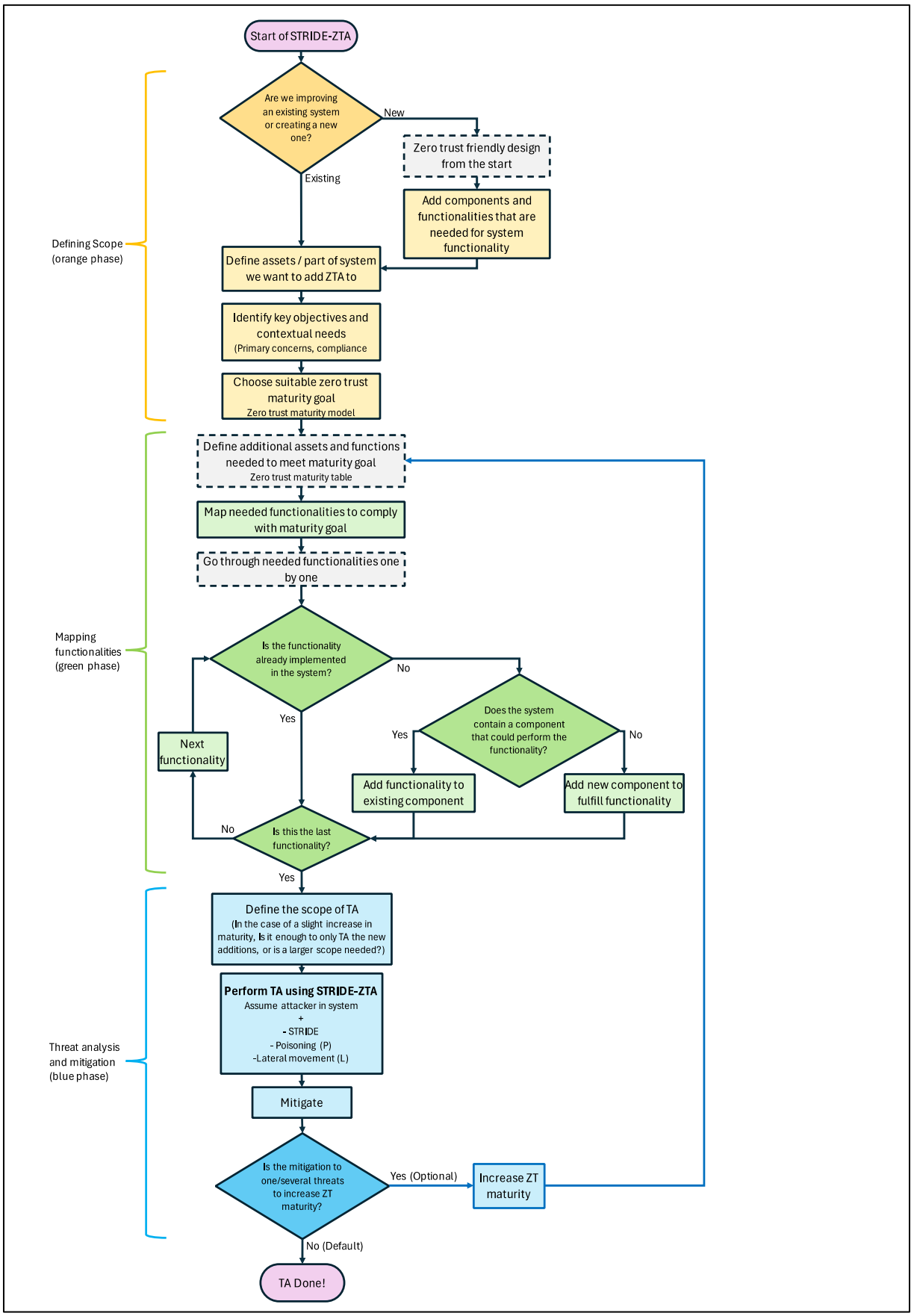

Figure 5: STRIDE-ZTA flow chart. Diamond = decision point, colored rectangle = something needs to be done, gray rectangle = extra explanation.

3.3.1 Defining Scope and Goals

The ‘defining scope’, or the orange phase is the first phase of STRIDE-ZTA as depicted in Figure 5. This phase focuses on determining the level of zero trust maturity to be implemented into our system and consists of one decision point and three or four processes depending on if we are improving an existing system or creating a new one.

Our first path depends on if we have an existing system that we want to make more zero trust compliant, or if we are creating a new zero trust compliant system from scratch. In the case of a new system, we have one extra process to perform compared to an existing system, which is adding all the functionalities and necessary components needed for our system to work properly. This step is preferably done with zero trust already in mind, leaving room for zero trust components and designing connections to easily be integrated with zero trust architecture. Security is not necessarily a main concern at this stage, since we will add zero trust security later on in the process and the possible gaps left by the zero trust implementation can be fixed in the mitigation phase.

Our next steps concern both new and existing systems. We need to specify where in our system we want zero trust architecture. The scope can be larger or smaller, depending on the current need. After we have narrowed down the scope, we want to identify our key security objectives and contextual needs. This will become relevant when we choose a zero trust maturity goal for our system. This stage involves considering compliance requirements and primary security concerns that we want to make sure are taken into consideration.

The last step in the orange phase is choosing a suitable zero trust maturity goal. For this we need to refer to a maturity model, for example CISA’s maturity model [27]. The maturity model should fit the system at hand, so if no suitable maturity model exists, modifying one that exists to better fit the environment or creating a new specific maturity model can be done. Also, the maturity model does not necessarily need to be complex with many maturities and different functions, however this requires further study.

Following the model, we choose a suitable zero trust maturity goal from the chosen maturity model based on our key objectives and goals. Once the zero trust maturity goals have been decided, we can move on to implementing the maturity into our system in the ‘mapping functionalities’, or the green phase.

3.3.2 Mapping Functionalities

The ‘mapping functionalities’, or the green phase is the second phase of the STRIDE-ZTA model as depicted in Figure 5. This phase involves implementing functionalities needed to meet the set maturity goals in the orange phase and consists of multiple decision points and processes.

The first step of the green phase is to define functionalities we need to meet the chosen maturity goal. At this point we might have several functions with different maturity goals, so we need to map the functionalities we need for each and every maturity goal. One maturity goal might map to several needed functionalities, and the smaller and simpler the functionalities are, the easier it will be to add them to the system in the next step. As an example, if the maturity goal requires “encryption of all data”, we can break it down into the functionalities “encryption of data at rest” and “encryption of data in transit”.

Once the needed functionalities have been mapped, it is time to implement the functionalities into our system. Since this process can be performed on an already existing system with existing security solutions, some functionalities mapped might already be implemented in the system. This brings us to the first decision point of this phase, “Is the functionality already implemented in the system?”. If yes, we can move on to the next functionality. If no, we need to implement the functionality into our system. At the next decision point “does the system contain a component that could perform the functionality?” we assess whether the functionality could be implemented with existing components, or if new software or hardware or other components need to be installed to apply the functionality. This process is done incrementally for every functionality we want to implement, so if one functionality requires a new component, that same component might be usable for the next functionality as well.

By going through every functionality one by one, and concluding whether the functionality already exists, can be implemented with existing components, or needs additional components, we can efficiently map how the zero trust functionalities can practically be implemented into our system. Every system architecture is different, and if a functionality can be implemented with existing components it might be beneficial to do so. Implementing all zero trust components that might not even be needed for the chosen maturity, could complicate the architecture in vain. After we have done the functionality addition loop for every functionality, we can move on to the next phase.

3.3.3 Threat Analysis and Mitigation

Once every functionality has been implemented into our system, we can move onto the last phase: ‘threat analysis and mitigation’, or the blue phase. This phase includes the STRIDE-ZTA threat modeling and mitigating the threats, with the optional step of increasing zero trust maturity.

Before proceeding with the threat analysis itself, we should consider how big the scope of our threat analysis should be. In a case where we have used the model to improve a small part of our system, like adding a few lines of code to one single function, we might need a partial analysis only involving the asset relevant to the improvement. However, this step necessitates extreme caution and consideration for a possible butterfly effect. A small modification might affect the system on a bigger scale. If we have made a lot of changes, or if this is the first zero trust threat analysis done for the system, we should use a wider scope.

After choosing the scope, we can move on to the threat analysis. This analysis follows the threats of STRIDE but with a few tweaks and some zero trust specific additions.

What makes STRIDE-ZTA different from normal STRIDE, is that when evaluating the threats, we should consider the possible threats from the perspective of an insider or other attacker already accessing some part of the system. For example, if a network consists of component A and B, we can start the threat analysis from the point of view of an attacker having access to component A. This way we can consider the different threats from the perspective of an attacker already in the system, which is very essential from a zero trust point of view. By explicitly stating the perspective of the possible threat and threat analysis, we can wean off the “outside-in” mindset often present in traditional threat modeling [13]. In addition to the added perspective to the threat analysis, the STRIDE-ZTA threat modeling framework contains the following threats to consider:

- All the normal STRIDE threats: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.
- Poisoning (P) threat is an addition from CAPITALS [3], one of the threats STRIDE does not consider, but which can become prevalent in a zero trust architecture system. Poisoning can occur when an attacker tries to modify policy creation or enforcement mechanisms to their liking by adjusting the data used for policies. One way this can be done is simply by inserting false data into the system that makes AI components act

incorrectly. Another more subtle way an AI component could be poisoned, is through gradually altering data or behaving in a way that makes the components think an abnormal situation is the norm. This way big changes could be made to the system over time, without alerting the system of an issue.

- Lateral movement (L), this threat goes hand in hand with elevation of privilege but is separated because of the possible movement of the attacker, in worst case scenarios between control and data planes to get access to policy mechanisms. This threat is inspired by the CAPITALS segmentation threat.

After the threat analysis performed using the above threats from an insider attack perspective, we can move on to mitigate the identified threats. This can be done the same way as in any other threat analysis. What is different however, is that we can check whether a possible mitigation for an identified threat is found on a higher level of maturity in the zero trust maturity model we used at the beginning of the process. This is an optional step where we can decide to increase the zero trust maturity if it would help in mitigating the threat. By increasing the maturity, we would have to add additional functionalities and we would have to go through the green and blue phases again. This is because if we increase the maturity, we need to see if the possibly added components and functions are prone to any security risks themselves.

3.4 Usage of STRIDE-ZTA

The main objective for STRIDE-ZTA is to be used as a high-level guide in the process of performing threat modeling on zero trust compliant architecture. However, the model could also be used as a high-level guide for implementing zero trust into a system. Even if the objective isn't the threat analysis itself, the orange and green phases can be used to get an abstract view on what functionalities and components should be implemented into the system to make it zero trust compliant to the maturity level specified.

STRIDE-ZTA is designed to be usable across different domains and environments. Since zero trust is a concept that can be implemented almost in any kind of system, the goal of STRIDE-ZTA is to be inclusive and not focus on any specific technology domain. This is why STRIDE-ZTA only encourages to choose a suitable maturity goal but does not specify a maturity model to choose a maturity goal from. Creating or using a maturity model is left for the different domains STRIDE-ZTA can be used for.

The usage of the model is flexible, as it can be used to add single zero trust maturity functions to specific components or it can be used to do big maturity changes. The green phase is designed to work in both scenarios, be it adding many functionalities or just one. The threat analysis scope definition in the blue phase further helps narrowing down the scope for the threat analysis in a case where only a small part of the system was changed in the green phase.

The STRIDE-ZTA process does not necessarily need to start at the beginning of the orange phase, but it can be used by starting at the blue phase as well. When a system that already has zero trust implementations in place should be threat modeled, it is possible to begin from the blue phase. If the threats found can be mitigated by increasing the zero trust maturity, the process can move on to the green phase and afterwards back to the blue phase. Ultimately, STRIDE-ZTA can be used in any way the user wants.

4 STRIDE-ZTA on the Xn-Interface (proof of concept)

In this section we are going to use the STRIDE-ZTA model created in section 3 to perform threat modeling on the Xn-interface. The aim of this proof of concept is to test the viability and performance of STRIDE-ZTA, while at the same time study how zero trust affects threat modeling of mobile networks, specifically the Xn-interface in 5G. After the threat modeling is complete, we are interested to know if STRIDE-ZTA is a suitable model for performing threat modeling on mobile networks in a zero trust context, as well as the general usability of the model.

Some studies on threat modeling for mobile networks [39] as well as studies on threat modeling for zero trust exist [13], but we have yet to find a study combining the two, especially involving zero trust maturity. This is why we want to perform our proof of concept using a 5G environment. O-RAN studies do venture into zero trust and some form of threat modeling [46], however, since the Xn-interface is not an O-RAN specified interface, but instead a 3GPP specified interface, studies related to O-RAN interfaces are not as relevant for this work.

This proof of concept is going to follow the steps of the STRIDE-ZTA model. But before we proceed, we need to have a suitable maturity model ready for mobile networks. CISA's maturity model focuses on enterprise networks, which means they need to be reviewed to make sure they also fit a 5G context.

In this section, we will first examine how zero trust currently maps to 5G, and how applicable the zero trust tenets are to mobile networks. Afterwards, we will create two separate maturity models that could possibly be used as maturity goals for mobile networks. Finally, we will follow the STRIDE-ZTA model step by step to test it.

4.1 Applicability of Zero Trust Tenets to 5G

To know how zero trust can be added to a 5G system, we first need to determine if the entire scope of zero trust is even applicable to 5G. To do this, we can examine which of the NIST zero trust tenets are relevant in a 5G context, which tenets are already considered in 5G, and see if there are tenets that do not need to be considered when designing zero trust security for 5G.

Some already zero trust compliant mechanisms standardized in 5G include access to resources, authentication, authorization and secure communication. These are all well defined in the 3GPP space. The specifications have strict mechanisms in place for what capabilities the networks

should have when it comes to authentication and authorization, including some least access principles. 3GPP requires user identification, authentication, and authorization for system functions, however, MFA is not required, but authentication must be based on a non-spoofable parameter. Authorization must be done with the minimum access required for the task, which is well aligned with zero trust principles. [47] These mechanisms are well aligned with NIST tenets 2 and 3, and according to 3GPP, there are no further actions needed for example for these tenets [48]. However, even if 5G is aligned with some criteria of the tenets, for example the lack of compulsory MFA and trust evaluation shows that the zero trust compliance still could be improved even for tenet 3.

ATIS note that all NIST tenets are in fact applicable to 5G zero trust architecture and any tenets that 3GPP considers out of scope, should instead be addressed by other relevant industry organizations [11]. Based on this, we can conclude that all tenets are applicable to 5G, and we can create our 5G maturity models using all the tenets.

Even if 5G has a lot of zero trust architecture aligning features, it is important to remember that 5G is not fully a zero trust architecture. Further evolution and study on zero trust architecture is expected to better align future networks, like the upcoming 6G, with zero trust principles [11].

4.2 5G RAN Compatible Zero Trust Functions

To concretize the zero trust tenets into needed functionalities, CISA have developed functions to go along with their Zero Trust Maturity Model pillars [27]. The functions embody zero trust principles, providing practical, but still very high-level guidance on how to implement zero trust within each pillar. Since the CISA Zero Trust Maturity Model is made for enterprise networks, the functions are not necessarily applicable as is with mobile networks or 5G. For this reason, we might have to develop a new maturity model suitable for mobile networks as specified in the orange phase of the STRIDE-ZTA flow, or we can modify an existing maturity model.

For this study we did not create new tailored functions fit for mobile networks, but instead modified CISA's existing functions to better suit the 5G RAN, with the exception of the cross-cutting capabilities that are taken from [30]. In general, this modification means small changes in the maturity explanations, adding terminology, and referring to components used in mobile

networks rather than enterprise networks. We also left out a function or two that did not seem at all relevant for mobile networks.

In addition to the maturity model based on CISA's model, we made a second simple maturity table based on the zero trust tenets. The idea is for the user to be able to choose between a more refined approach, which is the complex function-based approach, or a more generic and simpler one that can be used as a good starting point for zero trust maturity. While the CISA based model has over 40 functions to decide maturity for and implement, the tenet-based maturity table has only 7, one for each tenet.

The maturities of both tables are not exclusive, but they build on top of each other, meaning higher level maturity must also fulfill the lower levels of maturity. The only exception to this is a case where the lower-level maturity is conflicting with the higher-level maturity.

4.2.1 Function Based Zero Trust Maturity Table for Mobile Networks

The mobile network zero trust maturity tables can be seen in Table 3 to Table 8. The maturity tables consist of the 5 pillars in CISA's maturity model with their respective functions, including the cross-cutting capabilities. All the pillars have been separated into their own tables. Table 3 consists of the cross-cutting capability functions, Table 4 includes the identity pillar functions, Table 5 includes the devices pillar functions, Table 6 includes the Networks pillar functions, Table 7 includes the application and workloads pillar functions, and Table 8 includes the data pillar functions. The maturity levels in all the tables are the same as in CISA's, apart from the traditional level, which has been left out for the mobile network maturity model. We saw no need to include the traditional level, since the goal is to increase zero trust maturity anyway, so the traditional level is not relevant. This leaves the initial (level 1), advanced (level 2), and optimal (level 3) levels for the modified maturity model. We also added a column in the table that shows the corresponding zero trust tenets that the functions relate to, to easily grasp which tenet the function is trying to improve.

Like in CISA's maturity model, the higher levels of maturity in the mobile network maturity table entail more automation and dynamic processes. While many of the functions can be performed manually, or with simple automation on the initial level, the optimal level for many functions requires sophisticated automation and possibly artificial intelligence (AI) tools.

Table 3: CISA based zero trust maturity table of the cross-cutting capabilities for mobile networks [27].

Zero Trust Maturity specifications for mobile networks (especially RAN) based on 3GPP, no operator specific solutions considered.	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Cross-Cutting Capabilities				
Visibility and Analytics	Automate collection and analysis of logs and events for mission critical functions. Continuous monitoring of security configurations.	Collections of logs and events is expanded network-wide. Telecom specific threat detection. Attack surface assessment.	Centralized dynamic network-wide monitoring and advanced analysis of logs and events. Risk profiles for network functions.	5,7
Automation and Orchestration	Automate orchestration and response activities. Automate selected manual tasks. Managing backhaul IPsec certificates.	Expand network-wide. Automate selected processes. Certificate automation for mTLS.	Activities dynamically respond to network-wide changing requirements and environmental changes. Automated and streamlined processes.	(7)
Governance	Network-wide policies defined and started to be implemented, but still with minimal automation and manual updates. (Select 3GPP security controls for implementation.)	Network-wide tailored policies, with automation to support enforcement where possible.	Implemented fully automated network-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.	7

Table 4: CISA based zero trust maturity table of the identity pillar functions for mobile networks [27].

	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Identity				
Authentication	Identity authentication using MFA or passwords.	Phishing resistant versions of the initial stage. Short authentication expiry. Mandatory MFA.	Continuous identity validation and reauthentication throughout processes.	2,6
Risk Assessments	Risks are identified using manual methods and static rules.	Some automated analysis and dynamic rules.	Real time analysis and identity risk determination based on continuous analysis and dynamic rules.	5,7
Access Management	Any access is always authorized. Authorization expires automatically.	Access is authorized on a need- and session-basis. The access is also tailored to actions and resources.	Automated just-in-time and just-enough access tailored to individual actions and resources.	3,6
Visibility and Analytics Capability	Identity related activity logs are collected, and routine manual analysis is performed with some automated analysis as well.	Automated analysis across identity activity logs of all identities across all environments.	Comprehensive visibility and situational awareness across the network through automated analysis of user activity logs, including behavior-based analysis.	5,7
Automation and Orchestration Capability	Manual orchestration of critical and external identities, but automated orchestration of self-managed entities and other users.	Still manual orchestration of critical identities, but otherwise automated orchestration across all environments.	Automated orchestration of all identities integrated across all environments based on behavior, deployment needs etc.	None
Governance Capability	Manually maintained network-wide enforcement of identity policies.	Some automated enforcement and periodic updates	Automated, continuous policy enforcement with dynamic updates.	7

Table 5: CISA based zero trust maturity table of the devices pillar functions for mobile networks [26].

	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Devices				
Policy Enforcement & Compliance Monitoring	NFs and other devices report behavioral characteristics, but policy enforcement mechanisms are limited.	Enforced compliance for NFs and other devices and assets. Automated management processes (approve software, identify issues…)	Continuous verification compliance enforcement throughout the lifecycle of NFs.	5
Asset and Supply Chain Risk Management	Tracking of all physical and virtual assets. Risk management through policies and control baselines.	Automated processes for comprehensive tracking across assets for risk management purposes.	Real-time view of assets and NFs, automating the risk management as applicable.	1,7
Resource Access	Basic level of access monitoring. NFs / other entities must provide some data (identity, location, security posture...) before being granted access.	Requesting NF/entity must be verified before being granted access (security status, access credentials...).	Real-time risk characteristics and analytics are used to make access control decisions. Continuous assessment of NFs and other entities. Access is dynamically granted based on assessment.	1,2,3,4,6
Threat Protection	The network has some automated processes for deploying and updating threat protection capabilities to NFs. Limited integration of policy enforcement and compliance monitoring.	The threat protection capabilities are being combined into centralized solutions. Initial integration with policy enforcement and compliance monitoring.	Centralized threat protection for all network functions and other network components. Complete integration with policy enforcement and compliance monitoring.	None
Visibility and Analytics Capability	Manual inventory of NFs and other assets. Some anomaly detection might be in place.	Automated inventory collection, monitoring, and anomaly detection.	Automated status collection of all devices and assets. Correlation with identities with monitoring and anomaly detection.	1,5
Automation and Orchestration Capability	Some tools and scripts in place for automating configuration etc. for devices and assets.	Monitoring and enforcement mechanisms to identify and manually disconnect/isolate flagged devices and assets as needed.	Fully automated processes for monitoring and isolating devices and assets. Provisioning, remediation among other possible automation objectives are automated as well.	5
Governance Capability	Policies for the procurement of new devices. Regular monitoring and scanning of devices.	Network wide device lifecycle policies, with some automated enforcement mechanisms.	Automated lifecycle policies for all devices and assets.	1,5,7

Table 6: CISA based zero trust maturity table of the networks pillar functions for mobile networks [26].

	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Networks				
Network Segmentation	Network isolation of critical workloads, where connectivity is constrained according to the principle of least privilege.	Network architecture with some micro perimeters and service specific interconnections.	Extensive micro-segmentation with fully distributed micro perimeters and dynamic just-in-time and just-enough connectivity.	1,2,4
Network Traffic Management	Traffic management mapping of network functions, introducing static rules and manual audits of risk-profiles.	Dynamic network rules that are periodically adapted based on risk-assessments of entity- and network-profiles.	Dynamic network rules throughout the network that continuously evolve based on the current status of the network.	2,7
Traffic Encryption	Encryption of control-information and some user-plane data. Beginning to formalize key management policies.	Rotation of keys and certificates. User-plane data is also encrypted.	All sensitive data sharing and communication is encrypted. Secure key management with best practices.	2
Network Resilience	Expansion of resilience mechanisms for most common scenarios. Network capabilities to manage growing user loads.	Dynamic management of availability demands and resilience mechanisms for majority of scenarios.	Awareness in adapting changes in availability demands, providing proportionate resilience.	5,7
Visibility and Analytics Capability	Network monitoring based on known indicators of compromise. Some threat hunting activities.	Anomaly based network detection capabilities for situational awareness across the network. Automated processes for robust threat hunting activities.	Visibility into all communication with advanced monitoring capabilities and situational awareness.	5
Automation and Orchestration Capability	Some automated methods for managing network configurations. All resources have a lifetime based on policy.	Mostly automated management of configuration and resource lifecycles for networks. Responding to risks and enforcing policies and protection.	All management of configuration and resource lifecycles for networks is automated. Also automated change management methods.	7
Governance Capability	Implementation of individually tailored policies for different parts of the network.	Automation for implementing tailored policies. Facilitate transition from perimeters to micro perimeters.	Automated network-wide policies that enable tailored controls with dynamic updates.	7

Table 7: CISA based zero trust maturity table of the applications and workloads pillar functions for mobile networks [26].

	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Applications and Workloads				
Application Access	Some implementations of authorization access based on contextual information. Requests with expiration.	Automated application access decisions with expanded contextual information. Enforced expiration with least privilege principles.	Continuous authorization of application access. Incorporate real-time risk analytics based on factors like behavior patterns.	3,4,6
Application Threat Protections	Threat protection as part of mission critical workflows. Protection against some application specific threats in addition to general purpose protection.	Threat protection as a part of all application workflows. Some targeted threat protection.	Advanced threat protection in all application workflows. Real-time visibility and protection against sophisticated and targeted attacks.	7
Secure Application Development and Deployment Workflow	Infrastructure in place for adequate development, testing and deployment of applications. Good access controls with least privilege principles.	Distinct and coordinated teams for development, security and operations. No unnecessary developer access.	Changes allowed only through redeployment. More automated processes instead of administrator access to deployment environments.	7
Application Security Testing	Some dynamic security testing prior to application deployment.	Security testing integrated into the development and deployment processes. Included periodic dynamic testing methods.	Security testing integrated throughout the software development lifecycle. Routine automated testing of already deployed applications.	7
Visibility and Analytics Capability	Some automated application profile and security monitoring for improved log collection and analytics.	Profile and security monitoring is automated for most applications.	Continuous and dynamic monitoring across all applications.	5,7
Automation and Orchestration Capability	Periodic modification of application configurations to meet relevant performance and security goals.	Automated application configurations for response to operational and environmental changes	Automation to continuously optimize configurations for security and performance.	7
Governance Capability	Some automated policy enforcement for application development, deployment and management.	Network wide tailored policies for application development, deployment and lifecycle.	Fully automated policies governing the application lifecycle from development to end of life.	7

Table 8: CISA based zero trust maturity table of the data pillar functions for mobile networks [26].

	Initial (level 1)	Advanced (level 2)	Optimal (level 3)	zero trust tenets
Data				
Data Inventory Management	Some automated data inventory processes, some solutions in place for protection against data loss.	Automated data inventory and tracking. Data loss prevention based on static attributes and/or labels.	Continuous inventories of all applicable data with robust data loss prevention strategies.	1
Data Categorization	Some data categorization strategy in place. Manual enforcement mechanisms.	Some data categorization is automated. Labeling in simple, structured formats.	Automated data categorization and labelling, taking all the different data types and formats into account.	1
Data Availability	Off-site backups for important data.	Automated data access controls.	Dynamic methods for optimizing data availability.	None
Data Access Identical to Application access	Some least privilege automated data access controls.	Automated data access controls that consider various attributes. Access is time limited where applicable.	Automated just-in-time and juts-enough data access controls. Continuous review of permissions.	3,4,6
Data Encryption	Encryption of critical data in transit and critical data at rest. Some key management policies and secure keys.	Encrypts all data in rest and transit. Cryptographic agility, with protection of encryption keys.	Encrypts all data where appropriate (also data in use). Secure key management with up-to-date standards.	1,2
Visibility and Analytics Capability	Some automated analysis of data. Visibility obtained through data inventory management.	Comprehensive data visibility with automated analysis.	Predictive analytics hat support comprehensive views of data and continuous posture assessment.	7
Automation and Orchestration Capability	Some automated processes to implement data lifecycle and security policies.	Data lifecycle and security policies are implemented primarily through automated methods in a consisted and targeted manner.	Automation of data lifecycles and security policies to the maximum extent possible.	1,7
Governance Capability	High-level data governance policies. Manual implementation.	Integration of data lifecycle policy enforcement across the network.	Policies are dynamically enforced across the network.	7

4.2.2 Tenet Based Zero Trust Maturity Table

The simple maturity table based on the zero trust tenets can be seen in

Table 9. Instead of functions, the maturity table assesses the maturity of the 7 zero trust tenets. The contents of the different maturity levels have been decided on with the help of the zero trust tenet correlation of the maturity table based on CISA's maturity model. By combining the message of the tenets and suitable function maturity from CISA's maturity model, we came up with the tenet maturity table. The maturity levels 1, 2, and 3 correspond to the initial, advanced, and optimal maturity levels in Table 3 to Table 8.

In this subsection we will explain the motivation behind the choices for the tenet-based maturity table. The tenet maturity table is designed to be a simple and high-level guide for what the maturity levels for the zero trust tenets could look like, and what aspects need to be considered if we want to comply to a certain maturity for specific tenets.

For tenet 1, we decided to build on the description of "all data sources and computing services are considered resources." This tenet description is very vague and only requires the consideration of assets. We wanted to build on this; thus, we added increasingly sophisticated asset tracking and inventory requirements to the different maturities so that the highest-level maturity requires full real-time view of all assets.

Tenet 2 maturity levels are straight forward. They require increasingly more encryption and key management on the higher levels. For this tenet, the functions from Table 3 to Table 8 corresponding to tenet 2 were used to create suitable maturity levels for it. In a similar way, the maturity for tenet 3 is based on the access management function in Table 4. The access authorization is defined more granularly with the higher maturity.

For tenet 4, we thought the sensible solution would be to increase the complexity of the dynamic policy, making security posture evaluation much more elaborate on the higher levels. This tenet also includes the increasingly extensive micro segmentation with the increasing maturity. Similarly for tenets 5, 6 and 7, it is logical that the network wide monitoring, automation, reauthentication processes, and policy creation become more complex with the higher maturity levels.

Table 9: Maturity table for zero trust tenets.

Maturity for zero trust tenets	**Maturity level**		
Tenet	1	2	3
1: "All data sources and computing services are considered resources."	All assets in the system are known and tracked (devices, data, networks...) Manual asset inventory.	Automated processes for asset tracking and asset inventory collection and management.	Real-time view of all assets, including asset status.
2: "All communication is secured regardless of network location."	Encryption of control-information and some user-plane data. Formalize some key management policies.	All Control-information and user-plane data is encrypted. Also, data at rest is encrypted.	All sensitive data sharing and communication is encrypted. Secure key management.
3: "Access to individual enterprise resources is granted on a per-session basis."	Access is authorized and expires automatically.	Access is authorized on a need- and session-basis	Automated just-in-time and just-enough access tailored to individual actions and resources.
4: "Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes."	Basic level of access monitoring. Entities must provide some data or contextual information (identity, location, security posture...) before being granted access. Network isolation of critical workloads.	Automated application access decisions with expanded contextual information. Some procedures in place for security posture evaluation. Some microperimeterization and service specific interconnections.	Real-time risk characteristics and continuous assessment of entities based on attributes such as behavior to evaluate security posture. Dynamic access based on the assessment. Extensive micro-segmentation with fully distributed micro perimeters.
5: "The enterprise monitors and measures the integrity and security posture of all owned and associated assets."	Devices report behavioral characteristics. Risks and anomalies are identified using manual methods and static rules.	Parts of analysis and anomaly detection automated with dynamic rules. Mechanisms to identify and manually disconnect/isolate flagged devices and assets.	Centralized dynamic network-wide monitoring and status collection of all devices and assets. Automated processes for isolating assets as needed.
6: "All resource authentication and authorization are dynamic and strictly enforced before access is allowed."	Human users: Identity authentication using MFA or strong password before access granting. Devices etc: Must provide some data to prove legitimacy (identity, location..)	Human users: Mandatory phishing resistant MFA before access granting. Devices etc: Must be verified before access (security status, access credentials...)	Human users: Frequent re-authentication and identity validation. Devices etc: Dynamic access based on real-time risk characteristics and analytics.
7: "The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture."	Automated collection and analysis of logs and events for mission critical functions. Network wide policies defined and implemented, manual maintenance.	Network-wide collection of logs and events. Tailored, network wide policies are automated where possible and periodically updated.	Advanced analysis of logs and events with real time risk determination. Fully automated network wide policies that enable tailored local controls. Policies are dynamically updated.

4.3 Following the STRIDE-ZTA Model

In this subsection we will follow the STRIDE-ZTA methodology in Figure 5 step by step to see how zero trust affects threat modeling of the Xn-interface. The main focus will be on the execution of the different steps and the flowchart as a whole. Because of this, once we get to the threat analysis and mitigation part, we will not perform a thorough threat analysis of the system since performing the threat analysis in its entirety would be too time-consuming at this point in time and a bit out of scope for this work. Instead, we will touch aspects that need to be taken into consideration when performing the threat analysis.

4.3.1 Choosing a Maturity Goal – the Orange Phase

Starting with the orange phase, we must first know the system we are examining. In this case we are examining the Xn-interface in the 5G RAN, so we move on in the "Existing" direction in Figure 6.

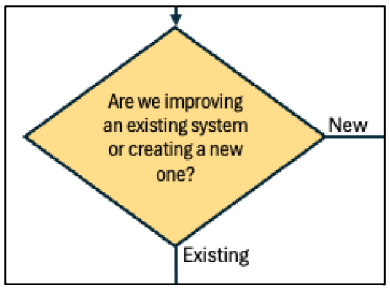

Figure 6: First step of the orange phase.

Next, we need to define the assets that are going to be relevant for our zero trust analysis as stated in Figure 8. We are studying the Xn-interface, concentrating on the Xn procedures, mostly the Xn handover scenario. For this, we need to consider some entities and interfaces, as well as the data flow over the interfaces and possibly data at rest and in use at the entities. The relevant entities include the target and source gNBs, the UPF, the AMF, and the UE. The interfaces include the Xn, N2, N3, and Uu interfaces. The entities and interfaces are visualized in Figure 7. The relevant data includes control plane data, which in this case consists of various handover related messages, data plane data, and data at rest and in use at entities, particularly the gNBs.

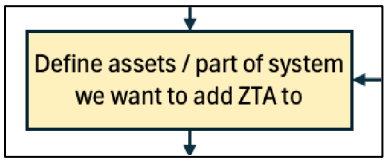

Figure 8: Second step of the orange phase.

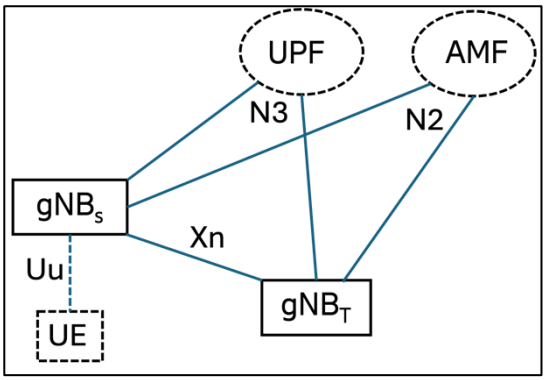

Figure 7: Relevant entities and interfaces for the analysis.

Next, we want to identify the key objectives, and after that choose a suitable zero trust maturity goal as specified in Figure 9. To simplify this proof of concept, we will only choose two key objectives we want to fulfill. The key objectives are:

1. All confidential data is to be secured, at rest and in transit.
2. Entities should only have the authorization to perform tasks they need to function properly.

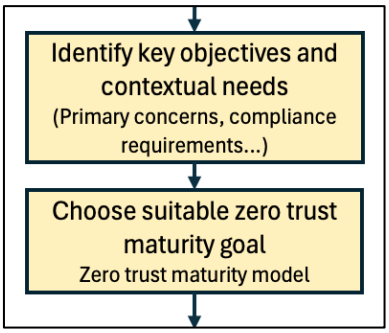

Figure 9: Last steps of the orange phase.

Now that we have chosen our key objectives, we need to determine a suitable zero trust maturity goal. Since we want to keep this proof of concept simple, we will use the tenet maturity model in Table 9 for choosing a maturity goal instead of the function-based maturity tables in Table 3 to Table 8 To choose a suitable maturity goal, we compare our key objectives with the tenet maturity table and choose the maturity goals for the tenets that seem to fit our objectives.

The first key objective directly correlates with zero trust tenet 2; “All communication is secured regardless of network location.” For this tenet, our objective aligns with the maturity level 3, which states that “All sensitive data sharing and communication is encrypted. Secure key management.” This maturity definition does not specify encryption of data at rest, but since the maturities build on top of each other, we also need to take the maturity levels 1 and 2 into account if they do not contradict with maturity level 3. In this case, maturity level 2 specifies that data at rest should be encrypted, so our objective is fulfilled with maturity level 3 of tenet 2. We choose level 3 instead of level 2 because of the secure key management criteria. If we want all data to be secured, secure key management is beneficial as well.

Our second key objective is more complicated and involves multiple tenets. For this task, we will select tenet 3 as most relevant, since it covers access authorization. In addition, we are interested in tenet 1, since we need to know and keep track of the assets in our system so that we can regulate their access permissions. For tenet 3, maturity level 2; “Access is authorized on a need- and session-basis” fits well with our key objective. For tenet 1, a basic understanding of the assets in our system is enough, so maturity level 1; “All assets in the system are known and tracked (devices, data, networks...). Manual asset inventory” is suitable for our objective.

Other tenets that could be seen as relevant are tenets 4 and 6. However, our objective does not exactly specify the need for making sure only authorized and safe entities have access to resources, so we will not include these tenets for this task. In a real scenario we would probably have a key objective of "only authorized and confirmed safe entities should have access to resources," or similar, in which case tenets 4 and 6 would become very relevant.

Now that we have a zero trust maturity goal, we can move on to the green phase of STRIDE-ZTA, to map what functionalities we need to incorporate the tenets into our system. To summarize, the maturities we are going to fulfill are the following:

- Tenet 1, maturity level 1: "All assets in the system are known and tracked (devices, data, networks...). Manual asset inventory."
- Tenet 2, maturity level 3: "All sensitive data sharing and communication is encrypted. Secure key management."
- Tenet 3, maturity level 2: "Access is authorized on a need- and session-basis."

4.3.2 Mapping Functionalities Needed for Maturity Goal – the Green Phase

To begin with the green phase, we need to first find out what kind of functionalities we need to implement into our system to meet the set maturity goal as stated in Figure 10. We will define the functionalities for the needed tenets in Table 10.

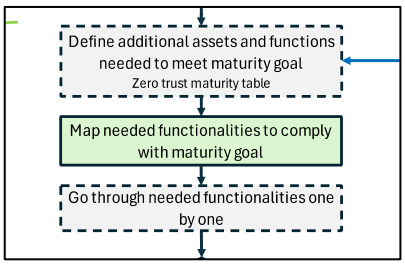

Figure 10: First step of the green phase.

Table 10: Needed functionalities for tenet maturities.

Tenet & Maturity	Needed Functionalities
Tenet 1, maturity 1	Manual asset inventory and tracking (devices, data, networks..).
Tenet 2, maturity 3	Encryption of all sensitive data sharing.
	Encryption of data at rest.
	Secure key management.
Tenet 3, maturity 2	Access authorization and expiry.
	Access policies - what can be accessed and for how long.

We now have 6 different functionalities in Table 10 that we need to implement into our system. Next, we will follow the functionality implementation loop in Figure 11 to add the 6 functionalities to the Xn-interface. We will do this one by one for the functionalities in Table 10.

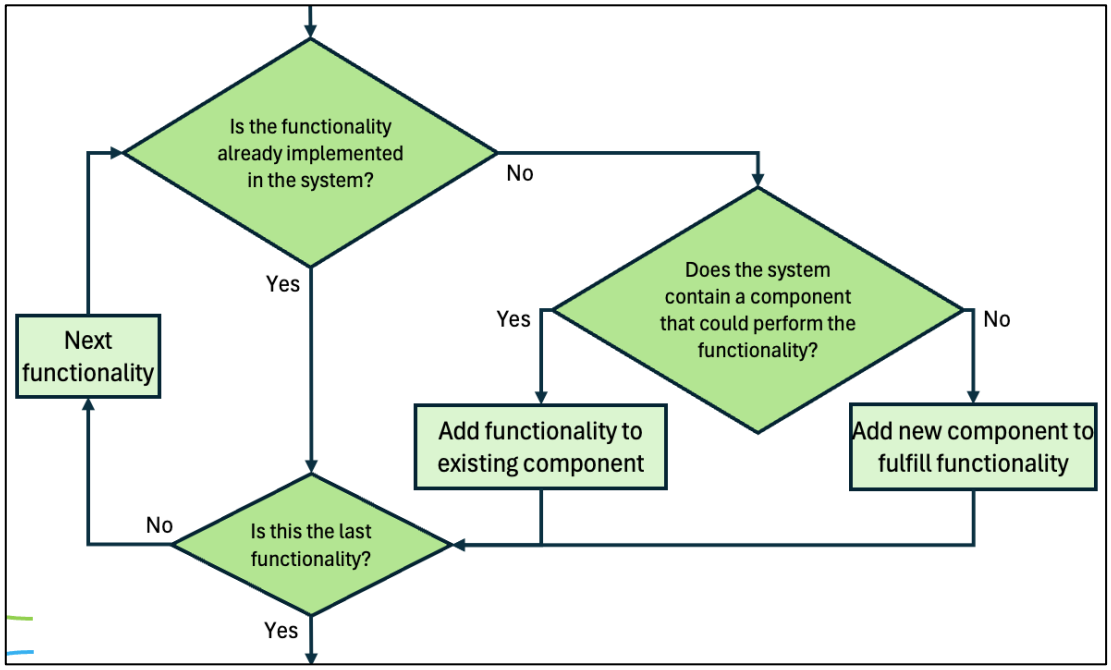

Figure 11: Functionality addition loop of the green phase.

The first functionality we add is “Manual asset inventory and tracking”. We are unsure if this functionality is already implemented, so we will add it just in case. This functionality will most likely not need new components, but to make this process simple, we will add a *Manual Inventory* component to our base architecture.

The second functionality we need is “Encryption of all sensitive data sharing.” This is mostly already implemented in the system with IPsec connections between the gNBs and gNBs and the core network [24], so we can move on to the next functionality.

The third functionality is “Encryption of data at rest.” This might not always be true in the 5G network, so just in case we will add encryption of data at rest at the gNBs, AMF and UPF. This does not however require any additional components but can be done at the gNBs.

The fourth functionality to be implemented is “Secure key management.” This functionality is already in place in the existing system [24], but we will add a public key infrastructure (PKI) component to our test system make it more visible.

The fifth functionality, “Access authorization and expiry” can be implemented through the zero trust components policy enforcement point and policy decision point. This functionality is the reason we needed tenet 1 maturity as well, since we need to keep track of the entities in our system to be able to decide on any authorization policies. For implementing the policy enforcement point and policy decision point, we will add policy enforcement points as gatekeepers for the gNBs, AMF and UPF, which are connected to a single policy decision point that controls them all.

The sixth and last functionality is “Access policies - what can be accessed and for how long.” For this functionality we have already added the needed components when implementing access authorization and expiry, so we now only need to implement the access policies to the policy engine in the policy decision point.

After we are finished with the green phase, we should have all needed functionalities implemented in our system. All the functionalities added to the Xn-interface and handover related components are illustrated in Figure 12 . Now we can move on to the actual threat analysis in the blue phase.

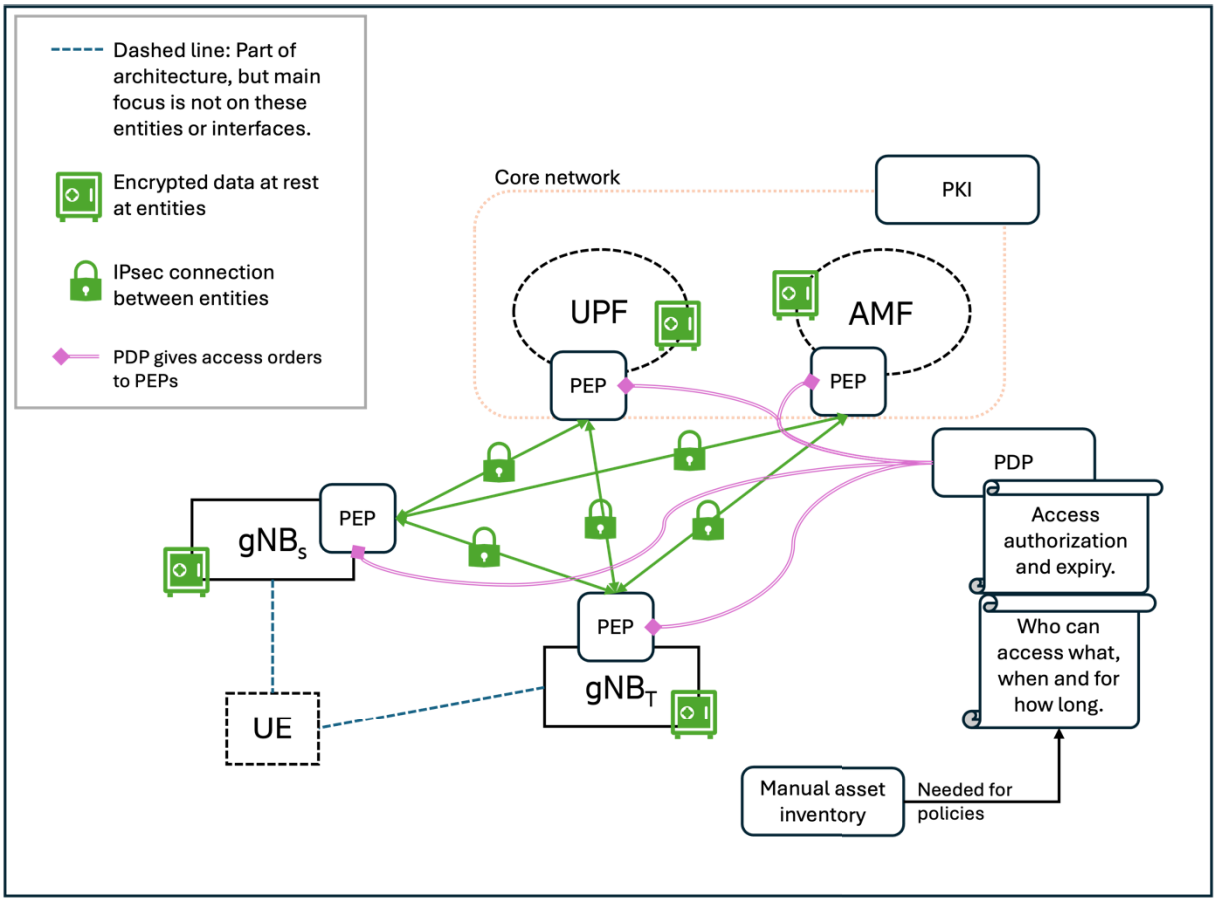

Figure 12: Illustration of the functionalities added to the Xn-interface and other handover related components.

4.3.3 Threat Analysis – the Blue Phase

Since this phase is time consuming, and finding threats for this proof of concept is not the main focus of this work, we will simplify this phase. Instead of doing the threat analysis fully, we will consider what things need to be considered for the threat analysis when we follow the STRIDE-ZTA threat model.

What we need to do before the threat analysis is to redefine our scope as illustrated by Figure 13. Since we started the zero trust function addition process technically from scratch, we do not want to narrow down our scope for the threat analysis process. We added new components around the entire system we chose at the start, so we also need to perform threat analysis on the entirety of the system.

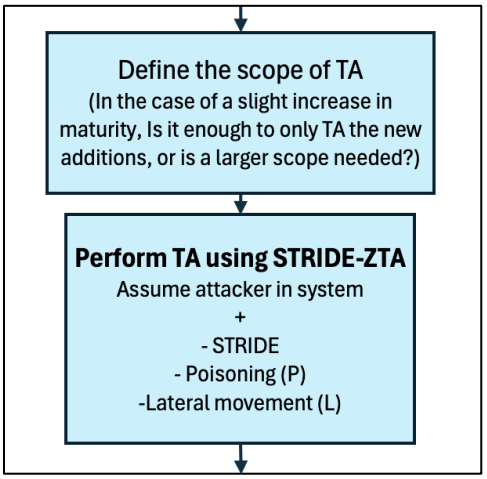

Figure 13: First half of the blue phase, including scope definition and the threat analysis.

For the threat analysis we will go through the STRIDE-ZTA threats, but without actually finding any threats, only discussing the things we need to consider for STRIDE-ZTA. Starting with spoofing, we would figure out if there is something in our system the attacker could spoof, like a UE or a gNB. For tampering, we would need to see if an attacker could tamper with anything. Since we are doing this from a zero trust perspective, it could be a good idea to see if the attacker is able to tamper with data or something else if they have access to, for example a gNB, creating a sort of insider attack scenario.

Next we need to look into repudiation threats. For this threat, we would need to check if for example the logging in our system is sufficient for not letting an insider do anything in the system without it being logged. We also need to look for information disclosure threats. Is the attacker able to access data at rest or data at transit? What about data in use? Denial of service threats should also be checked. What kind of different attacks are possible, especially if the attacker can access resources on the inside, like a gNB. Could the attacker potentially use a gNB to cause wider disturbance?

The last of the ordinary STRIDE threats is elevation of privilege. Any elevation threats should be checked, especially in the case if an attacker has some form of access to a network component, like a gNB and see if they would be able to elevate that access.

After the normal STRIDE threats, we still need to consider the STRIDE-ZTA specific additions. The poisoning threat becomes relevant if we have components in the system that can be poisoned, which in this case might include the policy decision point. So poisoning threats on the policy decision point need to be checked. Lateral movement relates to elevation of privilege, so when checking for elevation of privilege threats, possible lateral movement, for example to other gNBs needs to be analysed.

Once we have performed a thorough analysis of our system, we can move on to mitigating the threats as illustrated by Figure 14. Since we did not actually find any threats in this proof of concept, we do not have any threats to mitigate. If we did have threats we could, after finding mitigations, see if they would be possible by increasing zero trust maturity and if yes, we could increase the zero trust maturity and do the threat analysis process again.

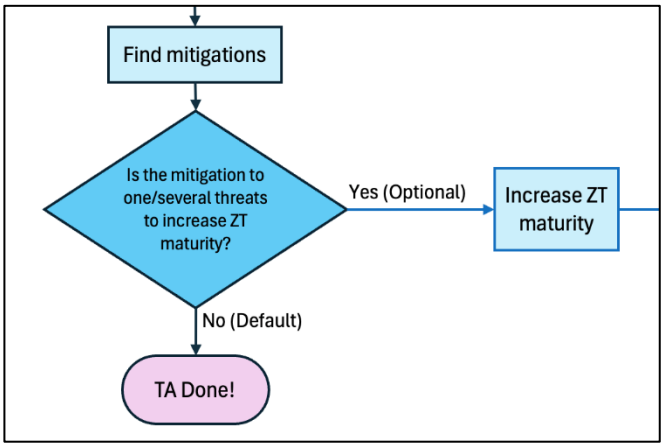

Figure 14: Last steps of STRIDE-ZTA.

After this phase our STRIDE-ZTA threat analysis is complete.

5 Analysis and Results

In this section we will analyze STRIDE-ZTA and the proof of concept introduced in section 4. This analysis aims at evaluating the usability of the proposed solution, while simultaneously looking for possible flaws in the model. In addition, we examine possible future research directions based on this work.

5.1 Evaluation of STRIDE-ZTA

Deciding whether a model like STRIDE-ZTA is "good" is not an easy task. A process like this is not a math equation where we can check if we got the right answer. Instead, it is a process designed to be used by people in various scenarios, and people might perceive these things subjectively. Something that works for one person, might not be optimal for somebody else.

To fully grasp the performance of STRIDE-ZTA, it would need to be tested multiple times in different scenarios by different people. For this work, we can only use the observations from the proof of concept performed by ourselves in section 4 as a guide on whether it works. Therefore, this analysis will be slightly biased.

Based on the proof of concept, the STRIDE-ZTA model is usable and easy to follow. However, there are some concerns regarding the effectiveness of it.

The advantages of the model are its ease of use and the flexibility to start the process from any of the three stages, depending on what the model is being used for. The steps are simple and easy to follow, while also being thorough. There is no need to perform anything beyond what the model requires, it will still work, hence the model can be seen as complete in that regard.

The first issue is the loop in the green phase. We have not specified the order in which functionalities are to be added. This might result in a case, where a functionality is added to an existing component, but afterwards another functionality requires a new component, which would have been a better component for the previous functionality as well. This might create a suboptimal scenario, where functionalities are not performed by the most suitable components. This is not a huge issue in most cases but might become relevant in bigger systems with many functionalities to add. One possible solution for this would be to add a step at the beginning of the green phase, that would necessitate the arrangement of the functionalities into categories depending on what kind of components they would prefer, and what they would necessitate. This way, the functionalities requiring new components could be added first, which would leave

the rest of the functionalities more component options and a bigger possibility of getting the optimal placement.

Another possible issue that might arise is the STRIDE-ZTA threat model itself. Since zero trust specific threat modeling has not been performed much, it is very hard to know at this stage if the model itself can be used to find all relevant threats. This can only be found out through countless iterations, and the model might even evolve over time.

To conclude, the model does work and is usable. However, it will need more work and testing to address the issues that might require small changes made to the model.

5.2 The Effect of Zero Trust on Threat Analysis

Zero trust does not fundamentally change the way threat modeling is done using the proposed model. It still requires the same steps and can partly be performed using the same methods as non zero trust threat modeling. However, zero trust threat modeling does benefit from certain additional steps. Performing the threat modeling from the point of view of insider attack and already compromised assets helps in understanding how the zero trust principles and security measures aim to prevent lateral movement and further exploits. It prepares the developers for the worst-case scenario and might even help in creating a response plan.

The same can be said about zero trust threat modeling in 5G. Compromised components should also be taken into account when performing threat modeling on mobile networks as well. The likelihood of 5G components getting compromised is probably low, but it will never be impossible, especially with the advancement of cyber threats and AI. This makes it necessary to take the threats into consideration.

Zero trust specific components need to be considered in the threat model as well. This includes policy engines, policy administrators and policy enforcement points. Policy engines and other components within a zero trust architecture may incorporate AI technologies, which necessitate modeling threats that differ from the system's usual threat dimensions. In addition to poisoning, STRIDE-ZTA should evolve to include more AI related threats, to enable comprehensive threat modeling for systems that utilize AI.

Finally, traditional threats do not disappear in a zero trust environment. At least not until the zero trust environment is perfect, which might never happen. As long as different stages of maturities and human error are in play, traditional threats will need threat modeling as well.

5.3 Ideas and Future Research

The STRIDE-ZTA model and the other deliverables of this work can act as a stepping stone for future research, and the ideas brought forward in this thesis can be cultivated and further developed.

The STRIDE-ZTA model and the maturity tables are still prototypes. With further research and experimentation they can be refined to cover a wider range of systems. One such area is studying the tradeoff between complexity and efficiency of the maturity models. As an example of this, a comparison could be made of the tenet based maturity table (Table 9) and the CISA function based maturity tables (Table 3 to Table 8), to examine which one is better suited for designing zero trust systems. Maybe one is well suited for smaller networks, while the other is superior for large enterprises.

Besides the further research on the maturity models themselves, future studies could focus on developing a comprehensive system for assessing zero trust maturity. This could help companies aim for different maturity levels and would better concretize how "good" it is to comply with a certain level. With a maturity scale companies could claim they are *zero trust compliant on level 2* or that they have a *zero trust score of 8*. A possible example of this is the tenet maturity rating table in Figure 15. A rating system like this would enable companies to be able to aim for and reach certain zero trust maturity levels and ratings and be able to advertise those levels. It would be a similar system like energy ratings on electronics today [49]. A rating system like this would need to be standardized, so that everyone follows the same rating system and are indeed conforming to the specified requirements for optimal zero trust compliance.

Tenet Maturity Rating Table

Tenet \ Maturity	0	1	2	3	Chosen M: (0, 1, 2 or 3)	(points)
1	0	0.5	0.75	1	1	0.5
2	0	0.5	0.75	1	3	1
3	0	0.75	1	1.5	2	1
4	0	1	1.25	1.75	1	1
5	0	0.5	1	1.5	2	1
6	0	0.75	1.25	1.5	1	0.75
7	0	1	1.5	1.75	1	1
Total max for maturity levels:	0	5	7.5	10		
				Total Rating:	6.25	

Figure 15: Example of tenet maturity rating system.

6 Conclusion

This work aimed to find answers on how zero trust affects the threat modeling process, as well as finding a suitable threat model for zero trust systems. As a secondary goal, the thesis also aimed to find out if zero trust in mobile networks affects the threat modeling performed on it.

The previous research on zero trust maturity and zero trust threat modeling is scarce, so this work had the opportunity to develop new ideas surrounding the subject. The work resulted in STRIDE-ZTA, a proposed threat modeling methodology designed specifically for zero trust systems. The proposed model was tested and analyzed, contained small flaws, but worked and was usable. However, the model will need future testing and research to make it functional without issues in real life systems. In addition, different systems and environments are going to need tailored zero trust maturity models to go along with STRIDE-ZTA.

The effects zero trust had on threat modeling were not major, but big enough to need consideration. The insider threat and compromised assets have a major role in zero trust security, so taking those into account was crucial for this work. Similarly with mobile networks, the need for insider attack considerations was relevant.

The zero trust specific components might also bring new attack surfaces not covered sufficiently by traditional methods, such as STRIDE, so expanding the threat model was crucial as well. Despite zero trust having a different ideal threat modeling approach compared to traditional systems, the traditional threats still exist, so it is not enough to threat model zero trust systems only using the zero trust specific additions.

This thesis combined zero trust maturity research with zero trust threat modeling research. The results and deliverables in this work can be used to further expand on the domain of zero trust maturity threat modeling. With further research, the utility of STRIDE-ZTA and the tenet maturity table can be better assessed and further polished, maximizing their effectiveness and usability.

References

[1] A. Poirrer, "Formal Security of Zero Trust Architectures," Institut Polytechnique de Paris, Paris, 2024.

[2] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "NIST Special Publication 800-207: Zero Trust Architecture," National Institute of Standards and Technology (NIST), Gaithersburg, 2023.

[3] C. Romeo, "Zero Trust Threat Modeling," Devici, 8 November 2023. [Online]. Available: https://devici.com/resources/blog/zero-trust-threat-modeling. [Accessed 11 March 2025].

[4] Microsoft, "Microsoft Threat Modeling Tool," Microsoft, 25 August 2022. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool. [Accessed 08 April 2025].

[5] B. Ali, S. Hijjawi, L. H. Campbell, M. A. Gregory and S. Li, "A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing," *Security and Comunication Networks,* vol. 2022, no. 1, 29 June 2022.

[6] B. Karabacak and T. Whittaker, "Zero Trust and Advanced Persistent Threats: Who Will Win the War?," in *ICCWS 17th International Conference on Cyber Warfare and Security*, Albany, 2022.

[7] H. Kim, Y. Kim and S. Kim, "A Study on the Security Requirements Analysis to build a Zero Trust-based Remote Work Environment," Arxiv, 2024.

[8] A. Kantchelian, C. Neo, R. Stevens, H. Kim, Z. Fu, S. Momeni, B. Huber, E. Bursztein, Y. Pavlidis, S. Buthpitiya, M. Cochran and M. Poletto, "Facade: High-Precision Insider Threat Detection Using Deep Contextual Anomaly Detection," Arxiv, 2024.

[9] A. Manan, Z. Min, C. Mahmoudi and V. Formicola, "Extending 5G services with Zero Trust security pillars: a modular approach," in *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, 2022.

[10] K. Ramezanpour and J. Jagannath, " Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN," Computer Networks, vol. 217, Article 109358, Nov. 2022.

[11] Alliance for Telecommunications Industry Solutions (ATIS), "ATIS-I-0000095: Enhanced Zero Trust and 5G," Alliance for Telecommunications Industry Solutions, Washington, D.C., 2023.

[12] M. Lyu and J. Farooq, "Zero Trust in 5G Networks: Principles, Challenges, and Opportunities," in *2024 Resilience Week (RWS)*, Austin, 2024.

[13] J. P. Mello Jr., "Zero trust and threat modeling: Is it time for AppSec to get on board?," ReversingLabs, 15 November 2023. [Online]. Available: https://www.reversinglabs.com/blog/zero-trust-and-threat-modeling-is-it-time-for-appsec-to-get-on-board. [Accessed 15 April 2025].

[14] Ericsson, "5G Explained," Ericsson, [Online]. Available: https://www.ericsson.com/en/5g. [Accessed 2 12 2024].

[15] 3GPP, "5G System Overview," 3GPP, 11 10 2022. [Online]. Available: https://www.3gpp.org/technologies/5g-system-overview. [Accessed 29 11 2024].

[16] 3GPP, "Introducing 3GPP," 3GPP, [Online]. Available: https://www.3gpp.org/about-us/introducing-3gpp. [Accessed 29 11 2024].

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

[18] 3GPP, "TS 38.300: Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 18)," 3GPP, 2024.

[19] 3GPP, "TS 23.501: 5G; System architecture for the 5G System (5GS)(Release 18)," 3GPP, 2024.

[20] 3GPP, "TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 18)," 3GPP, 2024.

[21] 3GPP, "TS 23.502: Procedures for the 5G System (Release 18)," 3GPP, 2024.

[22] S. Poretsky, "Evolving the security posture for critical infrastructure," Ericsson, 10 April 2025. [Online]. Available: https://www.ericsson.com/en/blog/north-america/2025/evolving-the-security-posture-for-critical-infrastructure. [Accessed 2 June 2025].

[23] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi and A. Matrawy, "Security Analysis of Critical 5G Interfaces," *IEEE Communications Surveys & Tutorials,* vol. 26, no. 4, pp. 2382 - 2410, 2024.

[24] 3GPP, "3GPP TS 33.501: Security architecture and procedures for 5G System (Release 18)," 3GPP, 2024.

[25] E. B. Fernandez and A. Brazhuk, "A critical analysis of Zero Trust Architecture (ZTA)," *Computer Standards & Interfaces,* vol. 89, Article 103832, 2024.

[26] M. A. Enright, E. Hammad and A. Dutta, "A Learning-Based Zero-Trust Architecture for 6G and Future Networks," in *IEEE Future Networks World Forum (FNWF)*, Montreal, 2022.

[27] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," Cybersecurity and Infrastructure Security Agency (CISA), 2023.

[28] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access,* vol. 10, pp. 57143 - 57179, 2022.

[29] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, "Department of Defense (DoD) Zero Trust Reference Architecture, version 2.0," Department of Defense (DoD), 2022.

[30] H. Byström , H.-Y. Chen and S. Poretsky, "Zero Trust Architecture for advancing mobile network security operations," Ericsson, 2024.

[31] S. Faehl, "New Microsoft guidance for the CISA Zero Trust Maturity Model," Microsoft, 19 December 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2024/12/19/new-microsoft-guidance-for-the-cisa-zero-trust-maturity-model/. [Accessed 19 May 2025].

[32] A. Dutta, E. Hammad, M. Enright, A. Chorti, A. Cheema, K. Kadio, J. Urbina-Pineda, K. Alam, A. Limam, F. Chu, J. Lester, J.-G. Park, J. Bio-Ukeme, S. S. Pawar, R. Layton and P. Ramchandran, "INGR Roadmap Security and Privacy Chapter," in *2023 IEEE Future Networks World Forum (FNWF)*, Baltimore, 2023.

[33] O. Mämmelä, J. Suomalainen, K. Ahola, P. Ruuska, M. Majanen and M. Uitto, "Micro-Segmenting 5G," in *3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, Funchal, Madeira, 2018.

[34] J. Olsson, A. Shorov, L. Abdelrazek and J. Whitefield, "Zero trust and 5G – Realizing zero trust in networks," *Ericsson Technology Review,* vol. 5, 2021.

[35] S. Elmadani, S. Hariri and S. Shao, "Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks," in *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, 2022.

[36] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," *Computers & Security,* vol. 84, pp. 53-69, 2019.

[37] Z. Braiterman, A. Shostack , J. Marcil, S. de Vries, I. Michlin, K. Wuyts, R. Hurlbut, B. S. Schoenfield, F. Scott, M. Coles, C. Romeo, A. Miller, I. Tarandach, A. Douglen and M. French, "Threat Modeling Manifesto," Threatmodelingmanifesto.org, [Online]. Available: https://www.threatmodelingmanifesto.org/#values. [Accessed 11 March 2025].

[38] MITRE, "ATT&CK," MITRE, [Online]. Available: https://attack.mitre.org. [Accessed 19 May 2025].

[39] B. Santos, L. Barriga, B. Dzogovic, I. Hassan, B. Feng, N. Jacot, V. T. Do and T. V. Do, "Threat Modelling for 5G networks," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, Dubrovnik, 2022.

[40] D. J. Bodeau, C. D. McCollum and D. B. Fox, "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," The Homeland Security Systems Engineering and Development Institute (HSSEDI), McLean, 2018.

[41] L. Mauri and E. Damiani, "STRIDE-AI: An Approach to Identifying Vulnerabilities of Machine Learning Assets," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, 2021.

[42] C. Hashemi-Pour, "What is the CIA triad (confidentiality, integrity and availability)?," TechTarget, December 2023. [Online]. Available: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [Accessed 14 April 2025].

[43] Microsoft, "Secure by Design," Microsoft, [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/practices/secure-by-design. [Accessed 28 May 2025].

[44] S. Coble, "Micro-Segmentation Used by 83% of Cybersecurity Leaders," Infosecuirty Magazine, 9 November 2021. [Online]. Available: https://www.infosecurity-magazine.com/news/microsegmentation-now-used-widely/. [Accessed 26 May 2025].

[45] OWASP, "Threat Modeling Cheat Sheet," OWASP, [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html. [Accessed 8 April 2025].

[46] S. Sun, M. Repeta, M. healy, V. Nandall, E. Fung and C. Thomas, "Towards 5G Zero Trusted Air Interface Architecture," Arxiv, 2022.

[47] 3GPP, "TS 33.117: Catalouge of general security assurance requirements (Release 18)," 3GPP, 2024.

[48] 3GPP, "TR 33.894: Study on applicability of the zero trust security principles in mobile networks (Release 18)," 3GPP, 2023.

[49] European Comission, "Understanding the Energy Label," European Comission, [Online]. Available: https://energy-efficient-products.ec.europa.eu/ecodesign-and-energy-label/understanding-energy-label_en. [Accessed 21 May 2025].