Université Libre de Bruxelles

5G Security Analysis - Security of Critical Interfaces and Zero Trust Architecture

Students:
Ali-Khodja Myriam Erin Johanna
Hassani Mortaza
Amanor Deborah
Bouta Ali

Supervisor:
Prof. Dricot Jean-Michel

January 6, 2025

Contents

List of Acronyms

Nomenclature

1G	First Generation
2G	Second Generation
3G	Third-Generation
3GPP	3rd Generation Partnership Project
4G	Fourth-Generation
5GC	5G Core Network
AN	Access Network
AS	Application Server
CDMA	Code Devision Multiple Access
CN	Core Network
FDMA	Frequency Devision Multiple Access
IMT-2000	International Mobile Technology-2000
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union Radiocommunication
LTC	Long Term Evolution
MBB	Mobile Broadband
MIMO	Multiple-Input Multiple-Output
NFV	Network Function Virtualization
NG-RAN	Next Generation Radio Access Network
NR	New Radio
NS	Network Slicing
OFDMA	Orthogonal Frequency Division Multiple Access
RAN	Radio Access Network
SDN	Software-Defined Networking
SDOs	Standard Development Organizations
TDMA	Time Devision Multiple Access
UE	User Equipment

Abstract

Zero Trust Architecture (ZTA) has been implemented in 5G networks to enhance security between fragmented components, such as the NG-RAN and 5GC. However, its application to securing 5G critical interfaces and the broader 5G architecture remains underexplored. 5G networks face significant security challenges, particularly at critical interfaces like N1, N2, N3, and SBIs, which handle sensitive data and interconnect network functions. This report analyzes vulnerabilities in these interfaces, evaluates ZTA's potential for enhancing their security, and highlights gaps in existing literature. The findings provide valuable insights into leveraging ZTA for a unified and resilient security framework across 5G systems.

1 Introduction

The transition to 5G networks presents significant security challenges due to their highly dynamic, distributed, and virtualized architecture. Traditional perimeter-based security models are no longer sufficient, as the complexity and interconnectedness of the network expose new vulnerabilities. One promising solution to these challenges is the adoption of Zero Trust (ZT) security architecture, which assumes no implicit trust within the network and enforces strict verification of all entities, regardless of their origin. This approach is well-suited for the 5G environment, where constant authentication, granular access control, and the principle of least privilege are essential for maintaining security.

In parallel, critical interfaces within the 5G architecture play a central role in connecting the various network functions. These interfaces—such as N1, N2, N3, and Service-Based Interfaces (SBIs)—enable communication between different components across OpenRAN, vRAN, and CloudRAN deployments. However, their pivotal role in data exchange and signaling also makes them potential targets for cyber-attacks. As these interfaces connect a wide range of network functions, securing them is paramount.

This report aims to assess the current state of Zero Trust implementation in 5G networks and analyze the security principles applied to critical interfaces. By evaluating existing security measures, identifying vulnerabilities, and examining best practices recommended by standardization bodies, this work will provide insights into strengthening the security of 5G interfaces and the overall network infrastructure.

1.1 Problem Statement

Security analyses of 5G networks often lack a targeted focus on the critical interfaces that connect the NG-RAN and the 5G core network to external entities. Although Zero Trust Architecture has been applied to the network functions within the 5G core and RAN, its implementation across the entire 5G system architecture remains fragmented. This limitation leaves critical interfaces vulnerable to emerging threats.

1.1.1 Research goal

This study aims to achieve the following objectives:

- Conduct a comprehensive analysis of the threats and vulnerabilities associated with 5G critical interfaces, including N1, N2, N3, and SBIs.
- Explore the application of Zero Trust Architecture across the entire 5G system to.
- Identify security gaps and propose enhanced security measures to strengthen the protection of critical interfaces using ZTA.

1.2 Methodology

To achieve the goal of this research, we conducted a comprehensive literature to analyze existing studies on 5G critical interface security and the application of Zero Trust Architecture (ZTA). Research questions were formulated to guide the study which will be discussed in detail in subsequent sections.

2 Background

The evolution of 5G

The fifth generation of mobile networks, represents a revolutionary leap compared to its predecessors (2G, 3G, and 4G). While earlier generations primarily focused on improving voice communication, data speeds, and internet access, 5G goes much further by enabling entirely new applications and use cases. With speeds up to 100 times faster than 4G and latencies as low as 1 millisecond, 5G introduces the capacity to support massive device connectivity and mission-critical, real-time applications.

Unlike previous networks, 5G is designed to seamlessly integrate with emerging technologies such as autonomous vehicles, augmented reality (AR), industrial automation, and the Internet of Things (IoT). Its architecture supports network slicing, which allows operators to create virtualized networks tailored to specific applications or industries. These capabilities make 5G a cornerstone for the digital transformation of industries and services.

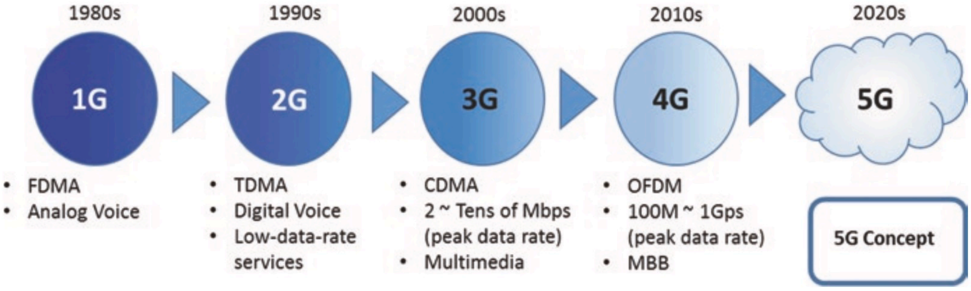

Figure 1: Cellular network evolution by generation [2]

Security Challenges in 5G Networks

While 5G holds immense potential, it also brings new security challenges due to its highly distributed and software-driven architecture. Features such as virtualized network functions (VNFs), edge computing, and dense device connectivity expand the attack surface, increasing the risk of cyberattacks. Traditional security models that relied on perimeter-based defenses are no longer sufficient, as attackers can exploit vulnerabilities across interconnected systems and networks.

The Need for Zero Trust

To address the security challenges posed by 5G networks, adopting a Zero Trust (ZT) security model is essential. Unlike traditional models that assume trust within the network perimeter, Zero Trust operates on the principle of ”never trust, always verify,” assuming that both internal and external threats are always present. This approach requires strict verification of all entities—whether users, devices, or applications—before granting access. It emphasizes continuous monitoring, dynamic policy enforcement, and granular access controls based on factors such as user identity, device posture, and other contextual elements. Zero Trust aligns perfectly with the dynamic and distributed nature of 5G, helping to mitigate risks like lateral movement and unauthorized access within a network. By reducing implicit trust, it ensures that all interactions are continuously verified, providing high levels of security without compromising the performance or scalability required by 5G networks.

3 5G Architecture

This section highlights the 5G components, the different deployment type and the protocols used.

3.1 5G Components

1. **User Equipment (UE)**: Refers to devices such as smartphones, IoT devices, and wearables that connect to the 5G network. They interact with the network through radio access, enabling 5G services for users.

2. **Core Network (CN)**: Manages data traffic, authentication, and service delivery across the 5G network. It connects access networks and handles functions like routing, security, and service management.

3. **Radio Access Network (RAN)**: Facilitates wireless communication between User Equipment and the Core Network. Composed of base stations and antennas, it provides the radio signals necessary for 5G connectivity.

3.2 The evolution of RAN

- *Traditional RAN:* The traditional RAN, used from 2G to 5G, connects end users with remote-control systems via the core network and consists of base stations, baseband units (BBUs), and controllers; however, its proprietary technologies limit options for equipment and software.
- *Centralized RAN (CRAN):* CRAN moves the baseband unit (BBU) from the individual base stations to a centralized location, allowing for more efficient use of resources, reduced costs, and better coordination of network traffic, but it requires high-bandwidth backhaul connections.
- *Virtualized RAN (vRAN):* With the advancement of network function virtualization (NFV) and software-defined networks, vRAN replaces traditional hardware by virtualizing the baseband unit into separate distribution and control units, allowing for a more flexible, cloud-based architecture with centralized BBUs and software-based controllers, though it still relies on proprietary radios and interfaces.
- *Disaggregated vRAN:* Disaggregated vRAN further evolves from traditional vRAN by separating hardware and software elements across different vendors, enabling greater flexibility and scalability; it allows baseband units to be virtualized and deployed across distributed locations, reducing reliance on a single vendor and fostering a more open ecosystem.
- *Open RAN (ORAN):* Building upon vRAN, ORAN focuses on openness and standardization, promoting interoperability between vendors through open interfaces, and uses NFV and SDN to enable network slicing, providing a more flexible and scalable architecture, though it still faces challenges related to integration and multi-vendor compatibility.

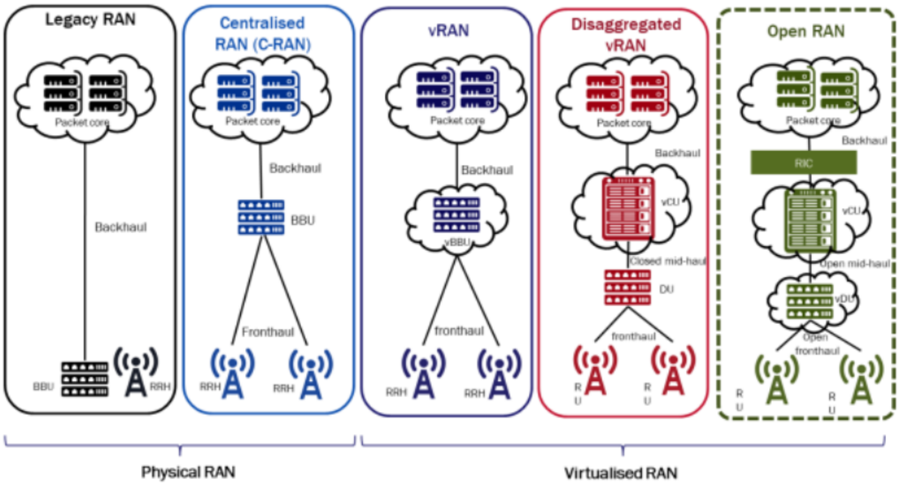

Figure 2: Evolution of the RAN architecture [4]

3.3 5G Core Network

The 5G Core Network (5GC) is the central component of the 5G architecture, responsible for managing data traffic, providing essential network functions, and enabling advanced capabilities such as network slicing and low-latency communication.

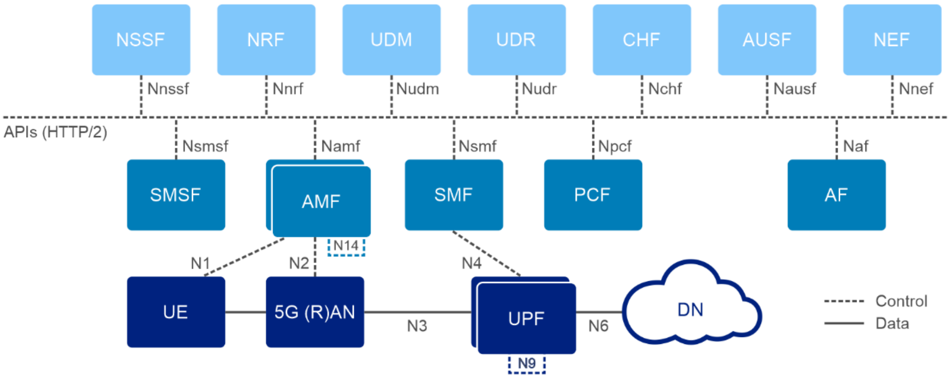

Figure 3: 5GC Architecture [1]

Function	Main Role
Access and Mobility Management Function (AMF)	Supervises network access, connection, and mobility.
Session Management Function (SMF)	Manages network sessions, QoS parameters, routing, and billing information.
Authentication Server Function (AUSF)	Facilitates the authentication of UE (User Equipment).
Network Slice Selection Function (NSSF)	Selects network slice instances (NSI) based on UE performance requirements.
Network Repository Function (NRF)	Manages the lifecycle of network function profiles.
Policy Control Function (PCF)	Generates and applies network control policies.
Network Exposure Function (NEF)	Exposes network functionalities securely to external applications.
Unified Data Management (UDM)	Manages subscription-related information.
Unified Data Repository (UDR)	Stores subscription information accessible by UDM.
User Plane Function (UPF)	Manages the transmission of user data.

3.4 The Critical 5G interfaces

Critical interfaces are those that connect to external networks or carry sensitive data. For each critical interface, the 3GPP defines two operational planes:

- **Control Plane (CP):** Responsible for exchanging signaling information that supports NF operations and manages the User Plane (UP).

- **User Plane (UP):** Handles user data traffic, enabling its transportation across the network.

The CP spans the entire 5GS, including the 5G Access Network (NG-RAN) and the 5GC. The UP manages the data forwarding path between the User Equipment (UE), NG-RAN, User Plane Function (UPF), and Data Network (DN).

3.4.1 Interfaces and their Functions

In the context of 5G networks, various interfaces play crucial roles in ensuring seamless communication between different network components. These interfaces connect different entities within the 5G Core (5GC) and the Radio Access Network (RAN), enabling the transfer of signaling, user data, and management information. Below is a breakdown of key interfaces and their respective functions within the 5G architecture.

1. **N1 Interface:** Connects the User Equipment (UE) to the Access and Mobility Function (AMF). It carries sensitive information like user identity and location data.
2. **Xn Interface**: Connects two gNBs at the NG-RAN side. This interface is involved in handover procedures and data forwarding.
3. **F1 Interface:** Connects the Distributed Unit (DU) and Central Unit (CU) of the gNB. This interface carries both signal and user data. [3]
4. **N2 Interface:** Connects the NG-RAN and the AMF. It carries signaling information during the UE registration procedure.
5. **N3 Interface:** Connects the NG-RAN to the User Plane Function (UPF). This interface is involved in all PDU session establishments. [3]
6. **N4 Interface:** Connects the Session Management Function (SMF) with the UPF. It is responsible for session management and QoS parameters.
7. **SBI Interface:** Connects the Control Plane Network Functions (NFs) in the 5GC. It allows for communication between various network functions. SBI typically uses protocols like HTTP/2.
8. **N9 Interface**: Connects UPFs and is crucial during roaming between networks. It also handles mobility management.
9. **N32 Interface:** Connects network functions in different PLMNs (Public Land Mobile Networks). It's used for establishing secure roaming connections. [3]
10. **N6 Interface:** Connects the UPF and the Data Network (DN). It transmits user traffic to and from external networks.

4 Zero Trust

The traditional approach of perimeter-based security is no longer sufficient, leading to an architecture where implicit trust is often granted between various functions. With the Zero Trust (ZT) model, the emphasis is on eliminating this implicit trust and assuming that no entity—whether inside or outside the network—can be trusted by default. This principle was formalized by John Kindervag in 2010. While Zero Trust is still considered a ”new approach,” it has evolved over time. Following numerous studies in various domains and official publications like those from NIST, it is clear that Zero Trust is no longer merely a concept but an essential goal to achieve in modern architectures. [5]

4.1 ZT principles

A Zero Trust Architecture (ZTA) is based on several key principles that emphasize security across all aspects of the enterprise. [5]
- All resources are considered data sources and computing services : A network may consist of various devices, including small footprint devices, SaaS, and systems sending instructions to actuators. Enterprises may also classify personally owned devices as resources if they can access enterprise-owned assets. This approach ensures that all components are treated with the same security measures, regardless of their origin.
- All communication is secured, regardless of network location: Network location alone does not imply trust. Access requests from assets located on enterprise-owned networks should meet the same security requirements as those from external networks. Communication must always be secure, ensuring confidentiality, integrity, and source authentication.
- Access is granted on a per-session basis: Trust in the requester is continuously evaluated before access is allowed, with the principle of least privilege applied. This means that users are granted only the minimum necessary permissions to complete their tasks. Authentication and authorization to one resource do not automatically grant access to other resources.
- Access is determined by dynamic policies: These policies are based on various attributes, such as client identity, the requesting asset's state, and behavioral attributes. Resources are protected by defining the access needs of members and applying least privilege principles. The state of a client, including device characteristics, behavioral patterns, and environmental factors, plays a role in granting or denying access.
- Continuous monitoring and evaluation of assets' integrity and security posture: No asset is inherently trusted. Enterprises must continuously monitor the security of their devices and applications and apply necessary updates or patches. Subverted or vulnerable assets are treated with heightened scrutiny, and monitoring is required for both enterprise-owned and associated devices.
- Dynamic authentication and authorization enforcement: Access is granted only after continuous assessments, which may include multi-factor authentication (MFA). Access is re-evaluated throughout user interactions, with monitoring and reauthorization based on established policies. This ensures a balance between security, availability, and cost-efficiency.
- Collection and use of data to improve security posture: Enterprises should gather information on asset security, network traffic, and access requests. This data is processed to improve security policies and enforcement, ensuring that security measures evolve with emerging threats and operational needs.

4.2 Logical components of ZTA

Deploying ZTA in a network counts multiple components with different roles. Table 5 presents the various components and their functions, aiming to understand how they address specific needs.

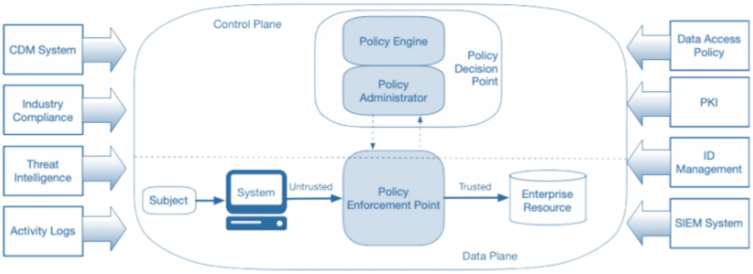

Figure 2: Core Zero Trust Logical Components

Figure 4: Logical components of the ZT [5]

4.3 The ZT importance in 5G

Given the numerous benefits that Zero Trust (ZT) brings in terms of enhanced security and the challenges associated with 5G networks, it seems like a promising approach to integrate ZT into the 5G architecture. The dynamic and distributed nature of 5G, coupled with its increasing complexity, makes traditional security models inadequate. Zero Trust's ability to provide continuous authentication, strict access controls, and robust threat mitigation aligns well with the evolving security needs of 5G, making it an ideal candidate to address these emerging challenges.

5 Threat modelling and Risk Assessment

In this section, we analyze the security of 5G networks with a particular focus on the critical interfaces that interconnect Network Functions (NFs). These interfaces play a vital role in the operation of the 5G system (5GS) and are crucial to prioritize as they carry sensitive signaling information, user data, and other confidential details that are potential targets for attackers.

Rather than providing a broad overview of 5G security, this analysis emphasizes interface-level security, which is essential for identifying vulnerabilities and risks that span multiple architectural implementations. These critical interfaces are integral to various 5G RAN architectures, including Open RAN, Virtualized RAN, Cloud RAN, and the 5G Core (5GC). Through this detailed assessment, we aim to identify vulnerabilities and risks that could compromise the security and performance of the 5G network.

5.1 Threat Analysis Methodology

The interface-level security assessment covers the following aspects:

- **Identification of Critical Interfaces:** Recognizing interfaces that handle sensitive signaling information, user data, and confidential information.
- **Threat modelling:** Assessing potential threats to these interfaces Using the STRIDE threat model.
- **Risk Mitigation**: Discussing security measures that protect these interfaces, such as encryption, authentication, and continuous monitoring.

5.2 Security Goals

To secure the 5GS, the 3GPP outlines five primary security goals: [3]

1. **Confidentiality:** Ensures only authorized users can access sensitive information.
2. **Integrity:** Protects data from unauthorized modification during transmission.
3. **Authentication:** Verifies the identities of entities (e.g., NFs, UEs) before communication.
4. **Replay Protection:** Prevents attackers from capturing and reusing packets to impersonate legitimate users.
5. **Privacy:** Protects user-sensitive data, ensuring it is only used for its intended purposes.

6 Threat modelling of Critical interfaces

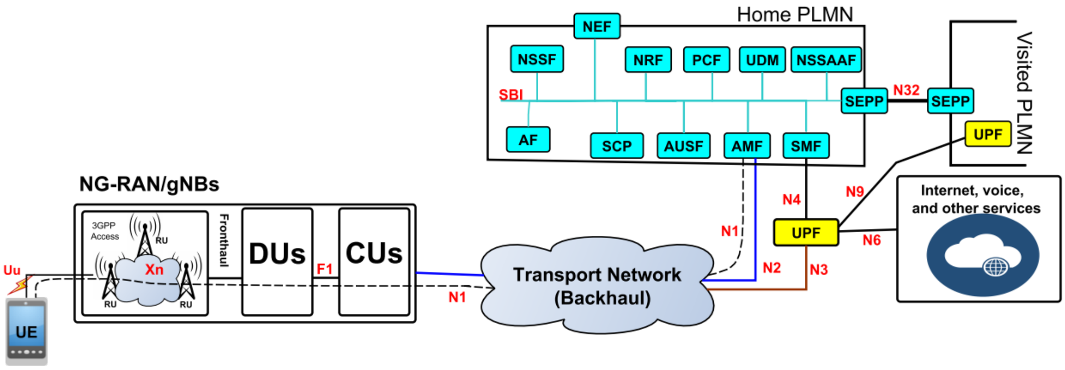

Figure 5: 5G Architecture with Critical interfaces in Red
[3]

6.1 N1 interface

The N1 interface is critical to the functionality of the 5GS, enabling user session management, mobility management, and network access control. It facilitates NAS (Non-Access Stratum) signaling between the UE and the AMF, including authentication, authorization, data connection management, and mobility-related information exchange.

6.1.1 Vulnerability and Threats

Several attacks can exploit the N1 interface if proper security measures are not implemented. Key threats are presented below.A summary of all threats are presented in Table 6.

- **AMF Impersonation:** If an attacker pretends to be the legitimate AMF and successfully serves the UE, false UE authentication could occur, revealing the SUPI and compromising authentication and authorization activities. [3]
- **IMSI Catcher:** Although mitigated in standalone 5G deployments, this attack is still possible in non-standalone deployments, especially if SUPI concealing isn't correctly implemented.
- **Request Flooding:** A malicious gNodeB or rogue UE can exhaust UE resources by sending [3] multiple identifier request messages, forcing the UE to respond with its SUCI each time.
- **NAS Protocol Vulnerabilities:** The NAS protocol supports critical signaling functions such as UE mobility, authentication, identification, and session management. If the authentication procedure fails during initial registration from a rogue UE, an attacker can exploit this to perform DoS attacks, MiTM attacks, or leak subscriber identities.
- **Bidding Down Attacks:** These attacks can force the system to use weaker security algorithms, increasing vulnerability. [3]

6.1.2 Security Recommendations

To mitigate these vulnerabilities, the following security measures are recommended by 3GPP, ETSI, ITU, and GSMA. [3]

1. **Confidentiality:** Null ciphering algorithm (NEA0), 128-bit SNOW 3G-based algorithm (128-NEA1), and 128-bit AES-based algorithm (NEA2). 128-bit ZUC-based algorithm (128-NEA3), where regulations permit.
2. **Integrity:** NIA0, 128-NIA1, and 128-NIA2 for message authentication code integrity protection.
3. **Authentication:** EAP-TLS and improved EAP-AKA' (using HMAC-SHA-256) to prevent bidding down attacks. EAP-TLS 1.3 for enhanced security and reduced latency.
4. **Replay Protection:** Receivers should accept each NAS/PDCP COUNT value only once and periodically update KSEAF keys.
5. **Privacy:** SUPI should not be transmitted in plain text, except for routing information and unauthenticated emergency calls. SUCI (Subscription Concealed Identity) and 5G-GUTI (Globally Unique Temporary Identity) should be used instead.

6.2 Xn, F1 and N2 interfaces

Xn Interface: The Xn interface facilitates handovers between source and target gNB/NG-eNB during mobility. It transfers sensitive information such as UE security capabilities, ciphering algorithms, and integrity algorithms, which require robust protection [3].

F1 Interface: The F1 interface connects gNB-DUs and gNB-CUs within the 5G RAN. As it carries both signaling and user data, it is a critical target for potential attacks [3].

N2 Interface: The N2 interface links the RAN and AMF, facilitating NAS message exchange between 3GPP and non-3GPP access networks to the 5GC. Control Plane (CP) data on the N2 interface is protected with integrity, confidentiality, replay protection, and mutual authentication mechanisms between the NG-RAN and AMF.

6.2.1 Vulnerability and Threats

The table below presents the threats to the interfaces.

Table 1: Threats to Xn, F1, and N2 Interfaces [3]

Interface	End Points	Vulnerability	Assets	S	T	R	I	D	E
Xn	gNB ↔ gNB	CP integrity protection	CP data, processing capacity	●			●		
		UP confidentiality at gNB	UP data	●			●		
		Bidding down on Xn-handover	Mobility management data, processing capacity	●	●				
		CP confidentiality protection	User account data and credentials, mobility management data		●		●		
F1	gNB-DU ↔ gNB-CU	Malicious CP/replay CP	User credentials, RAN resources	●	●				
		Fake UP/replay UP	User credentials, RAN resources	●	●				
		Eavesdropping	User credentials, RAN resources	●			●		
N2	gNB ↔ AMF	False base-station attack	gNBs and AMFs	●					
		De-synchronization attack	User subscription profile data, gNBs	●	●				
		Authentication complexity	Subscriber data and application/network data	●		●			
		Jamming attack	Network services, business services, RAN	●	●			●	
		Replay attacks	User credentials and user account data	●	●				
		Improper ciphering	System resources	●	●		●		
		Bidding down on Xn-handover	User credentials and user account data	●	●				
		Lack of integrity protection and verification of user data	User credentials and user account data	●	●		●		

6.2.2 Security Recommendations

To mitigate threats on the Xn, F1, and N2 interfaces, 3GPP and ETSI recommend the following:

- **Confidentiality, Integrity, and Replay Protection:** Use IPsec ESP for encryption, IKEv2 certificate-based authentication for mutual key exchange, and Datagram Transport Layer Security (DTLS) for both control and user plane interfaces [3].
- **Authentication:** DTLS is the recommended mechanism for authentication.
- **Privacy:** no specific recommendations identified [3].

6.3 N3, N4 and SBI Interfaces

N3 Interface: The N3 interface connects the RAN to the UPF, requiring confidentiality, integrity, and replay protection. It carries user plane data from the 5G-AN to the UPF and facilitates bearer connections and mobility management by tracking user devices' movements [3].

N4 Interface: The N4 interface links the SMF with the UPF, handling PDU session management, traffic steering, and reporting PDU events to the SMF. It also transmits lawful intercept targets and packet filtering templates, necessitating robust security measures due to the critical information it transports.

SBI Interface: The SBI connects the control plane's NFs in the 5GC. Security measures for the SBI depend on whether it is considered a trusted interface, with operators deciding on the implementation of security mechanisms.

6.3.1 Vulnerability and Threats

The table below presents the threats to the interfaces.

Table 2: Threats to N3, N4, and SBI Interfaces [3]

Interface	End Points	Vulnerability	Assets	S	T	R	I	D	E
N3	gNB ↔ UPF	Misconfigured routing table	UEs	●					
		Flooding	System resources (UPF)	●	●				
		TEID uniqueness failure	UP and billing	●			●		
		MiTM attack	UE and 5G-SN location information, system resources	●		●	●		
N4	SMF ↔ UPF	Data redirection	Network services, system resources	●	●				
		Flooding of fake PDU session creation request	System resources	●	●				
		Weak protection for signaling data	Session-related data		●		●		
		Session deletion/modification request	System resources	●	●				
SBI	NF ↔ NF	JSON parser exploits	OS, NF file, user data and credentials, system resources, log data	●	●				
		JSON parser not robust	NF API, NF application, system resources		●		●		
		Rogue container	Other NF, the host, services	●		●	●		
		Flawed validation of credentials assertion	Core NFs resources, data, and services	●	●		●		

6.3.2 Security Recommendations

For confidentiality, integrity, replay protection, and authentication, 3GPP and ETSI recommend the following measures for the interfaces:

- **N4 Interface:** IPsec, TLS, HTTPS.
- **SBI :** TLS 1.2, IPsec, PKI, OAuth 2.0.
- **N3 Interface:** IPsec, ESP,IKEv2 certificates-based authentication [3].

6.4 N9, N32 and N6 Interfaces

N9 Interface: The N9 interface connects two UPFs, carrying inter-PLMN UP traffic, including sensitive data that require protection from external exposure or alteration. This interface demands robust confidentiality and integrity protection, especially for signaling messages and security keys [3].

N32 Interface: The N32 interface links SEPPs in different PLMNs, used during roaming. It ensures integrity and confidentiality through protection policies, topology hiding, and message filtering at the application layer [3].

N6 Interface: The N6 interface conveys signaling and privacy-sensitive data to outside networks. It is vulnerable to attacks from connected Data Network Names (DNNs), making it crucial to secure this interface to mitigate external threats.

6.4.1 Vulnerability and Threats

The table below presents the threats to the interfaces.

Table 3: Threats to N9, N32, and N6 Interfaces [3]

Interface	End Points	Vulnerability	Assets	S	T	R	I	D	E
N9	UPF ↔ UPF	No protection for UP data	UP data	●	●				
		Invalid UP data forwarding	UP data			●			●
N32	vSEPP ↔ hSEPP	SEPP impersonation	UP and system resources	●		●			
		Incorrect handling for PLMN ID mismatch	Application layer security data, sufficient processing capacity	●	●				
		IPX impersonation	User data and system resources	●	●	●			
		Weak JWS algorithm	SEPP application	●			●		
		Exposure of confidential IEs in N32-f messages	SEPP application, service message transfer	●	●		●		
		Misplacement of encrypted IEs in JSON object by IPX	SEPP		●				
		Missing cryptographic material of peer SEPPs and IPX providers	SEPP		●		●		
		Policies mismatch	SEPP application, protection policies, system resources		●		●		
N6	UPF ↔ DN	Malformed GTP-U messages	Processing capacity						●

6.4.2 Security Recommendations

For the N32, N9, and N6 interfaces, 3GPP and ETSI recommend the following measures:

N32 Interface:

- Use TLS between SEPPs in the absence of IPX entities.

- Use the PRINS protocol in the presence of IPX, which selectively encrypts necessary parts of transmitted messages.
- Implement JOSE as an application layer security mechanism for protecting roaming traffic [3].

N9 Interface: Use IPsec for confidentiality, integrity, and replay protection.

N6 Interface: Use IPsec for securing data transmission.

7 Literature review

This section provides a synthesis of the articles reviewed on the security analysis of critical 5G interfaces and the integration of Zero Trust (ZT) principles in 5G networks.

Articles	**Summary**
Security Analysis of 5G Critical Interfaces	This paper examines the security of key interfaces in the 5G system (5GS), emphasizing their role in interconnecting Network Functions (NFs) for data and service exchange. The study highlights the vulnerability of critical interfaces such as N1, N2, N3, SBI etc. due to their exposure to external networks and sensitive data handling. It categorizes threats using the STRIDE framework and analyzes security measures proposed by standardization bodies like 3GPP and ETSI. The paper also identifies gaps in existing security recommendations and suggests measures for confidentiality, integrity, authentication, replay protection, and privacy. It emphasizes the need for robust security mechanisms, including encryption protocols (e.g., IPsec, DTLS), key management strategies, and mutual authentication processes, to mitigate risks like spoofing, tampering, and information leakage. This work is notable for its interface-specific focus, offering a detailed analysis of vulnerabilities and threats, and providing insights for enhancing 5G interface security.
Penetration Testing of 5G Core Network Web Technologies	This papermpresents a comprehensive security assessment of the 5G core from a web security perspective, focusing on vulnerabilities in service-based architectures and web technologies. Leveraging the STRIDE threat modeling framework, the authors identify key threats, including spoofing, tampering, information disclosure, and denial of service, in open-source 5G core implementations such as Open5GS, Free5GC, and OpenAirInterface. The study highlights specific vulnerabilities, such as SQL/NoSQL injections, brute force attacks, and directory traversal, emphasizing the importance of proper input sanitization, robust authentication mechanisms, and adherence to the principle of least privilege.

Articles	Summary
ZT and Defense in depth	This article explores the principles of Zero Trust (ZT) applied to six components of 5G: endpoints, the air interface, radio base stations, Multi-Access Edge Computing (MEC), the 5G core network, and IoT applications. The goal is to propose an architecture and a defense-in-depth strategy aligned with ZT principles. The key proposals include: 1. **Endpoint/IoT Device Security:** Data encryption, PKI-based authentication for end devices and authentication of firmware and SIM cards for 5G network devices. 2. **Air Interface Security:** Use of cyphering, integrity protection, and end-to-end encryption. 3. **Radio Base Station Security:** Certificates generating keys for each node, enhancing security over pre-shared keys and reducing key leakage. 4. **MEC Security:** Multiple controls based on the MEC architecture, with end-to-end encryption of control and user plane interfaces to ensure only authorized recipients can access and manipulate messages. 5. **5G Core Network Security:** Multiple controls to protect core functions from various attack surfaces, with each service-based architecture SBA function required to authenticate before accessing other functions. 6. **IoT Application or Internet Access Security:** Multiple controls to secure core exposure to external applications ensuring any application connecting to 5G functions is properly authenticated. This analysis highlights security strategies that reinforce critical 5G components in accordance with ZT principles, aiming to limit unauthorized access and strengthen network integrity.
ZTRAN: prototyping zero trust security xApps for Open Radio Access network deployments	This article explores integrating Zero Trust (ZT) methods into Open RAN (O-RAN), introducing the ZTRAN security framework comprising three microservices: authentication, intrusion detection, and secure slicing. O-RAN's components (O-CU, O-DU, O-RU) present new challenges in user/network authentication, access control, data confidentiality, and resource integrity. 1. ZTRAN Authentication xApp: Ensures secure user equipment (UE) identification through multi-factor authentication (MFA) and temporary random tokens for each UE, enforcing least privilege access. 2. ZTRAN Intrusion Detection xApp: Continuously monitors data traffic for anomalies, using user behavior profiling to detect and flag suspicious activities, promptly sending alerts to mitigate threats. 3. ZTRAN Secure Slicing xApp: Manages resource allocation by creating tailored slices for specific user requirements, with continuous monitoring to ensure optimal Quality of Service (QoS). This framework enhances security in O-RAN by integrating continuous authentication, anomaly detection, and precise resource control.

Articles	Summary
iZTA: Prototyping Zero Trust for 5G Networks	The i-ZTA framework incorporates real-time monitoring, risk evaluation, and access decision-making using a dynamic trust algorithm (MED components). It aligns with the 3GPP 5G specification, leveraging the O-RAN architecture and machine learning for enhanced security. This paper is the first to propose an architectural concept for i-ZTA, setting a foundation for developing AI-driven security solutions in 5G/6G networks. In the i-ZTA architecture integrated into the O-RAN, each component plays a key role in managing the security of 5G/6G networks. 1. Agent and Portal: The agent, a lightweight module on each network asset, collects data for risk assessment. The portal, intended for resource-constrained devices (IoT, sensors), manages access requests and supports federated learning with the agent. 2. Intelligent Network Security State Analysis (INSSA): A graph neural network (GNN) is used to model the behavior of network nodes and assess access risks to resources. This model helps detect anomalies, including Denial of Service (DoS) attacks, and ensures compliance with security rules. 3. Intelligent Policy Engine (IPE): The IPE makes the final decision on access authorization based on the agent's evaluation and the network's state. It uses a neural network to analyze historical activities and adjust security policies. This architecture relies on open interfaces in the O-RAN for data collection and real-time control, allowing for flexible and programmable security management. Integration with cloud platforms, MEC, and fog computing is planned for future research.
Enhancing Security in 5G Cloud-Native Architectures through Zero Trust and Risk-Based Access Control	This article discusses the security challenges in 5G networks, which are built on a highly distributed, open service-based architecture, increasing the attack surface compared to traditional networks. The shift to cloud-native architectures, where monolithic applications are divided into microservices, has resulted in untrusted communication between these services, necessitating new cybersecurity measures. The article proposes integrating the Zero Trust model, which operates on the principle of ”Never Trust, Always Verify,” into access control systems. It emphasizes dynamically adjusting trust levels based on user behavior and recommendations. - **TRBAC (Trust-Based Role-Based Access Control):** This model extends traditional RBAC by incorporating trust and risk elements, evaluating users not only by their roles but also by their behavior, trustworthiness, and associated risk. This dynamic approach helps secure assets by continually assessing user actions and adjusting privileges accordingly. This dynamic approach helps secure assets by continually assessing user actions and adjusting privileges accordingly, addressing the evolving security needs of 5G cloud-native environments.

Articles	Summary
5GC-SDP: Security Enhancement of 5G Core Network with ZT	The following article addresses the 5G core network (5GC) architecture, based on Service-Based Architecture (SBA), which brings significant flexibility and innovation but also introduces security challenges due to the integration of various signaling protocols and virtualization complexities. The proposed solution is a 5GC-SDP architecture that combines Zero Trust principles with a Software-Defined Perimeter (SDP) approach, focusing on secure communication within the core network through Single Package Authorization (SPA). This ensures that only authenticated and authorized Network Functions (NF) can interact securely. - SPA enhancement module: Using machine learning algorithms designed to counter SPA-related DoS attacks. - 5GC-SDP architecture: This enhances core network security by reducing network exposure and implementing fine-grained access control, as demonstrated through tests against port scanning, DoS, and DDoS attacks. The 5GC-SDP architecture effectively enhances core network security by reducing network exposure and implementing fine-grained access control.

8 Results and Discussions

The various articles reviewed have provided valuable insights into how Zero Trust (ZT) can be leveraged to enhance the security of 5G networks. These studies reveal a clear trend toward implementing ZT at the component level, allowing for a security model that operates independently from the core 5G components, whether in the Radio Access Network (RAN) or the Core Network.

While these approaches demonstrate significant progress, they also highlight that the issue of achieving a truly comprehensive ZT framework for the entire 5G system remains unresolved. The goal of implementing Zero Trust across the entire network infrastructure is still a work in progress, as the current solutions address specific components or functions rather than securing the entire ecosystem.

Furthermore, ZT is often applied by layering additional security measures onto existing network functions, rather than fundamentally altering their operation. This approach introduces new technologies and components without disrupting the core functionality of these systems. While this ensures minimal operational disruption, it also suggests that ZT is being added incrementally, and not yet fully integrated at the system-wide level.

A key limitation in the implementation of Zero Trust is the interdependence and interoperability of the various solutions. While multiple technologies and approaches exist, the challenge lies in aligning them seamlessly to create a cohesive and unified ZT model across the entire 5G infrastructure. The heterogeneity of the technologies, including various vendors, network architectures, and legacy systems, creates significant barriers to achieving full interoperability. To realize a comprehensive Zero Trust implementation, it is crucial to address these challenges by ensuring that the diverse technologies can be integrated and aligned to work together effectively.

8.1 Research Gap

While there's growing interest in ZTA and 5G security, a focused analysis on applying ZTA principles specifically to 5G critical interfaces appears to be relatively unexplored in existing literature. Hence there is a need to bridge this gap in future research.

9 Conclusion

The objective of this work was to assess the current state of efforts surrounding the implementation of Zero Trust (ZT) within 5G networks. Our analysis highlighted a growing interest in leveraging ZT principles, as evidenced by an increasing number of studies focusing on this approach due to its ability to address various security challenges. However, these studies primarily target specific components of the system rather than providing security for the entire 5G ecosystem. This limitation often stems from a ”trade-off” between achieving comprehensive security and maintaining operational efficiency.

Additionally, our research involved conducting a threat modeling exercise for the interfaces connecting the various Network Functions (NFs). This analysis revealed a significant gap: while security measures have been applied to critical interfaces, there is no existing literature or research specifically addressing the implementation of Zero Trust (ZT) on these interfaces. This finding opens up a new avenue for research, emphasizing the need for holistic security strategies that extend beyond individual components to secure the entire system.

References

[1] Filippo Dolente, Rosario Giuseppe Garroppo, and Michele Pagano. A vulnerability assessment of open-source implementations of fifth-generation core network functions. *Future Internet*, 16(1):1, 2023.

[2] Wan Lei, Anthony C. K. Soong, Liu Jianghua, Wu Yong, Brian Classon, Weimin Xiao, David Mazzarese, Zhao Yang, and Tony Saboorian. *5G System Design: An End to End Perspective*. Springer, Beijing, China, 2020. ISBN 978-3-030-22236-9 (eBook).

[3] Mohammed Mahyoub, AbdulAziz AbdulGhaffar, Emmanuel Alalade, Ezekiel Ndubisi, and Ashraf Matrawy. Security analysis of critical 5g interfaces. *IEEE Communications Surveys & Tutorials*, 2024.

[4] Ahmed Moniem. What is the difference between vran and open ran?, 2024. Accessed: 29-2024.

[5] VA Stafford. Zero trust architecture. Technical Report 207, NIST, 2020.

A Appendix A

A.1 Components of a Zero Trust Architecture

Component	**Function**
Policy Engine (PE)	Responsible for real-time access decisions, evaluating access requests based on policies considering identity, device status, time, location, and continuous diagnostics and mitigation (CDM) data.
Policy Administrator (PA)	Defines and manages access policies based on the decisions of the PE, instructing the PEP to allow or terminate sessions based on access approvals or revocations.
Policy Enforcement Point (PEP)	Activates, monitors, and terminates connections between subjects and resources according to policies defined by the PA and decisions from the PE.
Continuous Diagnostics and Mitigation System (CDM)	Collects and analyzes real-time data to identify and mitigate security threats, ensuring the system's health and compliance.
Industry Compliance System	Ensures compliance with regulatory requirements and industry standards relevant to the enterprise.
Threat Intelligence Feeds	Collects data from various sources to inform access decisions, including information on attacks, vulnerabilities, and software flaws.
Network and System Activity Logs	Records active logs, network traffic, and resource access activities to provide real-time information on the security state of the system.
Data Access Policies	Defines the rules and regulations governing access to enterprise resources, either dynamically generated by the PE or encoded via a management interface.
Public Key Infrastructure (PKI)	Manages certificates for resources, subjects, services, and applications, ensuring secure authentication and communication.
Identity Management System	Manages user accounts, roles, access properties, and assigned resources within the enterprise, ensuring accurate identity verification.
Security Information and Event Management System (SIEM)	Gathers and analyzes security-related information to adjust policies and prevent potential attacks on the enterprise's assets.

Table 5: Key Components of a Zero Trust Architecture

A.2 Security focuses in 5G

With the growing sophistication and frequency of attacks, the integration of Zero Trust (ZT) into 5G has become essential. This involves strengthening network access security, implementing continuous monitoring to detect threats, and preventing attackers from moving laterally within the network.

1. **Network Access Security**: Focuses on user equipment (UE) authentication and secure network access, addressing threats to the physical/radio interface and aligning with TS 33.501.

2. **Network Domain Security**: Ensures secure data exchange between network nodes, including advancements in SDN, NFV, and MEC.

3. **User Domain Security**: Protects user devices, following NIST guidelines to address device security concerns.

4. **Application Domain Security**: Secures communication between users and application providers, leveraging blockchain and post-quantum cryptography for 5G applications.

5. **Service-Based Architecture (SBA) Security**: Introduces new features for secure communication between network functions, focusing on registration, discovery, and authorization.

6. **Visibility and Configurability**: Informs users about active security features across devices, the core network, and Open-RAN.

A.3 Threats to the N1 Interface

Table 6: Threats to the N1 Interface [3]

Interface	End Points	Vulnerability	Assets	S	T	R	I	D	E
N1	UE ↔ AMF	A bidding down of UE capabilities	UE radio capabilities	●			●		
		AMF impersonation	UE identity	●		●	●		
		Registration request flooding	System resources	●	●				
		Inaccurate SUCI deconcealment	System resources		●		●		
		NAS protocol-based attack	UE data	●	●		●		
		Reuse 5G-GUTI	Mobility management data	●		●	●		
		IMSI catcher	UE identity	●		●	●		
		IMEI visibility	Device and user identity	●		●	●		
		Incorrect implementation of UE security capacity handling	User accounts, data, and credentials	●	●	●	●		
		AMF re-allocation	User data and credentials	●	●		●		
		5G-GUTI and IMEI correlation	User location	●		●	●		
		Logical gNB jamming	Service availability	●	●				
		Physical radio jamming	Service availability and system resources	●	●				