2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS) | 979-8-3315-3119-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/COMSNETS63942.2025.10885674

Zero-Trust Security in 5G and Beyond Networks: An Overview

K Sowjanya
Bharti School TTM
Indian Institute of Technology Delhi
New Delhi, India
sowjanya.kandisa@gmail.com

Dhiman Saha
Computer Science and Engineering
Indian Institute of Technology Bhilai
Bhilai, India
dhiman@iitbhilai.ac.in

Brejesh Lall
Department of Electrical Engineering
Indian Institute of Technology Delhi
New Delhi, India
brejesh@ee.iitd.ac.in

***Abstract*—The evolution of 5G and anticipated 6G networks presents new opportunities for connectivity, performance, and services, but it also introduces substantial security risks due to increased complexity and attack surfaces. Traditional perimeter-based security models fall short in these environments, prompting a shift towards Zero Trust Architecture (ZTA), which enforces principles of strict identity verification, least-privilege access, and continuous monitoring. As ZTA gains traction, standardization bodies such as NIST, 3GPP, and ETSI are developing guidelines to incorporate Zero Trust principles into 5G and 6G infrastructures. This paper explores how these standardization efforts, alongside core ZTA principles, provide a resilient and adaptable security framework for 5G and future 6G networks. Furthermore, the paper highlights the challenges of implementing Zero Trust in 5G and 6G networks and suggests future directions for overcoming these obstacles.**

***Index Terms*—ZTA, ZTS, 5G and Beyond Networks, NIST, 3GPP, ETSI.**

I. Introduction

Zero Trust Security (ZTS) is a vision that challenges the traditional network security model. ZTS provides an additional vigorous and flexible approach to security, based on the assumption that trust should never be granted by default, even inside the organizational circumference. It is mainly focused on resource security and on the fact that trust must be evaluated continuously [1]. Further, Zero Trust Architecture (ZTA) is an end-to-end interconnecting infrastructure that comprises organization resources, access management, hosting environment, operations, and data security. The concept of zero trust has been initiated by the Department of Defense, USA [2] where the migration from a perimeter-based security model to the security of individuals is highlighted. Mobile technology extends its services to numerous verticals that require more significant resiliency in fields like privacy, security, robustness, trust, etc. An end-to-end approach to system security is the basis for resilient communication. Communication resiliency with respect to 5G and beyond networks can be illustrated using five verticals: Privacy, Identity, Robustness, Trust, and Security as depicted in Figure 1.

The 5G and beyond networks are devised to be consistent with zero-trust principles, where no network function or user can be trusted. On a continuous basis, verification is always preferred for access to various resources [3]. This approach requires fine-grained access control/authorization and robust authentication. Zero Trust is based on the premise of "never trust, always verify." It emphasizes strict identity verification, network segmentation, and least-privilege access, assuming that both external and internal threats could compromise the system. ZTS focuses on securing resources like devices, networks, applications, identities, infrastructure, and data as illustrated in Figure 2. ZTS stands at the core of any resilient system.

Fig. 1. Communication resiliency w.r.t. 5G and beyond networks [3]

A. Zero Trust in 5G Networks

In 5G networks, which rely on virtualization and software-defined architectures, ZTA can enhance security by enforcing strict access control and real-time monitoring. Key areas of focus include [4]:

- **Access Control:** 5G uses network slicing, where each slice operates as a virtualized network for specific applications. ZTA can ensure secure access to these slices by authenticating users and devices at every access point.

This work was supported by the project "Next Generation Wireless Research and Standardization on 5G and Beyond (RP04156G)", Ministry of Electronics and Information Technology, Government of India.

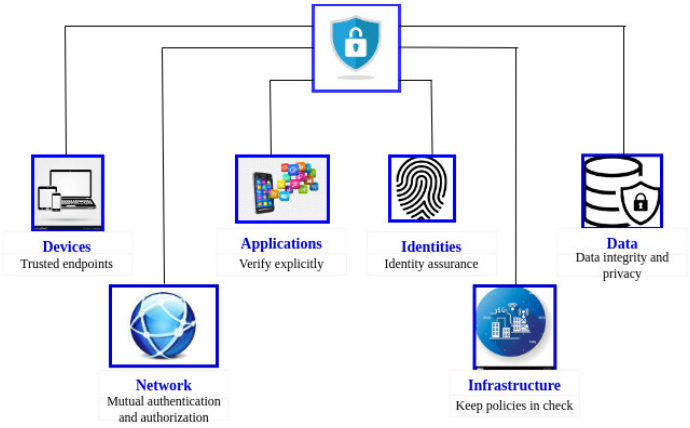

Fig. 2. Zero Trust Security Model [3]

- **Micro-segmentation for Network Slicing:** Zero Trust aligns well with network slicing by applying micro-segmentation to enforce security policies within and between slices, limiting the impact of a potential breach.
- **Dynamic Policy Enforcement:** With the help of AI and machine learning, Zero Trust policies can adapt to the dynamic nature of 5G networks, allowing for real-time, context-aware security enforcement.
- **Continuous Monitoring:** Tracking user and device activity in real-time to detect and mitigate suspicious behavior promptly.

B. Zero Trust in 6G Networks

Although 6G is still in its early research stage, it is expected to be characterized by extreme speeds, AI-driven applications, and pervasive connectivity, leading to even more complex security demands [5], [6]. Zero Trust principles can address the unique security challenges in 6G by:

- **AI-Driven Access Control:** With AI deeply embedded in 6G, Zero Trust policies can leverage AI for continuous identity verification, anomaly detection, and behavioral analysis.
- **Enhanced Micro-Segmentation:** 6G's reliance on edge computing and ultra-low latency services can benefit from Zero Trust's micro-segmentation, securing data at distributed network edges.
- **Quantum-Resilient Encryption:** Given the anticipated threat of quantum computing, Zero Trust in 6G will likely integrate quantum-resistant cryptographic algorithms to protect sensitive data.

C. Contribution

This paper illustrates the standardization aspects of ZTS concerning 5G and beyond networks and the current progress in 3GPP along with challenges in implementing Zero Trust Security in 5G and 6G. Furthermore, it presents related use cases where ZTS helps to achieve a robust and secure 5G System (5GS).

II. Background

This section presents the basics of zero trust followed by zero trust in 5G and 6G networks.

A. Zero trust

Zero trust is defined as a paradigm that focuses on resource protection where trust is never granted utterly rather it should be verified continuously [1]. In simple words, the focus is on authorization, authentication, and reducing the trust areas while preserving the availability and lessening the time delays in authentication schemes. Similarly, access policies are built as fine-grained as possible to impose the least privileges to execute the requested action. According to NIST [1] zero trust access is permitted through a policy decision point (PDP) and its correlated policy enforcement point (PEP). As depicted in Figure 3, resource access is ensured when the user's request is valid and authentic. Proper decision on the access to resource is handled by the PDP/PEP.

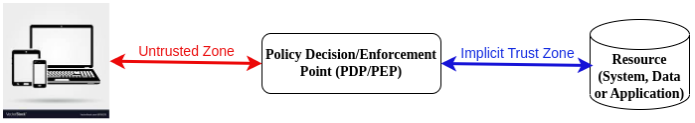

Fig. 3. Zero Trust Access [1]

An implicit trust zone implies a region where all the resources/entities are trusted. One real-time scenario of implicit trust: a boarding agent's trust in the issuing government exemplifies implicit trust in the passport model, removing the need for direct passenger verification [7].

B. Zero trust models w.r.t. 5G and beyond networks

The diverse nature of 5G and beyond networks is increasing the difficulty of ensuring the security of network resources with the traditional perimeter-based security mechanisms. By assuming the situation where the attacker is present inside the network domain, the ZTS model provides an efficient secure framework by overcoming illegal and unauthorized access to the resources [8], [9]. Inherent trust is the basis of the traditional (or perimeter) security model, where it is considered that everything inside the network domain is trustworthy. Perimeter model defenses the outside attacker but fails in the insider's attack scenario. The ZTS model overcomes this concern without considering any trust factor.

According to the 3GPP 5G standards [10], [12], [13], zero trust security is considered in three major domains: SBA domain security, network domain security, and network access security [11]. To enable scalability and flexibility, the 5G SBA employs the separation of user and control planes. Furthermore, the deployments are based on virtualization and container-based technologies where the secure communication between various Network Functions (NFs) is ensured by the SBA domain security. Network domain security focuses on the secure communication of user data and signaling data between radio and the 5G core network. Similarly, network

access security ensures secure access to services provided by the NFs of the 5G system.

C. 5G enablers of zero trust security

Authors in [8] have presented the four primary security attributes in 5G that enable the ZTS model: secure monitoring, secure digital identities, policy frameworks, and secure transport. **Security monitoring** refers to the measurement of network assets' security posture and the detection of security threats by considering the security policies. Monitoring is vital in terms of trust while permitting access to resources. The European Telecommunications Standards Institute (ETSI) [14] bonds with the concept of zero trust and describes the effective continuous monitoring of the level of trust w.r.t. NFs. **Digital identities** play a crucial role in accessing resources and are also a primary parameter in the ZTS model. Secure digital identities are defined by two parameters: the first parameter consists of a serial number, username, domain name, and the second parameter has a token, private key, and password. Here, the second parameter is used to authenticate the first parameter. To ensure the right access to resources by authorized users, the interaction between the physical and logical components of the network must be addressed properly. Policies describe the requirements and access rules to govern the validity of any resource access request. The policy frameworks enable these policies to be managed and distributed properly [1]. Hence, enabling a fine-grained access control based on environmental characteristics, credentials, and roles.

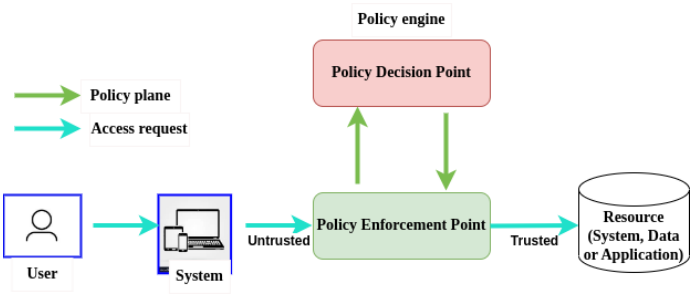

Fig. 4. Components of policy framework [8]

As illustrated in Figure 4, the **policy framework** comprises of two key components: PDP and PEP. A user has to request PEP/PDP to gain access to a specific resource. According to the Tenet 2 of NIST [1], all communications must be secured. A detailed explanation of the Tenets of NIST [1] is presented in the following section.

III. Standardization Aspects

Several leading standardization bodies, including NIST, 3GPP, and ETSI, are actively working to define security frameworks and guidelines that incorporate Zero Trust principles into the next generation of network architectures. Their efforts aim to standardize secure practices for emerging 5G and 6G infrastructures, as well as ensure interoperability and resilience across platforms and service providers.

A. 3rd Generation Partnership Project (3GPP)

The 3GPP Technical Report (TR) [12] describes the existing security mechanisms based on the NIST 800-207 [1] followed by the key issues and the respective solutions w.r.t. the 5G core network.

The first draft TR on ZTS principles in mobile networks is proposed in 2022-06 (SA3#107 eAdhoc), where the scope, architectural, and security requirements along with the key issues and respective solutions are planned for inclusion. Consequently in 2022-08 (SA3#108 e), the evaluation of the current security mechanisms w.r.t. NIST Tenets is added in the draft. After regular updation of evaluation, key issues, and solutions, the final draft of the ZTS enabler in the 5G systems core network is approved in 2023-09 (SA#101). Furthermore, the study on ZTS is still being continued in the SA3 group of 3GPP.

A brief overview of tenants: There are a total of seven tenets illustrated in [1]. The 3GPP TR 33.894 [12] evaluates these tenets concerning the 5G core network.

*1) **Tenet 1. Resources**:* According to NIST SP 800-207 [1] all the computing devices and data sources are referred to as resources. Similarly, with respect to the 5G core, any network functions and their corresponding services are considered resources under the ZTA deployment scenario.

*2) **Tenet 2. Communication security irrespective of the network location**:* According to [1], all communication must be secured irrespective of the network location. In the context of a 5G Core Network (5G-CN), all communication must provide integrity, confidentiality, and source authentication. 5G-CN security provides two ways of communication security: network layer security relies on IPSec and transport layer security depends on TLS. Besides secure communication all other aspects illustrated in tenet 2 of [1] are not pertinent to mobile networks.

*3) **Tenet 3. Access granularity**:* This tenet focuses on access control and authentication to resources, i.e., access is permitted on a per-session basis. 5G-CN provides TLS sessions to provide authentication and OAuth 2.0 mechanism is used to offer authorization [10].

*4) **Tenet 4. Resource access**:* NIST suggests providing access to resources using the dynamic policy which includes the state of the user's identity, service, and other environmental and behavioral parameters. In the context of 5G-CN, an OAuth2.0 token-based authorization does not consider these parameters. Hence, there should be a study to include these behavioral and other attributes to be a part of the access control mechanism in 5G-CN.

*5) **Tenet 5. Continuous monitoring of security posture and integrity**:* According to NIST [1], all the network infrastructure assets must be monitored continuously to guarantee a secure and legitimate state, which includes security patches and regular updates. In 5G-CN, the continuous monitoring of data obtained from the NFs (like network logs and traffic) can be used for threat analysis in order to provide a secure posture and integrity to the network. In the current 3GPP standards, there is no explicit continuous security monitoring is

provided within NetWork Data Analytics Function (NWDAF: core network function) or in any other NF.

6) ***Tenet 6. Access security****:* This tenet is mainly focused on how the access to service producers by the service consumer is secured. At present, the access control and authentication of network service is based on identity and credentials and does not consider monitoring information. Hence, this may result in indirect attacks, where the malicious behavior of any NF is unidentifiable and continues to obtain the services.

7) ***Tenet 7. Data collection****:* This tenet reuses the concepts of tenets 5 and 6, however, adds some clarification on type of the data to be collected for security monitoring. The collected data facilitates the operator for data processing and based on the result of processing, the security posture of the 5G-CN can be improved. At present, there is no standard procedure for this data collection is described in 3GPP.

B. National Institute of Standards and Technology (NIST)

NIST has been a significant proponent of Zero Trust, establishing detailed guidelines and frameworks to implement ZTA across a variety of industries, including telecommunications. Key documents include:

- **NIST Special Publication 800-207:** Published in 2020, this document provides a comprehensive framework for Zero Trust Architecture. While not specifically tailored to 5G, the principles outlined are adaptable to the unique characteristics of 5G and 6G networks, such as network slicing and edge computing. The document emphasizes continuous monitoring, strict Identity and Access Management (IAM), and the principle of least privilege, which are directly applicable to securing network slices and distributed services in 5G and 6G

NIST is also exploring Post-Quantum Cryptography (PQC), recognizing that Zero Trust in 6G will require quantum-resistant encryption methods to protect against future quantum threats.

C. European Telecommunications Standards Institute (ETSI)

ETSI has been proactive in developing cybersecurity standards that address Zero Trust concepts, especially in the context of 5G network security and IoT. Key initiatives include:

- **ETSI Zero Trust Framework (ETSI GS ZSM 002) :** ETSI's Zero Trust framework for network management and orchestration includes security requirements that focus on micro-segmentation, dynamic access control, and continuous risk assessment. This framework provides guidance on implementing Zero Trust principles in complex and heterogeneous 5G environments and is adaptable to 6G [15].

Furthermore, attestation strengthens Zero Trust by validating platform integrity, detecting boot threats like UEFI malware, and securing credentials with hardware-bound key attestation [16].

IV. ZTS USECASES

Many research works [17]–[20] are focused on ZTS model which will enhance the security framework of 5G and beyond networks. This section illustrates two usecases where ZTS provides a robust security framework concerning the 5G core network and serving network.

A. Cross network slice disruption

The point no. 3 of section 6.1.3 of [12], states that the handling of any compromised potential NFs depends on the operator's specific implementation. Based on this concept the authors in [21] demonstrated the cross-slice disruption when the core network function, Session Management Function (SMF) is compromised. They presented two scenarios: 1. Compromised SMF can initiate cross-slice disruption during PDU session establishment through swapping of the tunnel data (uplink) transmitted between the radio and User Plane Functions (UPFs). 2. The same attack can be launched using downlink tunnel data coming from the radio to the core network. A detailed explanation of these attacks and the proposed zero trust security mechanisms to mitigate this cross-slice disruption can be obtained from [21].

B. 5G-based Smart Healthcare System

The passive security measures, such as data encryption and isolation employed in traditional medical platforms, fall short of delivering sufficient protection for a healthcare system deployed in a distributed fashion. They also do not address the demand for data and service sharing across the 'cloud-edge-terminal' in the 5G era. In this regard, the authors of [18] propose a security awareness and protection system that leverages zero-trust architecture for a 5G-based smart medical platform.

C. Mobile Core Networks in 5G and Beyond

The exponential growth in data traffic is compelling mobile network operators to enhance and extend their network infrastructure to meet the evolving demands of customer Service Level Agreements (SLAs). Network Function Virtualization (NFV) offers a means to abstract core network functions from vendor-specific hardware, enabling these functions to seamlessly migrate within the cloud, delivering improved performance and scalability. Nonetheless, deploying a virtualized mobile core network in a cloud environment raises significant security apprehensions, encompassing not only the communication between the Radio Access Network (RAN) and the mobile core network but also within the core network itself. In this regard, the authors of [17] propose a framework called virtual Evolved Packet Core - virtual Software Defined Perimeter (vEPC-vSDP) to provide secure communications within the mobile core network by using an authentication-based approach. The components of the SDP are virtualized and positioned within the virtualized core network, establishing a zero-trust environment in which solely authenticated and authorized core network elements can interact with one another.

D. Defense Against Lateral Movement in 5G IoT Networks

The growing connectivity within the 5G IoT has rendered traditional security defenses insufficient against advanced attackers. It is imperative to transition from perimeter-based defense to a zero-trust security framework that centers on agent-centric trust assessment and access policies for identifying malicious attackers. In this regard, the authors of [19] propose a GAme-theoretic ZEro-Trust Authentication framework to design interdependent trust evaluation and authentication policies using dynamic game models.

V. Challenges in Implementing Zero Trust in 5G and 6G and Future Directions

While ZTA offers robust security solutions, there are challenges in applying it to 5G and 6G:

- **Scalability:** Enforcing Zero Trust principles across thousands of interconnected devices in IoT environments is complex and may strain network resources.
  Solution: Implementation of AI-driven orchestration tools to automate security policies across massive IoT and device networks in real-time. AI and machine learning can dynamically adjust security policies based on usage patterns, device behavior, and contextual data.
- **Latency and Performance:** Continuous authentication and monitoring may impact network performance, especially for latency-sensitive applications.
  Solution: Use of lightweight authentication protocols optimized for speed to reduce latency. For example, fast re-authentication mechanisms can maintain Zero Trust requirements without affecting latency-sensitive 5G/6G applications.
- **Interoperability:** The decentralized nature of 5G and 6G requires ZTA to be compatible across diverse platforms, devices, and standards.
  Solution: Follow standardized frameworks like those developed by NIST, 3GPP, and ETSI to ensure interoperability across diverse devices, applications, and vendors. Zero Trust policies must integrate seamlessly across different network slices, devices, and providers.
- **Privacy Concerns:** Monitoring and verifying user activity at all times may lead to concerns over user privacy and data protection.
  Solution: Implementation of privacy-preserving mechanisms, , such as homomorphic encryption, which allows data processing without exposing private data, and differential privacy, which obscures individual identities in data analysis.

VI. Conclusion

Zero Trust Architecture represents a paradigm shift essential for securing advanced 5G and 6G networks. By treating every access request as untrusted, ZTA provides a robust framework for protecting critical infrastructure and data in these highly interconnected environments. As 6G networks evolve, integrating AI, machine learning, and quantum-resistant cryptography into Zero Trust models will be crucial. Despite challenges, Zero Trust offers a promising solution to address the intricate security demands of next-generation networks. Future research should focus on optimizing ZTA to balance security and performance, ensuring scalability and interoperability across diverse 5G and 6G environments.

References

[1] NIST Special Publication 800-207.: Zero Trust Architecture, Zero Trust Architecture (nist.gov), August 2020.

[2] Department of Defense CIO, "Department of Defense Global Information Grid Architecture Vision, Version 1.0 June 2007. Available at http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

[3] Qualcomm, "How 5G is enabling resilient communication for the connected intelligent edge," Jan 2023. Available at https://www.qualcomm.com/news/onq/2023/01/how-5g-is-enabling-resilient-communication-for-the-connected-intelligent-edge

[4] N. Nahar, K. Andersson, O. Schelen, and S. Saguna, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," IEEE Access, Vol. 12, pp. 94753-94764, 2024.

[5] X. Chen, W. Feng, N. Ge and Y. Zhang, "Zero Trust Architecture for 6G Security," IEEE Network, Vol. 38, Issue, 4, pp. 224-232, 2024.

[6] Y. Liu, Z. Su, H. Peng, Y. Xiang, W. Wang, and R. Li, "Zero Trust-Based Mobile Network Security Architecture, " IEEE Wireless Communications, Vol. 31, Issue. 2, 2024.

[7] RFC 9334, https://datatracker.ietf.org/doc/html/rfc9334#name-passport-model.

[8] J. Olsson, A. Shorov, L. Abdelrazek and J. Whitefield, "Zero trust and 5G – Realizing zero trust in networks," Ericsson Technology Review, 2021. Available at https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g

[9] B. Smeets and P Teppo, "Why Enterprise Zero Trust Architecture matches 5G security," Ericsson blog, 2022. Available at https://www.ericsson.com/en/blog/2022/2/zero-trust-architecture-enterprise-5g-security

[10] 3GPP TS 33.501, "Security architecture and procedures for 5G system," V18.3.0 (2023-09).

[11] National Security Agency Central Security Service, Zero Trust Security Model, 2021.

[12] 3GPP TR 33.894, "Study on applicability of the Zero Trust Security principles in mobile networks," Release 18.

[13] 3GPP TS 23.501, "System architecture for the 5G System (5GS)," v18.1.0 (2023-03).

[14] ETSI GS NFV-SEC 003, "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance," V1.1.1 (2014-12).

[15] ETSI GS ZSM 002, " Zero-touch network and Service Management (ZSM); Reference Architecture ," V1.1.1 (2019-08).

[16] P. Srivastava, "Attestation: A necessity for Zero Trust," https://techcommunity.microsoft.com/blog/microsoftsecurityandcompliance/attestation-a-necessity-for-zero-trust/3667604

[17] Y. Bello, A. R. Hussein, M. Ulema, J. Koilpillai, "On Sustained Zero Trust Conceptualization Security for Mobile Core Networks in 5G and Beyond," IEEE Transactions on Network and Service Management, Vol. 19, Issue. 2, pp.1876-1889, 2022.

[18] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H.Chen, H. Lu and Y.Zhai, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," IEEE Internet of Things Journal, Vol. 8, Issue. 13, pp. 10248-10263, 2020.

[19] Y. Ge and Q. Zhu, "GAZETA: GAme-Theoretic ZEro-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks," IEEE Transactions on Information Forensics and Security, Early Access Article, 2023.

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

[21] S. Vittal, U. Dixit, S. P. Sovitkar, K Sowjanya, and A. Franklin A, "Preventing Cross Network Slice Disruptions in a Zero-Trust and Multi-Tenant Future 5G Networks," IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, June 2023.