Deriving Security Controls through Verification on Open-Source 5G Testbeds*

Toshiro Sawamoto[1†], Yutaro Osako[1,2], Mio Suzuki[1], Takahiro Kasama[1] and Koji Nakao[1]

[1] National Institute of Information and Communications Technology (NICT), Japan
{sawamoto,y.osako,mio,kasama,ko-nakao} @nict.go.jp

[2] Graduate School of Information Science and Technology, The University of Osaka, Japan

Abstract. While 5G networks introduce new functionalities and flexible architectures, they also inherit protocols from previous generations, leading to emerging and unique security challenges. Prior studies have primarily focused on reproducing vulnerabilities and proposing best practices, but little attention has been paid to systematic approaches for transforming such findings into actionable and policy-applicable security controls.

This paper uses an open-source testbed to reproduce 5G-specific threats such as sequence number desynchronization and cascading failures between network functions, thereby deriving corresponding security measures (controls). The derived controls were later incorporated into Japan's national 5G security guidelines[1] and reflected alongside the threats in ITU-T Recommendation X.1818[2]. To our knowledge, this represents the first instance of concretely implementing a methodology that incorporates results from empirical verification using an open-source 5G testbed into domestic policy-based security framework and international standardization. We hope this pioneering research will serve as a guideline for researchers.

Keywords: 5G, Security, Testbed, DoS, OSS, 5G-AKA, ITU-T SG17

1 Introduction

5G networks are expected to play a vital role not only in entertainment but also as a critical component of social infrastructure. To meet the stringent requirements for high capacity, ultra-low latency, and massive connectivity, 5G introduces flexible and dynamic architectures such as Network Function Virtualization (NFV) and the Service-Based Interface (SBI). At present, the 3rd Generation Partnership Project (3GPP) continues to develop specifications for 5G-Advanced (Release 19[3]), expanding 5G's functionality and performance. However, in examining these expansion paradigms, new conceptual considerations and new issues have emerged later in the standardization process, inevitably expanding the attack surface. While design and construction work for the 6G standardization succeeding 5G has already begun, the security of operational 5G and 5G-Advanced systems remains a critical and ongoing challenge.

Network operators and technology suppliers face increasing challenges in implementing both mandatory and optional security functions specified in 3GPP SA WG3[4]. Historically, the translation of theoretical security requirements into concrete implementation practices has largely been left to individual organizations. Yet, as mobile systems evolve into large-scale, cloud-native infrastructures intertwined with internet technologies and incorporating conventional network systems, ensuring consistent and reliable security implementation across diverse environments is becoming increasingly complex. Therefore, developing practical, policy-oriented security guidelines that serve as essential benchmarks for operators and suppliers is indispensable not only for enabling the implementation and operation of secure 5G use cases but also for preparing the transition toward 6G.

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 53, December 16-18, 2025, Sapporo , Japan.
† Corresponding author

Traditionally, the development of such guidelines has relied primarily on conceptual risk analysis and expert review, as exemplified by frameworks such as ISO/IEC 27005[5] and NIST SP 800-30[6], which define processes for risk assessment and management but do not explicitly require empirical validation. However, as architectures and protocols grow in scale and complexity, relying solely on theoretical assessment becomes insufficient. Empirical verification using real or open-source systems is increasingly necessary to complement these traditional processes and to ensure that security controls are grounded in observable system behavior.

Previous studies on 5G security have extensively examined vulnerabilities in various layers, including radio, core network (CN), user privacy, and signaling protocols. Most of these works follow a similar structure: identifying vulnerabilities, reproducing them via simulations or open-source testbeds, and proposing security best practices or mitigation measures. However, such studies typically produce scenario-specific mitigations that depend heavily on individual network configurations, resulting in "best practices" rather than generalized and policy-applicable security controls. In addition, several large-scale initiatives have published comprehensive whitepapers based on commercial-grade 5G testbeds. While these initiatives offer invaluable insights as explained in Section 2, their objectives are primarily validation-oriented—verifying the effectiveness of existing mechanisms—rather than deriving new, generalizable security controls that can inform policy-based security framework or standardization.

In contrast to prior studies that propose technical best practices tied to specific attack scenarios, our work focuses on bridging empirical verification and formulation of policy-based security framework. We reproduced 5G-specific vulnerabilities on open-source testbeds and systematically analyzed the resulting behaviors to derive generalized, policy-applicable security controls. Rather than enumerating mitigation measures for individual attacks, we abstracted the empirical results into high-level security controls suitable for guideline and standardization frameworks, where scenario-specific details were left implementation-dependent. This process demonstrated that empirical verification using open-source testbeds can provide credible evidence for policymaking and standardization, as exemplified by its direct reflection in Japan's national 5G security guideline and ITU-T Recommendation X.1818.

The main contributions of this paper are as follows:

1. Empirical Reproduction: We reproduced 5G-specific vulnerabilities using open-source 5G testbeds and identified reproducible threats (attacks) patterns.
2. Control Derivation: We derived a set of practical and policy-applicable security controls based on empirical observations.
3. Integration to Policy-Based Security Framework: We demonstrated how these controls were reflected in Japan's national 5G security guideline and ITU-T Recommendation X.1818.
4. Evaluation and Outlook: We considered the advantages and limitations of open-source-based verification and explored its potential application for future 6G security initiatives.

2 Background

2.1 Security Whitepapers and Testbed Initiatives

As mentioned in Section 1, several international initiatives have evaluated the effectiveness of 5G security mechanisms and published their findings in the form of whitepapers.

The CTIA 5G Security Test Bed (5G STB[7]), for instance, performs empirical validation of FCC's CSRIC[8] recommendations using commercial equipment from Ericsson, focusing on the verification of standard 3GPP security features.

Similarly, the NIST NCCoE 5G Cybersecurity Project[9] utilizes Nokia's commercial-grade 5G systems to evaluate 3GPP-defined security functions, as well as broader aspects such as infrastructure, applications, and virtualization challenges faced by mobile operators.

Although these facilities offer valuable insights, their closed environments and high operational costs limit accessibility and reproducibility for academic or public-sector researchers. Consequently, open-source 5G testbeds have emerged as practical and cost-effective alternatives for empirical verification, providing accessible platforms to evaluate 5G security in realistic settings.

2.2 Major Open-Source 5G Testbeds

Open-source 5G systems have been developed by numerous research institutions worldwide to accelerate the adoption and understanding of 5G technology.

Early efforts such as [10] and [11] modified open-source 4G frameworks to evaluate network slicing, while more recent projects employ pure 5G implementations for comprehensive experimentation. For example, [12] assesses decoding performance for PSS and SSS signals used in initial cell search, and [13] introduces containerized 5G CN/RAN solutions for network slicing evaluation. Prominent open-source platforms such as OpenAirInterface (OAI) [14] and free5GC[15] now cover most key functionalities up to 3GPP Release 17, including mutual authentication, PDU session establishment, multi user data transfer, and slice-specific UPF selection via SST.

Our preliminary evaluation confirmed that these open-source implementations achieve throughput in the hundreds of Mbps and sub-10 ms latency, sufficient for realistic security testing. Therefore, the maturity of open-source 5G systems is now adequate to support meaningful empirical research on 5G security.

2.3 Security Verification of 5G Authentication

While 5G introduces many new mechanisms, it also inherits legacy components such as modulation schemes, physical-layer protocols, and authentication algorithms like the Authentication and Key Agreement (AKA) protocol. This inheritance implies that certain vulnerabilities identified in legacy generations may persist under 5G environments.

The AKA protocol—used since 3G—relies on synchronized sequence numbers (SQN) for mutual authentication. Previous studies [16] demonstrated that an attacker could manipulate network-side SQN counters, causing desynchronization and authentication failure. To investigate this, we constructed an open-source 5G testbed using Docker-based virtualization and developed a C-based attack tool to replay initial NAS messages. Our experiments successfully reproduced the SQN desynchronization attack under 5G conditions, confirming the presence of inherited vulnerabilities. Moreover, beyond authentication failure, we observed unexpected behaviors such as NF instability and cascading crashes (e.g., Access and Mobility Management Function (AMF) → User Data Repository (UDR)), highlighting the importance of empirically derived security controls. These findings form the foundation for the methodology and security control derivation discussed in Section 4.

3 Methodology & Findings

Our verification focused on reproducing 5G-specific threats related to the AKA protocol by leveraging an open-source 5G testbed. We describe here our verification environment, attack scenario, and the assumptions considered in our study. We then summarize the findings observed through our experiments.

3.1 Verification System

Fig.1 provides an overview of the verification environment, which consisted of a radio access network (RAN) and a CN deployed in our internal laboratory. The RAN included a Linux PC running an open-source-based user equipment (UE) simulator and base station (gNB) simulator, together with a USRP-2901 software-defined radio (SDR) device capable of transmitting and receiving sub-6 GHz 5G signals (Fig.2). The antenna system was installed inside an anechoic box to prevent leakage. Two omni-directional antennas were used, one each for the UE and gNB, with separate transmitting and receiving elements. The CN was implemented on Linux servers using Docker containers, with all network functions (NFs) deployed on a single subnet via Docker Compose. This setup allowed reproducible and flexible deployment of open-source 5G systems.

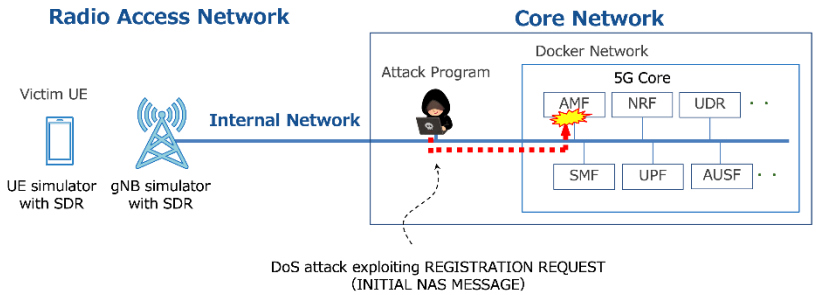

Fig.1. 5G Security Verification System

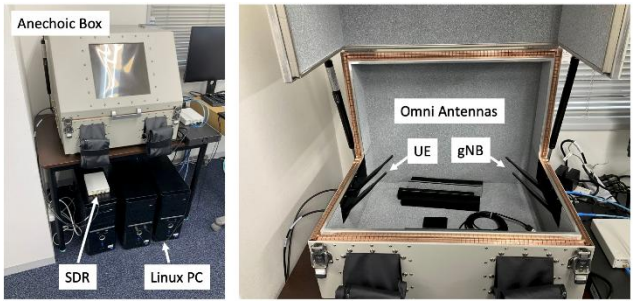

Fig.2. 5G Radio Access Network Verification System

3.2 Attack Scenario

As illustrated in Fig.3, a UE begins the connection procedure by decoding system information broadcast by the gNB, synchronizing the radio link, and performing initial registration with the 5G core in bootstrapping process. This process includes Security Mode Control (SMC) for negotiating encryption algorithms.

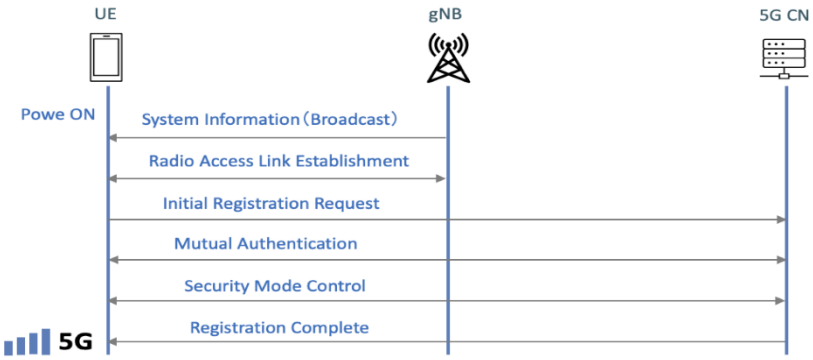

Fig.3. 5G Bootstrapping Sequence

The initial step requires the UE to send a Registration Request, which contains the Subscription Concealed Identifier (SUCI)—an encrypted form of the Subscription Permanent Identifier (SUPI). Only UEs registered in the network are expected to succeed in mutual authentication.

In our attack, we captured a legitimate Registration Request from a victim UE and replayed it against the AMF as illustrated in Fig.1. A custom program written in C was used to establish an SCTP session with the AMF, transmit an NG Setup Request, and then repeatedly send the captured Registration Request. While the AMF responded with Authentication Requests as specified, our program ignored these responses and continued sending replayed Registration Requests unilaterally.

3.3 Assumptions

Although an attacker could exploit the air interface to capture and replay messages, our experiments targeted attacks from within the CN domain. We assumed that the adversary had already intruded into the 5G network and obtained the ability to interact directly with NFs. This assumption reflects realistic attack

vectors in virtualized 5G deployments, where NFV enlarges the potential attack surface, particularly when network configurations are inadequately secured by operators.

3.4 Findings

Our verification produced two major findings: the reproducibility of legacy vulnerabilities in 5G environments, and cascading failures triggered by repeated replay attacks.

Reproduction of inherited threats. In our verification, we confirmed that the SQN count-up vulnerability, previously demonstrated in 4G networks, can also be reproduced in 5G through a denial-of-service (DoS) attack exploiting replayed Registration Requests. While earlier studies suggested that this vulnerability might persist in 5G, our experiments verified its reproducibility on two different open-source 5G networks. The attack caused inconsistencies in the SQN integrity check at the UE side, leading to authentication failures (Fig.4). Notably, the exploited Registration Request is an initial NAS message transmitted in plaintext before mutual authentication is completed. Because such unauthenticated messages are implicitly trusted by the network, they can be misused as triggers for attacks that severely compromise network availability.

Cascading failures triggered by threat reproduction. During the experiments, we also observed cascading failures of NFs deployed as Docker containers. The AMF, as the direct target of the DoS attack, crashed first. Subsequently, other NFs such as the UDR also experienced failures in a chain reaction. This behavior appears to result from repeated queries to dependent NFs initiated by the AMF upon receiving each Registration Request. Although not every NF crashed consistently, abnormal states were observed, such as containers becoming unresponsive or sending Authentication Requests to unrelated IP addresses. These behaviors are unlikely to be identified through specification analysis alone, highlighting the necessity of verification on actual 5G systems.

Overall, these results demonstrate that open-source 5G testbeds can reveal vulnerability-driven behaviors originating from both protocol design and implementation aspects. Such findings provide critical evidence for deriving comprehensive security controls, which are discussed in Section 5.

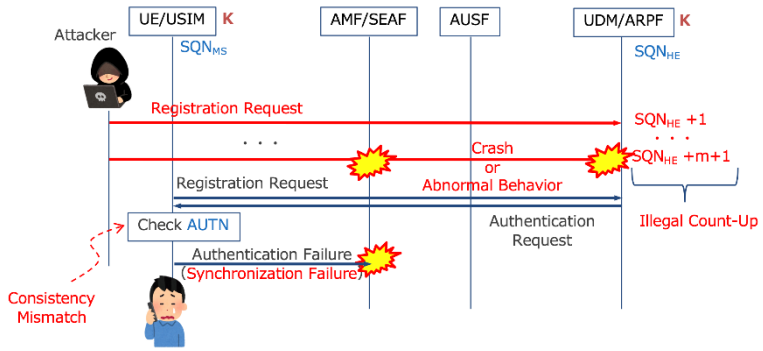

Fig.4. Mechanisms Triggering Authentication Failure in 5G-AKA

As a part of our frameworks, these findings are interpreted to threats (attacks) patterns as Table 1, which is a crucial process for deriving security controls.

Table 1. Derivation of Threats (Attacks) Pattern

Observed in open-source testbed	Threats (Attacks) pattern
Authentication failure due to SQN mismatch from replayed Registration Request and chain-reaction failures (AMF → UDR)	Lack of replay detection and sequence validation logic
Continuous replay causing AMF crash	Insufficient network segmentation and lack of secure inter-NF boundary protection (no gateway/firewall enforcement)
Unauthenticated signaling during initial registration (implicit trust in AKA pre-authentication phase)	Design dependency on unauthenticated control messages (implicit trust assumption)

4 Derivation of Security Controls

Section 4.1 to 4.3 demonstrate translation of threats (attacks) patterns into implementable mitigation measures that form the basis for generalized security controls. Whilst some controls, such as error handling mechanisms of Section 4.1, are closer to operational best practices, others such as Section 4.2 and 4.3 reflect higher-level design principles that transcend specific deployment models.

Furthermore, Section 4.4 systematises and generalises these, elevating them into a framework of security controls applicable across the entire 5G network, independent of specific conditions or architectures.

4.1 Mitigation 1: Error-handling for Repeated Identical Requests

In our verification, authentication failures caused by SQN mismatches were reproduced by replaying the Registration Request message. A possible mitigation is to incorporate an error-handling mechanism that can automatically reject abnormal signaling sequences not explicitly defined in 3GPP specifications.

According to the 3GPP standard, a Registration Request is expected to be transmitted only once — or at most a few times — during a single registration procedure initiated by a UE. Therefore, a large number of consecutive and identical Registration Requests from the same UE within a short period can be reasonably regarded as malicious control traffic targeting the AMF.

Once such abnormal signaling patterns are detected, the system should immediately discard these requests to prevent unnecessary processing or resource exhaustion at the AMF. To achieve this, One feasible approach is to analyze the legitimate message flow defined in the 3GPP specification and implement a verification scheme that can identify and ignore any messages deviating from valid signaling sequences.

4.2 Mitigation 2: Proper Isolation of NFs and Resilience Design

As a fundamental principle, 5G networks must be properly isolated from the Internet to prevent potential attacks originating from external domains. Modern 5G architecture is designed around flexible and virtualized network construction, leveraging the concept of NFV. Instead of deploying dedicated hardware within closed operator networks as in legacy systems, segmented NFs are now often deployed on general-purpose computing platforms in the cloud or even on the public Internet. Another architectural option is to distribute user-plane functions (UPFs) from the CN to the edge in order to provide flexible and scalable user-plane processing according to traffic demand. Since 5G networks, like 4G, are fully IP-based, it should be noted that even attacks exploiting the mutual authentication process between UE and the network—such as those demonstrated in our verification—can be initiated not only via the radio access domain but also directly from the Internet. In addition, 5G networks are actively promoting openness through APIs for third-party service providers via the network exposure function (NEF), and through integration with non-3GPP networks via the N3IWF. While such openness and flexibility are key advantages of 5G, operators must design and operate their networks with extreme caution to avoid expanding the attack surface that accompanies these new capabilities.

It is also important to recognize that these considerations may appear to contradict the Zero Trust principles proposed by NIST[17]. Zero Trust, defined by seven core tenets, is based on the philosophy of “never trust, always verify.” In essence, Zero Trust abandons the traditional perimeter-based security

model and instead requires continuous, context-aware verification of communications and connections, regardless of their origin. Conversely, 3GPP adopts a pragmatic stance that implicitly trusts internal domains[18], assuming that communications are properly protected and authenticated using mechanisms such as TLS and IPsec.

Considering these perspectives, we propose that NFV-based 5G networks ensure proper isolation from external networks through secure gateways implementing TLS and VPN connections employing IPsec. Such measures are expected to maintain the integrity of the 5G security domain and to ensure resilient network operation. By introducing these measures, network operators can effectively prevent malicious intrusions or unauthorized access to individual NFs from external sources, thereby mitigating the occurrence of the demonstrated threats.

4.3 Mitigation 3: Moving Away from Implicit Trust in Initial Access Procedure

As discussed in Section 4.2, the 3GPP security architecture allows a degree of implicit trust within the network domain, assuming that communications are protected by TLS or IPsec. A similar form of implicit trust also exists during the bootstrapping procedure—the focus of our threat verification—where the AKA protocol continues to rely on unauthenticated signaling messages at the beginning of the registration process. This reflects a design philosophy that has persisted across multiple generations of mobile networks. Such provisional trust is not merely an oversight but rather a trade-off inherent to mobile network operations. Real-time service requirements, ultra-low latency targets, and the lack of pre-established security contexts for UEs make it practically difficult to eliminate implicit trust completely during the registration phase. Consequently, 3GPP specifications prioritize seamless service continuity and system performance while acknowledging that some unauthenticated messages must be temporarily accepted. Therefore, it is important to consider how the measures discussed in Sections 4.1 and 4.2—such as error-handling for replayed messages and network isolation for resilient operation—can be integrated with ongoing efforts to reduce implicit trust at the protocol level. This balance between performance and security remains an open challenge, requiring continuous evaluation as new architectures such as Zero Trust and cloud-native 6G systems evolve. In this subsection, we briefly introduce some of existing studies that explore cryptographic approaches to reduce implicit trust in the initial access procedure.

The work in [19] highlights that implicit trust at both ends of communication—for instance, messages that may originate from malicious base stations—remains a critical issue in 5G networks. To address this problem, the authors propose utilizing a Public Key Infrastructure (PKI) architecture and deploying a trusted Certificate Authority (CA), enabling mobile devices to efficiently verify the authenticity of all messages received from base stations. They argue that this approach can effectively mitigate the challenge of pre-authentication messages and prevent spoofed devices from sending unauthenticated signaling. The study further suggests embedding hash values in signaling messages to ensure freshness and to protect against replay attacks. Similarly, [20] proposes a digital certificate–based scheme for signing and authenticating broadcast messages from base stations. By incorporating a hash of timestamps into the signature, replay attacks can be avoided while maintaining message integrity.

Although these methods provide valuable insights into the reduction of implicit trust, practical deployment challenges—such as certificate management overhead and latency implications—remain and should be considered in future standardization efforts.

4.4 Generalization of Derived Controls

The mitigation measures discussed in Sections 4.1 through 4.3 were initially derived from a limited experimental condition involving insider replay attacks that caused SQN desynchronization between the UE and the CN. While this specific scenario revealed authentication failures and network function instability, the resulting insights extend far beyond the particular conditions of the experiment. By abstracting these empirical findings, we generalized the observed threats (attacks) into broader architectural principles applicable across heterogeneous 5G deployments.

Rather than defining narrowly tailored mitigation steps for individual incidents, our analysis focused on identifying root causes and systemic vulnerabilities underlying the observed failures. This abstraction process revealed three recurring patterns: a lack of robust error-handling mechanisms, inadequate network isolation, and implicit trust assumptions between NFs. These issues are not unique to the 5G-AKA procedure but instead potentially represent fundamental threats in 5G network architectures as a whole.

Through this abstraction, we formulated three general security control domains:
1. Robust Error Handling. It is recommended that authentication failures and state inconsistencies be isolated and managed through explicit fault-handling mechanisms that prevent imposing illegal process as well as cascading effects across multiple NFs. Rather than assuming the validity of signaling, NFs should autonomously detect and recover from abnormal or repeated message sequences.

2. Network Isolation and Resilience. 5G network isolation from the Internet is vital to do away with a direct attack by attacker. This principle holds regardless of network topology—whether monolithic, virtualized, or containerized—and provides the foundation for resilient system design.

3. Reduction of Implicit Trust. The reliance on unauthenticated signaling during registration and intra-domain communication introduces latent attack vectors. To mitigate such risks, it is essential to reduce implicit trust assumptions among NFs by promoting authentication, validation, and assurance mechanisms across both internal and external interfaces. Continuous monitoring can serve as an effective means of enhancing intra-domain assurance and reducing implicit trust, particularly in dynamic and virtualized 5G environments. However, its actual implementation should depend on each operator's policy, operational requirements, and architectural design. While such measures are encouraged to strengthen system-wide trust management, they must remain adaptable to diverse deployment models and service characteristics defined by individual operators.

These generalized security control domains transcend individual protocol behaviors and remain architecture-agnostic, allowing them to be applied consistently across diverse deployment models. For example, the need for robust state management identified in 5G-AKA also applies to PFCP session control, SBI-based NF communications, and service orchestration mechanisms in cloud-native environments. Similarly, the implicit trust observed in the bootstrapping process parallels challenges found in other service-based interfaces where static trust boundaries persist. By generalizing empirical observations into architecture-independent principles, we establish a conceptual bridge between incident-driven analysis and policy-level security control derivation. This process enables open-source empirical evidence to serve as a credible foundation for guideline formulation and international standardization, as further discussed in Section 5.

5 Discussion

This section outlines our 5G Security Guideline and discusses how the security controls derived from open-source-based threat verification were reflected in the development of the 5G Security Guideline. It also examines the practical limitations of open-source-based approaches when used for deriving security controls. Finally, we study the appropriate scope of open-source 5G networks utilization to develop security controls with a view to enhancing to 6G.

5.1 Reflection of Results on Guidelines and Standardization

This study derived a set of security controls based on threat reproduction using open-source 5G networks. Combining these empirical findings with a detailed theoretical analysis following the STRIDE-LM methodology, we developed " The First Edition of 5G Security Guidelines " for safe and reliable 5G network deployment and operation. The overall structure of the guideline, shown in Fig. 5, was designed according to the framework described below.

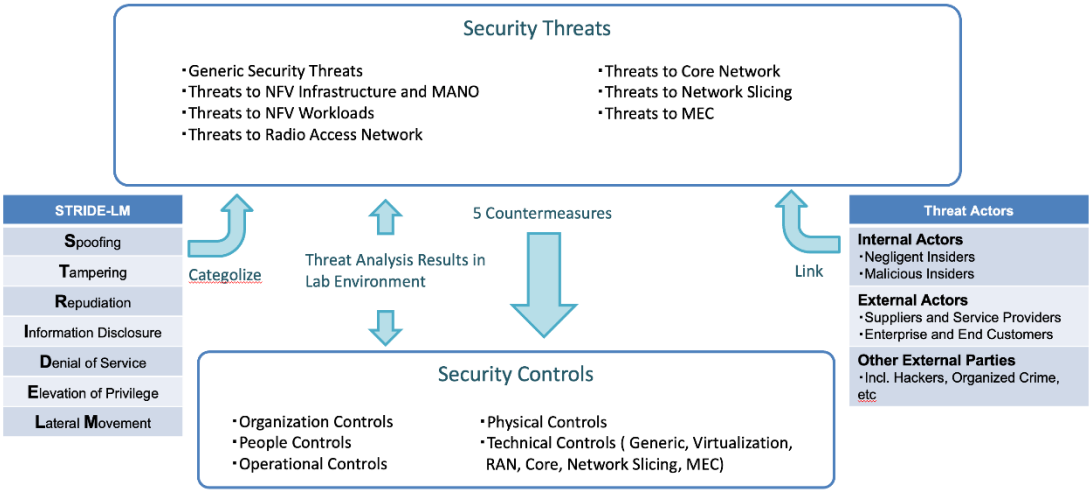

Fig. 5. Outline of 5G Security Guideline

First, through analytical assessment, we identified major security threats across seven domains: Generic, NFV Infrastructure and MANO, NFV Workloads, Radio Access Networks, CN, Network Slicing, and MEC. Each threat was further classified according to the STRIDE-LM model and associated with relevant threat actors: Internal, External, or Other Correspondingly, five categories of security controls—Organizational, People, Operational, Physical, and Technical (including Generic, Virtualization, RAN, CN, Network Slicing, and MEC aspects)—were extracted as countermeasures. The guideline provides practical and high-level recommendations to operators addressing common security challenges in 5G network deployment and operation. In addition to technical issues, it also covers process- and human-related aspects of cybersecurity management. The derived security controls described in Sections 4.1–4.3 were generalized in 4.4, correspond to the high-level principles defined the guideline. Specifically, they are mapped respectively to Operational Controls (error handling), Technical Controls for CN and Virtualization (isolation and resilience), and Authentication and Key Management (reduction of implicit trust). It represents the first comprehensive guideline in Japan intended for both network operators and technology suppliers and is now published on the Ministry of Internal Affairs and Communications (MIC) website as a foundational national document of policy-based security framework. Building on this guideline, we further initiated standardization activity in ITU-T SG17. As a result, ITU-T Recommendation X.1818, "Security controls for operation and maintenance of IMT-2020/5G network systems", was approved at the September 2024 meeting and is now an internationally recognized standard.

This outcome demonstrates that open-source-based verification should no longer be regarded as a supplementary technique inferior to theoretical analysis, but rather as a credible evidential basis for policy-based security framework and standardization. Traditional guideline and standardization processes have largely relied on risk analysis and expert review, with limited support from reproducible experiments. The unique contribution of this work lies in bridging theoretical specification analysis with empirical validation, showing that real-world behavior observed through open-source testbeds can substantiate and refine policy-based controls by a generalization of security controls. Notably, the approach proved effective in deriving security controls against implementation-dependent vulnerabilities that are difficult to identify through static specification review alone.

5.2 Limitation of Open-Source-Based Verification

While the open-source-based approach proved effective in deriving practical security controls and influencing both domestic and international standardization, its applicability remains bounded by several inherent limitations. This section discusses the advantages and drawbacks identified through our experiments and provides a mapping between standardized 3GPP interfaces and their current implementation coverage in representative open-source platforms.

Advantages:

- *Low Cost:*

Open-source software is freely available and can be deployed using general-purpose hardware such as commodity PCs or SDRs, significantly reducing setup costs.

- *Openness:*

Source code transparency enables users to inspect and modify implementations, facilitating reproducibility and extensibility.

- *Ease of Deployment:*

Most open-source testbeds (e.g., OAI, free5GC, Open5GS) support NFV-based deployment via VMs or Docker containers, allowing complete 5G networks to be built through automated scripts.

Limitations:

- *Dependency on Open-Source Scope:*

Verification coverage is inherently limited by the functionality implemented in each open-source distribution. These projects primarily aim for protocol conformance rather than faithful replication of commercial implementations; hence, results may not always generalize to production systems.

- *Difficulty of Use-Case Implementation:*

While simple configuration changes—such as adding NFs or duplicating slices—are feasible, realistic use cases (e.g., URLLC or eMBB deployments) are rarely implemented, confining security testing to basic protocol behavior.

- *Incomplete Implementation:*

During our experiments, we observed partial or missing implementations of certain encryption protocols and signaling sequences, particularly for TLS, OAuth 2.0, and IPsec, which are critical for 5G security protection.

Mapping of 3GPP Interfaces and Open-Source Coverage:

Table 2 summarizes the relationship between major 5G interfaces, their standardized security requirements, and the extent to which these are implemented in current open-source platforms. In our experiments focusing on the N1 and N2 interfaces, the relevant security mechanisms were fully implemented, enabling accurate vulnerability reproduction and control derivation.

Table 2. Security Requirements on 5G interfaces and Verification Feasibility with Open-Source 5G Testbeds

Interface	Communication Entities	Encryption Requirement(3GPP)	Remarks	Verification Feasibility with Open-Source
N2	AMF↔gNB	Not mandatory	Assumed operator domain isolation	✓
N3	gNB↔UPF(U-Plane)	Not mandatory	Encryption may affect latency in high-speed traffic	✗
N4	SMF↔UPF	Not mandatory	PFCP over UDP, trust domain assumed	✗
F1-C/U	gNB-CU↔gNB-DU	Not mandatory	Local RAN deployment assumed	✗
Xn	gNB↔gNB(Handover)	Not mandatory	Within same operator domain	✗
E1	gNB-CU-CP↔gNB-CU-UP	Not mandatory	Internal interface within RAN	✗
N1 NAS	UE↔AMF	Mandatory	Encryption and integrity protection after authentication	✓
N6	UPF↔DN(Internet etc.)	Conditional	IPsec / HTTPS commonly used for external paths	✗
SBI(Nn)	AMF, SMF, PCF etc.	TLS mandatory	HTTP/2 over TLS defined in TS 33.501	✗(partially implemented)

These observations suggest that future empirical studies should strategically focus on open-source-implemented domains while complementing unimplemented areas through hybrid verification combining commercial or simulated modules.

5.3 Toward a Framework for Empirical Security Control Derivation Using Open-Source 5G Testbeds

Considering the above limitations, practical utilization of open-source 5G testbeds should concentrate on domains where authentication and signaling mechanisms are fully implemented—such as the N1 and N2 interfaces. Combining multiple open-source platforms to exploit their complementary strengths can further expand the scope of verification. Establishing a continuous feedback loop—where open-source-based empirical findings are systematically reflected in guideline development and standardization processes—can accelerate evidence-driven policymaking in cybersecurity. This study suggests that such integration between experimentation and standardization may serve as a sustainable model for future 6G security initiatives. Ultimately, open-source-based verification should not be viewed merely as a technical exercise but as an essential component of an evidence-driven standardization ecosystem. This approach has arguably formed a new paradigm where experimental verification can continuously improve both the technical security controls and the security framework that relies on policies.

6 Conclusion

This paper discussed the derivation of security controls for 5G networks through empirical verification using open-source testbeds. Building on theoretical threat modeling and reproducing 5G-specific vulnerabilities/threats on open-source environments, we demonstrated how the findings can directly contribute to policy-making and international standardization. Our approach, which integrates practical threat reproduction with systematic analysis of empirical observation, led to the development of the national 5G Security Guideline and its subsequent incorporation into the international standard ITU-T Recommendation X.1818.

This study revealed that open-source 5G testbeds are not merely tools for academic experiments but can serve as credible platforms for deriving and validating security controls. They provide actionable evidence that complements theoretical analysis, thereby strengthening the robustness of policy-based security framework and standardization processes. At the same time, we acknowledged that open-source verification has inherent limitations—it depends on implementation completeness, lacks certain commercial-grade features, and cannot fully emulate real network conditions. Therefore, any future efforts should also consider hybrid approaches that combine multiple open-source platforms and, where feasible, incorporate commercial systems to ensure comprehensive validation.

Looking ahead, the derived controls and the framework defined in ITU-T Recommendation X.1818 are expected to serve as practical references for operators and vendors around the globe in designing secure 5G and beyond-5G systems. Continuous updates and refinements will be required as emerging technologies—such as AI-driven network management, Zero Trust principles, and PQC/256bit key length encryption —reshape the threat landscape. Future work will focus on identifying residual gaps between standard-based security controls and field implementations, and exploring how these findings can guide the evolution of 6G security framework and principles. In this context, empirical validation—whether through open-source or hybrid environments—will remain a cornerstone for ensuring that international standards evolve hand-in-hand with real operational experience, forming a sustainable bridge from 5G to 6G security assurance.

References

1. Ministry of Internal Affairs and Communications (MIC): 5G Security Guideline, Version 1.0, Tokyo, Japan (2022). https://www.soumu.go.jp/main_content/000812253.pdf

2. International Telecommunication Union (ITU-T): Recommendation X.1818 — Security controls for operation and maintenance of IMT-2020/5G network systems, Geneva, Switzerland (2024). https://www.itu.int/epublications/publication/itu-t-x-1818-2024-09-security-controls-for-operation-and-maintenance-of-imt-2020-5g-network-systems
3. 3rd Generation Partnership Project (3GPP): 5G System Specifications, Release 19, Valbonne, France (2024). https://www.3gpp.org/specifications-technologies/releases/release-19
4. 3rd Generation Partnership Project (3GPP) SA Working Group 3 (SA3): Security and Privacy Aspects for 5G System, Valbonne, France (ongoing since 2016). https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3
5. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC): ISO/IEC 27005:2022 — Information Security, Cybersecurity and Privacy Protection — Guidance on Information Security Risk Management, Geneva, Switzerland (2022). https://www.iso.org/standard/80585.html
6. National Institute of Standards and Technology (NIST): NIST Special Publication 800-30 Rev.1 — Guide for Conducting Risk Assessments, Gaithersburg, MD, USA (2012). https://csrc.nist.gov/pubs/sp/800/30/r1/final
7. 5G Security Test Bed (5G STB): Official Website, Washington, D.C., USA (2022). https://5gsecuritytestbed.com/
8. Federal Communications Commission (FCC): Communications Security, Reliability and Interoperability Council (CSRIC) — Official Website, Washington, D.C., USA (2023). https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0
9. National Institute of Standards and Technology (NIST): National Cybersecurity Center of Excellence (NCCoE) — 5G Cybersecurity Project, Gaithersburg, MD, USA (2023). https://www.nccoe.nist.gov/5g-cybersecurity
10. Shorov, A.: 5G Testbed Development for Network Slicing Evaluation. In: Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus 2019), Saint Petersburg and Moscow, Russia, pp. 39–44. IEEE (January 2019)
11. Chen, S., Lee, C.-N., Lee, M.-F.: Realization of 5G Network Slicing Using Open Source Softwares. In: Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2020), Auckland, New Zealand, pp. 1549–1556. IEEE (December 2020)
12. Drozdova, V.G., Kalachikov, A.A.: SDR-Based Evaluation of the Initial Cell Search in 5G NR OpenAirInterface Implementation. In: Proceedings of the XV International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE 2021), Novosibirsk, Russian Federation, pp. 248–251. IEEE (October 2021)
13. Atalay, T.O., Stojadinovic, D., Stavrou, A., Wang, H.: Scaling Network Slices with a 5G Testbed: A Resource Consumption Study. In: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2022), Austin, TX, USA, pp. 2649–2654. IEEE (April 2022)
14. OpenAirInterface Software Alliance: OpenAirInterface 5G Project. https://openairinterface.org/
15. Free5GC Project: Free5GC - Open Source 5G Core Network. https://free5gc.org/
16. Hussain, S.R., Chowdhury, O., Mehnaz, S., Bertino, E.: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In: Proceedings of the Network and Distributed System Security Symposium (NDSS 2018), San Diego, CA, USA. Internet Society (February 2018)
17. Rose, S., Borchert, O., Mitchell, S., Connelly, S.: Zero Trust Architecture. NIST Special Publication 800-207, National Institute of Standards and Technology (August 2020). https://csrc.nist.gov/pubs/sp/800/207/final

18. 3GPP: Study on Applicability of the Zero Trust Security Principles in Mobile Networks (Release 18). Technical Report 33.894, Version 18.0.0. 3rd Generation Partnership Project (September 2023)

19. Jover, R.P.: The Current State of Affairs in 5G Security and the Main Remaining Security Challenges. arXiv preprint arXiv:1904.08394 (2019)

20. Hussain, S.R., Echeverria, M., Singla, A., Chowdhury, O.: Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil. In: Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019), Miami, FL, USA, pp. 1–12. ACM (May 2019).