Validation of Traceability Attacks in NAS Registration Procedure*

DongHoon Lee, YoungJae Kim, Taeho Won, Bonam Kim, and Ilsun You

Kookmin University, Seoul, Republic of Korea
{dhsama51, zeroash1225, xoghdnjs12, kimbona, isyou}@kookmin.ac.kr

Abstract

5G NAS Security Mode Command is integrity-protected but not encrypted, which has led to suggestions that it could cause traceability attacks. In this work, we analyze the attack scenario and reproduce it in an open-source testbed. Our experiments show that the SMC-based traceability attack is not vaild in practice.
Keywords: 5G, 5G NAS, UE Registration, traceability attack, NAS Count

1 Introduction

5G is widely deployed for its high throughput, low latency, and massive connectivity. UE(User Equipment) and the AMF(Access and Mobility Management Function) exchange NAS(Non-Access Stratum) messages for authentication and mobility management. During registration, the Security Mode Command(SMC) is a key NAS message that activates the NAS security context on the UE. Its integrity is protected but not encrypted, allowing an adversary to detect when an SMC is sent[1]. X. Hu et al. proposed a location-tracking scenario that leverages an attacker's ability to observe SMCs[2]. In this study, we reproduce the scenario in an open-source environment and experimentally evaluate its feasibility.

2 Background

The NIA(NR Integrity Algorithm) computes the NAS-MAC using K_{NASint} with following inputs: NAS COUNT, MESSAGE, DIRECTION, and BEARER. When an SMC is sent, the NAS COUNT is initialized to 0 within the security context and incremented by one for each NAS message after SMC[3]. In other words, the NAS COUNT in SMC is always 0.

Figure 1: 5G hierarchical key derivation

As shown in Figure 1, K_{NASint} is derived through a hierarchical key derivation chain. K_{AUSF} is derived using CK and IK, which are computed by RAND exchanged in 5G-AKA. Consequently, even if the same UE re-registers to the same AMF, K_{NASint} will differ from each session and the NAS-MAC on the SMC cannot match a previous MAC. Therefore, when a malicious gNB replays a previous captured SMC, the UE always responds with Security Mode Reject.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-42, December 16-18, 2025, Sapporo, Japan.

3 Experiment

Experiments were conducted on Ubuntu 24.04 with the open-source 5G core and RAN simulator, Open5GS and UERANSIM.

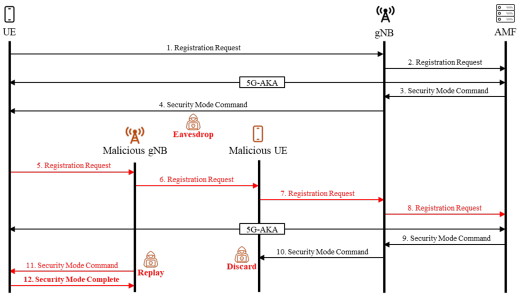

Figure 2: NAS SMC-based traceability Attack Scenario

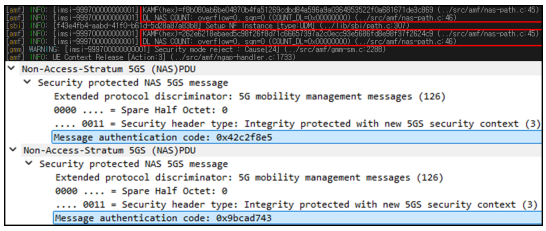

Figure 3: NAS SMC-based traceability Attack Result

According to X. Hu, a Malicious gNB and Malicious UE perform a MitM(man-in-the-middle) between UE and gNB[2]. The attacker discards fresh SMC from the AMF and then replays a previous captured SMC from the same AMF.

Across two registration attempts by the same UE, the AMF's NAS COUNT for the SMC was 0 in both cases, but the derived K_{AMF} differed between sessions. Consequently, NAS-MACs did not match (0x42c2f8e5, 0x9bcad743), and the UE responded with Security Mode Reject to the replayed SMC.

4 Conclusion

This paper verifies in an open-source environment that the NAS SMC-based traceability attack fails since K_{NASint}, used to compute NAS-MAC is re-derived and varies with RAND in the 5G-AKA procedure. Our results strengthen confidence in the integrity protection of the NAS procedure. In future work, we will analyze potential vulnerabilities in other NAS registration messages.

Acknowledgment: Following are results of a study on the 'Convergence and Open Sharing System' project, supported by the Ministry of Education and National Research Foundation of Korea(A2025-0374).

References

[1] 3GPP(3rd Generation Partnership Project), "Non-Access-Stratum (NAS) Protocol for 5G System (5GS)," Tech. Spec. 3GPP TS 24.501 v19.4.0, 3GPP, Sept. 2025.

[2] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security," *IEEE Access*, 2019.

[3] 3GPP(3rd Generation Partnership Project), "Security Architecture and Procedures for 5G System," Tech. Spec. 3GPP TS 33.501 v19.4.0, 3GPP, Sept. 2025.