Revisiting the Unsafe GUTI Reallocation Practices in Commercial 5G Networks

Dong Hyeok Kim
School of Computing
KAIST
Daejeon, South Korea
kimdh98@kaist.ac.kr

Min Suk Kang
School of Computing
KAIST
Daejeon, South Korea
minsukk@kaist.ac.kr

***Abstract*—In this paper, we revisit a well-understood security vulnerability in cellular networks, infrequent and predictable reallocation procedure of globally unique temporary identifiers (GUTI). We conduct measurements on the GUTI values assigned by two South Korean commercial 5G networks to investigate the prevalence of the known vulnerability. Our results show that despite the security enhancements introduced by 5G GUTI reallocation procedures, the unsafe practices discovered in LTE networks nearly a decade ago continue to persist in commercial networks today. We hope that this result will contribute towards accelerating the deployment of the latest security features to phase out known vulnerabilities in cellular networks.**

***Index Terms*—cellular networks, radio access network, privacy**

I. Introduction

Cellular networks have become an irreplaceable part of modern infrastructure, facilitating communications for millions of devices in various application areas. Over the multiple generational upgrades of cellular networks, a wide range of vulnerabilities and attacks that threaten the security and privacy of users have been discovered. Continuous research efforts have proposed mitigation strategies to these vulnerabilities, which many, in turn, have been added as new security requirements in protocol specifications. However, previous measurement studies on 5G security deployment rates [5], [6] have shown that extent to which these mechanisms have been consistently implemented and deployed in commercial networks remains uncertain.

One such example is the unsafe methods used to randomly reassign temporary user identifiers, making them predictable. Temporary identifiers are a core component of cellular network security, playing a critical role in protecting user privacy and location confidentiality. Among them, the Globally Unique Temporary Identifier (GUTI) is used in place of permanent identifiers, to prevent traceability across different communication sessions. In practice, however, the effectiveness of this mechanism critically depends on the frequency and unpredictability of GUTI reallocation. Prior work [2], particularly in the context of LTE networks, has demonstrated that commercial networks often perform GUTI reassignment in a infrequent or predictable manner that can expose users to long-term tracking attacks, undermining the intended privacy guarantees of the system.

To address this issue, Fifth-generation (5G) networks have introduced security requirements in identity protection and mobility procedures [1], including more robust mechanisms for GUTI allocation and reallocation.

In this work, we revisit the GUTI reallocation procedure in the context of a commercial 5G network to assess whether the vulnerabilities previously documented in LTE deployments persist today. Through passive measurements of GUTI assignment behavior in two South Korean commercial carriers, we evaluate the frequency and randomness of reallocation events across real user sessions.

Our findings reveal that, despite the protocol-level advances introduced by 5G, the operational practices of measured commercial networks remain largely unchanged. In particular, we observe that GUTIs are still reallocated infrequently and with high predictability, similar to when it was first discovered nearly a decade ago.

This study underscores the continuing gap between the security capabilities of modern cellular standards and their deployment. We raise awareness of these issues and highlight the importance of adopting best practices in security configuration and deployment. Our findings serve as a call to action for operators and standards bodies to accelerate the retirement of legacy behaviors that continue to put users at risk.

II. Background

The Globally Unique Temporary Identity (GUTI) in cellular networks is a temporary identifier allocated to UEs connected to the network [2]. The GUTI is a combination of the Globally Unique AMF Identifier (GUAMI), and the Temporary Mobile Subscriber Identity (TMSI). The TMSI is a 32-bit temporary identifier for the UE, which is used to minimize the use of permanent identifiers like International Mobile Subscriber Identity (IMSI) in control messages.

By design, the TMSI is meant to be short-lived identifiers that is periodically refreshed through the GUTI reallocation procedure, to prevent correlating the TMSI to specific UEs. Knowing the target UE's TMSI value is a common prerequisite to many known attacks in the cellular network, with location tracking attacks being a prominent example. Location tracking attacks [3], [4] are a thoroughly studied class of exploits that utilizes vulnerabilities in the paging mechanisms of cellular

networks to identify whether a target is present within a monitored area. These attacks typically involve inducing paging messages directed toward the victim, through voice calls or silent text messages, leveraging the TMSI contained in the corresponding paging message generated by the RAN to infer location-related information. Typically, these attacks would require the attacker to re-obtain the victim's TMSI every time the GUTI reallocation procedure is initiated by the network, greatly increasing the difficulty of the attack if done frequently.

However, in LTE networks, weaknesses discovered in GUTI reallocation procedures have significantly increased the effectiveness of such location tracking attacks. Hong et al. [2] have highlighted two major flaws: firstly, the TMSI values are rarely refreshed, leaving extended windows for attackers to exploit. Secondly, even when refreshed, the updated TMSI values often exhibit predictable patterns, such as fixed bytes in specific positions, undermining their intended randomness and security. Capitalizing on this vulnerability, the smart tracking attack was proposed to continuously track targets without needing to re-obtain TMSI values.

To address these vulnerabilities, 5G standards have introduced stricter requirements for TMSI management [1]. In particular, the specification mandates reallocation to triggered following messages revealing TMSI in plaintext such as paging messages and recommends the use of unpredictable identifier values.

III. Methodology

Two COTS UE devices, each with a SIM card registered to a different South Korean cellular carrier, are used to measure assigned GUTI values. We then test whether the following two security properties of the GUTI reallocation procedure are well implemented:

- **Frequent reallocation.** In principle, as GUTI values should be short-lived they need be refreshed periodically and especially after transmitting messages that contain the GUTI in plaintext over-the-air. We repeatedly invoke such GUTI-revealing messages in the UE attach and paging procedures, by detaching/reattaching the UE and voice calling the UE respectively. We measure how many invocations of each procedure is required to trigger a GUTI reallocation.
- **Random value assignment.** We repeatedly invoke GUTI reallocation by moving the UE across multiple tracking areas (spanning 150 km) to trigger tracking area updates, which induces GUTI reallocations. We collect the GUTI values assigned by the network throughout this process and analyze for any repeated bytes or correlation between them.

IV. Results

- **Reallocation frequency.** For each carrier, the UE attach procedure and the paging procedure were repeated 30 times and 10 times, respectively. As shown in Table I, while the GUTI was reallocated after every UE attach procedure in carrier A, no reallocation occurred throughout the measurements for paging in carrier A and for UE attach and paging in carrier B, violating the 5G security requirements.

TABLE I
Procedure invocation count per GUTI reallocation.

	Carrier A	Carrier B
UE Attach	> 30	1

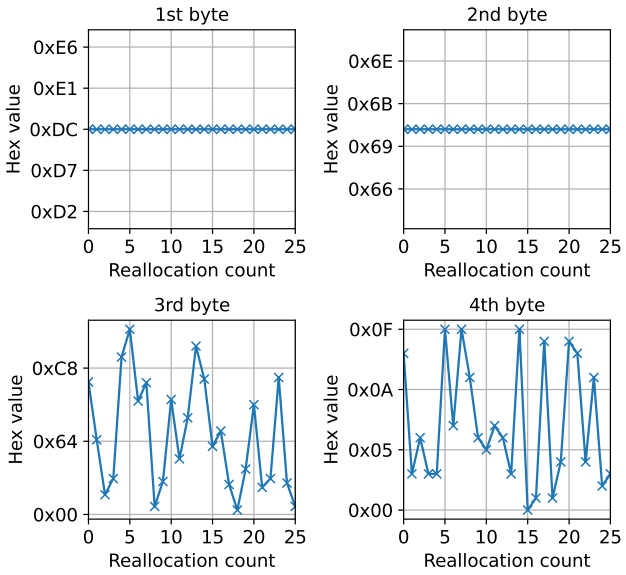

Fig. 1. The value of each of the four bytes in the M-TMSI across multiple reallocations in carrier A.

- **Randomness.** Figure 1 plots the value of each byte of the last 4 volatile bytes of GUTI (also known as M-TMSI), across 27 reallocation instances for carrier A. Although the last two bytes of the M-TMSI is updated in an unpredictable manner after each reallocation, the first two bytes remained constant throughout the measurement. Carrier B also exhibited an identical pattern of updating only the last two bytes while keeping the first two bytes fixed. This behavior is similar to the initial discovery of flaws in the reallocation of GUTI by Hong et al. [2].

V. Conclusion

Despite continuous research efforts to discover new cellular vulnerabilities and design security enhancements, there is still a considerable gap between security requirements in specifications and real-world deployments. By revisiting a near-decade-old vulnerability to show that it still persists in commercial deployments, we hope to bring this gap to the attention of the community, fostering discussion for the swift deployment of security requirements in commercial networks.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2024-00444170, Research and international collaboration on trust model-based intelligent incident response technologies in 6G open network environment)

REFERENCES

[1] 3GPP, "TS 33.501 v17.5.0: 5G; Security Architecture and Procedures for 5G System," 2022.

[2] B. Hong, S. Bae, and Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," in *NDSS*, 2018.

[3] R. P. Jover, "Lte security, protocol exploits and location tracking experimentation with low-cost software radio," *arXiv preprint arXiv:1607.05171*, 2016.

[4] M. Kotuliak, S. Erni, P. Leu, M. Röschlin, and S. Čapkun, "{LTrack}: Stealthy tracking of mobile phones in {LTE}," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1291–1306.

[5] O. Lasierra, G. Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez, "European 5G Security in the Wild: Reality versus Expectations," in *ACM WiSec*, 2023.

[6] S. Nie, Y. Zhang, T. Wan, H. Duan, and S. Li, "Measuring the Deployment of 5G Security Enhancement," in *ACM WiSec*, 2022.