Procedure Collision Testing for 5G SA Network*

Yeongbin Hwang
KAIST
Daejeon, South Korea
kyh3565800@kaist.ac.kr

Mincheol Son
KAIST
Daejeon, South Korea
mcson@kaist.ac.kr

Yongdae Kim
KAIST
Daejeon, South Korea
yongdaek@kaist.ac.kr

Abstract

The service area of the 5G SA network is increasingly expanding. However, since it is still in its infancy, the network technology is continually being tested and updated. Considering the instances in which several vulnerabilities existed in prior cellular networks, security testing for 5G networks is also important. For this, we propose to analyze the security of the 5G network by implementing a testing framework that can automatically execute attack scenarios that could cause procedure collisions in various states. We configured the security-related field for impersonating a victim UE and systematically created test cases so that the test could cover the comprehensive fields and scenarios. Our testing framework sent test cases to the target network and classified problematic behaviors using the UE side log. Using the framework, we tested 2 networks (one commercial network and one open-source network) and found 8 implementation flaws, which can cause DoS attacks.

Keywords: 5G StandAlone, NAS Protocol, Procedure Collision

1 Introduction

The 5G Standalone (SA) services are being commercialized and are used by many telecommunication companies, including T-Mobile and KT. However, there has been little research conducted yet, and there are difficulties in testing the network due to the lack of commercial equipment or open-source projects. Furthermore, previous works are challenging to apply because the core network in 5G SA differs from the existing 5G non-standalone (NSA) and long-term evolution (LTE) networks.

Previous research[1, 2, 3, 4] has discovered that an attacker with the same identity (e.g. IMSI, TMSI) as a victim UE might induce **procedure collision**, resulting in a failure to appropriately handle security contexts between the two UEs in the network and that these flaws cause DoS attacks. However, these studies only tested one state of networks without considering the various states of the network or only focused on procedures that contained certain keywords, such as abort.

Motivated by this fact, we propose to analyze the security of the 5G network by implementing a stateful testing framework focused on procedure collision in the NAS protocol. Unlike previous works, we test a large number of procedure collisions in various states that can occur during communication between a 5G core network and a legitimate UE. Using the framework, we tested 2 networks (one commercial network[5] and one open source network[6]) and found 8 implementation flaws, which can cause DoS attack.

The 6th International Symposium on Mobile Internet Security (MobiSec'22), December 15-17, 2022, 2021, Jeju Island, Republic of Korea (eds.): Article No. 6343, volume 1, issue: 1, pp. 1-8

*This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government [Ministry of Science and Information & Communication Technology (MSIT)]. (No.2019-0-00793, Intelligent 5G Core Network Abnormal Attack Detection & Countermeasure Technology Development)

2 Background

2.1 5G Network Architecture

Figure 1 shows an overview of the 5G network, which consists of User Equipment (UE), the 5G Radio Access Network (5G-RAN), and the 5G Core Network (5G-CN).

UE can use services such as phone calls and the Internet by connecting to the gNodeB (gNB) as a mobile device. The UE can authenticate and uniquely identify with the core network using the identity and key in the Universal Subscriber Identity Module (USIM) that exists in the UE.

5G-RAN consists of a UE and a 5G base station that is gNB that establishes a radio connection before interacting with the UE and the core network. gNB communicates with a 5G core network and delivers control plane and user plane messages between the UE and the core network.

5G-CN is built on a service-based architecture that differs from the architecture used in current 4G LTE networks. The core network has the Access and Mobility Management Function (AMF) that manages mobility such as registration and handover. When AMF receives a `Registration Request` message, the Authentication Server Function (AUSF) initiates the authentication procedure with UE. Unified Data Management (UDM), which serves as the HSS in LTE, decrypts SUCI and generates an authentication vector for use in the authentication procedure. This paper focuses on the control plane, which manages authentication and mobility of UE, rather than the user plane.

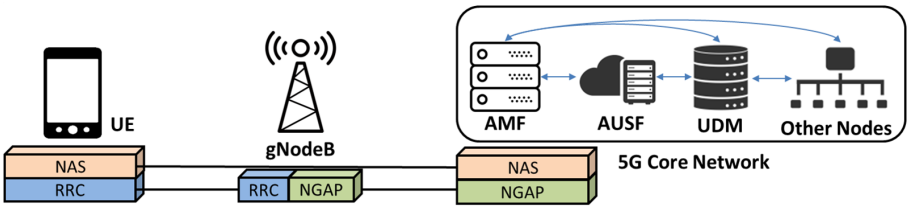


Figure 1: 5G Network Architecture

2.2 NAS Layer Procedures

Non-Access Stratum (NAS) is the highest layer protocol used for communication between the UE and the core network. The main function of the protocol is to support the UE mobility management and session management to enable IP connection support.

Registration procedure. Registration procedure is similar to the attach procedure in LTE and is used when the UE accesses the core network in Figure 2. The UE connects to the gNB via radio first, then communicates to an AMF. The procedure for the UE to connect to the radio with the gNB is performed through the `RRCSetup-SetupRequest` message. A registration procedure is then conducted between the AMF and the UE through a `Registration Request` containing the user's identity. This identity value is usually Subscription Concealed Identifier (SUCI) if there is no security context, and Globally Unique Temporary Identifier (GUTI) if there is security context. This procedure occurs through various 5G Mobility Management (5GMM) processes such as authentication and security mode procedures. In the case of authentication, the `Authentication Request-Response` message consisting of mutual authentication between AMF and UE is exchanged and a NAS partial security context is generated. After that, the algorithm used for ciphering and integrity protection is selected by exchanging the `Security Mode Command-Complete` message, and the NAS full security context is obtained. The AMF now sends a `Registration Accept` message to the UE. The registration procedure is then completed when the UE responds `Registration Complete` message.

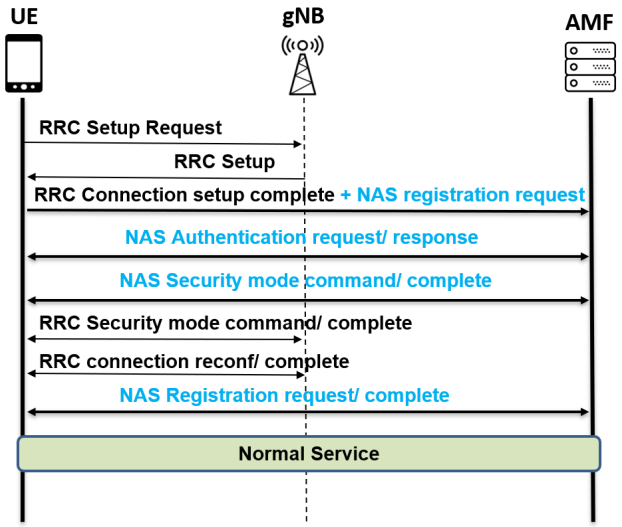


Figure 2: Registration Procedure

Deregistration procedure. Deregistration procedure is used when the UE wants to end the connection with the network (UE originating) or the network tries to disconnect the UE from the network (UE terminated). When the UE initiates, it sends a `Deregistration Request` to the AMF, which the AMF responds with a `Deregistration Accept` and disconnects from the UE.

Service procedure. Service procedure is triggered if the UE receives a paging message from the network (network triggered) or if uplink data is pending in the UE's idle state (UE triggered). The UE starts the process by sending a `Service Request` to the AMF. The process is completed when AMF responds with a `Service Accept`.

3 Related Work

Procedure collision. A procedure collision refers to a situation in which an attacker with the same identity as a victim UE sends a message impersonating a victim and a collision between the contexts of the two UEs occurs on the network. In a recent study[3, 4], an attacker established a Radio Resource Control (RRC) connection using a Temporary Mobile Subscriber Identity (TMSI) of a victim and sent an invalid NAS message to disconnect the victim UE.

Stateful testing. Chen *et al.*[1] proposed a new framework that applies NLP to analyze the 3GPP specifications. Vulnerabilities have been reported in identity spoofing, which proceeds to another session during the control plane procedure in LTE. It aborted the victim's message and triggered the DoS on the victim. In addition, Merlin *et al.*[7] presented active automata learning for LTE protocol state machines. They send an invalid message during the control plane procedure and create a reachable state machine through the invalid path. Consequently, a logical flaw was found that causes a crash and accepts an unauthenticated message. However, these studies only tested specific messages that contain specific keywords like abort or required strong assumptions that modify the messages between victim UE and networks. In 5G, it is more difficult to modify the message in the MitM situation than in LTE because the UE should replay the NAS messages in authenticated messages such as `Security Mode Complete`. Therefore, in this work, we conducted a more comprehensive test, including many states of the network and message fields in the NAS protocol.

5G. In other studys[8, 9], security problems that may arise from the emerging network slices were analyzed and solutions were presented.

4 Methodology

4.1 Attack Model

For our framework, we assume an attacker knows the victim's identity (e.g. SUCI, TMSI) and can send a NAS message as a fake UE using the identity. However, she does not have a cryptographic key, so she cannot create valid messages that should be integrity protected or ciphered.

4.2 State Machine Extraction

State machines in each network are needed because we test all possible collisions that can occur in the registration procedure of legitimate UE in the network. However, we cannot accurately grasp the internal state of the network; we have to infer the state using other information. The information used here is the network's response to the outgoing message. When we send a `Registration Request`, several NAS messages, including `Identity Request` and `Authentication Request`, can be a response message. We use these response messages to create the state machine of the network. Thus, while the legitimate UE goes through the registration procedure, the Pcap log is collected from the UE side. Based on this, we create the state machine of the network in Figure 3. As a result of state machine extraction in Open5GS[6] and Amarisoft[5], we were able to obtain the same state machine by receiving the same response message.

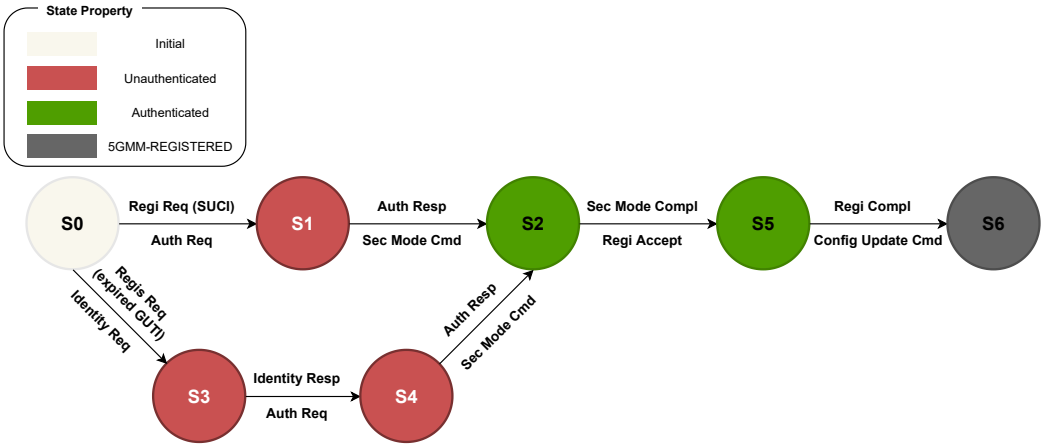


Figure 3: Amarisoft classic state machine

4.3 Test Message Generation

We carried out an experiment focusing on the NAS protocol for network testing. There are some reasons why we conducted experiments focused on the NAS protocol among the RRC and NAS protocols. First, the NAS protocol is a protocol that directly communicates with the core network and manages the mobility and session management of a User. Therefore, many vulnerabilities that have occurred exist in the NAS protocol. Second, there is no implementation of the 5G SA open source in other protocols. Unlike srsRAN[10] and openLTE[11], which are used in LTE, open source is not yet adequately implemented

Table 1: Target messages

Message	Field
Registration Request	security header type, ngKSI, MAC, registration type, 5GS mobile identity
Deregistration Request	security header type, ngKSI, MAC, deregistration type, 5GS mobile identity
Service Request	security header type, ngKSI, MAC, service type, 5GS mobile identity

in 5G SA. Therefore, the other layers could not be tested, and only the NAS, which is a protocol used directly between the UE and the core network, was tested.

Based on the state machine mentioned above, we have selected a message that can be sent in each state and a field that allows procedure collisions to occur in each state.

- **Message selection.** In order to cause a procedure collision, the network must recognize that the victim UE is the same UE as the attacker UE. Therefore, a message that has a field containing mobile identity and can be initialized by the UE was selected. There are three messages: `Registration Request`, `Deregistration Request`, and `Service Request`.
- **Field selection.** There are various fields in the NAS message. Even in the case of a `Registration Request` message, there are 39 fields including optional things. Since it is impossible to test all of the fields, mandatory and security-related fields were selected. These fields can be viewed in Table 1.

A fixed value is required in some fields because the attacker must send a message as if it were a victim during the test. As for Figure 3, since there are many states before 5GMM-REGISTERED, other identities, such as TMSI, cannot obtain the identity of the victim, so the SUCI value was used in the 5GS mobile identity field. The ngKSI field was also set to be the same as the value of the victim. The test was conducted by setting these fixed fields and changing the remaining fields.

4.4 Network Testing

We implemented UE and gNB entities via Open5GCore[12] to send NAS messages directly from the UE to the core network, which we connected to the core network to send NAS messages over NGAP protocol, as shown in Figure 4. For each test case, when the target state was reached in the network, a message was sent through the attacker UE, and each result was logged. This framework consists of a message generator and UE-gNB tester for automating the stateful test. The test message generator is made in Python, and the UE-gNB tester is made in C++ and C based on Open5GCore.

Using this framework, we conducted all generated tests based on the state machine in two 5G core networks (Open5GS and Amarisoft).

4.5 Post Analysis

We need to determine whether the behavior of the network is appropriate by looking at the response and state of the test messages. We made the following scenarios and determined that it was wrong behavior if it was violated.

- **If network returns the normal response,** This is normal behavior. This means that the session of the victim UE was not affected by the message sent by the attacker.
- **If network ignores the message of the victim UE after attacker sends the message,** This is an implementation flaw. In this case, since the context of the victim UE was affected by the attacker,

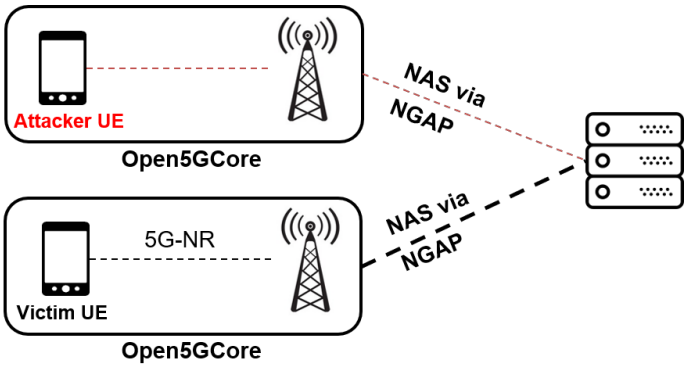


Figure 4: Test setup

Table 2: Result overview

state	Amarisoft classic			Open5GS			studied (LTE, 5G)		
	m_1	m_2	m_3	m_1	m_2	m_3	m_1	m_2	m_3
S1	●	-	○	●	○	○	-	-	-
S2	○	-	○	●*	○	○	[1]	[1]	-
S3	○	-	○	○	○	○	[1]	[1]	-
S4	●	-	○	●	○	○	-	-	-
S5	○	-	○	●*	○	○	[1]	[1]	-
S6 (5GMM-REGISTERED)	○	-	○	●*	○	○	[3, 4]	[3, 4]	[4]

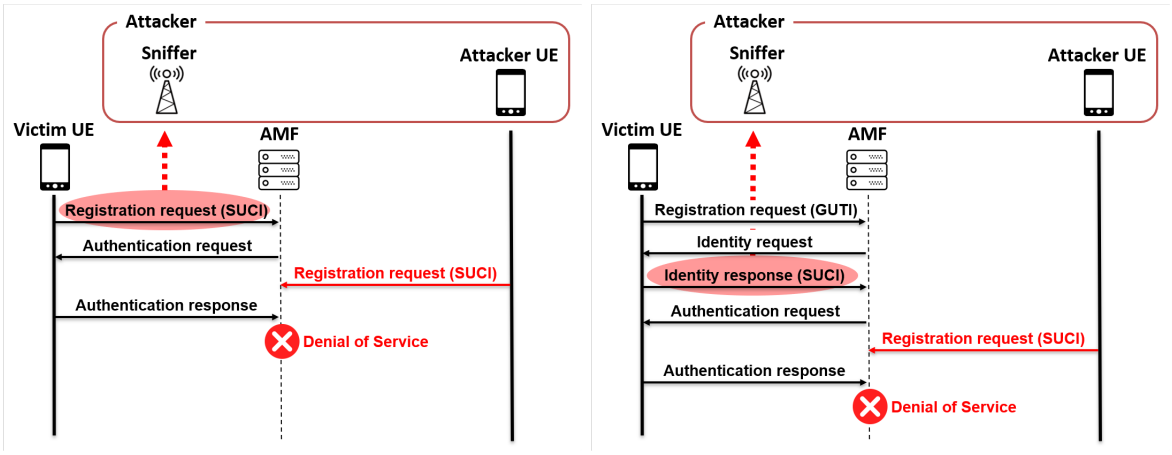
m_1: registration request, m_2: deregistration request, m_3: service request
● Implementation flaw, ○ No, − do not support
(*) Additional DoS attack

the context is deleted from the network and ignored even if a message comes later. Even if the attacker has the same identity as the victim, she does not have any cryptographic keys in a normal network. This means that the procedure can not move forward and should not affect other sessions.

- **If receive the reject message in the victim UE,** This is also an implementation flaw. In this case, it can be regarded as the security context of the two UEs cannot be properly distinguished in the network. The network does not identify the message sent by the attacker, so it makes the network send a reject message to the victim UE.

5 Result

In this work, we tested the core network of one commercial equipment (Amarisoft classic) and one open source (Open5GS). We tested 2904 cases for each network by changing the fields of three messages and states in Table 1 using our testing framework. It covers various states and messages compared to previous studies. The test results indicate that procedure collisions occur in two states out of a total of six states in Amarisoft and five states out of a total of six states in Open5GS. In addition, we found 8 implementation flaws that cause this procedure collision. In all marked states shown in Table 2, there is an implementation flaw that causes the victim UE to disconnect by sending a reject message or ignoring the message, and in the case of authenticated states (S2, S5, S6) in Open5GS, there is another implementation flaw that results in additional DoS attacks by sending a rejected message in the network even if the victim attempts to register again.



(a) DoS attack in state 1 (b) DoS attack in state 4

Figure 5: DoS attack scenarios in two states

5.1 Attack Scenarios

Cellular networks with implementation flaws are easily exposed to DoS attacks. Figure 5 shows examples of DoS attacks in S1 and S4. To conduct the attack, the attacker has a sniffer that can eavesdrop on radio communications between a victim UE and the cellular networks, and the malicious UE can send any NAS messages she wants using a fake UE. In states 1 and 4, the attacker can obtain a victim's SUCI by sniffing a `Registration Request` or `Identity Response` message. After that, if the attacker sends a `Registration Request` message using the victim's SUCI, the AMF ignores the victim's `Authentication Response` message. Consequently, the victim UE cannot access the cellular networks. Even if the victim UE attempts to access again, the attacker may repeatedly perform the attack procedure to cause persistent DoS.

6 Countermeasure

The root cause of the above attack is to cut off existing sessions by checking only the identity value without guaranteeing authenticity for the user. The attacker cannot proceed with the procedure after sending the first message because she does not have any cryptographic keys. Therefore, an existing session should be terminated by recognizing it as a legitimate UE only in receiving authenticated messages such as `authentication response` in the network. In other words, the network should maintain all sessions binding to the same identity until it is validated that the added session is a session of legitimate UE that have a valid cryptographic key. Then, it is possible to prevent an existing connection from being terminated by a fake UE.

7 Conclusion and Future Work

In spite of many existing studies, there are still undiscovered vulnerabilities due to the lack of research on 5G SA network testing. Therefore, in this work, uplink stateful testing based on procedure collision was performed to resolve this limitation, and for this, we implemented a testing framework for automating a test by changing the state of the network. As a result, we found 8 implementation flaws in the 2 networks (one commercial network and one open-source network). Currently, only NAS messages that contain SUCI as 5GS mobile identity are tested because there is no UE-gNB simulator that is fully implemented.

Since the identity value of the user varies depending on each state, the extension of message fields to include some identities remains a future work.

References

[1] Y. Chen, Y. Yao, X. Wang, D. Xu, C. Yue, X. Liu, K. Chen, H. Tang, and B. Liu. Bookworm game: Automatic discovery of lte vulnerabilities through documentation analysis. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1197–1214. IEEE, 2021.

[2] S.R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino. Lteinspector: A systematic approach for adversarial testing of 4g lte. In *Network and Distributed Systems Security (NDSS) Symposium 2018*, 2018.

[3] S. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino. 5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 669–684, 2019.

[4] H. Kim, J. Lee, E. Lee, and Y. Kim. Touching the untouchables: Dynamic security analysis of the lte control plane. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1153–1168. IEEE, 2019.

[5] AMARI Callbox Series. `https://www.amarisoft.com/products/test-measurements/amari-lte-callbox`.

[6] open5GS. `https://github.com/open5gs`.

[7] M. Chlosta, D. Rupprecht, and T. Holz. On the challenges of automata reconstruction in lte networks. 2021.

[8] B. Bordel, A. B. Orúe, R. Alcarria, and D. Sánchez-De-Rivera. An intra-slice security solution for emerging 5g networks based on pseudo-random number generators. *IEEE Access*, 6:16149–16164, 2018.

[9] B. Bordel, R. Alcarria, J. Chung, R. Kettimuthu, T. Robles, and I. Armuelles. Towards fully secure 5g ultra-low latency communications: A cost-security functions analysis. *Computers, Materials & Continua*, 74(1):855–880, 2023.

[10] srsRAN. `https://github.com/srsran/srsRAN`.

[11] openLTE. `http://openlte.sourceforge.net/`.

[12] open5Gcore. `https://www.open5gcore.org`.