Individual Research Project Final Report

Research Participation Project

이동통신 네트워크 장비 프로토콜 상태 기계 추출 기반의 표준 위배 동작 검출

Detecting standard violations in the commercial cellular network based on state machine extraction

Department electrical engineering (20160718)

Contents

Abstract

4G LTE (Long-Term Evolution) and 5G are the latest technologies currently in use by mobile communication. Since many people use it, telecommunication companies and manufacturers also consider personal security and privacy in many ways. In addition, because the mobile communication environment is a black box environment in which implementation is closed, the operation of the commercial network is unknown and it was difficult to find vulnerabilities.

In this work, we conducted a systematic security analysis to discover the state of various protocols that were not found in existing LTE networks and verify their behavior when sending unacceptable messages from those states. In more detail, first, the request and its response were recorded while various LTE NAS messages send and the state machine of commercial network equipment was extracted. Second, the differences are identified through comparative analysis between state machines of several commercial network equipment. Third, we found abnormal behavior by comparing it to standard documents. We have also found that the state machine is created differently for each carrier and that the contents covered in standard documents are implemented differently among carriers. Finally, we found a total of 7 abnormal behaviors in 3 carriers. These abnormal behaviors do not immediately lead to security vulnerabilities, but if it is combined to other protocols' abnormal behaviors, it may result in vulnerabilities.

1. Research Purpose

With the recent emergence of 5G technologies, mobile communication technology is expected to contribute significantly to the growth of the industry. However, LTE is still dominant in the mobile communication. LTE subscribers are accounted for 77% of the overall users in South Korea while 5G subscribers are accounted for 13% [2]. Moreover, LTE is also closely related to social safety, such as being used for railway networks (LTE-R: LTE-Railway) and public safety networks (PS-LTE: Public Safety LTE). Therefore, it is essential to enhance mobile communication security, especially LTE security.

Unlike the pace at which technology is evolving, security technology has not been developed as much. Unlike general protocols such as TCP, new technologies are introduced every 10 years. Unsurprisingly, various vulnerabilities come with new technologies as they become commercially available. Each manufacturer will implement the protocol based on the standard documents presented by the standard organization 3GPP. However, these documents are written in natural language, making it difficult to prove mathematically safe and there are cases where detailed implementation methods are not provided, so the implementation varies by manufacturer. In addition, depending on the policies and configuration of the carriers, same standard procedures of the same manufacturer's equipment can behave differently. As a result, the implementation of network equipment depends on the carrier and manufacturer combination. Furthermore, such different implementation mistakes by manufacturers and misconfigurations by carriers create different security threats.

LTE security threats are divided into threats on the control plane and the data plane. In order to use services on the data plane such as voice call or data use, control plane procedures that is in charge of network connectivity and mobility management must be preceded. In other words, the vulnerability on the control plane can lead to serious threats such as Denial-of-Service of users or location tracking. In addition, most LTE security measures are operated on the control plane. Therefore, it is necessary to verify whether the control plane procedure of commercial equipment is properly implemented.

There have been many efforts to find security threats in LTE control plane but most studies have targeted to find vulnerabilities in LTE cellphone. There have been studies discovering for network vulnerability only recently, but they have the following limitations: 1) Impossible to detect implementation vulnerabilities by analyzing only standard behaviors [3], 2) Impossible to execute found vulnerabilities by analyzing only part of the protocol operation [4], [5], 3) Vulnerability analysis only in a limited state [1]. As aforementioned, commercial network equipment is threatened with both standard and implementation vulnerabilities. Also, since it is composed of many and complex protocols, it has various states during LTE control plane procedures.

In this work, we verified that the operation of the commercial LTE network equipment complies with the standards. To do this, we sent various LTE NAS messages with the commercial network equipment and checked the response of the network. Since it is impossible to directly debug the code of the equipment, the operation of the

equipment was verified through black-box testing, and the confirmed operation was expressed in the form of a state machine. Straightforwardly, accurate state machine extraction depends on various LTE NAS messages that are sent. In order to discover more diverse states and transitions in commercial LTE network, we tested valid messages in the standard as well as both undefined and invalid messages. This approach can find both standard vulnerabilities and implementation vulnerabilities and takes into account the tested state coverage as well.

In summary, this work aims to first validate processing at all the states that exist within the NAS protocol implementation of LTE network equipment. As a result, our contribution is as follows:

- We extract the state machine from commercial LTE network equipments by sending various NAS messages.
- We conduct comparative analysis between state machines of several commercial network equipment.
- We discover 7 abnormal behaviors through experiments with various combinations of carriers and manufacturers.

2. Research Background

2.1. LTE Network Architecture

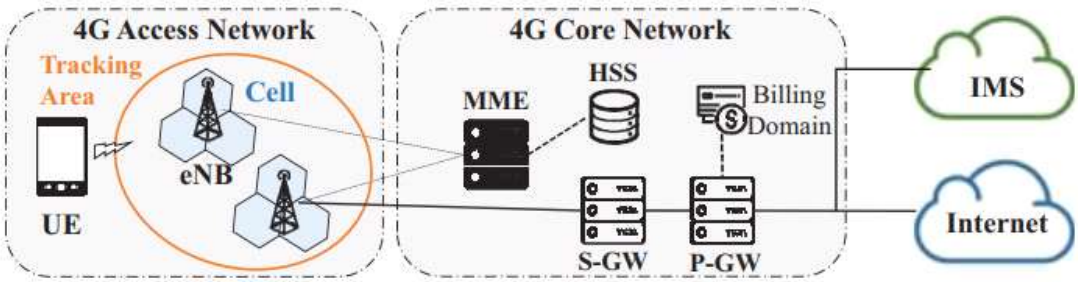

Figure 1 LTE network architecture

LTE network called EPS (Evolved Packet System) is a packet-switching based network. It consists of an E-UTRAN (Evolved Universal Terrestrial Radio Access Network) section between a mobile terminal and a base station, and an EPC (Evolved Packet Core) including all core network equipment. Among many LTE components, equipment that performs the control plane procedure is mainly described below.

2.1.1 UE (User Equipment)

A UE is a mobile device that can provide legitimate information by connecting subscription services such as data and voice calls to a base station (i.e., the devices such as typical smartphones we use are called UEs). The UE is identified by a SIM (Subscriber Identity Module) that includes a unique identifier, IMSI (International Mobile

Subscriber Identity) and a symmetric cryptographic key. The network also databases an IMSI and cryptographic key for each user, so only users with the correct IMSI and cryptographic key pair can use the network.

2.1.2 eNB (evolved Node B)

An eNB is a base station that allows the UE to establish a wireless connection to LTE. In addition, it is used to communicate with MME to perform control plane procedures, and is connected to the IP network through LTE gateways to support user plane procedures.

2.1.3 MME (Mobility Management Entity)

The MME is the core node of the LTE network, authenticating the UE and managing user mobility and sessions. The cryptographic key for UE security protection resides in the HSS (Home Subscriber Server), and the MME receives the key from HSS to authenticate the UE and perform secure communication.

2.2 LTE Control Plane Protocol

In order to receive LTE service, the UE performs LTE eNB and MME and control plane procedures, respectively, and the protocols used are RRC and NAS protocols.

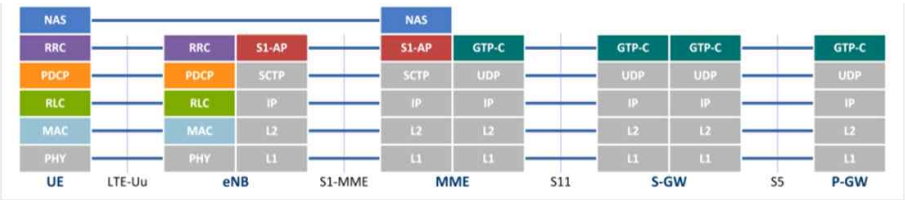

Figure 2 LTE control plane

2.2.1 RRC (Radio Resource Control)[1)]

The main function of the RRC protocol is LTE radio signaling connection control. It is responsible for managing the radio connection between the UE and the eNB. In addition, it is in charge of broadcasting core network (e.g., MME) information, delivering paging messages, managing UE context during handover. Moreover, RRC is the highest protocol layer among the wireless protocols in LTE, and is responsible for wireless communication security functionality to prevent threats such as eavesdropping and message spoofing.

2.2.2 NAS (Non-Access Stratum)

The NAS protocol is in charge of both the EMM (EPS Mobility Management) procedure for handling the registration and mobility management of the UE and the

1) According to the research proposal, RRC was also within the scope of the study, but it was difficult to analyze only NAS, so it was not covered.

ESM (EPS Session Management) procedure for managing the session and bearer. In the 3GPP standard, state and transition of EMM procedures are classified as shown in Figure 3 to express the progress of the procedure. Among them, the main states are EMM-DEREGISTERED and EMM-REGISTERED, which are divided to whether the terminal is registered or not.

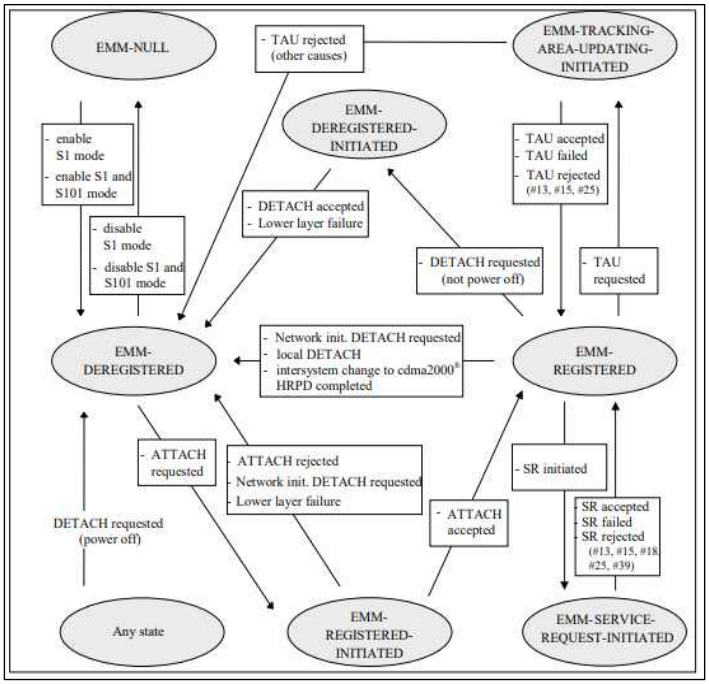

Figure 3 EMM main state in the UE

The EMM-DEREGISTERED state means a state in which no LTE service can be received because the UE is not registered in the network. That means, in order to use LTE service (e.g., voice call, SMS, and data), it must be registered in the network and be in the EMM-REGISTERED state. In order to be registered in the network, the LTE Attach procedure starting from the Attach Request, which is a NAS message, must be performed, and the UE can enter the EMM-REGISTERED state by receiving the Attach Accept message from the network.

2.3 Related Work

Our study attempted to find security threats in various protocol states that were not verified in the existing LTE network security analysis research by performing systematic security analysis on the LTE network protocol. In the most related study, Kim et al., [1] among the security threats in the implementation of network equipment, the threats that may occur in the initial state of the protocol RRC and NAS were analyzed. The network operation has been verified in the form of observing the response by sending a message that violates the security property (e.g., integrity protection, replay protection) to the network in a single shot.

Exploited NAS Messages	Implications		
	MME_1	MME_2	MME_3
Attach Request	DoS (**P**, **I**, **R**)	×	DoS (**P**, **I**, **R**)
TAU Request	DoS (**P**, **I**, **R**)	×	DoS (**I**), False location update (**R**)
Service Request	Spoofing (**R**)	×	Spoofing (**R**)
Uplink NAS Transport	DoS (**P**, **I**), SMS phishing (**R**)	SMS phishing (**P**, **I**, **R**)	-
PDN Connectivity Request	DoS (**I**)	×	DoS, DosS (**R**)
PDN Disconnect Request	DoS (**I**), DosS (**R**)	×	DosS (**R**)
Detach Request	DoS (**P**, **R**)	DoS (**P**, **I**, **R**)	DoS (**P**, **I**, **R**)

DosS: Denial of selective Service, **P:** Plain, **I:** Invalid MAC, **R:** Replay

Figure 4 exploited NAS messages in LTEFuzz[1]

Our study attempted to find security threats in various protocol states that were not verified in the existing LTE network security analysis research by performing systematic security analysis on the LTE network protocol. In the most related study, Kim et al., [1] among the security threats in the implementation of network equipment, the threats that may occur in the initial state of the protocol RRC and NAS were analyzed. The network operation has been verified in the form of observing the response by sending a message that violates the security property (e.g., integrity protection, replay protection) to the network in a single shot.

3. Approach

our systematic security analysis consists of finding various protocol states present in the network equipment to be verified and verifying message processing that is not allowed in the standard in the discovered protocol states. Unlike previous studies that verified the handling of standard violation messages in "restricted protocol state", various protocol states of the security analysis target equipment were found in a black-box testing environment and the standard violation message processing was verified.

Although the LTE standard exists, the degree of freedom to implement the functions defined in the standard is high, and there are some ambiguities as the function specification is described in natural language rather than formal language. Therefore, the state machine of LTE network equipment can appear in various forms.

In fact, many processes as shown in Table 1 are required for the transition between the NAS protocol states EMM-REGISTERED and EMM_DEREGISTERED to occur. So, we defined the network is subscribed to explore it, but other information (eg, previous connection record, location information, etc.) is not registered as the initial state and tried to search the hidden state in the network by sending various types of NAS messages.

#	direction	message type	note
1	UL(UE -> Network)	Attach request/ PDN Connectivity Request	
2	DL(Network -> UE)	Authentication Request	Performed when user's IMSI is identified
3	UL	Authentication Response	
4	DL	Identity Request	IMSI/ IMEI/ IMEISV request according to each situation
5	UL	Identity Response	
6	DL	NAS Security Mode Command	
7	UL	NAS Security Mode Complete	
8	DL	ESM Information Request	
9	UL	ESM Information Response	
10	DL	Attach Aceept/ Activate EPS bearrer context request	
11	UL	Attach	

Table 1 EMM_DEREGISTERED -> EMM-REGISTERED

In this study, the state machine will be extracted and analyzed preferentially for the "Attach" procedure that responsible for network connection/registration among mobile communication NAS and RRC protocol procedures. This is because "Attach" procedure is the first process that we execute to use LTE service and is a complex process that exchanges the most messages and contexts.

3.1. State Machine extraction tool (Fuzzer)

In order to identify the hidden state in the LTE network equipment, which is not revealed in the general situation, the number of message fields changed to include an abnormal message was increased. Also, although it is not a standard violation message, we tried to find a state that was not revealed by creating and testing message combinations defined as corner cases in the standard.

Message type	Modulated field	value
Attach Request	EPS mobile identity	Invalid GUTI, IMEI, IMSI Valid GUTI, IMEI, IMSI
	UE network capability	all algorithm available, only EEA0, EIA0 available, only EEA3, EIA3 available, Valid algorithm available
	MAC	Invalid MAC (random value), Invalid MAC (0xffff) Invalid MAC (0x0000) Valid MAC

	Attach type	emergency, combined EPS, Interpreted as EPS, EPS
	NAS key identifier	Invalid key identifier.
	Security header	plaintext, integrity, integrity and ciphered, integrity with new security context, integrity and ciphered with new security context, reserved
Identity Response - IMSI	Mobile identity	Invalid IMSI, valid IMSI
	MAC	Invalid MAC (random value), Invalid MAC (0xffff) Invalid MAC (0x0000) Valid MAC
	Security header type	Same as Attach request
Identity Response - IMEISV	Mobile identity	Invalid IMEISV, valid IMEISV
	MAC	Invalid MAC (random value), Invalid MAC (0xffff) Invalid MAC (0x0000) Valid MAC
	Security header type	Same as Attach request
Authentication Response	RES	Invalid RES, valid RES
	MAC	Invalid MAC (random value), Invalid MAC (0xffff) Invalid MAC (0x0000) Valid MAC
	Security header type	Same as Attach request
NAS Security Mode Complete	MAC	Invalid MAC (random value), Invalid MAC (0xffff) Invalid MAC (0x0000) Valid MAC
	Security header type	integrity and ciphered, integrity with new security context, integrity and ciphered with new security context, reserved
	IEMISV value	Invalid IMEISV, IMEI, IMSI valid IMEISV, IMEI, IMSI

Table 2 Field values used to extract the model

Table 2 shows the field values for each message that we used to extract the model. All of the contents of Table 2 were modulated using the state machine extraction tool and the test was conducted.

The NAS protocol state machine extraction tool tests a much larger number of messages to achieve the goal, and extracts the state machine of the LTE network equipment of the three companies (A, B, C) based on the responses.

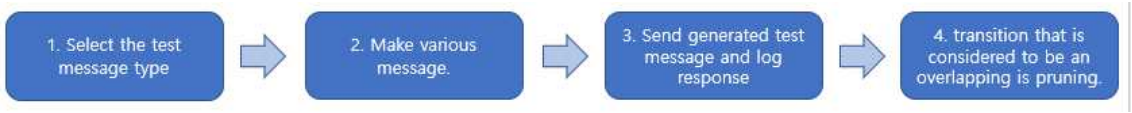

Figure 5 Protocol state machine extraction process

Protocol state machine extraction is performed in the order of Figure 5. Only task 4 is performed manually, and the remaining tasks 1, 2, and 3 are performed by a state machine extraction tool that is software. Since the 4th task which is performed manually, that is performed through the State Machine Analysis Tool, which will be described later, it will be described in detail in the result analysis tool description, and the 1st, 2nd, and 3rd tasks will be described in detail.

Task 1 is set manually as a NAS Attach Request only when no model has been extracted. Otherwise, it is automatically determined according to the network response message type. For example, when testing the NAS Attach Request message, if the network device responds with an Identity Request, it is an Identity Response.

```
Target message: ATTACH_REQUEST
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
Send: AUTHENTICATION_RESPONSE (IV, ITP, Plain, MIN, MIN)
Recv: AUTHENTICATION_REJECT (Plain)

Target message: ATTACH_REQUEST (IV, EPS, Plain, MIN, EPS, Native_valid, IMSI_valid, NULL)
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
Send: AUTHENTICATION_RESPONSE (IV, ITP, Plain, MIN, MIN)
Recv: AUTHENTICATION_REJECT (Plain)
```

Figure 6 Example of determined message type / generated message variant

Task 2 means creating all combinations (test cases) that can be changed into fields according to the message type determined in task 1. The generated test case is in the form of an input file of the protocol operation model extraction tool, and the format is shown in Figure 6 (above). As shown in Figure 6 (below), a file containing the determined message type (Target message) is read and options are added.

Task 3 receives information about the message variant (test case) in the first line of the file created in task 2 and sends the message variant. This test case is sent in the state that arrives when the network sends and receives the Send/Recv message string (message path) starting from the 3rd line of the input file from the starting state that does not have the terminal information. As shown in Figure 6, more fine-grained state machine extraction is possible because not only the message type but also options exist in the Send/Recv message sequence information. The protocol operation model extraction tool subdivided the transition (sending message) into a much more varied state (received message) based on the content in the received message.

3.2. State Machine Analysis Tool (Analyzer)

The number of input files used in the protocol state machine extraction process that is very large. For example, in the case of Attach Request, 4400 test message variants are used. In order to accurately identify the operation of the network equipment according to the transmitted messages, all 4400 responses must be checked, but it is almost impossible to handle these manually. In addition, it is necessary to prune unnecessary transmission messages (transitions) by checking the result of the transmitted test messages. If the number of transmission message is not reduced, the transmission/reception message files increase exponentially as the state machine extraction proceeds.

Therefore, it is necessary to collect the common points and differences between the transmitted messages by analyzing which response message comes when a transmission message is sent. In particular, it is necessary to select a representative message by analyzing transmission messages that cause the same response message in detail.

For the above purposes, in this study, a tool to compare sent and received messages, analyze common points and statistical characteristics was developed and research was conducted based on this.

The result analysis tool reads the output log output by the fuzzer (state machine extraction tool) to collect the transmitted/received message, and provides the result through the command-line user interface (CUI). The reason for using CUI is that you can quickly check the result flexibly regardless of the case of using ssh.

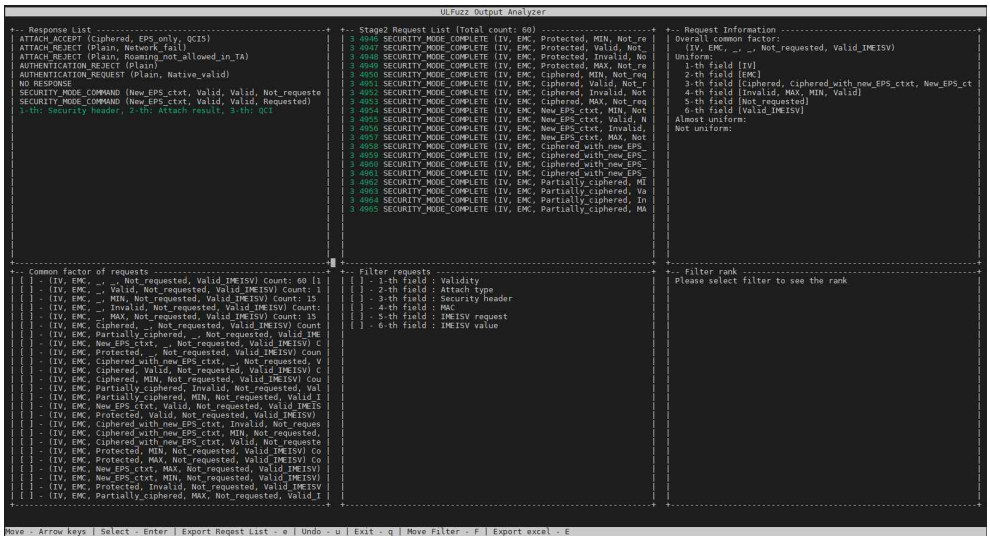

Figure 7 analysis tool

The Response List tab at the top left shows a list of received messages, and if you select one of the received messages, the list of transmitted messages that caused the received message is set in the Request List tab at the top center. So, by looking at the corresponding response, you can see which request state has changed.

4. Experimental Setup

The NAS message to be tested is transmitted through the wireless channel after establishing a wireless connection with the eNodeB like a real UE since there was no environment in which the NAS messages of the LTE network equipment (eNodeB/MME) to be tested could be exchanged by wire. To this end, the environment was built through the open source LTE software srsLTE and SDR (Software-Defined Radio) equipment USRP B210.

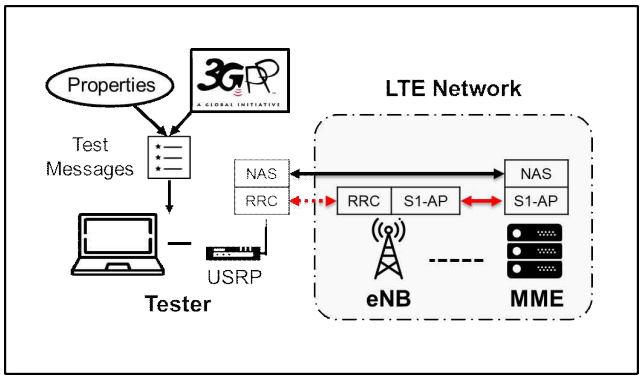

Figure 8 test environment

In testing environment, a test tool based on srsLTE is input to the USRP B210 equipment and a "test case" (ie, NAS message to be tested) is transmitted through the eNB and the wireless channel and a response is received. For the development environment, Ubuntu 16.04.6 LTS was used as the OS for smooth srsLTE and g++ 7.4.0 were used as the C++ compiler and Python version 3.5.2 and USRP 210 were used.

5. Evaluation

5.1 Operation Analysis

State machine extraction was progressed for all three carriers (A, B, C). Stage 0 is the stage where we start with an Attach Request, which means the result of analyzing the message received after sending the Attach Request. Stage 2 is the result of analyzing the results received after sending the request message that automatically generated after the stage 0 stage. Figures 9 and 10 are examples of messages at this stage.

```
Target message: AUTHENTICATION_RESPONSE
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
```

Figure 9 stage 0 message

```
Target message: ATTACH_REQUEST
Send: ATTACH_REQUEST (IV, ITP, Plain, MIN, Itp_as_EPS, Native_valid, IMSI_valid, NULL)
Recv: AUTHENTICATION_REQUEST (Plain, Native_valid)
Send: AUTHENTICATION_RESPONSE (IV, ITP, Plain, MIN, MIN)
Recv: AUTHENTICATION_REJECT (Plain)
```

Figure 10 stage 2 message

In the state machine, each transition corresponds to a message field sent from the UE to the MME and each state represents received messages. So, we want to check and compare the state change according to the message we send.

5.1.1 Carrier A

5.1.1.1 Stage 0

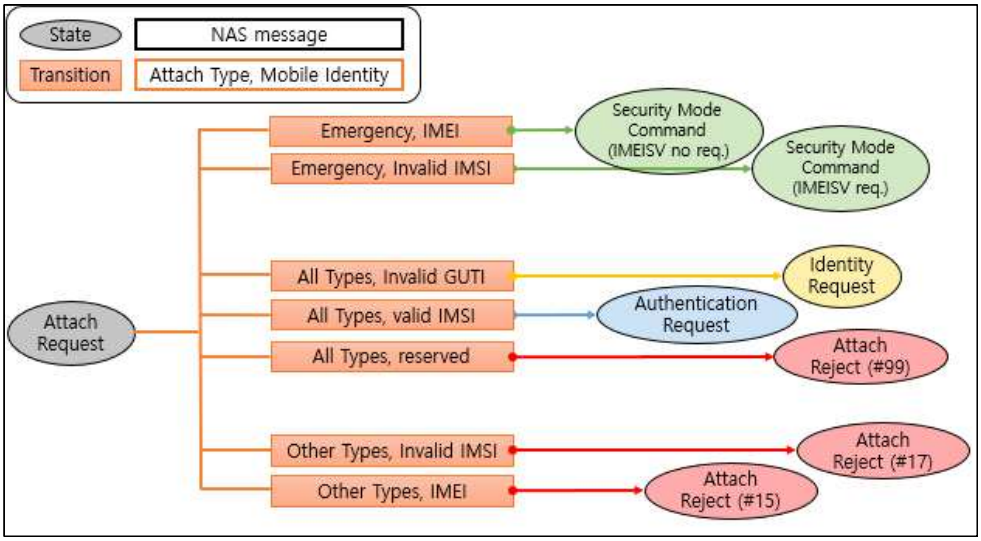

Figure 11 A stage 0

The result of security analysis for Carrier A's testbed MME is summarized using an analyzer and a part of it is expressed as a graph as shown in the figure 11. Each transition indicates which field was used when sending an Attach Request, and the state indicates the result of sending. Among them, the Attach Request state means the initial state. Both carriers B and C made state machines in the same way. As a result of the analysis, values such as security header type, UE network capability did not affect state separation and were not separately indicated. Also, the case of not receiving a response from the network is also excluded from the figure. There were 7 types of output state, and Security Mode Command is divided into two depending on whether or not IMEISV is requested, and Attach Reject is divided into 3 states according to EMM cause. EMM causes that can be observed are #15 (No suitable cells in tracking area), #17 (Network failure), and #99 (Information element non-existent or not implemented).

The facts that can be seen from the above example are as follows.

① Regardless of the attach type, an Authentication Request is responded to an Attach Request with an valid IMSI.

② Regardless of the attach type, an Identity Request is responded to an Attach Request with an Invalid GUTI.

③ Regardless of the attach type, when a reserved value is used as the mobility identity value, an Attach Reject (#99) is sent as a response.

④ When Invalid IMSI or IMEI is used as the mobility identity value, an Security Mode Command or Attach Reject message is used as a response depending on whether the attach type is emergency or not.

From the above, it can be seen that even with the same attach operation, different responses are sent depending on what the attach type and mobile identity values are used for.

5.1.1.2 Stage 2

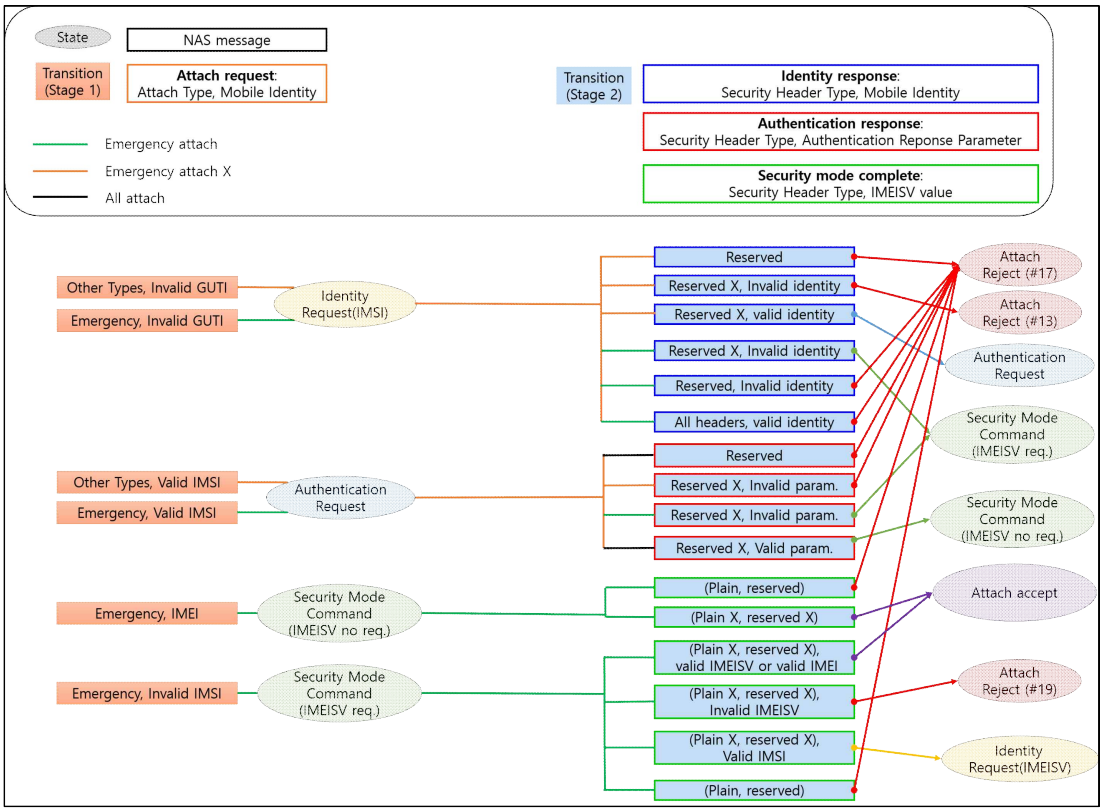

Figure 12 A stage 2

The above figure summarizes the analysis results for stage 2, largely states (oval), transitions according to the message content (orange and blue boxes), and detailed explanations of the contents included in the transition for each message type (outside the box). Stage 2 first sends an Attach Request from stage 0 as a transition according to the internal values of the message to obtain states, and analyzes the response received when various transitions are sent again based on this. In the stage2 figure, the initial state is omitted. Both carriers B and C made state machines in the same way. In stage 2, the transition is determined according to the field value used in the Identity Response, Authentication Response, and Security Mode Complete message. At this time, the MAC values of the messages as a result of the analysis were not separately indicated because they did not affect the state separation.

The reason why the previous state should be considered is that two transitions of the same state in the same message can become different states according to the transition of the previous stage 0. For example, in figure 12, in the Authentication Request state, the security header type of the Authentication Response message is set to "not

reserved", and the authentication response parameter is set as an "invalid parameter" and sent. At this time, depending on the case, you may receive an Attach Reject or a Security Mode Command message. In the former case, the transition from the previous state 0 is a case where valid IMSI is included in the attach type other than the emergency, and in the latter case, the valid IMSI is included in the emergency attach type.

In the result of Stage 2, a total of 8 types (3 Attach Reject, 1 Authentication Request, 2 Security Mode Command, 1 Attach Accept, and 1 Identity Response) messages are possible. Attach Reject is divided into 3 states according to EMM cause. EMM causes that can be observed are #13 (Roaming not allowed in this tracking area), #17 (Network Failure), and #19 (ESM failure). In the case of the Security Mode Command, it was confirmed that it was divided into two depending on whether or not the IMEISV was added.

The transition to the state and detailed explanation will be made in 5.2 Abnormal behavior analysis.

5.1.2 Carrier B

5.1.2.1 Stage 0

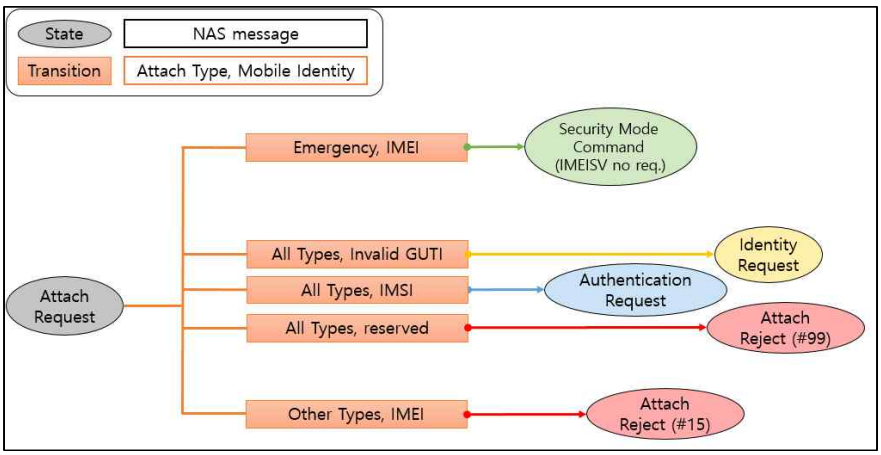

Figure 13 B stage 0

There were 5 types of output states, and in Security Mode Command, a message that does not request IMEISV is responded, and Attach Reject is divided into two states according to EMM cause. EMM causes that can be observed at this time are #15 (No suitable cells in tracking area) and #99 (Information element non-existent or not implemented).

The facts that can be seen from the above example are as follows.

① Regardless of the attach type, an Authentication Request is responded to an attach with IMSI.

② Regardless of the attach type, an Identity request is responded to an attach with an Invalid GUTI.

③ Regardless of the attach type, when a reserved value is used as the mobility identity value, an Attach Reject (#99) is sent as a response.

④ When IMEI is used as the mobility identity value, an Security Mode Command or Attach Reject message is used as a response depending on whether the attach type is emergency or not.

5.1.2.2 Stage 2

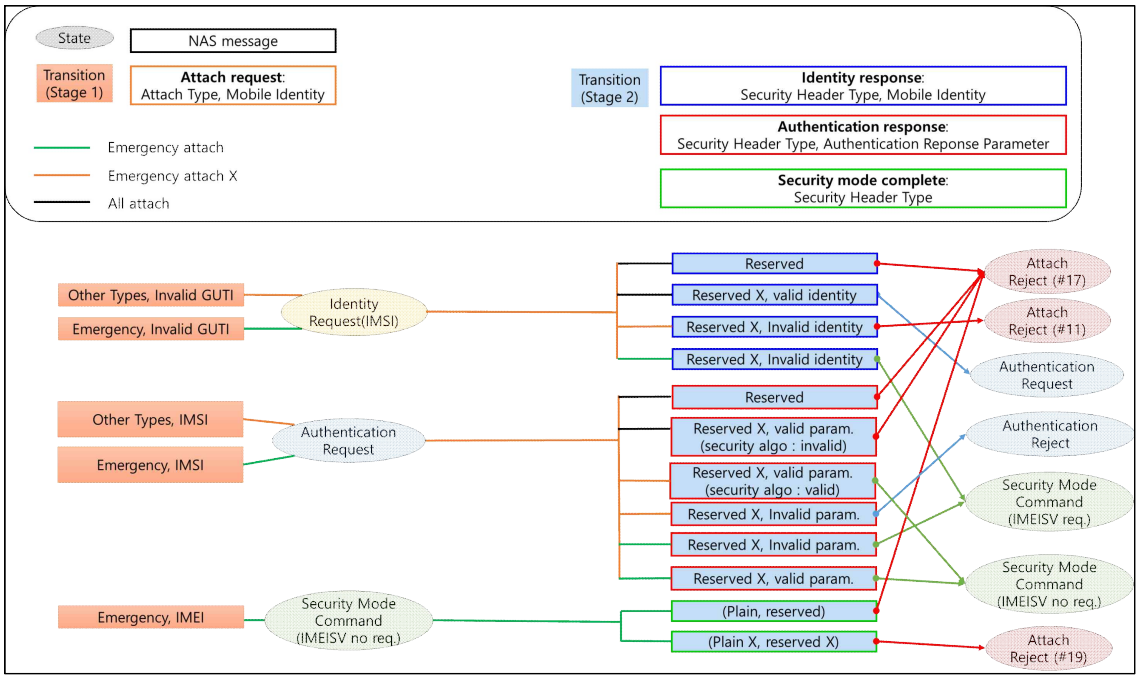

Figure 14 B stage 2

In the results of Stage 2, there are a total of 7 types (3 Attach Reject, 1 Authentication Request, 1 Authentication Reject, and 2 Security Mode Command) messages. Attach Reject is divided into 3 states according to EMM cause. EMM causes that can be observed are #11 (PLMN not allowed), #17 (Network Failure), and #19 (ESM failure). In the case of the Security Mode Command, it was confirmed that it was divided into two depending on whether or not the IMEISV was added.

The transition to the state and detailed explanation will be made in 5.2 Abnormal behavior analysis.

5.1.3 Carrier C

5.1.3.1 Stage 0

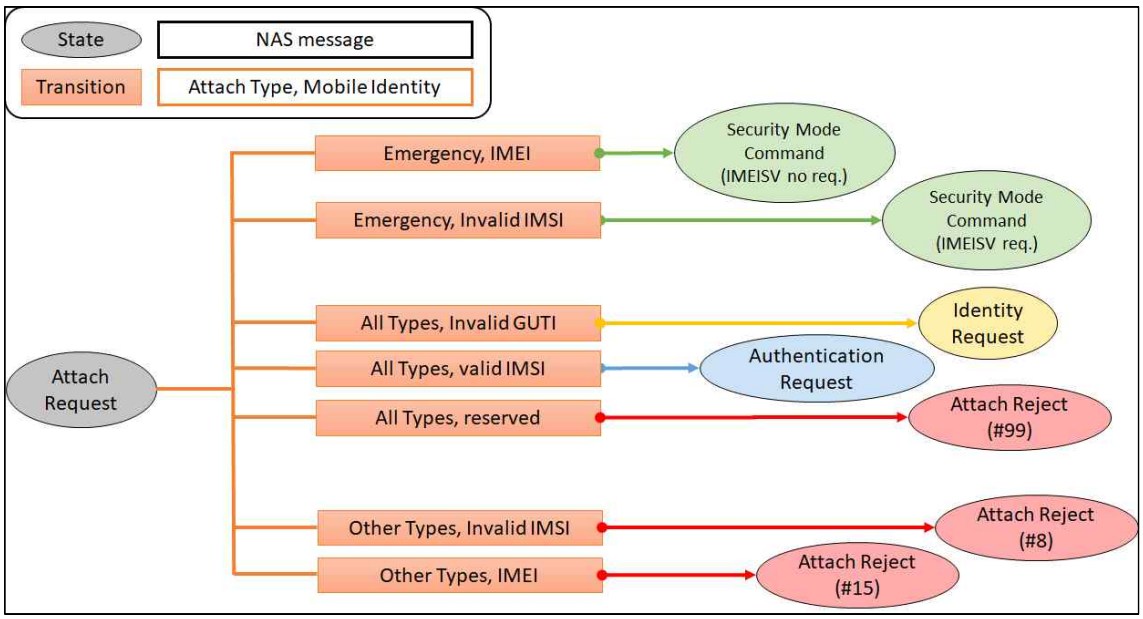

Figure 15 C stage 0

In the case of carrier C, it is the same as that of A except for the part where the attach reject cause is changed to #17 -> #8 when an invalid IMSI is sent from attach (not emergency type).

5.1.3.2 Stage 2

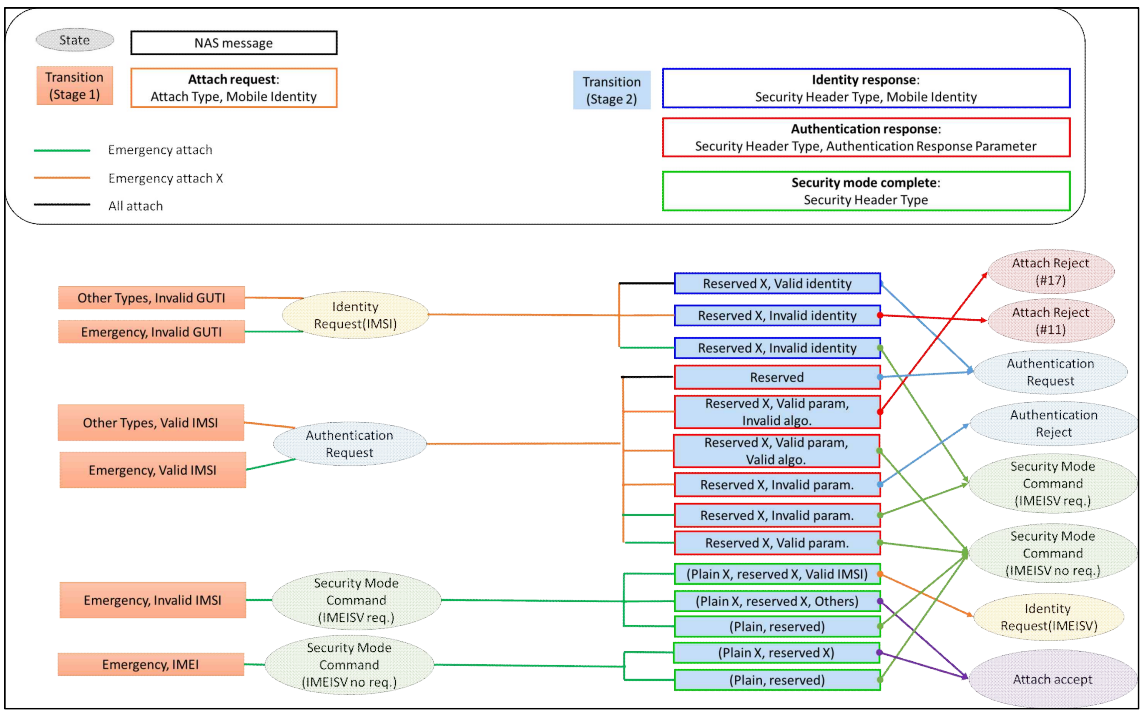

Figure 16 C stage 2

In the results of Stage 2, there are a total of 8 types (2 Attach Reject, 1 Authentication Request, 1 Authentication Reject, 2 Security Mode Command, 1 identity request, and 1 attach accept) messages. Attach Reject is divided into two states according to EMM cause. EMM causes that can be observed are #11 (PLMN not allowed) and #17 (Network Failure). In the case of the Security Mode Command, it was confirmed that it was divided into two depending on whether or not the IMEISV was added.

The transition to the state and detailed explanation will be made in 5.2 Abnormal behavior analysis.

5.2 Abnormal Behavior Analysis

According to the analysis conducted in 5.1, a state machine was created for each carrier. Using that, we will analyze whether each state works properly or if there is no abnormal behavior by comparing the results with the standard document in 3GPP.
First of all, I analyzed the contents of the standard. Figure 17 shows the attach operation described in the standard document. This does not explain all of the test cases we used. Red X indicate those not directly specified in the standard. Based on the attach process described in the standard, an analysis of the result example was conducted.

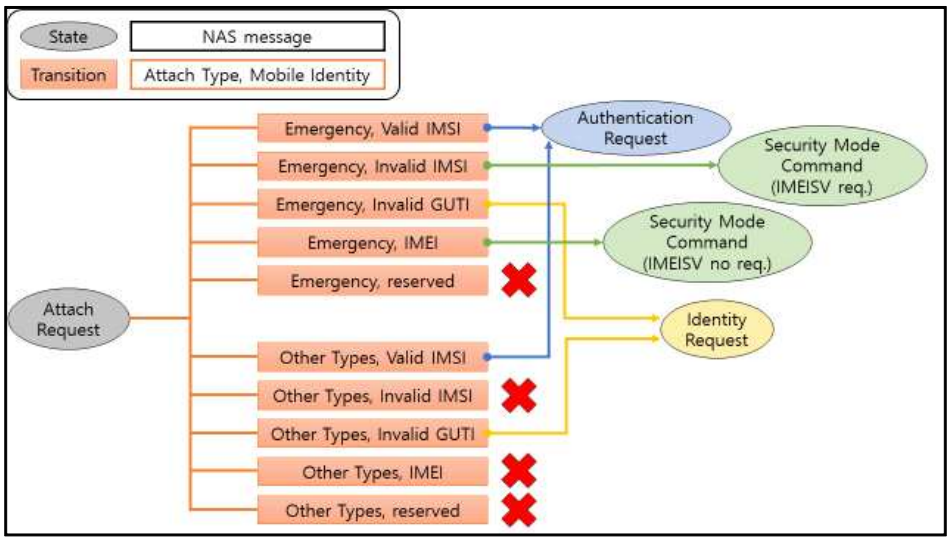

Figure 17 The stage0 case described in 3GPP TS 23.401.

The analysis with the standard is conducted according to the order analyzed in 5.1, and the standard document is processed based on Figure 17, which depicts the operation.
In the case of stage2, it is different from the state in Figure 17, and since the starting state is varied to three, this part was analyzed by comparing it with the standard document one by one.

5.2.1 Carrier A

5.2.1.1 Stage 0

① Valid IMSI

Executing the Authentication Request using valid IMSI is the same operation as specified in the standard. Therefore, it can be confirmed that it is working correctly.

② Invalid GUTI

As can be seen in the figure below, when invalid GUTI is used regardless of the attach type, the MME fails to load the UE context, so an Identity request requesting IMSI is performed.

4. If the UE is unknown in both the old MME/SGSN and new MME, the new MME sends an Identity Request to the UE to request the IMSI. The UE responds with Identity Response (IMSI).

Figure 18 Identity request case

③ Reserved mobile identity

According to 3GPP TS 24.008, Information element non-existent or not implemented is defined as shown in the figure below. This can be used when the IE does not exist or the function for the corresponding IE is not implemented. Therefore, if reserved is used as the mobility identity value, it can be regarded as 'not implemented', so sending an Attach Reject message with an "information element non-existent or not implemented" can be considered a correct operation.

H.6.4 Cause No. 99 "information element non-existent or not implemented"

This cause indicates that the equipment sending this cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Figure 19 EMM cause #99

④ When using Invalid IMSI or IMEI as the mobility identity value

First, in the case of emergency attach using IMEI, 3GPP TS 23.401 5.3.2.1 E-UTRAN Initial Attach specifies as follows. In the case of normal attach, when the MME cannot check the UE context, it sends an Identity Request to the UE, and then performs an Authentication Request and Security mode command operation. However, as shown in the figure below, only when IMEI is used as the identity for emergency attach, the Identity Request and Authentication Request process can be skipped. Likewise, when using Invalid IMSI, if the network allows emergency attach of unauthenticated IMSI, the authentication request process can be skipped.

For an Emergency Attach if the UE identifies itself with a temporary identity that is not known to the MME the MME immediately requests the IMSI from the UE. If the UE identifies itself with IMEI, the IMSI request shall be skipped.

Figure 20 Case that IMSI request can be skipped

If the MME is configured to support Emergency Attach for unauthenticated IMSIs and the UE indicated Attach Type "Emergency" the MME skips the authentication and security setup or the MME accepts that the authentication may fail and continues the attach procedure.

Figure 21 Case that Authentication can be skipped

However, in the two cases, the contents of the security mode command, that is, whether or not IMEISV is requested, appears differently, which can be found in the below document. In the case of emergency attach using IMEI as below, the process of asking the ME Identity is skipped. Therefore, it was confirmed that emergency attach using Invalid IMSI and IMEI well follows the contents of the standard document.

For an Emergency Attach, the UE may have included the IMEI in the Emergency Attach. If so, the ME Identity retrieval is skipped.

Figure 22 Case that ME retrieval can be skipped

The second is when attach using an attach type other than emergency sends an Attach Request message using Invalid IMSI and IMEI. In both cases, the network issues an Attach Reject message. However, the causes of reject appear differently, which are #15 (No suitable cells in tracking area) and #17 (Network failure). The standard (3GPP TS 24.301) defines each cause as follows.

Cause #15 – No suitable cells in tracking area

This EMM cause is sent to the UE if it requests service, or if the network initiates a detach request, in a tracking area where the UE, by subscription, is not allowed to operate, but when it should find another allowed tracking area or location area in the same PLMN or an equivalent PLMN.

Figure 23 EMM cause #15

Cause #17 – Network failure

This EMM cause is sent to the UE if the MME cannot service an UE generated request because of PLMN failures.

Figure 24 EMM cause #17

When Invalid IMSI is used, it can be considered correct operation for cause #17 to come down. This is because PLMN failure occurs and the service cannot be provided because PLMN values are invalidated when we make Invalid IMSI. However, in the case of Attach using IMEI, it is difficult to understand that cause #15 comes down. Of course, the standard specifies only IMSI and GUTI when attaching, so there will be no case of attempting IMEI in a general Attach, not an emergency. However, when IMEI attach occurs, #15 is not appropriate as a reject cause. Looking at 3GPP TS 36.523-1, the operation of the UE that received cause #15 is specified as follows. That is, attach is not attempted in the current TAI(tracking area list), and attach is attempted when moving to a cell of another TAI.

```
(1)

with { UE has sent an ATTACH REQUEST message }
ensure that {
  when { UE receives an ATTACH REJECT message with the EMM cause set to 'No Suitable Cells In
tracking area' }
    then { UE sets the EPS update status to EU3 ROAMING NOT ALLOWED, deletes any GUTI, last visited
registered TAI and KSI, resets the attach attempt counter, enters the state EMM-
DEREGISTERED.LIMITED-SERVICE and stores the current TAI in the list of "forbidden tracking areas for
roaming" }
            }


(2)

with { UE is in EMM-DEREGISTERED.LIMITED-SERVICE state and the current TAI is in the list of
"forbidden tracking areas for roaming" }
ensure that {
  when { UE re-selects a cell that belongs to the TAI where UE was rejected }
    then { UE does not attempt to attach }
            }


(3)

with { UE is in EMM-DEREGISTERED.LIMITED-SERVICE state and the current TAI is in the list of
"forbidden tracking areas for roaming" and KSI was deleted }
ensure that {
  when { in the same PLMN, UE enters a cell which provides normal service and belongs to the
tracking area not in the list of "forbidden tracking areas for roaming" }
    then { UE attempts to attach with IMSI indicated that no key is available }
            }
```

Figure 25 EMM cause #15 behavior

As mentioned above, the standard does not specify attach using IMEI. Therefore, a UE that attempts to attach a normal non-emergency using IMEI must be determined that it is not a normal terminal. In this case, sending an Attach Reject is a correct operation, but when the UE moves to another cell, it tries to attach again. Therefore, in this case, it may be appropriate to prevent the UE from accessing the network of the corresponding communication service provider by sending an Attach Reject of another cause such as cause #11 (PLMN not allowed).

5.2.1.2 Stage 2

Stage2 will perform analysis based on the received message (state).

Attach Reject (#17, network failure).

First, look for a message set as Security Header type reserved that causes Attach Reject due to #17 network failure. According to the standard, reserved is a message that is not used in the actual attach process. Therefore, it can be said that it is a correct operation that the network does not process when sending reserved in Identity Response and Authentication Response. Also, in the Security Mode Complete, the case of sending in plain is included. This is also a correct action that the network does not handle because it is the correct behavior to pass in ciphered.

Look at the case of "Attach Request (emergency, invalid GUTI)" -> "Identity Request" -> "Identity Response (valid IMSI)" -> "Attach Reject (network failure). In this case, regardless of the security header type, if a valid IMSI is sent, Attach Reject is always

received. It can be said that the behavior of such a network looks strange. The Identity Request was requested and a valid identity was sent in response, but in the end, Attach Reject was received. If you receive an Identity Request through attach rather than emergency attach, and then give a valid identity, you will receive an Authentication Request, but in case of emergency, a completely different reaction will be shown. This part is not clearly stated in the standard. In the standard (3GPP TS 24.301), cause #17 network failure is defined in figure 24.

However, PLMN failure is sent in all cases when the Security Header type is invalid, and since there is no detailed explanation for this, it is not sure whether the operation is correct. In the standard, cause is classified into the categories of "UE identification", "subscription options", "PLMN specific network failures and congestion/authentication failures", and "invalid messages", and cause #17 is in "PLMN specific network failures and congestion/authentication failures". It can be seen that it is a little strange that all Security Mode Complete messages with wrong Security Header type are classified as network failure.

Attach Reject (#13, Roaming not allowed in this tracking area)

In the case of "Attach Request (other types, invalid GUTI)" -> "Identity Request" -> "Identity Response (reserved X, invalid identity)" -> "Attach Reject (#13)". This is when the MME requests IMSI, and the UE responds with an incorrect IMSI. At this time, the network sends an Attach Reject message including the cause of #13. According to 3GPP TS 24.301, #13 (Roaming not allowed in this tracking area) is used in the following cases.

Cause #13 – Roaming not allowed in this tracking area

This EMM cause is sent to an UE which requests service, or if the network initiates a detach request, in a tracking area of a PLMN which by subscription offers roaming to that UE but not in that tracking area.

Figure 26 EMM cause #13

The standard provides roaming service to the UE, but if it is not in the current tracking area, attach reject is sent as cause 13. However, since invalid identity is sent, sending the cause is difficult to understand from the network standpoint. Looking at 3GPP TS 36.523-1, the operation of the UE that received cause #13 is specified as follows. That is, attach is not attempted in the current TAI, and attach is attempted when moving to a cell of another TAI.

(5)

```
with { the UE has sent an ATTACH REQUEST message including a PDN CONNECTIVITY REQUEST message }
ensure that {
  when { the UE receives an ATTACH REJECT message with the reject cause set to "roaming not allowed
in this tracking area" }
    then { the UE performs a PLMN selection }
          }
```

Figure 27 EMM cause #13 behavior

Since the IMSI is wrong, the network should determine that the UE is not a normal UE. In this case, sending an attach reject is a correct operation, but when the UE moves to another cell, it attempts to attach again. Therefore, in this case, it may be appropriate to prevent the UE from accessing the corresponding communication service provider network by sending an attach reject of another cause such as cuase #11 (plmn not allowed).

Authentication Request

Attach Request (other types, invalid GUTI)" -> "Identity Request (IMSI)" -> "Identity Response (Reserved X, valid identity)" -> "Authentication Request". When IMSI is asked through the Identity Request and a valid value is sent in the response, an authentication request is sent. As shown in the figure below, this is a correct operation when receiving a valid IMSI and sending an authentication request in the standard.

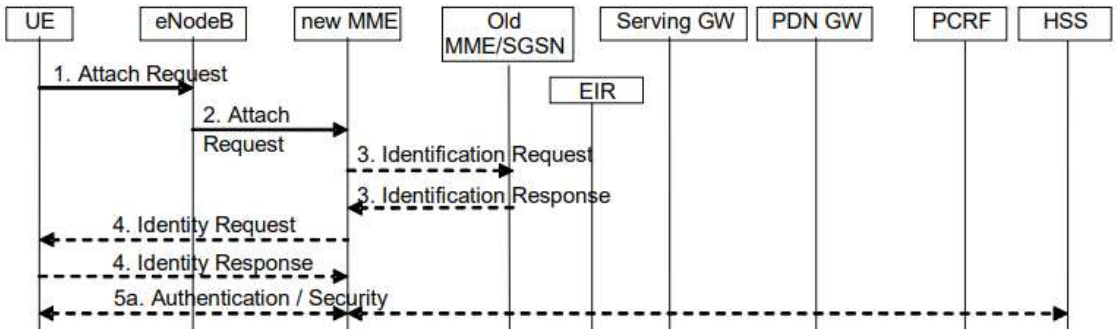

Figure 28 attach procedure

Security Mode Command (IMEISV req, no req)

In the case of attaching with Emergency type, invalid GUTI or valid IMSI in Attach Request, it reaches Security Mode Command (IMEISV req.) state through stage 0. First, when the UE attempts to attach with an invalid GUTI, ("Attach Request (emergency, invalid GUTI)" -> "Identity Request" -> "Identity Response (Invalid IMSI)" -> "Security Mode Command (IMEISV req)). This is because all the identities previously transmitted by the UE are wrong, so it is thought that you may ask for IMEISV. In case of emergency, even if IMSI is wrong, it is correct operation because it allows you to ask IMEI, IMEISV in figure 20.

Security Mode Command message asking for IMEISV also occurs through "Attach Request (emergency, valid IMSI)" -> "Authentication Request" -> "Authentication Response (Invalid authentication response parameter)" -> "Security Mode Command (IMEISV req.)". In this process, if a valid authentication response parameter is entered in the Authentication Response, the IMEISV is not requested in the Security Mode Command transmitted by the network.

The operation of such a network seems inappropriate. In case of emergency, since EEA0 and EIA0 are used for encryption, there is no need to check, but in case of

non-emergency, if an invalid security algorithm is used, it is necessary to transmit the Attach Reject including that algorithm is wrong.

Attach Reject (#19, ESM Failure)

"Attach Request (emergency, invalid IMSI)" -> "Security Mode Command (IMEISV req.)" -> "Security Mode Complete (Plain X, reservedX, invalid IMEISV)" -> "Attach Reject (#19)".

Cause #19 – ESM failure This EMM cause is sent to the UE when there is a failure in the ESM message contained in the EMM message.

Figure 29 EMM cause #19

This is the cause of reject that occurs when failure occurs in the content of the ESM message in the EMM message. If we give invalid IMEISV, ESM message content becomes invalid, so it can be said that it gives an appropriate cause.

Attach Accept

"Attach Request (emergency, IMEI)" -> "Security Mode Command (IMEISV no req.)" -> "Security Mode Complete (plain X reserved X)" -> "Attach Accept".

"Attach Request (emergency, invalid IMSI)" -> "Security Mode Command (IMEISV req.)" -> "Security Mode Complete (plain X reserved X, valid IMEISV valid IMEI)" -> "Attach Accept".

In both cases, Attach Accept is reached.

Looking at the above operation, the attach accept state is reached only when IMEI and IMEISV are obtained from the UE. In the standard document, in figure 21, in case of emergency attach, if attaching is requested by IMEI, the authentication process and the process of obtaining the ME identity may be omitted, so the above operation can be viewed as a correct operation.

Identity Request (IMEISV)

There was also a unique case that an Identity Request appeared in Stage 2. This is "Attach Request (emergency, invalid IMSI)" -> "Security Mode Command (IMEISV req.)" -> "Security Mode Complete (plain X reserved X, valid IMSI)" -> "Identity Request (IMEISV)". This is the case when an additional IMEISV was requested because IMSI was invalid during the attach process, but an IMSI message was sent instead of an IMEISV. In this case, even though Security Mode Complete is sent, Identity Request is sent again. Sending an IMSI when an IMEISV is requested is definitely an abnormal behavior, so analysis is required.

A total of 3 abnormal behaviors were found in carrier A.

5.2.2 Carrier B

5.2.2.1 Stage 0

① IMSI

When we send invalid, valid IMSI, it is always accepted as an Authentication Request regardless of validity. In the case of Invalid IMSI, since it is not registered in the network, an attach reject message must be sent without providing a service. However, in the case of carrier B, it can be said to be incorrect because it gives the same response as valid. This means that even if an invalid user is able to use the service when attach accept is performed.

②,③ Invalid GUTI, reserved mobile identity

It shows the same behavior as carrier A.

④ When IMEI is used as the mobility identity value

It shows the same behavior as carrier A.

5.2.2.2 Stage 2

Stage2 will perform analysis based on the received message (state).

Attach Reject (#17, network failure)

Among the messages that cause Attach Reject due to network failure, the message part in which the Security Header type is set to reserved shows the same result as carrier A.

Look at the case of "Attach Request (all type, IMSI, invalid algorithm)" -> "Authentication Request" -> "Authentication Response (reserved X, valid parameter)" -> "Attach Reject (network failure)". In this case, an invalid algorithm value was given in the attach request, but the authentication response was performed without rejecting immediately, but attach reject was given. Rejecting an invalid algorithm is a normal operation because the network does not support it.

Attach Reject (#11, PLMN not allowed)

The part corresponding to cause #13 of carrier A was treated as cause #11. In part of carrier A, we mentioned that it is appropriate to prevent the UE from accessing the communication network. Carrier B handled it so that it seems to be a normal operation.

Attach Reject (#19, ESM Failure)

"Attach Request (emergency, IMEI)" -> "Security Mode Command (no req)" -> "Security Mode Complete (plain X, reserved X)" -> "Attach Reject (ESM failure)"

If you look at the contents of cause 19 in figure 29, it is a message that is issued when the contents of the ESM message fail. Since we only sent a normal message, the operation is not correct.

Security Mode Command (IMEISV req.)

It shows the same behavior as carrier A.

Security Mode Command (IMEISV no req.)

It is almost the same as carrier A, but in case of non-emergency attach, carrier B also checks the validity of the algorithm used for encryption and processes it. In case of emergency, because EEA0 and EIA0 are used for encryption, there is no need to check, but if it is not an emergency, it is normal operation to check like carrier B.

Authentication Request

It shows the same behavior as carrier A.

Authentication reject

In the standard, when an invalid RES value is received, it is stated that if the request is made by IMSI in the attach request, the authentication reject is issued from the network. So, the action is correct.

If the authentication response (RES) returned by the UE is not valid, the network response depends upon the type of identity used by the UE in the initial NAS message, that is:

- if the GUTI was used; or
- if the IMSI was used.

If the GUTI was used, the network should initiate an identification procedure. If the IMSI given by the UE during the identification procedure differs from the IMSI the network had associated with the GUTI, the authentication should be restarted with the correct parameters. Otherwise, if the IMSI provided by the UE is the same as the IMSI stored in the network (i.e. authentication has really failed), the network should send an AUTHENTICATION REJECT message to the UE.

Figure 30 Authentication reject case

A total of 2 abnormal behaviors were found in carrier B.

5.2.3 Carrier C

5.2.3.1 Stage 0

In the case of carrier C, when an Invalid IMSI is sent by attach rather than an emergency, the reject cause is the same as that of A, except for the part where the reject cause is changed to #17 -> #8, so only the comparison for that part will proceed.

Cause #8 – EPS services and non-EPS services not allowed

This EMM cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services.

Figure 31 EMM cause #8

When Invalid IMSI is used, it is difficult to understand that cause #8 comes down.

When we make Invalid IMSI, we make the PLMN value invalid, so there is no satisfactory PLMN, so it cannot operate properly. Looking at 3GPP TS 36.523-1, the operation of the UE receiving cause #8 is specified as follows. It is specified that if the reject cause is received, the state enters the EMM-DEREGISTERED state. However, since the invalid IMSI is not a normal UE, it may be appropriate to prevent the UE from accessing the network of the corresponding carrier by sending an Attach Reject of another cause such as cause #11 (PLMN not allowed) so that it cannot be accessed again by attaching.

```
(1)

with { UE has sent an ATTACH REQUEST message including a PDN CONNECTIVITY REQUEST message }
ensure that {
  when { UE receives an ATTACH REJECT message with the reject cause set to "EPS services and non-EPS
services not allowed" }
    then { UE considers the USIM as invalid for EPS services and non-EPS services and enters state
EMM-DEREGISTERED }
            }


(2)

with { UE receives an ATTACH REJECT message with the reject cause set to "EPS services and non-EPS
services not allowed" }
ensure that {
  when { the UE has been switched off, then switched on }
    then { the UE sends an ATTACH REQUEST message with IMSI, including a PDN CONNECTIVITY REQUEST
message }
            }


(3)

with { UE receives an ATTACH REJECT message with the reject cause set to "EPS services and non-EPS
services not allowed" }
ensure that {
  when { the UE has been switched off, then switched on and a UMTS or GSM cell is found }
    then { the UE sends an ATTACH REQUEST message with IMSI }
            }
```

Figure 32 EMM cause #8 behavior

5.2.3.2 Stage 2

Stage2 will perform analysis based on the received message (state).

Attach Reject (#17, network failure), (#11, PLMN not allowed)
It shows the same behavior as carrier B.

Authentication Request
"Attach Request (other types, invalid GUTI)" -> "Identity Request (IMSI)" -> "Identity Response (Reserved X, valid identity)" -> "Authentication Request" is the same as A and B.

"Attach Request (all type, IMSI)" -> "Authentication Request" -> "Authentication Response (reserved)" -> "Authentication Request" is not same.

when a reserved header type is sent in response to an Authentication Request, an Authentication Request is requested again. In the case of carrier A and B, sending the

reserved header type immediately sends an Attach Reject message, but it seems that the carrier C actually uses the reserved header type to handle that way.

Security Mode Command (IMEISV req.)
It shows the same behavior as carrier A.

Security Mode Command (IMEISV no req.)
The message from the Authentication Request is the same as that of carrier A, but if a plain, reserved header type is included in the Security Mode Complete message and sent, the message is received.
In the case of reserved type, it may be correct to send a re-request to request a different security header type, but if it is sent as plaintext, it is definitely an incorrect behavior. Security mode messages should be messages that are encrypted and cannot be seen by other people. However, if the message is transmitted in plaintext and attach is completed, it becomes vulnerable immediately and sniffing becomes possible.

Authentication reject
It shows the same behavior as carrier B.

Attach Accept, Identity Request (IMEISV)
It shows the same behavior as carrier A.

A total of 2 abnormal behaviors were found in carrier C.

6. Conclusion

In this work, we present a systemized approach, which mainly uses the state machine extraction and comparative analysis to detect vulnerabilities stemming from misimplementation or misconfigurations. To this end, we devised two tools; 1) state machine extractor, and 2) analyzer. With the state machine extractor, it transmits various control plane messages to the cellular network in order to infer the operational logic of the network devices. In addition, using an analyzer, we have comparative analysis between the extracted state machine and standard specification documents. We adopt the proposed approaches to the testbed from the three commercial mobile networks, we discovered 7 misimplementations which can lead to security threats.

7. Future research plan & proposal

In this work, we present the standard violating results of the extracted state machine which only covers the initial three stages of the ATTACH procedure. During the given period for the URP research, we put lots of time into 1) building the state machine extractor, 2) debugging its implementation, and 3) analyzer. We have put the remaining

time to extract the state machine of the cellular network. Unfortunately, due to the numerous number of required test messages for the complete ATTACH procedure, it was hard to extract the whole state machine of the cellular network within the given research period.

However, as we have completed the building state machine extractor and analyzer, we could extract the state machine over the remaining stages effectively. Moreover, we believe that we can find out more vulnerability and misimplementations on the remaining stages once it completes all test cases for the ATTACH procedure. For example, the state machine extractor provides the full paths including the vulnerable paths by which the adversary can launch the impersonation attack.

Our future work is to expand the state machine to the remaining NAS/RRC procedures. Using the implemented state machine extractor, we believe that we can have several benefits on 1) understanding the operational logic on the various NAS/RRC procedures, and 2) detecting the misimplementation on each stage of the procedures by adopting the same approaches of this research. For example, we can adapt our state machine extractor on the TAU(tracking area update) procedure and radio bearer establishment procedure.

Lastly, we plan to propose the complete conformance test of the network devices (e.g, eNodeB, EPC and etc) to the 3GPP, standardization group for the cellular network. Comparing to the conformance test of UE, there are few test cases for examining the implementation of the network devices. As a result, we believe that our test cases generated from this research can be used as a stepping stone for improving the security of cellular networks.

8. Reference Literature

[1] Hongil Kim, Jiho Lee, Lee Eunkyu, and Yongdae Kim. Touching the Untouchables: Dynamic Security Analysisof the LTE Control Plane. In Proceedings of the IEEESymposium on Security & Privacy (SP). IEEE, May2019.

[2] South Korea reaches 9.25 million 5G subscribers: Report, November, 2020, https://www.rcrwireless.com/20201102/5g/south-korea-reaches-9-25-million-5g-subscribers-report

[3] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,” in Proceedings of the Network and Distributed Systems Security (NDSS), 2018.

[4] D. A. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A Formal Analysis of 5G Authentication,” in ACM Conference on Computer and Communications Security. ACM, 2018

[5] C. Cremers, M Dehnel-Wild, “Componen-Based Formal Analysis of 5G-AKA:Channel Assumptions and Session Confusion” in Proceedings of the Network and Distributed Systems Security (NDSS), 2019

[6] 3GPP. TS 36.331, “Evolved Universal Terrestrial Radio Access (EUTRA); Radio Resource Control (RRC); Protocol specification,” 2019.

[7] 3GPP. TS 24.301, “Non-Access-Stratum (NAS) protocol for Evolved Packet System(EPS); Stage 3,” 2019.

[8] 3GPP. TS 24.008, “Mobile radio interface Layer 3 specification; Core network protocols, Stage 3,” 2019.

[9] 3GPP. TS 33.401, “3GPP System Architecture Evolution (SAE); Security architecture” 2019.

[10] 3GPP. TS 23.401, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” 2019.

[11] 3GPP. TS 36.523-1, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification,” 2019.