Abnormal VoLTE Call Setup between UEs

Sekwon Kim, Bonmin Koo, and Hwankuk Kim
Mobile Security R&D Team, Korea Internet & Security Agency, Seoul, Korea

Abstract - *As the mobile environment has been rapidly changing recently due to advances in mobile communication technology, mobile traffic has been sharply increasing around the world. To respond to the increasing traffic, Korea's mobile carriers have been trying to build out their 4G networks early on rather than upgrading their existing 3G networks. However, due to the early build out of the LTE network and competition to improve it, network security was not sufficiently taken into consideration. Also, as the LTE network provides both data and VoLTE services on the All-IP-based network, it is exposed to the same types of security threats likely to occur on IP-based networks, such as forgery, alteration of information, and eavesdropping. This paper analyzes a particular security threat which is the vulnerability to hacking of call setup between terminals using VoLTE service in Korea, and proposes a counter technology.*

Keywords: LTE; VoLTE; Threat; Abnormal Call Setup.

1 Introduction

Recently the mobile environment has been changing rapidly due to advances in mobile communication technology. High-performance smartphones and personal tablets have become very popular, and as various mobile services have increased, anyone can now use high-speed mobile communication networks. Also, as an increasing number of customers, who used to be satisfied with downloadable-type contents only, are now using on-demand or streaming contents, mobile traffic is sharply increasing around the globe[1].

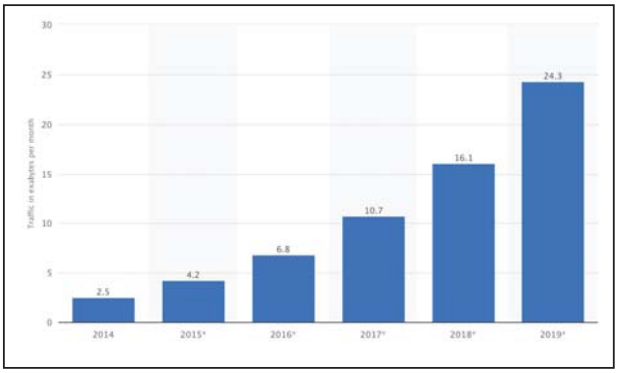


Fig. 1. Global mobile data traffic from 2014 to 2019 (in exabytes per month).

To respond to the increasing traffic, Korea's mobile carriers decided to install and build out 4G networks early instead of upgrading their existing 3G networks. As a result, LTE service began in Korea in 2011, and as of now Korea is the most advanced country in the world in terms of the LTE market and technology, i.e. Korea has become a global reference country for LTE.

However, in their scramble to publicize their technology and gain subscribers as quickly as possible they completed their LTE networks earlier than scheduled and launched services, and network security was not sufficiently taken into consideration due to the competition for network enhancement such as introduction of the LTE-A technology. Also, as the LTE network provides data and voice services on the All-IP-based network, it is exposed to security threats likely to occur on IP-based networks, such as forgery and alteration of information, and eavesdropping. In particular, if the SIP control messages for VoLTE service are forged or altered, then the result could be that voice call tolls could be used for crimes like voice phishing[2][3].

This paper will analyze the security threat to abnormal call setup between terminals using the VoLTE service, and propose a counter technology. This paper is organized as follows. Chapter 2 describes the LTE network, GTP protocol, IMS network and SIP Protocol. Chapter 3 analyzes the security threat to abnormal VoLTE call setup, and Chapter 4 proposes a counter technology. Lastly, Chapter 5 brings this paper to conclusion.

2 Background Information

2.1 LTE Network

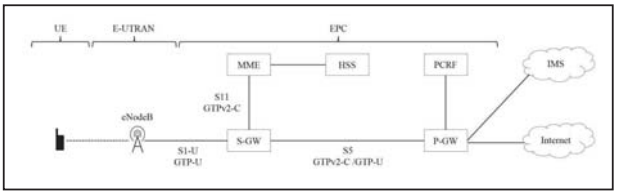


Fig. 2. LTE Network Structure.

LTE is a network infrastructure designed to provide all types of telecommunication services including voice calls, video calls, SMS and various mobile multimedia services, such as wireless Internet, to mobile terminals. As illustrated in Figure 2, it consists of an Access Network (E-UTRAN) that manages terminals and wireless resources, and a Core Network (EPC) that handles data transmission, authentication and billing.

The E-UTRAN, which provides the mobile communication environment, exists between the EPC and terminals. eNodeB allocates mobile resources to terminals, and manages them with certain coverages in each region.

LTE EPC consists of several key pieces of equipment. The MME, the S-GW and the P-GW each play important roles for providing data services, e.g. the mobile Internet. The MME authenticates the UE and manages the bearer. The S-GW is the terminal point of the E-UTRAN and the EPC. The P-GW is in charge of allocating terminal IP addresses and IP routing/ forwarding. In addition, there is the HSS that serves as the subscriber information DB, and the PCRF that determines the service quality policy for each subscriber[4].

2.2 GTP (GPRS Tunneling Protocol)

The GTP is the tunneling protocol for delivering the data sent by the UE on the LTE network. Equipment like the eNodeB, the MME, the S-GW and the P-GW use the GTP to create GTP tunnels for delivering data from equipment to equipment and communicate. The GTP is divided into the GTP-C for control (Create, Delete, Modify/Release) of GTP tunnels and the GTP-U for user IP packet transmission[5][6].

Figure 3 shows the GTPv2-C header used in the LTE network. Here, the Tunnel Endpoint Identifier (TEID) is a unique factor used to distinguish the GTP tunnels for individual UEs on the LTE network. For example, If 100 UEs are connected to the same S-GW and P-GW, one or more GTP tunnels will be created for each UE and more than 100 GTP tunnels will be created in total, with each GTP tunnel being identified with the TEID. And, the message type is a factor for distinguishing the GTP-C. Key message types are shown in Table 1[5].

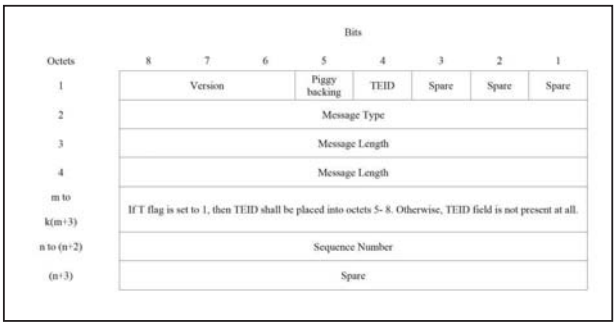


Fig. 3. General format of GTPv2 Header for Control Plane.

TABLE I. MESSAGE TYPES FOR GTPV2

Message Type	Message	Description
32	Create Session Request	Creates GTP tunnels
33	Create Session Response	
34	Modify Bearer Request	Modifies GTP tunnels
35	Modify Bearer Response	
36	Delete Session Request	Deletes GTP tunnels
37	Delete Session Response	

2.3 IMS (IP Multimedia Subsystem)

The LTE network is an All-IP-based network. Unlike the 3G network, it does not have a separate voice network, but rather LTE interworks with the IMS network to provide VoLTE, the voice service. As VoLTE supports the 50~7000Hz bandwidth, which is much wider than the 3G voice call bandwidth, clear high-quality voice calls are possible. Also, it is possible to switch to a video call in the middle of a voice call and easily share photographs, images and location information by interfacing with various data services. As VoLTE exchanges voices through the IP-based data network it is similar to VoIP technology, yet stable high-quality call service is possible thanks to separate quality management when data gets congested[7].

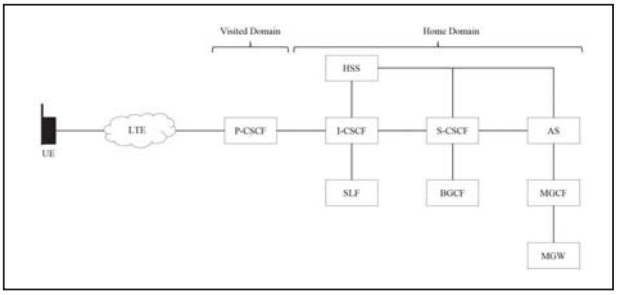


Fig. 4. IMS Network Structure.

Figure 4 illustrates the IMS network structure. VoLTE service is provided through the Call Session Control Function (CSCF) that handles the call and session control in the IMS network. The CSCF consists of equipment for processing the calls and sessions of IP-based multimedia services. It manages the registered information of VoLTE terminals, connects calls, and relays voice call origination and termination data. The CSCF can be divided into the P(Proxy)-CSCF, I(Inter-rogating)-CSCF, and the S(Serving)-CSCF depending on the function being referred to. The P-CSCF is the first point that the UE encounters when connecting to the IMS for the time. It serves as the proxy or user agent. The I-CSCF serves as the contact point for all incoming calls for connecting to subscribers in the network, queries the HSS to determine the S-CSCF, and allocates the S-CSCF to the UE in the registration process. Lastly, the S-CSCF performs key functions for call processing, and is responsible for all functions related to providing services like interfacing the service platform and providing service-related information. The AS is the service platform for providing service, the SLF provides HSS addresses to the CSCF. In addition, the BGCF, the MGCF and the MGW provide such functions as protocol and signaling conversion for interworking with other voice networks such as the PSTN[8].

2.4 SIP (Session Initiation Protocol)

VoLTE, the voice service through IMS network, uses SIP text-based signaling protocol the same as VoIP does to provide voice service over the Internet. The SIP is used to

control voice calls, e.g. voice call origination, termination and end-of-call, and is divided into the header and the body. The SIP header includes the Call-ID unique to each call and originating/ terminating MSISDN as well as the method field that defines the SIP message type. The body includes the media codec used for voice and video calls and information on IP and Port for sending and receiving the RTP Voice traffic. The key SIP method and its uses are shown in Table 2 below[9][10][11].

TABLE II. SIP METHOD AND USES

Method	Description
REGISTER	Registers the address listed in the To header field with a SIP server
INVITE	Indicates that a client is being invited to participate in a call session
SUBSCRIBE	Subscribes to event notification
NOTIFY	Notifies the subscriber of a new Event
REFER	Asks recipient to issue a SIP request (call transfer)

Figure 5 illustrates the procedures for VoLTE service. The UE registers itself with the CSCF, and uses the VoLTE service through the Call Setup process

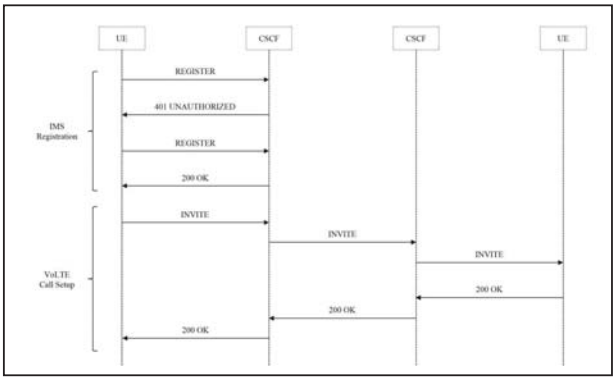


Fig. 5. IMS Procedures for VoLTE.

3 Abnormal VoLTE Call Setup

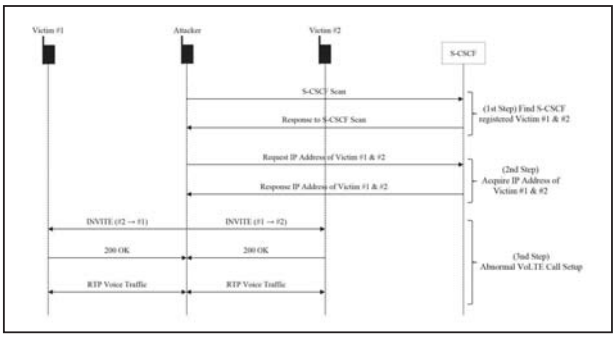


Fig. 6. Procedures for Abnormal VoLTE Call Setup.

The SIP is a text-based protocol that can be forged and altered easily. This chapter deals with the security threats that can connect phone calls abnormally between VoLTE users by altering the MSISDN in the SIP Header and the IP and port information for sending and receiving the RTP Voice traffic in the Body. Figure 6 shows the procedure.

For Abnormal VoLTE Call Setup, the attacker searches for the S-CSCF registered target UEs (Victim #1 & #2) by S-CSCF scanning. The attacker then obtains the IP addresses of victims from the S-CSCF. Finally, the attacker, disguised as the CSCF, sends each the altered SIP Invite to victims, and if victims terminate the Call, an abnormal call is set up between victims. As the RTP voice traffic between victims passes through the attacker at this time, eavesdropping is possible. The details are as follows:

3.1 Find S-CSCF Registered Victim

If the UE turns on the VoLTE, the IMS registration process will be carried out. At this time, the I-CSCF queries the HSS to determine the S-CSCF and then allocates the S-CSCF to the UE.

Fig. 7. Find IP Address of S-CSCF in SIP 200 OK packet.

The attacker can check the IP address of the S-CSCF allocated to his/her UE (x.x.227.129) in the SIP 200 OK packet during the VoLTE registration process as illustrated in Figure 7, and guess the IP address band of the S-CSCF on this.

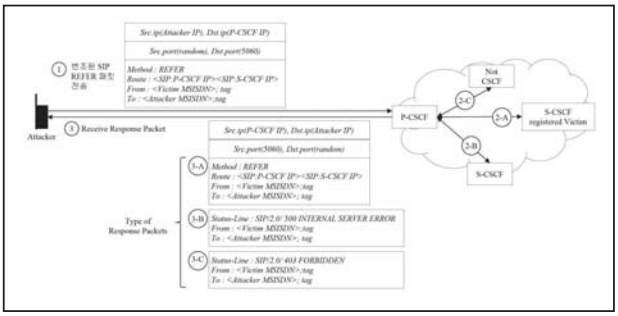


Fig. 8. Procedures for Finding S-CSCF Registered Victim by S-CSCF Scanning.

Figure 8 shows how the SIP REFER can be used to scan the IP address band of the S-CSCF and check the IP address of the S-CSCF which victim is registered by analyzing the response packets. The attacker sends SIP REFER packets as shown in Figure 9 in which the From field (Caller's MSISDN) and P-Preferred-Identity field were altered to the Victim's

MSISDN (800), the To field (Callee's MSISDN) and Refer-To field were altered to the attacker's MSISDN (203), and the Route field was altered to be the IP address of the S-CSCF (x.x.227.2~254) to the P-CSCF. The P-CSCF receives the packet sent by the attacker then forwards it to the IP address of the Route field (the IP address of the S-CSCF altered by the attacker).

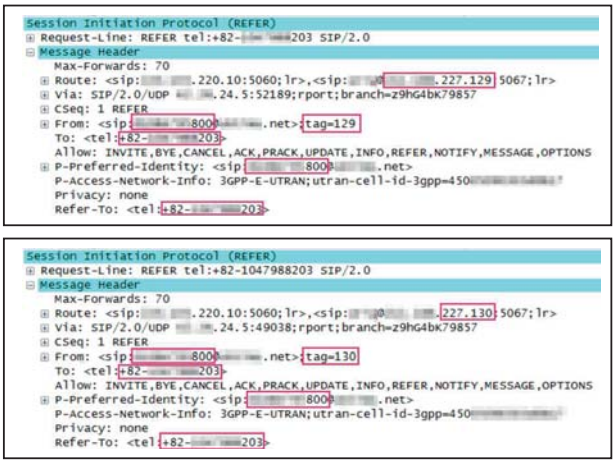


Fig. 9. Example of Altered SIP REFER Packets.

The attacker received three types of response packets as shown in Figure 10. "500 INTERNAL SERVER ERROR" means that the server that sent the response packet is not the CSCF, "403 FORBIDDEN" means that the CSCF has no registered victims, and "REFER" means that the S-CSCF has registered victims.

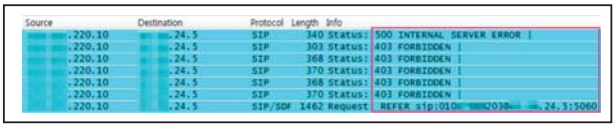


Fig. 10. Response Packets to S-CSCF Scanning.

Here, as the destination IP of the scanning traffic sent by the attacker is a P-CSCF IP, the Source IP of the response packet is also a P-CSCF IP. In other words, the attacker cannot use the Source IP of the response packet to check the S-CSCF IP with victims registered. The attacker can use the tag value of the From field in the received REFER packet to check the S-CSCF IP address with victims registered. Among the packets sent by the attacker, the S-CSCF IP address of the packet whose From field tag value matches the From field tag value (129) in the received REFER packet is the S-CSCF IP (x.x.227.129) with victims registered.

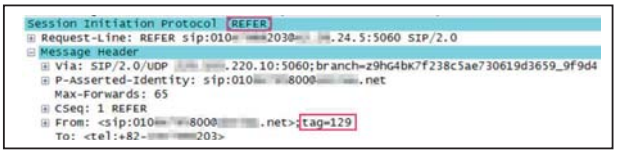


Fig. 11. Response Packet Details.

3.2 Acquiring IP Addresses of Victim

The SIP SUBSCRIBE message is used for requesting the CSCF for the status of VoLTE registered terminals. The CSCF sends the SIP NOTIFY message containing the registration status, including the IP address, in response to the SUBSCRIBE message. The attacker can obtain the IP address of the victim by transmitting the SUBSCRIBE message with an altered MSISDN to the S-CSCF with victims registered as illustrated in Figure 12.

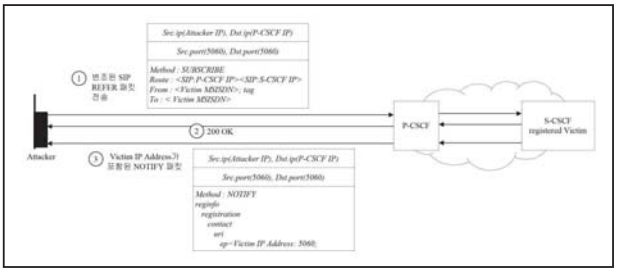


Fig. 12. Procedures for Acquiring IP Addresses of Victim.

The attacker sends the SIP SUBSCRIBE packet as shown in Figure 13, in which the Route field was altered to the IP address of the S-CSCF with victims registered (x.x.227.130), and the From field and To field were altered to the MSISDN of the victim (223).

Fig. 13. Example of Altered SIP SUBSCRIBE Packet.

The P-CSCF receives the packet sent by the attacker and forwards it to the S-CSCF IP address in the Route field. The S-CSCF then transmits 200 OK and NOTIFY to the attacker in response.

Fig. 14. SIP NOTIFY Packet Included Victim's IP Address.

The attacker can obtain the victim's IP address (x.x.135.169), included in the SIP NOTIFY packet, from the response packet as shown in Figure 14. This IP address matches the IP address

for the IMS, which is verified through the Network Info app installed in the victim's UE as illustrated in Figure 15.

Fig. 15. Victim's IP Address.

3.3 Abnormal VoLTE Call Setup

UEs using the VoLTE service receive the S-CSCF in the registration process, and if they terminate any VoLTE Calls, the UEs will receive SIP INVITE packets from the allocated S-CSCF server. At this time, however, the UEs do not test the integrity of the S-CSCF. That is, they do not check whether the S-CSCF, which transmitted SIP INVITE to them, matches the S-CSCF allocated to them in the registration process, and simply receive SIP INVITE unconditionally and process it. The attacker abuses this, and as shown in Figure 16, the attacker can eavesdrop on the RTP voice traffic by setting up abnormal calls between the two victims.

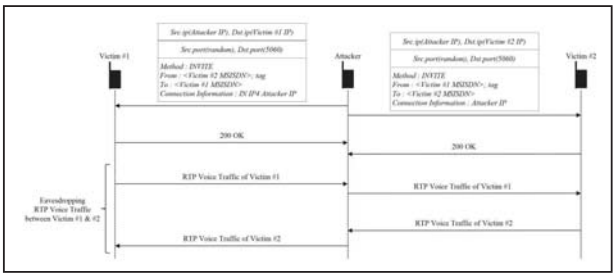


Fig. 16. Procedures for Abnormal VoLTE Call Setup between Victims.

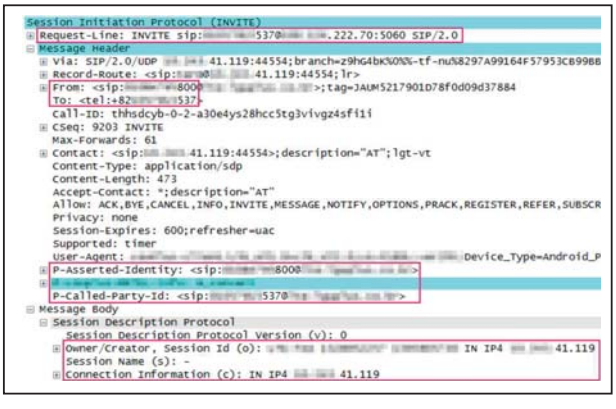


Fig. 17. Example of Altered SIP INVITE Packet.

The attacker sends the SIP INVITE packet as shown in Figure 17, in which Caller's Information (From field, P-Asserted-Identity field, etc.) was altered to Victim #2's MSISDN, Callee's Information (To field, P-Called-Party-ID field, etc.) was altered to Victim #1' MSISDN, and the IP address for receiving the RTP Voice Traffic was altered to the attacker's IP address (x.x.41.119), to Victim #1. The attacker sends the SIP INVITE packet, in which the Caller and Callee information is switched, to Victim #2.

The victim who received the altered SIP INVITE packet sent by the attacker will see a screen that says the VoLTE Call request was sent by the other victim, not the attacker, and if both victim #1 & #2 terminate the Call, the abnormal call setup will be completed. At this time, as the IP address for the RTP voice traffic in the SDP of the SIP INVITE packet is set up as the attacker's IP address, the RTP voice traffic between victims will pass through the attacker as illustrated in Figure 18. The attacker can demodulate it and eavesdrop on the call between victims.

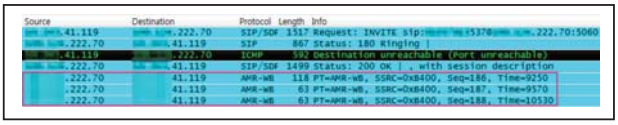


Fig. 18. RTP Voice Traffic between Victims Passed through The Attacker.

4 Counter Technology

The SIP is a text-based protocol that is easy to forge and alter. Chapter 3 described security threats whereby phone calls between VoLTE users can be hacked by altering the MSISDN in the SIP Header, the IP for sending and receiving the RTP voice traffic in the Body, and Port information.

The SIP standard recommends using TLS or IPSec for security and S/MIME for message integrity and confidentiality[12][13]. Actually, T-Mobile of the US uses TLS and Japan's NTT Docomo uses IPSec for communication between the UE and the CSCF to encrypt data in response to security threats. Also, the SIP-based VoIP system uses the SIP Digest Authentication function based on HTTP Authentication to authenticate all SIP Request messages[14]. As these encryption and authentication mechanisms slow down VoLTE service, however, they may cause some degree of dissatisfaction among LTE service subscribers who want and expect fast service.

It is possible to respond to security threats due to forged and altered SIP messages by adding security functions to the CSCF that controls calls and sessions in the IMS network. In other words, the IP addresses and MSISDN that the CSCF allocated to UEs will be managed separately, and thus make it possible to analyze whether the MSISDN is altered for all SIP Request messages and block fraudulent ones. However, as mobile communication networks provide "Always on" service, it is difficult to add functions without shutting down equipment, and service failures may result due to unexpected errors and equipment malfunction in the process of adding the functions. And functions added to equipment will inevitably increase the load on existing equipment. Increased load will eventually deteriorate availability and the introduction of additional CSCF may lead to increased costs.

This chapter proposes a technology for detecting SIP Request messages with forged and altered originator information by managing the UEs in the LTE EPC.

4.1 TEID-based UE Session Management

The S11 (MME↔S-GW) interface of the LTE EPC collects the GTP-C for creating, deleting and modifying GTP tunnels, analyzes it, and manages the session table of the TEID-based UEs. The management method consists of two stages: (1) pairing GTP-C Requests and Responses and (2) processing the GTP-C to manage the session table.

In the first stage, GTP-C Requests and Responses are paired through the buffer. This stage will check whether Requests and Responses are normally exchanged. Here, the buffer key is the combination of the MME IP and the Sequence Number included in the GTP-C. Figure 19 shows the procedure in detail.

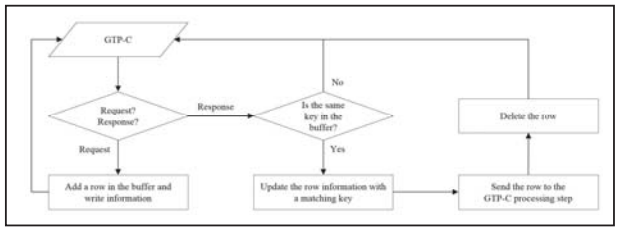


Fig. 19. Procedures for Pairing GTP-C Requests and Responses.

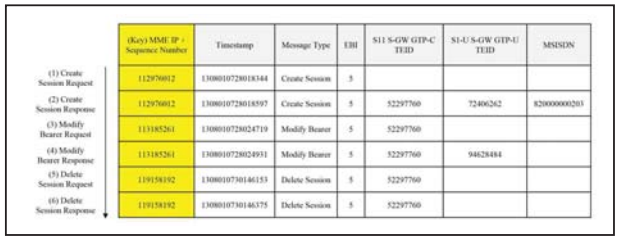
1) Receive the GTP-C Create Session, Modify Bearer and Delete Session.

2) If it is a Request, add a new row in the buffer, and write GTP-C information.

3) If it is a Response and the same key exists in the buffer, update the information in the row which matches the key, then transmit the information of the row to the second stage and delete the row.

4) If it is a Response and the same key does not exist in the buffer, receive the next GTP-C.

Figure 20 shows the changes of the buffer due to the creation, modification and deletion of GTP tunnel of a UE.



	(Key) MME IP + Sequence Number	Timestamp	Message Type	EBI	S11 S-GW GTP-C TEID	S1-U S-GW GTP-U TEID	MSISDN
(1) Create Session Request	112976012	1308010728018344	Create Session	5			
(2) Create Session Response	112976012	1308010728018597	Create Session	5	52297760	72406262	820000000203
(3) Modify Bearer Request	113185261	1308010728024719	Modify Bearer	5	52297760		
(4) Modify Bearer Response	113185261	1308010728024931	Modify Bearer	5	52297760	94628484	
(5) Delete Session Request	119158192	1308010730146153	Delete Session	5	52297760		
(6) Delete Session Response	119158192	1308010730146375	Delete Session	5	52297760		

Fig. 20. The Changes of The Buffer Due to The Creation, Modification and Deletion of GTP Tunnel.

The second stage processes the GTP-C when the GTP-C Request and Response were paired in the first stage, and manages the session table. The tables for managing sessions consist of the UC table for managing the control tunnels of the UE, and the UD table for managing data tunnels and detecting SIP packets with altered origination information. Here, the UC Table Key is a combination of the S11 SGW GTP-C TEID and EBI (EPS Bearer ID), and the UD Table Key is the S1-U SGW GTP-U TEID. Figure 21 shows the procedure in detail.

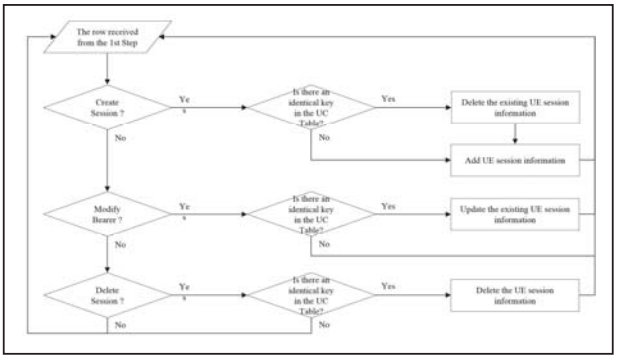


Fig. 21. Procedures for Processing The GTP-C to Manage The Session Table.

1) Receive the information on the GTP-C whose Requests and Responses were paired in the first stage.

2) If the Message Type is Create Session and the same key exists in the UC Table, delete the matching rows in the UC and UD Tables, and write the received Session information in the UC and UD Table.

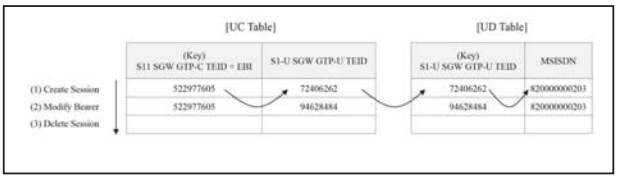
3) If the Message Type is Create Session, and the same key does not exist in the UC Table, write the received GTP-C Create Session information in the UC and UD Tables.

4) If the Message Type is Modify Bearer, and the same key exists in the UC Table, update the received GTP-C Modify Bearer information in the UC and UD Tables with matching keys.

5) If the Message Type is Delete Session, and the same key exists in the UC Table, delete the rows in the UC and UD Tables with the matching keys.

6) After the above process is completed, receive the following GTP-C information from the first stage.

Figure 22 illustrates the changes in the UC and UD tables due to the creation, modification and deletion of the GTP tunnel of a UE.



	[UC Table] (Key) S11 SGW GTP-C TEID + EBI	[UC Table] S1-U SGW GTP-U TEID	[UD Table] (Key) S1-U SGW GTP-U TEID	[UD Table] MSISDN
(1) Create Session	522977605	72406262	72406262	820000000203
(2) Modify Bearer	522977605	94628484	94628484	820000000203
(3) Delete Session				

Fig. 22. The Changes in the UC and UD Tables due to The Creation, Modification and Deletion of The GTP Tunnel.

4.2 Detecting Abnormal SIP Packet

The GTP-U will be collected from the S1-U (eNodeB↔S-GW) interface of the LTE EPC, and the MSISDN in the SIP will be compared with the value in the UD Table to detect

abnormal SIP packets with altered MSISDN. Figure 23 shows the procedure in detail.

1) Receive the GTP-U whose user packet payload is the SIP, and extract the TEID from the GTP Header and MSISDN information from the SIP Header.

2) Use the TEID to query the UD Table, and extract the value (MSISDN) from matching rows.

3) Compare the MSISDN extracted from the SIP Header with the value extracted from the UD Table.

4) If they match, and if they are judged to be normal but do not match, regard it as an abnormal SIP.

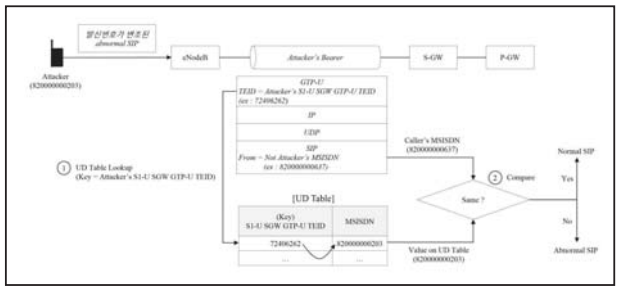


Fig. 23. Procedures for Detect Abnormal SIP Packets with Altered MSISDN.

5 Conclusion and Future Plan

The mobile environment has changed rapidly due to advances in mobile communication technology, and mobile traffic has been increasing sharply around the globe. Accordingly, mobile carriers are introducing LTE networks to secure network availability, and VoLTE, the voice service through the LTE network, has also become popularized. However, as the LTE network provides data and voice service on the All-IP-based network, it is exposed to security threats likely to occur on IP-based networks, such as forgery and alteration of information and eavesdropping. In particular, if the SIP control message for VoLTE service is forged or altered, it may open voice call tolls to crimes like voice phishing.

This paper analyzed the security threat that exists in VoLTE call setup due to the vulnerability of the procedure for checking the S-CSCF registered by the VoLTE UE and obtaining the IP address of the UE to being hacked and offers a countermeasure. The proposed technology can be easily implemented and used for an effective response to VoLTE security threats. Actually, the authors of this paper implemented the proposed technology, installed it on the LTE network of one of the mobile carriers in Korea, and are currently testing the performance. Also, as the proposed technology was implemented in the form of a module, it can be used to supplement the functions of the existing LTE network security equipment.

In the future, if the results of the trial test show a deterioration of performance, the authors are planning to enhance the proposed technology, and will, in any event, continue to conduct research on any security vulnerabilities of VoLTE.

ACKNOWLEDGMENT

This research was funded by the Ministry of Science, ICT & Future Planning, Republic of Korea, as part of its ICT R&D program for 2015.

6 References

[1] http://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/.

[2] Voice over LTE, Acme Packet, LTE World Summit 2014.

[3] Joo-Hyung Oh, Sekwon Kim, Myoungsun Noh, Chaetae Im, "Phone Number Spoofing Attack in VoLTE," 16th International Conference on Computer Networks and Security, vol. 08, pp. 1151–1153, December 2014.

[4] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[5] 3GPP TS 29.274: "General Packet Radio System (GPRS) Tunneling Protocol for Control Plane (GTPv2-C)".

[6] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)".

[7] Mike McKernan, "VoLTE vs. VoIP: What's the Difference?" SPIRENT 2012.

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] Internet Engineering Task Force (IETF) RFC 3261: "SIP: Session Initiation Protocol".

[10] Internet Engineering Task Force (IETF) RFC 3265: "Session Initiation Protocol (SIP)-Specific Event Notification".

[11] Internet Engineering Task Force (IETF) RFC 3515: "The Session Initiation Protocol (SIP) Refer Method".

[12] Kent, S., and Atkinson, R. "Security Architecture for the Internet Protocol" (RFC 2401, November, 1998).

[13] Ramsdell, B., "S/MIME version 3 message specification", 1999

[14] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and Stewart, L., "HTTP authentication: Basic and digest access authentication" (RFC 2617, June, 1999).