# Tracking Location Information of VoLTE Phones

Sekwon Kim, Bonmin Koo, and Hwankuk Kim
Mobile Security R&D Team
Korea Internet & Security Agency
Seoul, Korea
{heath82, bmkoo, rinyfeel}@kisa.or.kr

***Abstract*—As the mobile communications environment has undergone drastic changes in the wake of applicable technology development, mobile traffic is rapidly increasing around the world. To cope with such a rapid traffic increase, Korean mobile carriers chose to deploy their 4G networks early rather than upgrading the conventional 3G networks. However, as they were bent on deploying and advancing the Long Term Evolution (LTE) network faster than others, the mobile carriers did not make sufficient considerations for LTE network security. In addition, the LTE network is exposed to all security threats that can occur in any IP-based network such as falsification/alteration of information, eavesdropping, etc. as the LTE network is an all-IP based network providing data and Voice-over-LTE (VoLTE) services. This study attempts to describe the security threats associated with the tracking of location information of VoLTE phones.**

***Keywords—VoLTE; Security; Threat; Location Information***

## I. INTRODUCTION

The mobile communications environment has undergone drastic changes recently in the wake of applicable technology development. High-performance smartphones and tablets have become commodities and the rising number of mobile services is now enabling anyone to access high-throughput mobile communication networks. No longer content with simply downloading contents, consumers are using increasingly more on-demand or streaming contents, which causes mobile traffic to increase rapidly on a global scale[1].

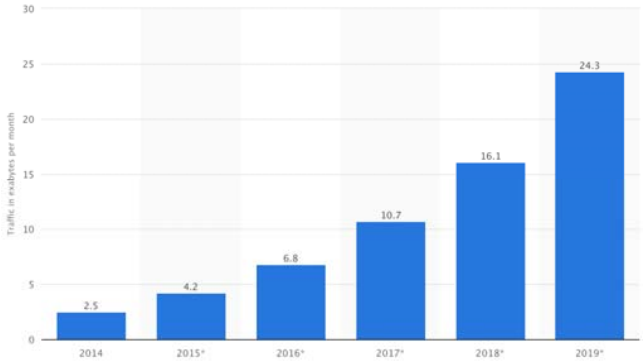


Fig. 1. Global mobile data traffic from 2014 to 2019 (in exabytes per month)

To cope with such a rapid increase in traffic, Korean mobile carriers chose to deploy their 4G networks early rather than upgrading the conventional 3G networks. Accordingly, Korea launched its first LTE service in 2011 and the country is now a global LTE reference, leading the rest of the world both in terms of the LTE market and technology.

However, the LTE network and service were launched earlier than originally planned to have first-mover advantages and promote technological prowess, etc. So sufficient considerations were not made for network security as the mobile carriers were preoccupied with their race to upgrade their networks. In addition, as the LTE network is an all-IP-based network providing data and voice communications services, it is exposed to security threats that can occur in any IP-based networks such as falsification/alteration of information, eavesdropping, etc. In particular, if the Session Initiation Protocol (SIP) control message for VoLTE service is falsified /altered, it can result in communication charges for voice calls and lead VoLTE phones to be vulnerable to abusive crimes such as voice phishing attempts[2][3][4].

This study attempts to analyze the security threats associated with the tracking of location information of VoLTE phones and suggests a strategy to cope with them. Chapter 2 of this paper describes the LTE network, E-UTRAN Cell Global Identifier (ECGI), IP Multimedia Subsystem (IMS) network, and SIP protocol. Chapter 3 analyzes the security threats associated with the tracking of location information of VoLTE phones, and Chapter 4 suggests a strategy to cope with them. Lastly, Chapter 5 states the conclusion of this paper.

## II. BACKGROUND INFORMATION

### A. LTE Network

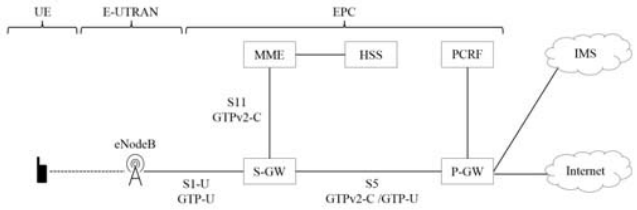


Fig. 2. LTE Network Architecture

An LTE network is a network infrastructure that provides telecommunication services including voice call, video call, and SMS as well as mobile multimedia services such as mobile Internet service on mobile handsets. As seen in Fig. 2, the LTE

978-1-4673-9795-7/15 $31.00 © 2015 IEEE
DOI 10.1109/CSCI.2015.101

network consists of an access network that manages the handsets, mobile resources and core network that transfers data and processes authentication, billing, etc.

Between the LTE handsets and the EPC, which is the LTE core network, there is the Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN) that provides the mobile communications environment. Evolved NodeB (eNodeB), a key component of E-UTRAN, has a certain geographical coverage and assigns/manages mobile resources to handsets.

The LTE EPC consists of several resources among which Mobility Management Entity (MME), Serving Gateway (S-GW) and PDN Gateway (P-GW) play key roles in providing data services such as the mobile Internet. MME authenticates the UE and manages the Bearer whereas S-GW is the terminal point between E-UTRAN and EPC. P-GW assigns IP addresses to phones and routes/forwards IP. In addition, the Home Subscriber Server (HSS) maintains the subscriber information DB while the Policy and Charging Rules Function (PCRF) determines the policies governing service quality per subscriber[5].

### *B. ECGI*

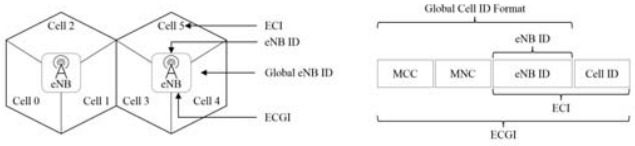


Fig. 3. eNodeB/Cell Identifier and Format

The eNodeB is identified by the eNodeB ID if it is identified within a mobile carrier's network but if it is identified out of the mobile carrier's network then identification is handled by the Global eNodeB ID (which combines the PLMN ID and eNodeB ID). Fig. 3 show the identifiers and their formats relevant to the eNodeB /Cells. The eNodeB Cell identifier is a combination of an eNodeB ID and Cell ID.

### *C. IMS*

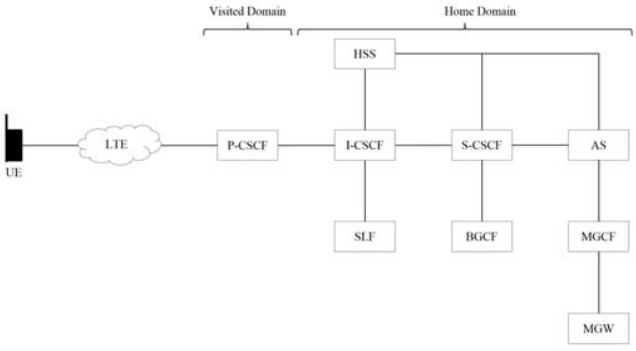


Fig. 4. IMS Network Architecture

Unlike a 3G network, an LTE network is an all-IP-based network that has no additional voice communications network. It interfaces with the IMS network to provide voice communication services or VoLTE service. As VoLTE supports a bandwidth of 50~700Hz wider than that of 3G voice communications, it delivers crisp high-quality voice service. In addition, voice calls can be switched to video calls on the fly and photos, videos, location information, etc. can be shared with ease by interfacing with various data services. Also, VoLTE is similar to Voice over IP (VoIP) in that both technologies exchange voice data over IP-based data networks, but VoLTE can ensure high-quality voice communications through a separate QoS policy even in the face of data traffic congestion[6].

Fig. 4 shows the architecture of an IMS network. VoLTE service is provided through the Call Session Control Function (CSCF) that controls the phone calls in the IMS network. The CSCF is responsible for processing calls and sessions of IP-based multimedia services. It manages VoLTE phone registration information, connects calls, and relays voice call transmission and reception. According to function, the CSCF can be classified as a Proxy (P)-CSCF, Interrogating (I)-CSCF, and Serving (S)-CSCF. P-CSCF is where the UE contacts the IMS first in which case it serves as the Proxy or User Agent. Then, the I-CSCF provides the contact point for all calls to access subscribers within a network, determines the S-CSCF by searching the HSS, and assigns the S-CSCF to the UE in the registration process. Lastly, the S-CSCF performs key functions for call processing being responsible for all functions related to service provision by providing information relating to the interface with the service platform and other information relating to the services. Additionally, the Application Server (AS) is the service platform for service provision whereas the Subscription Locator Function (SLF) provides the CSCF with the HSS address. In addition, the Breakout Gateway Control Function (BGCF), Media Gateway Control Function (MGCF), and MGW (Media Gateway) converts protocols and signals to interface with other voice communications networks such as the PSTN[7].

### *D. SIP*

TABLE I. 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) |

VoLTE, which is a voice communications service on the IMS network, uses SIP, which is a text-based signaling protocol at the application layer, in the same manner as VoIP. SIP is used for controlling voice calls during voice call transmission, reception and closure. It is divided into a header and body. The SIP header includes a Method field that defines the type of SIP message and Call-ID unique to each call and caller/callee phone numbers, etc. The SIP body includes

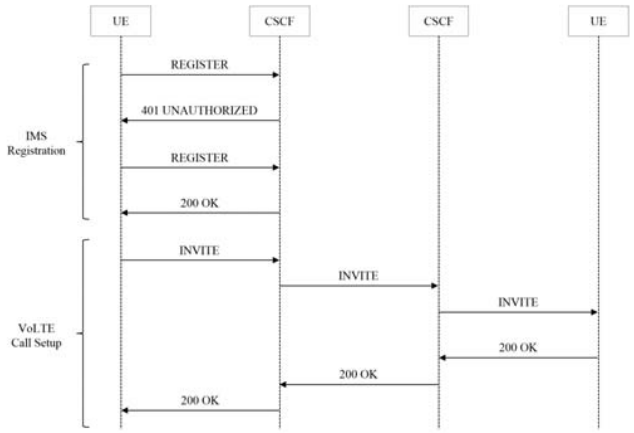


Fig. 5. IMS Procedures for a VoLTE Call

information on the media codecs used for voice and video calls, the IP and port, etc. required for RTP voice traffic transmission/reception. Key SIP Methods and their uses are as shown in Table 1[8][9][10].

Fig. 5 shows process for VoLTE Call. VoLTE Phone registers itself in CSCF and uses VoLTE service through Call Setup process.

## III. Tracking Location Information of VoLTE Phones

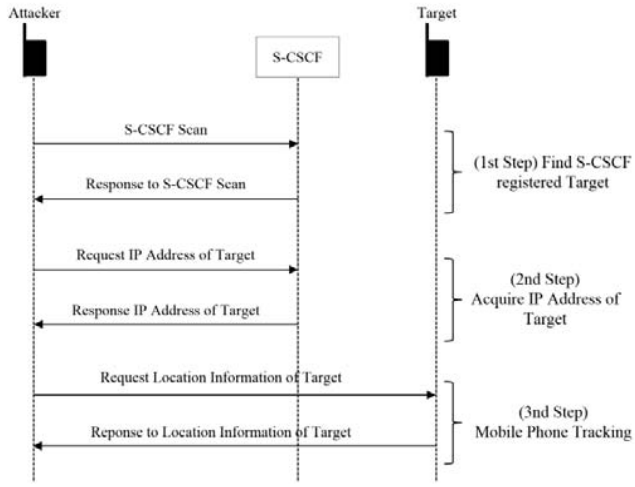


Fig. 6. The Procedures for Tracking Location Information of VoLTE Phones

SIP is a text-based protocol vulnerable to falsification /alteration. This chapter describes security threats associated with the tracking of location information of handsets through inter-handset communications via IMS network scan and the handset IP address assigning process. This chapter also presents location information tracking test results of VoLTE phones subscribing to the LTE service of a Korean mobile carrier identified as "A." Fig. 6 shows the tracking process.

To track location information of VoLTE phones, an attacker first scans the S-CSCF to find the S-CSCF where the targeted VoLTE phone is registered. Then the attacker acquires the IP address of the targeted VoLTE phone from the S-CSCF. Lastly, the attacker acquires the location information of the targeted VoLTE Phone. Relevant details are as follows:

### A. Find S-CSCF registered Targeted VoLTE Phone

When the VoLTE function of the VoLTE phone is on, the IMS registration process is initiated. At this time, the I-CSCF searches the HSS to determine the S-CSCF and assign it to the VoLTE phone. As shown in Fig. 7, the attacker can confirm the IP address of the S-CSCF (x.x.227.129) assigned to its phone in the "SIP 200 OK" packet in the VoLTE registration process and infer from it the IP address range of the S-CSCF.


Fig. 7. The S-CSCF IP address in the "SIP 200OK" packet of the VoLTE registration process

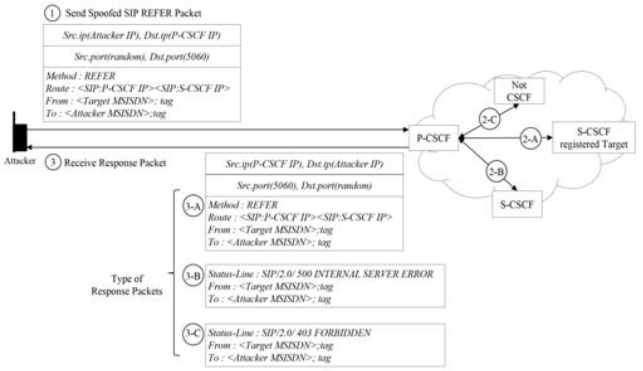


Fig. 8. The process of scanning to find the S-CSCF where the targeted VoLTE phone is registered

Fig. 8 shows how the SIP REFER message can be used to scan the IP address range of the S-CSCF and analyze reply packets to confirm the IP address of the S-CSCF where the targeted VoLTE Phone is registered. The attacker sends SIP REFER packets to the P-CSCF as shown in Fig.9 causing the From field (Caller's MSISDN) and P-Preferred-Identity fields to be altered to those of the MSISDN(800) of the targeted VoLTE phone, the To field (Callee's MSISDN) and the Refer-To field (altered) to the attacker's MSISDN(203), and the Route field (altered) to the IP address of the S-CSCF (x.x.227.2~254). The P-CSCF then receives the packets sent by the attacker and forwards them to the IP address in the Route field (IP address of the S-CSCF altered by the attacker).

The attacker sends SIP REFER packets to the P-CSCF as shown in Fig.9 causing the From field (Caller's MSISDN) and P-Preferred-Identity fields to be altered to those of the MSISDN(800) of the targeted VoLTE phone, the To field (Callee's MSISDN) and the Refer-To field (altered) to the

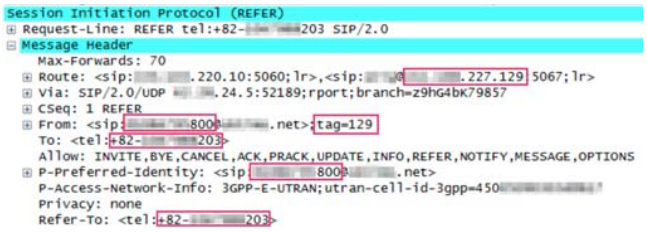


Fig. 9. SIP REFER packet for finding S-CSCF where the targeted VoLTE phone is registered

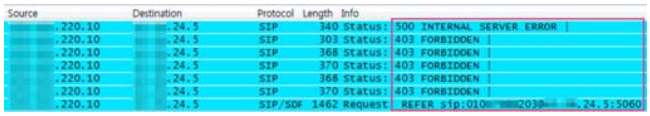


Fig. 10. Response packets for scanning traffic to find the S-CSCF where the targeted VoLTE Phone is registered

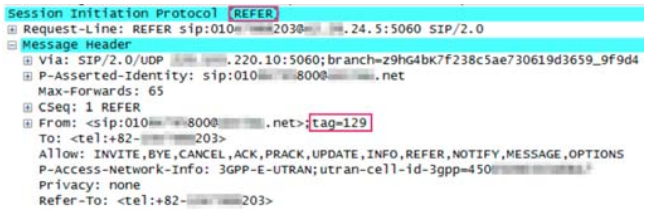


Fig. 11. Details of Response packet

attacker's MSISDN(203), and the Route field (altered) to the IP address of the S-CSCF (x.x.227.2~254). The P-CSCF then receives the packets sent by the attacker and forwards them to the IP address in the Route field (IP address of the S-CSCF altered by the attacker).

As shown in Fig. 10, the attacker receives three types of reply packets:

- "500 INTERNAL SERVER ERROR" indicates that the server sending the reply packet is not the proper CSCF
- "403 FORBIDDEN" indicates that the server sending the reply packet is not the CSCF where the targeted VoLTE phone is not registered
- "REFER" indicates that the server sending the reply packet is the S-CSCF where the targeted VoLTE Phone is registered

In this case, as the destination IP of the scanning traffic sent by the attacker is the IP of the P-CSCF, the Source IP of the reply packet is also the P-CSCF IP. In other words, the attacker cannot confirm the S-CSCF IP where the targeted VoLTE Phone is registered with the source IP of the reply packet. The attacker can confirm the IP address of S-CSCF where the targeted VoLTE Phone is registered with the tag value in the From field within the REFER packet sent as a reply. Among the packets sent by the attacker, the IP address of the S-CSCF of the packet of which the tag value of the From field matches the tag value (129) of the From field in the REFER packet is the S-CSCF IP (x.x.227.129) where the targeted VoLTE Phone is registered.

### *B. Acquiring the IP Address of the Targeted VoLTE Phone*

The SIP SUBSCRIBE message calls the CSCF for the status of the VoLTE Phone. In response, the CSCF sends the SIP NOTIFY message containing current registration data such as the IP address to SUBSCRIBE.

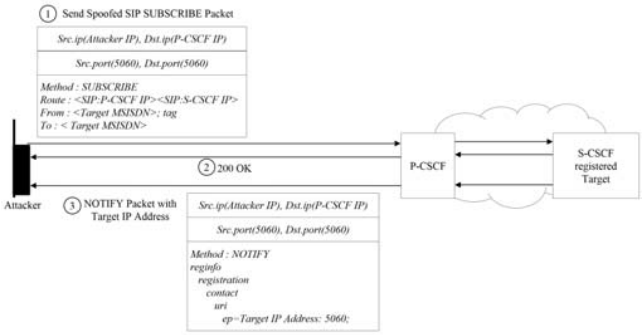


Fig. 12. The process of acquiring the IP address of a targeted VoLTE Phone

As shown in Fig. 12, the attacker can acquire the IP address of the targeted VoLTE Phone as the MSISDN sends the altered SUBSCRIBE message to the S-CSCF acquired in the previous step.


Fig. 13. SIP SUBSCRIBE packet for acquiring the IP of a targeted VoLTE Phone

As shown in Fig. 13, the attacker sends the P-CSCF SIP SUBSCRIBE packet of which the Route field is altered to the IP address of the S-CSCF (x.x.227.130) to which the targeted VoLTE phone is registered, and the From and To fields to the MSISDN of the targeted VoLTE Phone (223). After receiving packets sent by the attacker, the P-CSCF forwards them to the S-CSCF IP address in the Route field while the S-CSCF sends 200 OK and NOTIFY to the attacker in response.


Fig. 14. Response (SIP NOTIFY) packet containing the IP address of the targeted VoLTE Phone

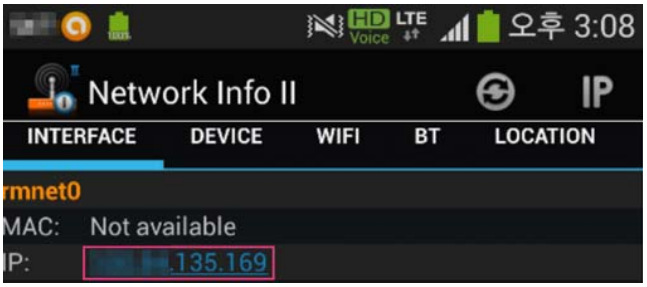


Fig. 15. IP Address of the Targeted VoLTE Phone

As shown in Fig. 14, the attacker can acquire from the reply packet the IP address of the targeted VoLTE Phone (x.x.135.169) included in the SIP NOTIFY packet. As shown in Fig. 15, this IP address matches the IMS IP address confirmed in the Network Info app. installed in the targeted VoLTE Phone.

### C. Acquiring the UTRAN Cell ID of a Targeted VoLTE Phone

The SIP REFER message is used for multilateral talks involving three or more people in a VoIP environment. However, as mobile carriers usually do not support multilateral VoLTE Call service, the SIP REFER message is not used, but VoLTE phones never the less support the SIP REFER method.

As shown in Fig. 16, the attacker can acquire the UTRAN Cell ID of the targeted VoLTE Phone by forwarding the SIP REFER packet to the IP address of the targeted VoLTE Phone acquired in the second step.

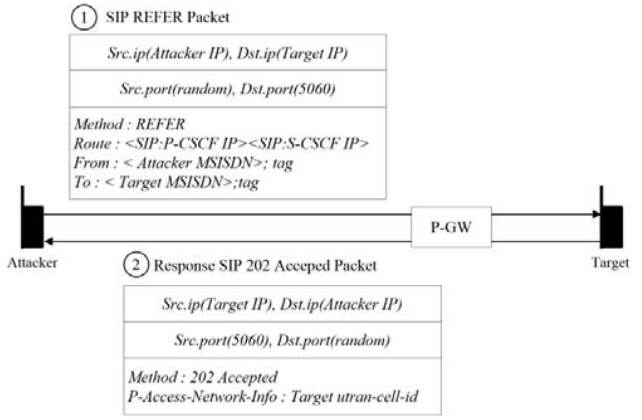


Fig. 16. Process of acquiring the UTRAN Cell ID of a targeted VoLTE Phone

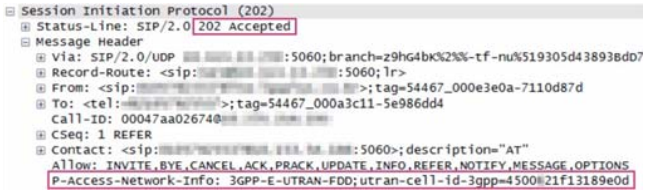


Fig. 17. Response packet (202 Accept) containing the UTRAN Cell ID of the targeted VoLTE Phone

The attacker sends to the targeted VoLTE Phone the SIP REFER packet where the From field is set to the attacker's MSISDN and the To field to the MSISDN of the targeted VoLTE Phone. The P-GW checks the destination IP of the IP header and routes the applicable packet to the targeted VoLTE Phone. The targeted VoLTE Phone sends a SIP 202 Accepted packet to the attacker in response to the SIP REFER packet sent by the attacker. As shown in Fig. 17, the attacker can acquire the UTRAN Cell ID of the targeted VoLTE phone from the P-Access-Network-Info field of the received packet.

### D. Coordinate Transformation

The Google Maps Geolocation API returns a location and accuracy radius based on information about the cell tower WiFi nodes that the client can detect[11].

```
{
  "cellTowers": [
    {
      "cellId": 21532831,
      "locationAreaCode": 2862,
      "mobileCountryCode": 214,
      "mobileNetworkCode": 7
    }
  ]
}
```

Fig. 18. An Example of a WCDMA Cell Tower Object[11]

The attacker can convert the acquired UTRAN Cell ID of the targeted VoLTE phone to coordinate information through the Google Maps Geolocation API. In this case, as the UTRAN Cell ID of the targeted VoLTE phone acquired by the attacker is "4050021f13189e0d," values shown in Table 2 below are entered and the "locationAreaCode" and "cellId" values that are hexadecimals are converted to decimals.

TABLE II. THE INPUT OF WCDMA CELL TOWER OBJECT

| Type | Variable | Input |
|---|---|---|
| MCC | mobileCountryCode | 405 |
| MNC | mobileNetworkCode | 00 |
| LAC | locationAreaCode | 8689 |
| Cell ID | cellId | 51944973 |

The UTRAN Cell ID is converted to coordinates as shown in Fig. 19 and the attacker can locate the targeted VoLTE Phone with a margin of error at about 200 meters.

```
{
  "location" : {
    "lat": 37.4937768,
    "lng": 127.1230953
  },
    "accuracy": 2055.0
}
```

Fig. 19. UTRAN Cell ID converted to coordinates

## IV. COUNTER-STRATEGY

SIP standards recommend that TLS or IPSec be used for security and S/MIME be used for message integrity and confidentiality[12][13]. For actual communications between the UE and CSCF, T-Mobile of the United States and NTT Docomo of Japan use TLS and IPSec respectively to encrypt data and thereby cope with security threats. In addition, SIP-based VoIP system authenticates all SIP Request messages, using the HTTP Authentication-based SIP Digest Authentication function[14]. However, as this encryption and authentication mechanism slows down VoLTE service, it may compromise the satisfaction level of LTE service subscribers who want faster services. To ensure fast VoLTE services, Korean mobile carriers use a different strategy from the above to deal with the security threats associated with the tracking of location information of VoLTE phone described in this paper. This chapter describes how the three Korean mobile carriers dealt with such security threats.

To track the location information of a VoLTE phone, Steps 1 and 2 described in Chapter 3 must be performed in advance. In these steps, the SIP packet spoofed as the MSISDN of the targeted VoLTE Phone is used. If the MSISDN spoofing of the SIP packet is checked through the session control of the VoLTE phone in the CSCF managing the VoLTE Call Session, the attacker can be prevented from acquiring the CSCF where the targeted VoLTE Phone is registered and the IP address of the targeted VoLTE Phone.

Another alternative is to block the SIP packet directly at the P-GW when routed from one phone to another. In no case is the SIP packet routed from one phone to another in the LTE network and the destination of the SIP packet sent from a phone is always the CSCF in IMS network.

## V. CONCLUSION AND FUTURE WORK

As the mobile communications environment has undergone drastic changes in the wake of applicable technology development, mobile traffic is rapidly increasing around the world. Accordingly, mobile carriers deployed the LTE networks to ensure network availability and now offer voice communication services on it, known collectively as VoLTE, which is becoming increasingly popular. However, as LTE network provides data and voice communication services on an all-IP-based network, it is exposed to security threats that can occur in any IP-based network such as falsification/alteration of information and eavesdropping. In particular, if the SIP control message for VoLTE service is falsified/altered, it can result in communication charges for voice calls and lead VoLTE phones to be abused in crimes such as voice phishing attempts.

This paper described the security threats associated with the tracking of location information of VoLTE phones and presented test results of Korean LTE networks. Also, a strategy employed by Korean mobile carriers to deal with such security threats was described.

Additional studies to cover security vulnerabilities and threats of VoLTE will follow subsequently, with particular focus on security vulnerabilities and threats anticipated in the wake of the migration of LTE and IMS networks to IPv6 address system.

## 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.

## REFERENCES

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

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, et al. SIP: session initiation protocol, 2002.

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

[4] 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.

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

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

[7] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

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

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

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

[11] https://developers.google.com/maps/documentation/geolocation/intro.

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

[13] Ramsdell, B., "S/MIME version 3 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).