International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 2 [ISSN : 2250-3757]
Publication Date : 30 October, 2015

Security Vulnerabilities and Threats of LTE Networks

Sekwon Kim, Seongmin Park, Hwanguk Kim

***Abstract*—The popularity of LTE and its entailing expansion of mobile services have led directly to the explosion of data traffic flowing through networks since LTE was launched in 2011. And as the tethering service based on LTE's high-speed capabilities has become popular, the malicious traffic of the wired environment consisting of PCs has been flowing into the LTE network. In response to this, mobile carriers have been configuring their LTE networks using NAT and have also installed IP-based security equipment between the LTE network and external Internet network. However, the NAT and IP-based security equipment cannot detect/block attacks from within LTE networks, and are limited in their ability to protect LTE networks from abnormal traffic from the outside. This paper describes the security vulnerabilities of LTE networks and security threats likely to occur due to attacks abusing such vulnerabilities.**

***Keywords*—LTE, security, vulnerabilities, threats**

I. Introduction

Mobile communication networks have evolved from voice-oriented 1G (FDMA) and 2G digital (TDMA/CDMA) systems to 3G (WCDMA) and 4G (LTE-A) and have extended into data services. Many subscribers switched to LTE soon after it was launched in 2011, and as mobile services delivering high-definition video and mobile games proliferated, data traffic flowing into LTE networks has been sharply increasing. Also, as LTE networks provide high-speed mobile data services, the tethering service, which allows you to use LTE terminals as Internet modems, has become popular, so the malicious traffic of the wired environment comprised of PCs is now flowing into LTE networks.

In response to this, most mobile carriers have configured NAT-based LTE networks, and installed IP-based security equipment to respond to DDoS and IPS between the LTE network and external Internet network. These steps were taken to protect their own LTE networks from abnormal/attack traffic coming from the outside.

However, the NAT and IP-based security equipment cannot detect/block attacks from within LTE networks, and have proven to be limited in their ability to protect LTE networks from abnormal traffic coming from the outside. As a matter of fact, presentations about depletion of wireless resources on LTE networks, inflow of abnormal traffic bypassing the IP-based security equipment, and attacks causing abnormal billing were made by domestic and overseas research institutions at various conferences[1].

Sekwon Kim, Seongmin Park, Hwanguk Kim
Korea Internet & Security Agency
Republic of Korea

This paper describes the security vulnerabilities of LTE networks and security threats likely to occur due to attacks abusing such vulnerabilities. Chapter 2 describes the structure of LTE networks, GTP protocol, and the billing method for data service use. Chapter 3 describes security vulnerabilities of LTE networks while Chapter 4 explains the security threats that take advantage of the vulnerabilities of LTE networks. Chapter 5 contains the conclusion of this paper.

II. LTE Network

A. *LTE Network Structure*

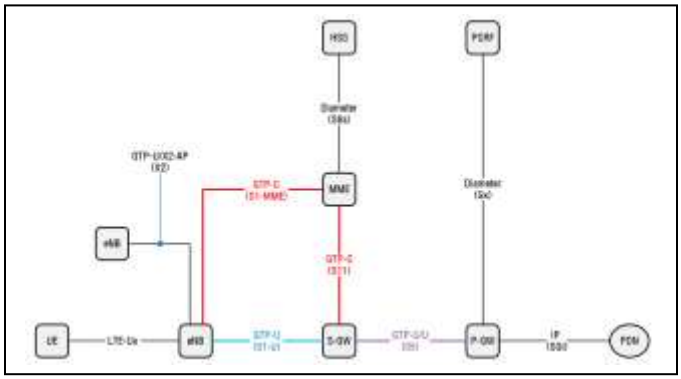


Figure 1. Structure of an LTE network

Figure 1 illustrates the overall structure of an LTE network. Basically it consists of LTE entities and EPC entities. LTE entities are the UE and the eNB, whereas EPC entities are the MME, S-GW, P-GW, HSS and PCRF[2].

- UE (User Equipment) : These are the user terminals that connect to an eNB through the wireless interface.
- eNB (evolved NodeB) : This provides users with wireless interface and wireless resource management functions like wireless bearer control, dynamic wireless resources allocation, and inter-cell interference coordination (ICIC)
- MME (Mobility Management Entity) : This communicates with the HSS for user authentication and user profile download, and provides the UE with the EPS (Evolved Packet System) mobility management and EPS session management functions.
- S-GW (Serving Gateway) : This becomes the anchoring point during the handover between eNBs and between 3GPP systems.
- P-GW (PDN Gateway) : This connects the UE to an external PDN network and provides packet filtering. Significantly, it allocates IP addresses to the UE, receives the PCC (Policy and Charging Control) rules

from the PCRF and applies them, and provides the billing function.

- HSS (Home Subscriber Server) : This is a central DB with a user profile. It provides the MME with user authentication information and user profiles.
- PCRF (Policy and Charging Rule Function) : This is a policy and billing control entity. It provides the policy control decision and billing control function. The PCC rules generated by the PCRF are delivered to the P-GW.

Most LTE networks are configured based on the NAT, and use dynamic IPs to efficiently utilize IP resources. Accordingly, no traffic can be introduced to LTE networks without traffic triggered by the UE. A dynamic IP address is allocated to each UE every time one connects to an LTE network, but when the UE connection is released that very same IP is returned to be reused on another (or possibly same) UE.

B. GPRS Tunneling Protocol (GTP)

The GTP is a tunneling protocol installed/used between equipment, such as S1-MME (eNB↔MME), S1-U (eNB↔S-GW) and S5 (S-GW↔P-GW) interfaces, to provide the GPRS (General Packet Radio Service) on LTE networks. They are classified into GTP-C (GTP control plane messages) and GTP-U (GTP user data messages). GTP-C is used to exchange bearer information and manage bearers, e.g. creation, update and deletion of bearers. Types and functions are as shown in Table 1[3]. A GTP-U is used to transmit user data (T-PDUs).

TABLE I. GTP-C MESSAGE TYPES AND FUNCTIONS

Message	*Type*	*Function*
Echo Request	0x01	Checks Peer status
Echo Response	0x02	
Create Session Request	0x32	Creates Default EPS Bearers
Create Session Response	0x33	
Modify Bearer Request	0x34	Creates S1 Bearers
Modify Bearer Response	0x35	
Release Access Bearer Request	0x170	Deletes S1 Bearers
Release Access Bearer Response	0x171	
Delete Session Request	0x36	Deletes Default EPS Bearers
Delete Session Response	0x37	

Figure 2 illustrates the protocol stacks of GTP-C and GTP-U (GTP is a protocol that operates on the basis of IP and UDP).

Figure 2. Structure of an LTE network

C. Billing on LTE Networks

On LTE networks it is the PCRF that determines billing rules, includes them in the PCC rules, and delivers them to the P-GW. The P-GW calculates the data usage of each UE based on the PCC rules it received and then bills it. Figure 3 illustrates the billing procedure for data usage[4]. The P-GW applies the billing rule to each bearer, and if the bearer is established, the billing information, i.e. CDR (Charging Data Record), will be opened. If IP packets are delivered through the P-GW, the P-GW records them in the CDR, and if the bearer is torn down, it closes the CDR. The closed CDR is delivered to the OFCS (Offline Charging System) and usage is measured and billed.

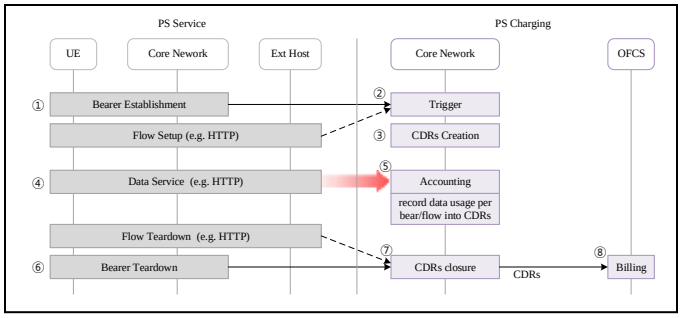


Figure 3. Structure of an LTE network

III. Security Vulnerabilities

A. GTP-in-GTP

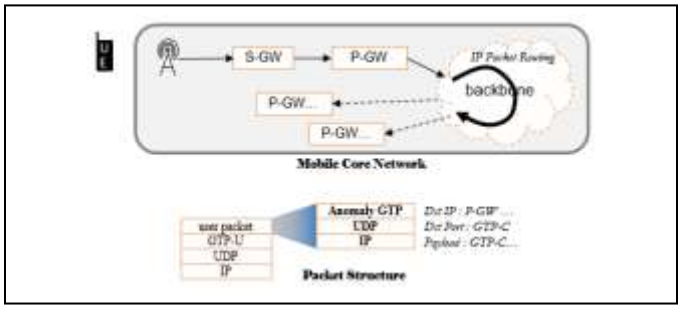


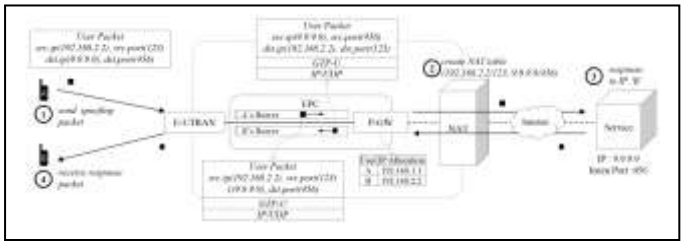
Figure 4. GTP-in-GTP security vulnerabilities

GTP is an important protocol used to allocate IPs on LTE networks or manage network resources, but it can be easily altered or forged as a UDP-based connectionless protocol. Attackers are able to launch various attacks, such as depletion of network resources, scan and data service interference by maliciously generating control messages (GTP-C) allocating, changing and deleting network resources[5].

B. IP Spoofing

IP spoofing entails altering of an IP address not allocated to the sender into a source IP and then sending the IP packet.

IP spoofing makes it difficult to trace the attacker's IP, or has been used in various attacks, such as DoS attacks, in the wired environment. IP spoofing may be filtered in a limited way by Network Ingress Filtering in switches or routers in the wired environment. However, IP spoofing has not been taken seriously on LTE networks, and attackers may use IP spoofing



to bypass the NAT, which protects LTE networks from the external Internet, and lets abnormal traffic penetrate LTE networks[6].

Figure 5. IP spoofing security vulnerabilities

C. *Reuse of IP Addresses*

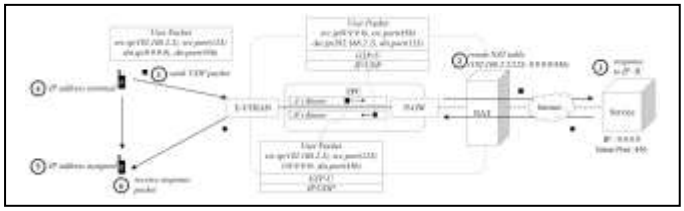


Figure 6. Security vulnerabilities of reusing IP addresses

The UE on LTE networks receives the allocated IP address when connecting to LTE networks, and returns it when connection is released. The IP address will then be allocated to another UE connecting to an LTE network. Attackers can use this IP address reuse process to bypass the NAT protecting LTE networks from the external Internet to let abnormal traffic penetrate LTE networks[7].

D. *Terminal-to-Terminal Communication*

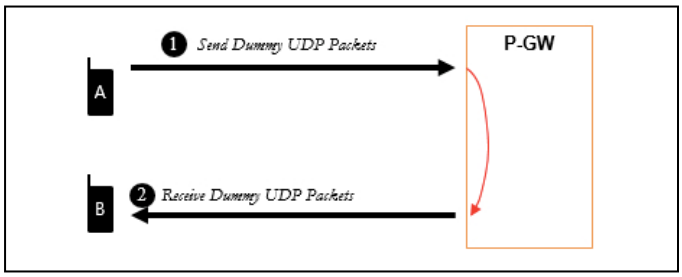


Figure 7. Security vulnerabilities of communication between terminals

Most mobile carriers providing LTE service allow communication between terminals because of various services. As packets generated by communication between terminals are routed from the P-GW to another UE, they do not pass through the IP-based security equipment installed between the LTE network and the external Internet network. Thus an attacker can use this route to send abnormal traffic to other terminals and even threaten the LTE networks.

IV. Security threats

A. *LTE Network Scanning*

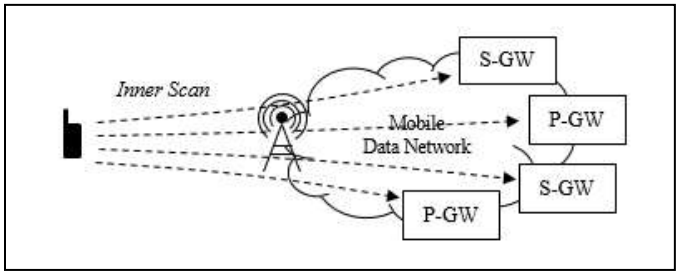


Figure 8. LTE networks scan for security threats

Germany's ERNW gave a presentation of scan attacks using the GTP protocol at the ShmooCon 2011 conference held in January 2011 in Washington DC. It is the key method for scanning mobile network equipment using GTP Echo messages. Special equipment using the GTP protocol interprets the GTP Echo Request message (similar to pinging on IP networks) and responds to it. According to the response, it is possible to check the IP address information of equipment using the GTP protocol inside LTE networks. After all, attackers will know the information on equipment constituting the EPC on LTE networks, which is a basic and important element for identifying targets as an advance preparation for attacks.

B. *Causing Equipment Loads on Networks*

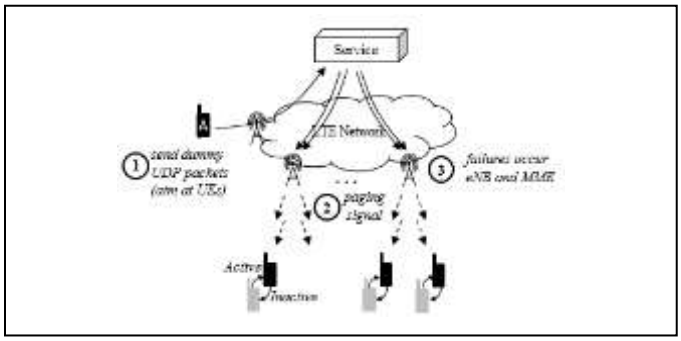


Figure 9. Security threats triggering equipment loads on LTE network

To efficiently use limited wireless resources, LTE networks release the wireless resources of UEs that are not used for a certain amount of time, and the status of the UE with released wireless resources will switch from active to idle. If the idle UE with released wireless resources has data to receive, LTE networks send a paging message to the recent location of this UE and inform it that there is data it must receive. However, if the idle UE does not respond, they extend the paging message transmission range to include MMEs. If attackers use IP spoofing (IP address reuse and communi-

cation between terminals to send abnormal traffic to multiple terminals periodically) a large number of paging messages will be generated and thus cause equipment on LTE networks, such as the eNB and MME, to fail.

C. Data Service Interference

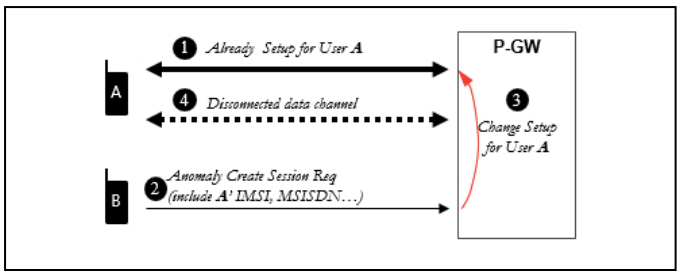


Figure 10. Security threats interfering with data service

If the GTP-in-GTP is abused, it is possible to interfere with data service for certain users. If attackers alter the MSISDN to the MSISDN of another user to generate the Create Session Request message, and send it to the P-GW on the LTE network, the data service for the user with the stolen MSISDN will be stopped. This is because the P-GW regards the GTP message, sent by the attacker, as normal without checking if this message is altered, and the P-GW retrieves the resources allocated to the user with the stolen MSISDN.

D. Abnormal Billing

Figure 11. Abnormal billing security threats

In order to determine billing rates, mobile carriers analyze the incoming and out-going traffic of the P-GW on LTE networks, calculate the data usage of each UE. In general, the IP packet accumulates the size (byte) of the user data and calculates usage. However, individual mobile carriers may have different sizes, serving as the standard for accumulation, and billing policies. If attackers use IP spoofing, IP address reuse and communication between terminals to continuously send data traffic that meets the billing policy of mobile carriers, the data usage of the UE will be increased by as much as the received traffic volume, resulting in abnormal billing.

E. Battery Consumption of Terminals

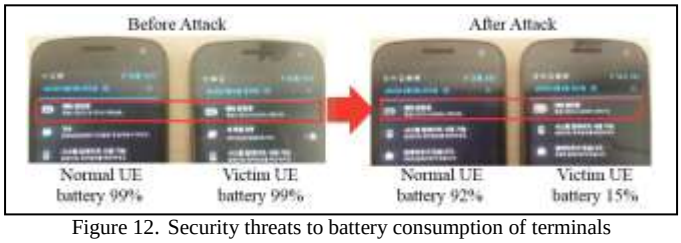


Figure 12. Security threats to battery consumption of terminals

As the UE does not send or receive signaling messages to and from LTE networks when it is idle, the battery can be saved. In contrast, when the UE is ready, the battery consumption will increase, and when data traffic is sent and received, the battery consumption will sharply increase. If attackers use IP spoofing, IP address reuse and communication between terminals to continuously send large amounts of data traffic to a specific UE, the battery of this UE will be consumed rapidly[8].

V. Conclusion

This paper describes the security vulnerabilities of LTE networks and the security threats likely to be caused by attacks abusing such vulnerabilities. On LTE networks, there are various security vulnerabilities, and various threats may be created by such vulnerabilities.

TABLE II. TABLE TYPE STYLES

Security vulnerabilities	*Likely security threats*
GTP-in-GTP	LTE network scan Data service interference
IP Spoofing	Loads on network equipment Abnormal billing Battery consumption
IP Address Reuse	
Communication between terminals	

Recently an increasing number of countries are introducing LTE networks to provide high-speed data services. However, considerations for security seem to be insufficient. The LTE network is a backbone network of the country. If service is stopped due to failures caused by attacks from attackers or abnormal traffic, significant damage or user inconvenience will result, unlike results in the wired environment. Mobile carriers need to check their LTE networks, take measures against security vulnerabilities, including those described in this paper, and protect their LTE networks.

Acknowledgment

This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2014.

References

[1] Peng, Chunyi, Chi-yu Li, Guan-hua Tu, Songwu Lu, and Lixia Zhang, "Mobile data charging: new attacks and countermeasures," in Proc. ACM CCS, pp. 195-204, 2012.

[2] 3GPP TS 23.401, "Evolved Universal Terrestrial Radio Access".

[3] 3GPP TS 29.274, "Evolved General Packet Radio Service Tunnelling Protocol for Control plane".

[4] 3GPP TS32.240, "Telecommunication management; Charging management; Charging architecture and principles," Sep. 2006.

[5] O. Whitehouse, G. Murphy, "Attack and counter measures in 2.5G and 3G cellular IP networks," Atstake Inc.

[6] Dong W. Kang, Joo H. Oh, Chae T. Im, Wan S. Yi, Yoo J. Won, "A Practical Attack on Mobile Data Network Using IP Spoofing," in Proc. Applied Mathematics & Information Sciences, pp. 2345-2353, 2013.

[7] Se K. Kim, Joo H. Oh, Myoung S. Noh, Chae T. Im, "Mobile Network Security Threats caused by Abusing Reuse of IP Addresses and Technology Countermeasures," in Proc. ITC-CSCC, 2014

[8] Denys Ma, Unique Vulnerabilities and Attacks on Cellular Data Packet Services, B.S. Computer Science and Engineering, 2004.