International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:8, 2013

Abnormal IP Packets on 3G Mobile Data Networks

Joo-Hyung Oh, Dongwan Kang, JunHyung Cho, and Chaetae Im

***Abstract*—**As the mobile Internet has become widespread in recent years, communication based on mobile networks is increasing. As a result, security threats have been posed with regard to the abnormal traffic of mobile networks, but mobile security has been handled with focus on threats posed by mobile malicious codes, and researches on security threats to the mobile network itself have not attracted much attention. In mobile networks, the IP address of the data packet is a very important factor for billing purposes. If one mobile terminal use an incorrect IP address that either does not exist or could be assigned to another mobile terminal, billing policy will cause problems. We monitor and analyze 3G mobile data networks traffics for a period of time and finds some abnormal IP packets. In this paper, we analyze the reason for abnormal IP packets on 3G Mobile Data Networks. And we also propose an algorithm based on IP address table that contains addresses currently in use within the mobile data network to detect abnormal IP packets.

***Keywords*—**WCDMA, 3G, Abnormal IP address, Mobile Data Network Attack

I. Introduction

LOOKING at the history of mobile communication, mobile communication started as voice service with focus on AMPS (Advanced Mobile Phone Service), the representative 1G (First Generation) mobile communication, in 1978, and voice and data service began to be provided at the same time with 2G represented by CDMA (Code Division Multiple Access). Afterwards, mobile communication is evolving beyond 3G WCDMA (Wideband Code Division Multiple Access) capable of providing faster data services, and LTE (Long Term Evolution) called 3.9G into 4G mobile communication. Early mobile communication service was developed for voice communication, but as the Internet in the wired environment advanced, demands for mobile service, which provides mobility based on mobile communication service, increased. Accordingly, data networks for providing data communication as well as voice service were added to mobile networks, and voice is processed as VoIP (Voice over Internet Protocol) in accordance with the All-IP communication paradigm. The importance of IP-based data networks is growing gradually.

The data service provided by early mobile networks started out as a type of mobile service provided by communication companies in a limited way, but the advances of the Internet and mobile operating system created a mobile ecosystem. At the same time, mobile networks are open to the Internet, and various services in the wired environment were offered in the mobile environment as well. As a result, the data communication volume of mobile networks increased explosively, and is expected to rise continuously in the future [1].

As the increased traffic includes not only the traffic for various mobile service, but also the traffic in the wired environment that could not be seen in existing mobile networks, unnecessary abnormal traffic also increased. In the conventional wired environment, the increased traffic did not mean much to the receiver unless there are large quantities of abnormal traffic like UDP (User Datagram Protocol) packets and TCP (Transmission Control Protocol) packets, which failed to connect. However, in mobile networks, due to the narrow bandwidth, complicated signaling for management of wireless resources, and operation of limited resources, traffic, which did not matter in the existing wired environment, can become a security threat in the mobile network. Also, aggressive security threats, likely to cause the failure of mobile networks, may cause not only data services, but also voice services to fail unless they are responded to in advance [2].

At present, as most security systems are optimized to IP-based wired networks, they processes mostly IP protocols, and identify send and receive objects based on IPs. However, mobile networks protocols specialized for mobile networks like GTP (General Packet Radio Service Tunneling Protocol) [3], and IP is not the unique value that can identify a user. Also, as abnormal traffic for mobile networks may look different than that for the wired environment, it is very difficult to bring the security systems for the wired environment inside the mobile network. In mobile networks, the IP address of the data packet is a very important factor required for billing. If one mobile terminal use an incorrect IP address that either does not exist or could be assigned to another mobile terminal, billing policy will cause problems. Therefore, we analyze the reason for abnormal IP packets on 3G Mobile Data Networks in this paper. And we also propose an algorithm based on IP address table that contains addresses currently in use within the mobile data network to detect abnormal IP packets. This paper is composed as follows: briefly describes the structure of the mobile network, and Chapter 3 discusses abnormal IP Packets on 3G Mobile Data Networks based on 3G mobile network monitoring results. Chapter 4 proposes countermeasures against these abnormal ip packets, and Chapter 5 presents the conclusion.

II. 3G Mobile Network and Related Works

A. 3G Mobile Network and Related Works

The basic configuration includes the mobile terminal (aka

JooHyung Oh is with the Korea Internet & Security Agency, Seoul, Korea (Phone: 82-2-405-5282; fax: 82-2-405-5129; e-mail: jhoh@ kisa.or.kr).
Dongwan Kang is with the Korea Internet & Security Agency, Seoul, Korea (Phone: 82-2-405-5257; fax: 82-2-405-5129; e-mail: lupin@ kisa.or.kr).
JunHyung Cho is with the Korea Internet & Security Agency, Seoul, Korea (Phone: 82-2-405-5495; fax: 82-2-405-5129; e-mail: scorch@ kisa.or.kr).
ChaeTae Im is with the Korea Internet & Security Agency, Seoul, Korea (Phone: 82-2-405-5540; fax: 82-2-405-5129; e-mail: chtim@ kisa.or.kr).

UE: User Equipment), base stations, and the mobile network for control and communication. In general, from the terminal to the external Internet, the mobile network has the hierarchical tree structure. The closer it is to the outside, the more integrated the components are. 3G network [4] provides data service through UTRAN (Universal Mobile Telecommunication System Terrestrial shown in Fig. 1. UTRAN consists of base stations that communicate with UEs and RNC (Radio Network Controller) that controls base stations. UTRAN communicates with PN, and PN is connected to the external network like the Internet.

B. IP Address Allocation in 3G Mobile Network

The protocols, used in the 3G mobile networks, are separately composed of the control protocol for controlling data communication and the data protocol for transmitting actual data. There are various protocols for communication between complicated mobile network components that perform different functions respectively, and particularly in the data network, GTP-C v1 is used as the core control protocol. In the data protocol, the IP packets sent from UEs are relayed to outside of PN. At this time, the core protocol used in PN is GTP-U. GTP-C v1 and GTP-U vary depending on the message type of GTP.

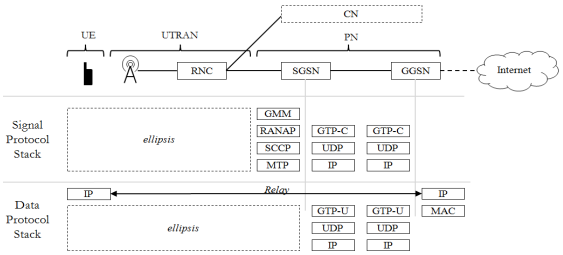

Fig. 1 3G mobile network structure

If a normal user attempts to access the Internet using the 3G data service, the GTP-C message is used to allocate the IP address to the user inside the network, and the user data is sent to the Internet network using the GTP-U message. As shown in Fig. 2, the IP address and tunnel ID possessed by the GGSN (Gateway GPRS Support Node) are allocated, using the GTP-C message transmitted between the SGSN (Serving GPRS Support Node) and the GGSN; the IP address and tunnel ID are sent to the user terminal; and user traffic is sent via the GTP tunnel that is created later on.

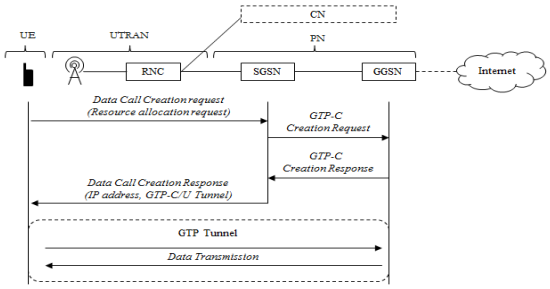

Fig. 2 GTP tunneling setup flow

The GGSN is responsible for the billing. When the GGSN receives data packets generated by user terminal and routes them to the internet. At this time, GGSN generates CDR (Call Detail Record)s based on the obtained IP address information from data packets, which will be passed to the charging gateway and on towards the operator's own billing system. In other words, IP address is a very important factor for billing purposes.

C. Related Works

Mobile networks like 3G and LTE have been monitored and security research projects are underway mostly in Europe, such as Germany and Austria. The DARWIN project [5] was led by Austria, defined unwanted traffic of 3G mobile networks, and conducted researches that can monitor and detect abnormal traffic likely to affect 3G mobile networks [6]. This study was conducted to monitor and analyze failures of mobile networks in various unexpected situations where mobile services are used. ASMONIA [7] was led by Germany which started in 2010. It monitors abnormal traffic of 4G mobile networks and conducts security researches. This study analyzed the security threats of each element of the 4G environment, that is, of each interface between the UE and mobile network components, and the possibility of attacks and repercussions.

III. Abnormal IP Packets on 3G Mobile Data Networks

A. 3G Mobile Network Traffic Monitoring Environment

To monitor 3G mobile data traffics, we develop GTP Packet Capture and Parser System and operate it on the 3G mobile network in Korea. Fig. 3 shows the operating environment. The GTP Packet Capture and Parser system is installed in the Gn interface of the mobile communication service provider. The input of the GTP Packet Capture and Parser system is the traffic tapping the in/ outbound GTP traffic from one of the GGSNs and the input is the traffic of approximately 2.5 million subscribers with an average of 6.5Gbps.

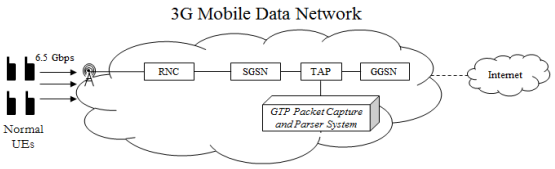

Fig. 3 The monitoring environment

B. Monitoring Results

For the monitoring period (about 7 days), we find 130 million abnormal IP packets, which use a incorrect source IP address that either does not exist or could be assigned to another mobile terminal. Fig. 4 shows some discovered abnormal IP packets.

IMSI	Allocated IP Address	Source IP Address	Destination IP Address	Destination Port
45[redacted]	10.15.182.253	192.168.100.10	211.234[redacted]	53
45[redacted]	10.17.255.152	192.168.100.11	211.234[redacted]	53
45[redacted]	10.17.255.152	192.168.100.11	203.22[redacted]	53
45[redacted]	10.17.255.152	192.168.100.11	168.12[redacted]	53
45[redacted]	10.17.255.152	192.168.100.11	210.220[redacted]	53
45[redacted]	10.17.182.114	10.16.145.171	210.220[redacted]	53
45[redacted]	10.17.211.10	10.13.156.219	168.12[redacted]	53
45[redacted]	10.20.175.43	10.17.55.157	211.234[redacted]	53
45[redacted]	10.15.182.251	10.14.88.249	211.234[redacted]	53
45[redacted]	10.15.182.251	10.12.162.31	211.234[redacted]	9900

Fig. 4 The monitoring result

Most of abnormal IP packets were DNS requests sent by mobile terminal. As you can see Fig 4, even though mobile networks allocate the private IP range starting with 10.x.x.x, source IP address of abnormal packets use another IP range such as 192.x.x.x. Also, some source IP address of abnormal packets use correct IP range, but IP address is actually incorrect. In other words, there are 2 type of abnormal IP packets in 3G mobile networks. The first one is that they use non-exist IP address and the second one is using an incorrect IP address.

C. Abnormal IP Packets Cause Analysis

To analyze causes of abnormal IP packets, we experiment with two scenarios: 1) Transition from 3G to Wi-Fi, 2) Switching from airplane mode to normal mode during the mobile internet surfing.

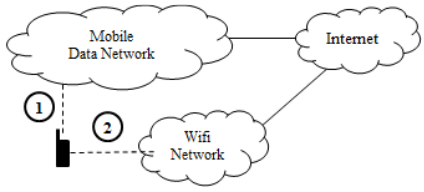

Fig. 5 Test scenario

If mobile terminal translates from 3G to Wi-Fi, then a new IP address is assigned to mobile terminal and mobile terminal does not connect 3G mobile network anymore. However, during the first scenarios test, we find that mobile terminal sends data traffic to 3G mobile network for a moment even if it is not connected 3G mobile network. We think that it is caused by mobile terminal software error. Also, when mobile terminal switch airplane mode to normal node, a new IP address allocation process is started as described in section 2.2. However, during the second scenarios test, even though mobile terminal has been received a new IP address, old IP address which is assigned is used for a moment. In conclusion, abnormal IP packets are caused by discordance of IP address Information between mobile application and network driver of operating system.

IV. Approach for Abnormal IP packets Prevention in Mobile Network

To detect abnormal IP packets in the mobile network, we must check if the source IP of the user packets transmitted by the Outbound GTP-U packet in the GTP tunnel section is valid. The process of generating the GTP tunnel using GTP-C v1 as an example is roughly illustrated in Fig. 6. To collect the valid source IP of the mobile terminal, it will be necessary to monitor IP address allocation.

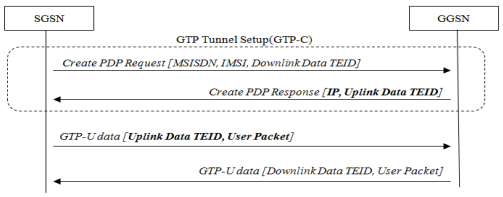

Fig. 6 Information exchange during GTP tunnel setup

To create the GTP tunnel, SGSN use the UE information (MSISDN, IMSI, etc.) regarding which UE the tunnel is for, and assign the IP the UE will use in response. TEID exists separately for each UE depending on directionality and packet type (GTP-C/GTP-U). When creation of a tunnel is requested, TEID (Downlink Data TEID) for sending data to the UE will be sent as well, and the response will include TEID (Uplink Data TEID) used for the data the UE sends outside. Accordingly, while the GTP tunnel is generated, depending on the direction in which the UE sends data, TEID to be used and the IP to be used by the UE will be determined. Accordingly, we can use the GTP tunnel information to detect abnormal IP packets as shown in the Fig. 7.

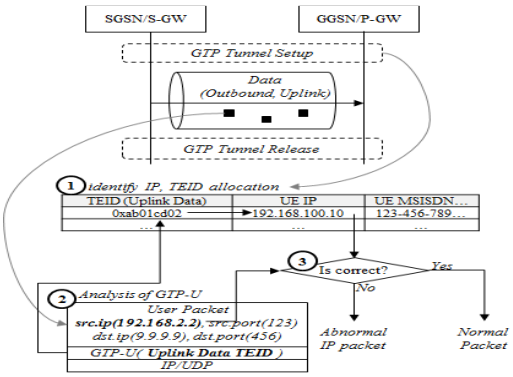

Fig. 7 Scheme for abnormal IP packets detection

V. Conclusion

In mobile networks, the IP address of the data packet is a very important factor for billing purposes. If one mobile terminal use an incorrect IP address that either does not exist or could be assigned to another mobile terminal, billing policy will cause problems. In this paper, we monitor and analyze 3G mobile data networks traffics for a period of time and finds some abnormal IP packets. Also, we describe why abnormal IP packets are happened. Most of abnormal IP packets on 3G mobile network are caused by discordance of IP address Information between mobile application and network driver of operating system. For example, when the mobile terminal translates suddenly from 3G to Wi-Fi, data packets sent by mobile terminal will include incorrect source IP address used for Wi-Fi network. To prevent abnormal IP packets, we presented a method of utilizing the GTP tunnel information,

used in the mobile network. Also, we are planning to develop a system for detecting and preventing abnormal IP packets on 3G mobile network.

ACKNOWLEDGMENT

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013

REFERENCES

[1] CISCO, Global Mobile Data Traffic Forecast 2011-2016, Cisco Visual Networking Index (VNI), 2012.
[2] F. Ricciato, P. Svoboda, E. Hasenleithner, W. Fleischer, On the impact of unwanted traffic onto a 3G network, Proceedings of the Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006, pp. 49-56.
[3] 3GPP, GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 10), TS 29.060 V10.2.0, 2011.
[4] H. Holma, A. Toskala, WCDMA for UMTS - Radio Access for Third Generation Mobile Communications (Willey, 2004).
[5] DARWIN Project, http://www.ftw.at/ftw/research/projects/
[6] F. Ricciato, Traffic monitoring and analysis for the optimization of a 3G network, Journal of Wireless Communication, Vol. 13, 2006, pp. 42-49.
[7] ASMONIA Project, http://www.asmonia.de/