International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:11, 2011

Security Threat and Countermeasure on 3G Network

Dongwan Kang, Joohyung Oh, Chaetae Im

***Abstract*—**Recent communications environment significantly expands the mobile environment. The popularization of smartphones with various mobile services has emerged, and smartphone users are rapidly increasing. Because of these symptoms, existing wired environment in a variety of mobile traffic entering to mobile network has threatened the stability of the mobile network. Unlike traditional wired infrastructure, mobile networks has limited radio resources and signaling procedures for complex radio resource management. So these traffic is not a problem in wired networks but mobile networks, it can be a threat. In this paper, we analyze the security threats in mobile networks and provide direction to solve it.

***Keywords*—**3G, Core Network Security, GTP, Mobile Network Security

I. Introduction

PRESENT communications environment with the proliferation of smartphones in a variety of mobile services are being spread. Existing Wi-Fi mobility is relatively limited, but the 3G network with high mobility than a Wi-Fi environment was provided. And smartphones and mobile devices as a platform for change in general (android, iOS) and the popular dissemination has done, it was possible based on a variety of mobile services.

Unlike traditional wired infrastructure, mobile networks has limited radio resources and signaling procedures for complex radio resource management. So these traffic is not a problem in wired networks but mobile networks, it can be a threat. If provide mobile services that moved from a traditional wired network services (messenger, etc.) are required to be connected anytime, and that can be an inefficient waste of limited radio resources. In addition, a narrow bandwidth of conventional wired infrastructure was not a significant problem, unnecessary traffic (scanning traffic and malicious traffic, etc.) a waste of resources, it can interfere with other users [1].

Recent connection between heterogeneous networks (mobile network and wired network) is sharing mutual security threats. Especially compared to the existing wired network, mobile network security for various abnormal traffic technologies was not ready. Mobile networks as a communications facility is viewed as a national infrastructure, because if it can be backed up with appropriate security technologies by hackers can be a victim of cyber terrorism, economic and social loss for mobile operators will be greater. We analyze the security threats in mobile networks and provide direction to solve it. In this paper, Chapter 2 overview of 3G mobile networks, Chapter 3 defines the security threats in mobile networks. Chapter 4 introduces the related research and Chapter 5 we introduction about security framework to develop for mobile network.

Dongwan Kang is with the Korea Internet&Security Agency, Seoul, Korea (South) (e-mail: lupin428@kisa.or.kr).
Joohyung Oh is with the Korea Internet&Security Agency, Seoul, Korea (South) (e-mail: jhoh@kisa.or.kr).
Chaetae Im is with the Korea Internet&Security Agency, Seoul, Korea (South) (e-mail: chtim@kisa.or.kr).

II. Introduction Of 3G Networks

A. Structure of 3G Network

In Fig. 1, 3G network, which consists of two main elements, circuit network (CN) for voice communications and packet network (PN) for data communications. And there are RAN that related to wireless connectivity, and the system for authentication and billing functions [2].

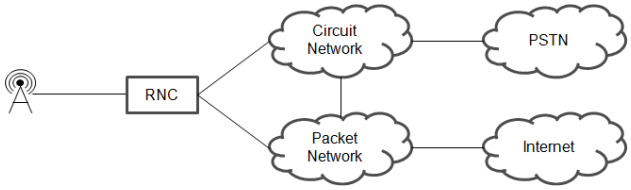

Fig. 1 Structure of 3G Network

The Radio Network Controller (RNC) manages radio resources for radio access, and Serving GPRS Support Nodes (SGSN) is responsible for management and support services in the PN. Gateway GPRS Support Nodes (GGSN) perform IP allocation for UE and support communication between PN and the external Internet network. Between each device uses a different protocol and tunneling. Between RNC and SGSN is called "Iu-PS" section usually used an ATM protocol, and SGSN and GGSN is called "Gn" section use the GPRS Tunneling Protocol (GTP) (ref. Fig 2). GTP is an IP-based protocol for tunneling between GGSN and SGSN. GTP can be categorized as GTP-U for the packet data, GTP-C for signaling, GTP ` (prime) for billing [3].

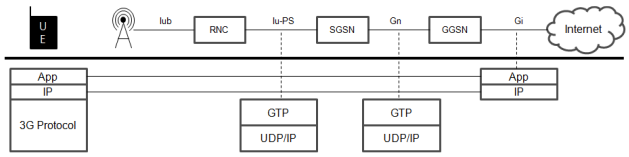

Fig. 2 Structure of 3G Protocol Stack

B. Mobile Terminal

Mobile terminals (aka UE; User Equipment) are information device that can communicate using 3G mobile networks. UE is representative of the smartphones but includes a variety of devices like laptop and tablet recently. In particular, variety UE that have not function for 3G mobile communication but have function for Wi-Fi communication can communication via 3G mobile networks using a tethering feature of smartphone.

Depending on the type of UE differed for the traffic. After all incoming traffic through 3G mobile networks are not only the smartphone but also multiple devices such as notebooks and netbooks. Thus, previously not seen in a mobile environment the traffic will now be observed in various forms.

III. Security Threat in 3G Network

Mobile networks have several features compared to traditional wired environment, it have relatively narrow bandwidth and limited radio resources, and complex signaling protocol for resource management. So these traffic which is not a problem in wired networks but mobile networks, it can be a threat [1].

A. Resource Consume of UE

Portable mobile device power management is very important. All work performed by the device is leads to power consumption, so if there are many unnecessary process, it will be leads to the consumption of power. In these cases, there are two broad, the first continuous communication, and the second is the high cost of process periodically.

First, in the case of resource consumption due to ongoing communication caused by an abnormal service continued communication and continuous communication with malicious host by infected with malicious code. In particular, the UE that is infected with malicious code continuous scanning to inside the network, the internal various UEs resources can be consumed unnecessarily at the same time.

In the second case, the allocation and release of radio resources for a short cycle can resource consumption [4]. In order to communicate via mobile networks, the base station must assign a radio resource to the UE, but each base station can allocate the limited radio resources. Therefore, the base station allocates radio resources to the UE, after a period of time if there is no communication from the UE then releases the previously allocated radio resource.

The allocation and release of radio resource is very high task from the perspective of the UE. The state transitions are sketched in Fig. 3. The timer automatically turn off the wireless resource is called t, (t that can decide the value of the carrier), this t, if the attacker can constantly send packets over a slightly longer period then t, these can cause the radio resource re-allocation when released repeatedly. Once this process is repeated, the UE's resources are largely consumed.

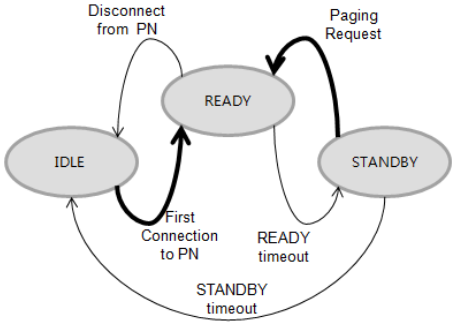

Fig. 3 UE State on 3G mobile network

B. Resource consume of mobile network

Compared with wired networks, mobile networks have a complex protocol stack, so mobile network is higher cost required in order to processing than wired network. Recently, Mobile networks receptive traffic to the inside that existed in the wired network, such as unnecessary traffic and malicious traffic scanning. In a wired network, a specific target for attack is important, but the existence of such traffic in mobile networks, can be viewed as an attack on network.

Radio resources of a mobile network can be seen as an important resource for each base station has limited radio resources. Thus, one base station is limited to accommodate the UE, so UE need to assign radio resources when the communication only and if there is a certain amount of time with no communication and then return to make it available to the other UE.

But if attacker sent packet to any mobile device with anomaly timer that has a shorter period then nomal timer t, the RNC keep radio resource to mobile device, and the UE will occupy the wireless resource and prevent use for other UEs. A small number of these abnormal communications from the UEs may not be serious, but voice and data services may fail of the area that covered by single base station if a large number of UEs rise at single base station.

C. The abnormal termination of Connected Service

The Messenger service is the most common connection-oriented services. In order to use instant messaging services connect with the server must be maintained. This connection to the regular communication is maintained for a period of time if you do not have a connection attempts to reconnect. The message service in a mobile environment while having the advantage of mobility has become a major mobile service. Communication between the PC as the existing constraints of mobility, but the mobile environment by using the 3G data network, while having high mobility can send and receive messages in real time.

Mobile messaging services emerged as the leading mobile killer service became mandatory. However, the mobile network takes a serious problem by the abnormal termination of service if messaging service is designed without consideration for the mobile environment. Abnormal termination of service, the UE will cause a continuous retry. In the attempt to reconnect the individual UE position is not a big problem, but the sides of mobile network it will be centralized at the request from the whole UE. And after a certain time, a time period of attempts to reconnect server is getting a short cycle and eventually all UE are constantly try to reconnect at the same time.

In this process, potential threats can be viewed as a three-part. In the first, UE resource is consumed by the repeated reconnection attempts, and the second occupying the wireless resource by repetitive reconnect to the service as short a period of time. The third, the RNC and the SGSN will be a failure by massive retries in a short time. In particular, centralized massive retries a short time can make a DDoS attack effect such as "SYN flood" attack to mobile network. In particular, a RNC is closely related both a data service and voice service, so the

failure of RNC will lead to the failure of both data and voice services.

IV. Related Research

Research on mobile networks security has been conducted in Europe. The METAWIN project [5] was research on the security threat of 3G mobile network in Austria since 2004. The purpose of METAWIN project was to develop a monitoring system for 3G mobile network, and to deploy it real field in Austria, and to analyze traffic in order to understand a nature of data traffic flows in 3G mobile network. In 2005, DARWIN project which the followed project of METAWIN was researched about collect and analyze data traffic to detect the abnormal behavior. Actually, DARWIN project is based on the results of a series of previous project started with METAWIN launched in 2004. In DARWIN project was handled a number of issues related to performance monitoring, anomaly detection and security aspects in the 3G network[6].DARWIN project performed a study of security threats and mobile network traffic monitoring, analysis method, and a study on the detection of abnormal traffic. They discuss the unwanted traffic, and pointed out the problems of resource consumption in 3G mobile network[1].

In order to analyze this phenomenon, the DARWIN project propose Traffic Monitoring and Analysis(TMA) infrastructure based on passive wiretapping at key network link. And research results show that not only the mobile networks cause failure by some abnormal signaling or paging traffic, but also can be detected based on practical experience with the analysis of real data[7]-[8].

V. Countermeasures

Compared with wired networks, wireless networks have a variety of security threats because a special feature of mobile network such as limited radio resource and narrow bandwidth. Although, one could apply of existing security equipment which IP based, but it cannot cover the core network in 3G mobile network. Therefore, we need optimal security system for the 3G mobile network. In Fig. 4, the security system can be divided into three parts, the first traffic acquisition system, the second abnormal traffic detection system, and finally control system that can monitoring and control for detected mobile device based on detection information.

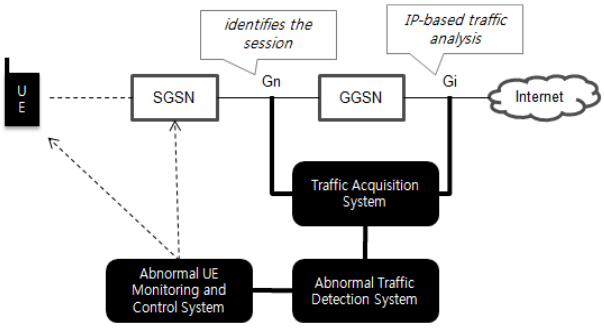

Fig. 4 Framework for optimal security system for the 3G mobile network

A. Traffic Acquisition System

The role of traffic-acquisition system (TAS) is to collect useful information from the traffic in PN. The Acquisition point will be Iu-PS, and Gn, Gi which main interface of PN and TAS designed able to analysis each communication session.

The main protocol architecture (see Figure) include: The main protocol are GTP-C, GTP-U, GTP`, GTP-C protocol use control the states of UE, GTP-U protocol use practical send and receive data. GTP` protocol use create CDR is used for the billing data.

In order to analyze end-to-end communication must see the inside of the tunnel because tunneling between the components of mobile network. In addition, the header for tunneling causes reducing the size of the entire PDU and fragmentation of packets. This phenomenon makes packet reassembly difficult. Therefore, we consider identifies the session at Gn interface, and IP-based traffic analysis at Gi interface. If traffic acquire at other interfaces except Gn, Gi interface, these case are on the costly disadvantages because required more financial and technical cost while more detailed monitoring is possible about the signaling and data traffic.

B. Abnormal Traffic Detection System

Abnormal traffic detection system consists of the two engines. One engine detects the engine has already revealed attack and other engine detects unknown abnormal traffic.

In terms of the network anomaly detection, there are false-positive and false-negative on the premises, so we need the clearly detected for known attack and more fine-grained analysis for the unknown anomaly attack detection. Anomaly Detection studied previously is based on the analysis of one-dimensional distributions of certain features across individual mobile users. However, the rapid growth of the mobile environment, we need to be verified result for depending on the nature of the carriers of each country.

In addition, we need consider recent trends in mobile services, and research should proceed according to the type of service, it is basis of selective detection measures.

C. Abnormal UE Monitoring and Control System

The monitoring and control system is responsible for control phenomenon caused by abnormal UE, based on detection information. Monitoring of the UE due to issues of privacy, collection and detection, and control systems cannot identify who the actual users, so only need to uniquely identify users by other information such as hash table, and also blind payload of the packet.

We need to control a UE which serious affect to availability of mobile networks. The control method of UE are use the delete function of the Android`s official provides that “Remote Application Removal”, or sinkhole the destination of malicious traffic as a basic countermeasures may be considered.

In addition, if an emergency situation, force blocking for data communication or control of HLR to temporarily prevent the authentication of the UE as an extreme way. But more important, control of the UE is a forced act for the actual user, so we need sensitive approach.

VI. Conclusion

Unlike traditional wired infrastructure, mobile networks has limited radio resources and signaling procedures for complex radio resource management. So these traffic is not a problem in wired networks but mobile networks, it can be a threat. Wireless networks have a variety of security threats because a special feature of mobile network such as limited radio resource and narrow bandwidth.

The security threats of 3G mobile networks cannot to solve even develop into LTE, LTE Advance, and 4G. Development of mobile networks is enhancing the current narrow bandwidth, but not enough to cover ever-increasing data traffic currently.

Therefore, we need optimal security system for the 3G mobile network.

We research the security system which can detect and countermove, and research future potential security threats for 4G. In addition, when the prototype is complete, we will have as a performance verification of security systems for mobile networks on real field.

Acknowledgment

This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency) (KCA-2011-11914-06001).

References

[1] F. Ricciato, E. Hasenleithner, P. Svoboda, W. Fleischer, "On the impact of unwanted traffic onto a 3G network," in *Proc. Security, Privacy and Trust in Pervasive and Ubiquitous Computing(SecPerU)*, June, 2006.

[2] H. Holma, A. Toskala, *WCDMA for UMTS - Radio Access for Third Generation Mobile Communications 3rd.* Willey, pp.95-96, 2004..

[3] 3GPP, "GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 10)," *TS 29.060 V10.2.0*, June, 2011.

[4] S. Jeremy, Z. Hui, B. Jean C, "Impact of paging channel overloads or attacks on a cellular network," in *Proc. WiSe '06 Proceedings of the 5th ACM workshop on Wireless security*, New York, Sept, 2006.

[5] DARWIN project. http://www.ftw.at/ftw/research/projects.

[6] F. Ricciato, "Traffic monitoring and analysis for the optimization of a 3G network," *IEEE Wireless Comm.* vol. 13, pp. 42-49, Dec, 2006.

[7] F. Ricciato, E. Hasenleithner, P. Romirer-Maierhofer, "Traffic Analysis at Short Time-Scales An Empirical Case Study From a 3G Cellular Network," *IEEE Trans. Network and Service Management,* vol. 5, .No. 1, pp. 11-21, March, 2008.

[8] V. Falletta, F Ricciato, F. T. Wien "Detecting Scanners: Empirical Assessment on a 3G Network," *International Journal of Network Security,* Vol.9, No.2, pp.143-155, Sept, 2009.