GTP Security in 3G Core Network
GTP Security in 3G Core Network

Xuena Peng1,2, Wen Yingyou1,2, Zhao Dazhe1,2, Zhao Hong1,2
College of Information Science and Engineering1, Education Ministry Engineering Research Center for Safety and Security of Complex Network System2, Northeastern University Shenyang, China
email: {pengxm, wenyy, zhaodz, zhaohl}@neusoft.com

Abstract—Nowadays, 3G network plays a very important role in mobile communication system. But the security concern of such network, especially the core network, is far from being satisfied. GPRS Tunnel Protocol (GTP), which is one of the key protocols in the core network, is quite vulnerable to attacks in the flat, full IP environment. Therefore solving such problem properly is very urgent and important for the operation of 3G network. In this paper, a security analysis of GTP is presented, a defense solution for these security threats and an event-based description language are also proposed. The experiment result shows the potential of our solution.

Keywords—3GPP; core network; security; GTP; event-based description language; Intrusion Prevention System

I. INTRODUCTION

With the fast deployment of 3G system in the world, 3G-based applications will be a very prospective field in the next a few years. While more and more applications and services are provided by countless providers in the 3G network, the security of these applications as well as the fundamental 3G system will become one of the most important concerns of the public.

In fact, 3G system has its unique security problems that are not quite similar with the security problems of either the traditional GSM system or the IP network[1]. With the introduction of IP techniques to the mobile communication system, 3G system becomes more open, more flexible, and provides more interfaces to the other systems, but at the same time it is also more vulnerable. The vulnerabilities come from two sides. On one hand, the widely use of IP techniques breaks the technical barriers in the core network, so that the vulnerabilities hidden in the traditional system may be absolutely exposed in a full IP-based 3G system. On the other hand, the vulnerabilities of IP techniques may also be introduced into the 3G system, so that the security vulnerabilities of the system are further increased.

As a result, 3G security is one of the most important concerns as to 3GPP. TSG SA WG3 is a dedicated work group in researching the 3G security issues. TS21.133[1] and TS33.200[2] are some of their products. In TS21.133, the threats and requirements of 3G security are briefed, and in TS33.200, the security issues of both the access network and the core network are discussed. Although 3GPP have made many efforts in 3G security, generally speaking, most of current efforts are focused on the 3G radio access network (RAN), while the security issues in the core network (CN) have been under estimated. With the complexity and importance of the 3G core network, more efforts should be made to ensure its security.

There are three kinds of 3G core network techniques, namely TD-CDMA, WCDMA and CDMA2000. TD-CDMA and WCDMA are developed from GSM system, and they inherit GPRS (General Packet Radio Service) techniques in their core-network, which means, in these two 3G systems, GPRS network is responsible for connecting the internet with the system; while CDMA2000 gets rid of the GPRS transformation, and connect the internet directly with PSTN devices. To make it clear, in the context of this paper, we only focus on the security of the GPRS core network, and the term core network is commonly used to infer GPRS core network if not explained specifically.

Not many researches have been done in protecting the core network. A. Prasad discussed the infrastructure security of 3GPP-UMTS network[3]. K. Boman proposes the MAPSec-based 7 signaling MAP protection, IPSec-based IMS SIP protection and WTLS-based application data protection schemes[4]. Unter Schafer focuses on the DOS and privacy issues in the IP-based core network[5]. Xiaoming Fu discusses the security implications of the session identifier[6]. C. K. Dimitriadis has proposed honeynet solution to secure 3G core network[7].

Since protocols are one of the most important scheme that make system work as expected, it is considered a possible solution to protect the network through protecting the protocols. In our point of view, among all the protocols used in the core network, GTP (GPRS Tunnel Protocol) is considered to be the most important protocol, for almost all user operations, protocols and data are carried by GTP. GTP is an IP-based tunnel encapsulation protocol in the GPRS core network, and it is an important transforming scheme to connect the PLMN with other networks (including the Internet).

While the design of GTP is lack of security concern, there are no embedded security schemes in GTP, so it has very obvious security vulnerabilities which can be easily exploited by attackers. With the widely usage of GTP, attacks toward this protocol could come from different directions, such as the air interface, internet and other PLMN (Public Land Mobile Network), so the attacks could make very huge damage not only to the core network infrastructure, but also to the internet and mobile users. According to this issue, in this paper, we briefly analyze the security issues of the GTP protocol in the first place, then, we propose a defense solution based on an event-based attack detection engine, and finally, the prototype system and experiment results are presented to show the effectiveness of such solution.

II. GTP SECURITY ANALYSIS

A. A Brief Introduction of GPRS and GTP

GPRS network techniques was first introduced to WCDMA in R99, developed in R4, R5, R6, R7/R8, and currently, they are still on the way of evolution. The GPRS core network is the kernel part of the GPRS system, it provides support for WCDMA and TD-CDMA based 3G networks. In 3G networks, the GPRS core network provides mobility management, session management, and transport for Internet Protocol packet
services. Besides, it also provides support for other additional functions such as billing and lawful interception. Fig. 1 shows the general logical architecture of GPRS network. For simplicity, some of the secondary function nodes are ignored in this figure. In this architecture, the core network mainly refers to the sub network composed of SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). Both SGSN and GGSN are known as GSN, which supports the use of GPRS in 3G core network. All GSNs should have a Gn interface and support the GPRS tunneling protocol. SGSN stands for Service GPRS Support Node, it is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. GGSN stands for Gate GPRS Supporting Node, it is responsible for the interworking between the GPRS network and external packet switched networks, like the Internet. GGSN can be viewed as a router to a sub-network, for it hides the GPRS infrastructure from the external network. Besides, it also plays an important role in mobility management and packet forwarding between the core network and external network.

![Figure 1. GPRS logical architecture with interface name denotations](image)

GTP is the most important carrier protocol suite in 3G core network. It stands for a suite of IP-based communication protocols used to carry GPRS within GSM and most 3G networks. Primarily it is the protocol which allows end users of WCDMA or TD-CDMA network to move from place to place while continuing to connect to the Internet as if from one location at the GGSN. It does this by carrying the subscriber's data from the subscriber's current SGSN to the GGSN which is handling the subscriber's session.

GTP can be decomposed into separate protocols, GTP-C (GTP control plane), GTP-U (GTP user plane) and GTP (GTP prime). GTP-C is used within the GPRS core network for signaling between GGSN and SGSN. This allows the SGSN to activate a session on a user's behalf (PDP context activation), to deactivate the same session, to adjust QoS parameters, or to update a session for a subscriber who has just arrived from another SGSN. GTP-U is used for carrying user data within the GPRS Core Network and between the RAN and the CN. GTP uses the same message structure as GTP-C and GTP-U, but has an independent function. It can be used for transfer of charging data from GSNs to the charging function.

### B. GTP Security Issues

The design of GTP is lack of security concern, and there are no embedded security schemes in GTP, so it has very obvious security vulnerabilities which can be easily exploited by attackers. Typical attacks range from over billing attack to infrastructure attack. Basically, GTP security issues can be classified as followings.

1) Protocol abnormal attack. This kind of attack often generates abnormal or damaged PDU packet, or PDUs not comply with the protocol. GTPowerGTP is a typical attack of this category. DoS or other impacts may be caused by this kind of attack.

2) Infrastructure attack. The impacts of this kind of attack often include illegal access of the infrastructure devices, such as SGSN, GGSN, OAM system and mobile terminals. By modifying his own address, the attacker can connect with the core network, and encapsulate attack packets into GTP, thus attack any mobile targets or targets from other network.

3) Resource consumption attack. This kind of attack can be raised from both the terminals and other network. SYN attack is a typical attack of this category. The impact of such attack may often be denial of service.

For protecting GTP from the above security issues, we consider that GTP traffic analysis and filter could be a possible solution. And in the next section, we will describe the solution in detail.

### III. Defense Solution for GTP

#### A. The Event-based Description Language

In order to analyze and filter the GTP stream more flexibly and more efficiently, we have introduced an event-based description language. In this context, event refers to any possible activity which can be detected in the packet or packet stream, and attack refers to a single malicious event or a serial of malicious or non-malicious events formed in a certain logic pattern to implement a malicious aim. The language that we propose is a simple script language which can be used to define the logic of the application protocol as well as that of the attacks. When application level protocol analyzer is defined in our event language, the underlying event engine can analyze the corresponding traffic according to the definition of the protocol and generate the events for further inspection. Besides, it can also be used to maintain the protocol state and deal with the security events. When an attack signature and logic is defined in our language, the underlying event engine can analyze the incoming event generated by the protocol analyzer according to the attack definition, and take action when attacks are detected. By unifying the description of the protocol and attack in the same descriptive manner, the system’s extensibility can be easily improved. By coupling protocol analysis and attack detection tightly in the runtime, the system efficiency can also be improved. Besides, by defining application protocol in this language, we simply need to focus on the protocol logic while let the event engine to deal with other less relevant processing details.

There are two categories of event in the context of our attack description language, namely atom event and abstract event. Atom event refers to the very specific event that is generated by the protocol analyzer module, such as “UDP event”, while the abstract event is made of one or several events (atom event or abstract event), the purpose that we introduce abstract event is to indicate any serials of atom events with different intensions, so that we can use the most proper abstract event to describe the attack.
In our language, we use “Atom” and “Event” as the key words to describe atom event and abstract event respectively. They can be used in the following style:

```
Event <type> abstract_event;
Atom <type> atom_event;
```

In GTP protocol description, when describing an atom event, such as SIMPLe IE, we can put it in the following pattern:

```
Event struct hdr_v0 SIMPLE_IE;
```

In which, `struct hdr_v0` is one of our predefined GTP_v0 data structure, and `SIMPLe IE` is an atom event which refers to a GTP_v0 packet with Information Element (IE).

When defining more abstract event, we need to use rules. Rules can be used to define the logic among events. A rule is composed of four parts: the left part, operator, the right part, and the action part. The following example shows what a rule looks like:

```
BAD_LONG_GTP_V0 : header_v0 ($1->gtp_hdr_v0_len >=160) {  
  GTP_v0_deny($0, "fault length header! Len = %d\n,  
  $1->gtp_hdr_v0_len); }  
```

The left part of the rule is composed of an abstract event, which is viewed as the object to be defined in the rule. In this example, it is the abstract event `BAD_LONG_GTP_V0`. The right part of the rule is composed of one or more events (including both atom event and abstract event) with predicates, in this example, is an atom event `header_v0` with a predicate `$1->gtp_hdr_v0_len >= 160`. The ':' in the middle of the first line is the operator of the rule, meaning the abstract event at the left part is a sum up of the events at the right part. So the whole line 1 indicates that when a header_v0 event with it parameter gtp_hdr_v0_len no less than 160 is detected, then `BAD_LONG_GTP_V0` event can be generated.

Lines 2-5 are the action part of the rule. `GTP_v0_deny` in line 3 is the rule action, which is enforced when the abstract in the left part is generated. In this example, when a `BAD_LONG_GTP_V0` event is generated, the action `GTP_v0_deny` should be enforced, and then the system will simply deny and discard the corresponding abnormal packet.

B. System Architecture of Intrusion Protection for GTP

Based on the event-based description language and event analysis engine, we propose a GTP IPS to protect GTP protocols against attacks. The architecture of the GTP IPS is shown in Fig. 2.

There are mainly four modules in this architecture. One is for system initialization and the other three are for runtime analysis.

The Language Interpreter is mainly used to fulfill the initialization and configuration phases of the system. During system initialization, it translates the GTP protocol scripts and attack scripts into event engine based GTP-X Analyzers and GTP Attack Detectors, and these analyzers and detectors are to be used to analyze GTP protocols and attacks during runtime.

The runtime GTP analysis and filtering scheme is implemented by three modules:

- **GTP Stream Filtering Engine** is implemented by a set of parallel processing hardware, which can perform simple analysis and filtering of thousands of packets simultaneously. Parallel analysis and filtering can assure the secure packets to pass through the system as soon as possible, without affecting the overall performance of the system.

- **GTP Event Analysis Engine** is composed of three parts: GTP Packet Parser (also Atom Event Generator in the context of event engine mentioned in III.A), GTP Protocol Analyzers and GTP Attack Detector. The GTP Packet Parser parses the incoming GTP packets according to the protocol specification at the lexical level, distills the essential protocol elements, encapsulates these protocol elements into “Atom Events”, and submits them to the corresponding protocol analyzers. The GTP Protocol Analyzer then matches the atom events to the predefined rules, which are predefined either by default or by the users, and generate various “Abstract Events” to facilitate further protocol analysis and attack detection. The system default rules are defined according to the various 3GPP specifications, such as R5, R6 or higher versions. The GTP Attack Detector finally analyzes the attributes of the relevant “Abstract Events” generated by GTP Protocol Analyzer, and examines whether the signatures of the attacks are existed.

- If attacks are detected, the Responder Module will be responsible for dealing with the reactions, such as logging, alerting, dropping the packets, and etc. If the relevant packets are to be dropped, the GTP Stream Filtering Engine is responsible for enforcing the corresponding action, as well as maintaining and updating the protocol state of the relevant GTP tunnel.

![Figure 2. GTP IPS Architecture](image)
C. Signalling Message Analysis and Detection for GTP-C

The protection for the signaling message of the GTP control plane is of the most importance for securing the GGSN and SGSN node in the core network. So in this paper we take the protection for GTP-C as an example to illustrate how the system actually works.

The signaling messages of the GTP control plane are composed of path management messages, tunnel management messages, location management messages, and mobility management messages. In our GTP protection system, the detection for GTP-C oriented attacks is performed by the GTP-C specific Event Analysis Engine, which includes GTP Packet Parser, GTP-C Analyzer and GTP Attack Detector.

*GTP Packet Parser* can perform the message parsing for GTP-C protocol, and examine the protocol abnormality according to the protocol specification. It usually generates one header and several IE atom events for each GTP message, and submits them to the corresponding analyzer in the parsing sequence. The parser only parses and distills the type of each IE, such as TLV or TV, but does not parse the detail segments in the IE message. It is up to the *GTP-C Analyzer* and the *GTP Attack Detector* to decide whether to parse the details or not.

After the packet parsing phase, the atom events are encapsulated and submitted to the upper modules to be further analyzed. The *GTP-C Analyzer* and the *GTP Attack Detector*, which are automatically generated by the protocol and attack detection scripts, are used to detect protocol abnormality and specific attacks. These two modules guarantee the validity and security of the GTP messages passing through the GTP IPS, and avoid possible attacks to the protocol and system vulnerabilities.

In order to guarantee the validity of the state of the GTP messages, PDP context information must be maintained and synchronized with the GGSN and SGSN. So in the whole analysis and detection process, a PDP context record is set up for each created and in use tunnel, and is updated whenever the signaling message passes the corresponding tunnel. The PDP context record is indexed in the data structure of binary tree, and it is indexed by each tunnel direction (up stream and down stream). In this way, the stateful protocol abnormal detection is implemented. Besides, this stateful scheme can also be used to support the extended protection and system maintenance.

IV. EXPERIMENTS AND RESULTS

Based on the architecture that is proposed in section III, a GTP IPS prototype system is implemented. Currently, the prototype system supports deep analysis and filtering functions for both GTP-C and GTP-U, and GTP protection will also be supported in the future.

![GTP IPS Experiment Environment](image)

**Figure 3. GTP IPS Experiment Environment**

![GTP IPS output in different experimental scenarios](image)

**Figure 4. GTP IPS output in different experimental scenarios**

The evaluation of the system is a very important phase to validate its functionality. Currently, since it is unrealistic to test our prototype system in a live GPRS system, the best way to test it is to carry out the experiments under the lab environment. Fig. 3 shows the emulation environment for testing the system. We employ OpenGGSN emulator suite[8] to emulate the
SGSN and GGSN nodes in the GPRS network. To emulate the protocol abnormal attack, we also implement a GTP packet generator to generate various abnormal GTP packets with incorrect headers or IEs as well as attack packets. For testing the functionality of GTP IPS prototype system, we deploy the device between the SGSN and the GGSN so that GTP messages can be intercepted and filtered.

A serial of experiments have been set up to evaluate the validity of the GTP IPS. For GTP-C protection functioning, the experimental scenarios include message filtering, abnormal message detection, access control, and traffic control; for GTP-U protection functioning, the experimental scenarios include content auditing and GTP-in-GTP attack detection. The experiment results show that the system can work correctly under all these scenarios. Fig. 4 shows some of the system output in different experimental scenarios.

V. CONCLUSION

The security of core network is very important to the overall healthy of 3G network. Since GTP is the protocol to tunnel user data across the core network, its security detrimentally affects the operations of the whole 3G network. In this paper, we have analyzed the security issues of GTP protocol suite in detail, proposed a event-based GTP IPS as a countermeasure to protect this key protocol suite, and also evaluate the prototype system in various scenarios. The experiment results show that the system can work pretty well under lab environment. In the future, we will embody more functions to the system as well as improve the performance of the system. Besides, we will also try to evaluate the system in a more real environment.

ACKNOWLEDGEMENT

This work is under the sponsorship of NSF of China, with the grant ID of 60602061 and 60803131.

REFERENCES