Security Analysis of Public Security Terminal Network and Its Peripheral Equipment

Yuqiang WU 1*, Yubao WU 1 and Wengan Yang2

1 Department of Information and Technology, Nanjing Forest Police College, Nanjing, Jiangsu, 210023, China
2 Shaoxing Public Security Bureau, Shaoxin, Zhejiang, 312000, China
*Corresponding author’s e-mail: wuyq@nfpc.edu.cn

Abstract. As a major focus of global Internet security, peripheral equipment security is getting more and more attention. Due to the serious asymmetry between the high access level and the low protection level of the public security network and its peripheral equipment, it is very easy to be attacked by hackers. This paper briefly describes the Internet of things access technology, introduces the public security terminal network interconnection access mode and part of the network topology. Based on the preliminary analysis of the security of the software and hardware of the public security terminal network and its edge equipment, this paper analyzes the security of the public security terminal network and its peripheral equipment for the subsequent security design, to ensure the reliability of the public security terminal network and its peripheral equipment, and to strengthen the network security of the public security terminal network.

1. Introduction
Nowadays, cloud computing, big data, artificial intelligence and other emerging technologies are constantly recognized by the public and gradually enter our daily life. Under the policy of vigorously promoting information power in our country, the construction of public security information system really lags behind the process of social information construction[1]. Multiple pressures and objective reasons lead to the increasing tasks and tasks of Cyberspace Security Maintenance in China. How to ensure the security of cyberspace and protect the normal operation and system security of the public security terminal network more efficiently and comprehensively has become one of the current research topics of network security, science and technology information and other departments of public security organs and major Internet Security enterprises.

2. Preparatory knowledge
2.1. Peripheral equipment
The peripheral equipment mentioned in this paper refer to the devices used to provide high-level network forwarding control and the server devices used to provide services at the top level, that is, the network packet traffic passing through such devices will only have two directions: one is sent back after being processed by the device itself, which refers to the peripheral equipment of server type; the other is sent to other peripheral equipment after being horizontally forwarded If the target device and the source device are all under the same peripheral equipment, the data packet can be sent directly
from this peripheral equipment without forwarding to other peripheral equipment. The schematic diagram of Internet peripheral equipment is shown in Figure 1. It can be said that the Internet has the logic structure function of these peripheral equipment, which can build the network business we use today.

![Figure 1. The schematic diagram of internet peripheral equipment.](image)

2.2. Peripheral equipment of public security terminal network

The term "peripheral equipment of public security terminal network" has not been defined generally and clearly. This paper defines it as: the computer network equipment built by public security organs to provide public security terminal network services and located at the edge of the network. Combined with the description of the peripheral equipment in the previous section, the peripheral equipment of the public security terminal network specifically refers to the large-scale services such as police landing, information query and event registration and reporting provided for the public security mobile terminal, including the border router, network gate, firewall, business server (including server cluster) built by the public security organ, except the network equipment provided by the network link operator Network devices.

Due to the infeasibility of the basic network links such as mobile equipment base stations built by the police, such a wide range and deep mobile network link can only be provided access services by the mobile service operators[2]. Once the physical network link of the operator is used, all the physical network devices from the base station to the peripheral equipment built by the police are connected with the Internet. We refer to the physical "hard connection" here. Although there are related technologies described below to realize the "soft separation" of the traffic and business dual networks, the dual networks are not physically isolated. The characteristics have a great impact on the security and reliability of public security mobile devices and peripheral equipment to a large extent, which has greatly hindered the subsequent security design. It can also be said that because of the fact that there is a physical connection, we need to strengthen the security design on the basis of the original protection, and turn all non-identification access out of the door, even to one Some malicious visits are used for anti-tracking, providing clues and evidence for the fight against cyber crime and Internet black industry.

3. Public security terminal network architecture

As mentioned above, the current public security terminal network is accessed by the Internet of things GPRS/4G service of the operator, and APN is provided by the cooperative operator. Starting from GPRS/4G communication technology, this chapter focuses on the current public security private network communication connection mode and related network topology.

3.1. Internet of things business

Internet of things business is a customized module with GPRS/4G online and online functions for Internet of things, such as NB IoT (narrow band Internet of things), which can be directly deployed in
3.2. Access mode of mobile terminal

The authentication we mentioned here is realized through SIM card. Many people think that SIM card is only used for dial-up call of mobile phone. Sim consists of CPU, ROM, ram, EEPROM and I/O circuit. When users use SIM, in fact, the phone sends commands to the SIM card. The SIM card should be executed or rejected according to the standard specifications, not just the information memory. In the process of using SIM card, the most important configuration is APN. Each SIM card needs to enter APN for communication through verification.

APN refers to access point name, that is, access point name. It is the name of a gateway between a GPRS or 4G mobile network and another computer network (usually the Internet). It is used to define the network path of all mobile data connections on the mobile device, and to identify the GPRS/4G service type. After using the SIM card, the wireless terminal accesses through the specific APN, resolves through the DNS domain name, and finally accesses the private application server of the company through the GGSN network element. Due to the uniqueness (authentication) of SIM, to a certain extent, it guarantees the security of the access subject, at the same time, it encrypts the data transmission, and uses different soft network links to isolate the public network[3], to a certain extent, it guarantees the security of the data transmission process. But in the third chapter of this paper, we will focus on the analysis of this kind of network access insecurity.

3.3. Operator APN and public security network APN

The Internet of things APN includes two types: General APN and special APN. The special APN can be divided into tunnel connection and special line connection through the connection between GGSN and private server of the company.

General APN refers to the use of Internet of things general APN "CMMTM". The terminal access mode of general APN is similar to that of ordinary mobile phone. For public network business, the access process sequence is BTS, BSC, SGSN, private network GGSN, operator Internet access point and access to operator Internet.

Special APN tunnel mode refers to the use of Internet of things special APN " CMIOTXXX ". Compared with general Internet access, in the early stage of access process, BSS link is still used (BSS is the general term of BTS and BCS). After SGSN and GGSN are used, a public network tunnel is established through operators or companies to connect operators' Internet with group customer data center (server). The operator's private network access generally provides the company's customers with the GRE VPN private network service based on GPRS network, which is based on L2TP, the second layer tunnel protocol. Generally speaking, compared with general Internet access, this terminal Internet access mode has security authentication mechanism and access control, but it still needs to intervene in the public network to use static IP, which means that all Internet users can directly connect to the server.

3.4. Network topology of public security terminal network

The whole network of the public security network has the characteristics of "flattening", the connection is not limited by the region and police types, and the access is only limited by the level and authority. Due to the unity of public security services, there are relatively high requirements for the synchronization and interaction delay of terminal network data. The service terminal network server can not keep on-line and synchronize data to the internal network environment. If it chooses direct access, it will create huge pressure on the performance of the core server, and it will also give hackers and illegal organizations a chance to take advantage of it. Therefore, in the actual environment, the
terminal network is usually equipped with a gateway to control the closure. Initial screening analysis and filtering are conducted for the incoming traffic, and interaction is allowed after confirming that the data contains the encrypted legal identification. Besides the terminal network, there are security system and operation management system to monitor the data and network status of the dual network.

4. Security analysis

Through the above analysis, we know the peripheral equipment of the public security terminal network and part of the topological structure of the public security terminal network. With these foundations, we start to conduct a preliminary analysis of the security of related equipment. This chapter analyzes the link security of operators and the security of peripheral equipment of public security terminal network, and it is carried out from two aspects of physical equipment security and system software security.

4.1. Security analysis of physical link

Because the current chain routing operator is responsible for the link security, also known as the operator's link security, strictly speaking, because of the "flat" design of the public security network, any reachable device can send data to the target server, so we will process the data from the terminal device to the public security terminal network server, and return to the original terminal. Link security is analyzed[4].

The terminal first establishes a connection with the base station through a similar NB IOT module, communicates through GPRS / 4G, and uses a special SIM card for authentication and authentication. In the next stage, for SGSN and GGSN gateways, since both are only connected to BSS devices downward, and there is no public IP assigned, only address access between device links will be allowed, and the possibility of trying to establish a connection from forged trusted BBS to SGSN is almost zero.

However, the attack feasibility of the edge router of the operators including the south north edge gateway (North South GGSN) is also very low. Although the mechanism of authentication of the edge router is weaker than that of the SGSN link in order to ensure the forwarding rate and response speed, the edge router needs to allocate the network traffic with different source attributes to different target routers through the APN access point name, which In one step, we also call the "soft separation" of traffic and business dual networks. Many types of traffic and destination traffic pass through the same physical device, but they are isolated from each other and cannot be accessed. At present, the most basic one can be realized at a low level by dividing different VLANs.

After the operator's basic link, the authorized and legal traffic will be connected to the public security equipment through the operator's Internet special line. Because the virtual special line / routing technology itself is controversial, a special communication line is established on the Internet through a special encrypted communication protocol, but a real optical cable and other physical lines are needed. For the link security of operators, generally speaking, due to the huge traffic volume, the filtering level of data is relatively low. Using eavesdropping or simulation to bypass APN verification, intrusion traffic can enter the backbone link and cannot be verified and searched. There are also attacks through router and other operators' equipment vulnerabilities, but the feasibility is relatively low and the cost is high[5]. According to this, we can draw a preliminary conclusion that in the security of the operator's link, the bypass and intrusion from the terminal is one of the main means to attack the public security terminal network and its peripheral equipment.

4.2. Security analysis of peripheral equipment in public security terminal network

In the public security terminal network, the so-called equipment security is the peripheral equipment security of the public security terminal network. For the security of peripheral equipment, we analyze the UTM protection devices such as firewalls and IPS and the devices provided by servers through the workflow of devices. Generally speaking, the security of equipment is often analyzed from three aspects: physical security, software security and surrounding equipment security. In the process of
actual evaluation and analysis, it is generally conditional to test and analyze the security of the device from the two perspectives of "known vulnerability verification" and "protocol fuzzy test". For the gateway and service data conversion equipment, these equipment will not actively identify the data itself, but will file the legal traffic and illegal traffic (misinterpreted data in case of APN analysis error). If the selected legal traffic is selected, it will enter the internal network and data exchange link through the gateway after the service data conversion. Relatively independent physical isolation makes it much safer than other online network devices, and does not consume network resources and local computing and storage resources.

For firewall equipment, because of its relatively single function, it mainly controls the flow of network data in and out. According to the flow control rules and flow filtering conditions set by users, it blocks and discards unauthorized data to ensure that the flow leaving the firewall is legal, so as to achieve the purpose of protecting the equipment behind the wall. However, due to the relative fixity of firewall, it has its inherent vulnerability. Once the firewall type is identified by the attacker, the attacker can find the firmware download of the corresponding firewall version and conduct a detailed offline analysis to find the firmware vulnerability and implement the attack. Because the firewall itself is also carried on the operating system, some firewall devices that cannot be updated in time are likely to suffer from vulnerability attacks against the operating system. For example, the "eternal blue" incident of wannacry, which has caused a great stir in recent years, is an attack against the operating system leak.

For IPS devices, as the name of "intrusion prevention system", they can defend against intrusion traffic and behavior, use online services and transparent ways to work as firewalls, disassemble traffic packets for analysis, and fill in the gap that firewalls and other devices can only work on the first to fourth layers of the network. However, due to the attributes of the public security network, China's public security terminal network is unable to connect the open virus database and vulnerability database online and respond to the global attack mode in real time[6]. At present, although Microsoft has provided a more convenient "online" update for free, so that end users can download and install the latest patches in time. However, the level of automation of the patch update service provided by itself is not high. In addition to the requirements of relevant configuration on the client side, the patch installation process also needs user configuration. The so-called timeliness is often compromised due to the slow network speed. If the end user computer is in the LAN, the online update service cannot be used at all. At the same time, due to the confidentiality of LAN level of public security network, the installation package of system update patch at the beginning of "KB4" provided by office needs to be reviewed by the superior department and integrated in the next generation of recognized system image version, so it is difficult to conduct real-time defense against the network attack based on a CVE vulnerability in the global Internet outbreak, and we can hardly believe that Wannacry is in flood, the relevant operation and maintenance personnel of the public security network didn't find out, and we guessed that they could not start more[7].

For the core code of the service, in the aspect of web, due to the strong pertinence of the public security terminal network service business, it generally focuses on query and report, and relatively few operations of modification nature, which also reduces the intrusion against the background SQL database to a certain extent, but because the page has more interaction and feedback, it is easy to cause XSS and other attacks on users through web page logic vulnerabilities.

For example, the hosting core of Web services, such as Apache, nginx and tomcat, will be updated with the version, and some global vulnerabilities will be found and exposed more or less in the old version of services. However, because some front-end development code will also be inconsistent with the new version, after the server operation and maintenance personnel communicate with the developers, the relevant department leaders may choose to ignore the update and continue to use the old version, which leads to the existence of the hidden dangers of the core vulnerabilities of Web services. In addition to the above key issues, in the current network attack means, for the non-public network similar to the public security network, physical intrusion is also a means. Here, it is not
necessary to directly penetrate the central computer room (edge server), but only the equipment that can connect to the specific network.

To sum up, the security analysis of the edge equipment of the public security terminal network and the public security terminal network is summarized as follows: first, in terms of links, as the carrier's network carrying capacity is far stronger than other access point server links, the main direction of attack and penetration of hackers or illegal organizations is terminal security vulnerabilities. In terms of system and software, although there are many aspects to attack, there are also aspects from firmware to service core, from authority control to port forwarding. The attack on server port, web logic vulnerability and new operating system level vulnerability has become an effective way to attack the public security terminal network accessed by APN.

5. Future work
After the preliminary analysis and research on the security of the public security terminal network and its peripheral equipment, we need reliable, credible and safe solutions and Countermeasures for the possible risk points and high-risk loopholes. And the implementation of this strategy must be carried out with point to area and three blockages simultaneously, so as to eliminate network attacks to a large extent. In the future, we will do the preliminary design of targeted security model for the above three high-risk directions.

Acknowledgments
Supported in part by National First-class Undergraduate Major (Network Security and Law Enforcement) Construction Project; in part by Jiangsu Brand Major (Network Security and Law Enforcement) Construction Project; in part by Central University Basic Scientific Research Business Fee Special Fund Project (LGYB202011).

References
[1] HUI Xinya, LIU Jianhua, LIU Hao. Construction and Analysis of Network Security Situation Awareness Model Based on Colored Petri Nets[J]. Computer and Digital Engineering, 2019, 47(2): 393-401.
[2] FreeBuf.2020 Network Security Industry Trend Forecast[EB/OL].https://cloud.tencent.com/developer/article/1582068,2020-1-5.
[3] Yan Yaping, Hu Yong. Analysis of CSRF vulnerability detection, utilization and prevention [J]. Communication technology, 2017, 50(03): 558-564.
[4] Hu Hongfu. Research on WAF bypass method and test framework [D]. Wuhan University, 2017.
[5] Meng Zhen. Design and implementation of HTTPS monitoring system [D]. Qingdao University of science and technology, 2018
[6] YUAN Yuan, SUN Fuchun. Secure the Control System Against DoS Attacks: A JDL Data Fusion Method [EB/OL]. https://ieeexplore.ieee.org/document/6997694, 2019-12-10.
[7] LIU Zhongqiang, YU Chengli. Exploring the Security Defense Strategy of Computer Virus in LAN from Wannacry Blackmail Virus[J]. Security Science and Technology, 2017(6): 18-21.