Research on security risks and countermeasures of IPv6 network in the new era

Bo Feng[1], Chuanzhong Xie[2],Chao Wang[1], Zhipeng Luo[2]
1.Jiangxi Branch of National Internet Security Administration Center, Nanchang 330038, China
2. Jiangxi Branch of China Telecom Corporation Limited, Nanchang 330029, China

Abstract: In recent years, with the development of new infrastructure, especially the needs of 5G, Internet of Things, cloud services, data centers and other incremental large-scale construction, these "new increments" can be completely based on IPv6, or even pure IPv6 deployment to improve quality, reduce costs, and increase efficiency. Therefore, in the process of constructing IPv6 network, how to ensure the overall security and stability of the network, and do a good job of network security protection and risk response to the maximum is very important. Based on this, this paper studies the security risk points of IPv6 network protocol and puts forward several security countermeasures for reference.

Key words: New era; IPv6 network; Security risks; countermeasures

1. The network security situation faced by IPv6 networks

From the perspective of technical factors, with the development and popularization of network technology, new means of network attack keep emerging, and the means of attack are more covert, complex and diversified. For example, injecting backdoors into Web applications can easily achieve the purpose of data theft, which also makes the attacker easily control the network system. And in the IPv6 network environment, attackers can use the new technology to carry out attacks and gain more benefits. In addition, the address assignment and access control mechanisms of IPv6 are very different from those of IPv4. As a result, attacks on IPv6 networks are more subtle and sophisticated.

From the perspective of human factors, with the continuous increase and expansion of Internet application scenarios, many criminals use network security vulnerabilities to carry out attacks such as malware transmission, stealing secrets, and malicious traffic analysis. With the deepening of people's attention to information security issues, criminals use these vulnerabilities to carry out data theft, information leakage and other attacks. In addition, with the continuous increase and expansion of Internet application scenarios, organized and premeditated denial of service attacks are gradually increasing. For example, injecting backdoors and backdoor programs into Web applications is to control the target host.

In short, the current situation of IPv6 network security in China is very serious:

First of all, attackers use the defects and vulnerabilities of IPv6 protocol itself to attack. With the large-scale application of IPv6 network in China and the replacement of IPv4 protocol in the world, the vulnerabilities and defects are increasing, which leads to the opportunity of attackers to exploit these defects and vulnerabilities.

Secondly, the research on IPv6 network security in China is still in its infancy. Because there is no institution or organization specifically for IPv6 network security to carry out systematic research work, China's understanding of IPv6 network security issues is not comprehensive, not in-depth, not thorough, not comprehensive and other problems are very prominent.

2. The main threats faced by IPv6 networks

2.1 Internet Protocol vulnerabilities

The IPv6 protocol contains multiple packet headers, but it is not secure in itself, and the packet headers are also vulnerable to attacks during transmission, resulting in the leakage of the entire network information. In IPv6, there are a large number of vulnerabilities, which are easy to be exploited by attackers. Attackers can use these vulnerabilities to attack the network, causing serious problems in the transmission speed and transmission quality of the network, thereby reducing the user experience. In view of these security vulnerabilities, you need to take measures to protect.

2.2 Denial of service attack

There are a large number of denial-of-service attacks in IPv6 networks, which can be used by attackers to disrupt and destroy the communication of target users. In an IPv6 network, an attacker can achieve access control over a target user if the IP address of the target user can be obtained by the attacker. If the attacker uses tunnel technology, the target user can obtain the control information through the tunnel. In addition, the attacker can also disrupt and destroy the communication of the target user through the network.

2.3 Malware attacks

There are a large number of malware attacks in IPv6 networks, which can steal the account passwords and personal privacy information of target users. If the attacker obtains the target user's account password and other information, he will use the information to control the target user, so as to achieve the purpose of attacking the target user. In addition, the attacker can also use the tunnel technology to control the target address and then send the data to the malicious server, so as to achieve the target user access control and other attacks.

2.4 Data eavesdropping and tampering

There are a large number of data eavesdropping and tampering attack methods in IPv6 networks, which will affect the theft and tampering of network data transmission. The first is data eavesdropping, the attacker can use the tunnel technology to intercept the data and transmit it to its designated location; The second is data tampering, the attacker can modify and tamper with the data packets received on other nodes in the network. Finally, data theft, attackers can collect and steal data packets received on other nodes in the network.

3. The main security risks of IPv6 networks in the new era

IPv6 network has a strong openness, but it also brings great security risks. The security risks are as follows:

3.1 Security risks of the client

1. User equipment. User equipment is the core of IPv6 network, and its security risks mainly include two aspects: First, the security vulnerability of the device, which is the security hidden danger of the user device itself, easy to be exploited by hackers; The second is the improper use of the user, the user device is prone to security problems in the operation process, resulting in the disclosure of user information.

2. Network application. Network application is an important part of IPv6 network, which mainly includes IPSec, TLS and other protocols. The use of these protocols requires a lot of network resources. Due to the large number of addresses and address formats in the IPv6 network, problems such as address conflict are easy to occur in network applications, which leads to the abuse of some IP addresses. In addition, there are also a large number of attack means in IPv6 network, which leads to some criminals can attack IPv6 network through various attack means. Therefore, it is very important to strengthen the security management of user devices in IPv6 network.

3.2 Security risks at the network end

1. Risk of IPv6 address spoofing. In the IPv6 network, there are a lot of address spoofing problems, attackers can use forged IPv6 addresses to deceive the target host, so as to achieve the purpose of spoofing.

2. Risk of address theft. Attackers can obtain the IP address of the target host through illegal means, and steal and steal it to achieve the purpose of attack.

4. Routing hides risks. On an IPv6 network, an attacker can use the route hiding technology to attack the target host and hide its real IP address.

3. The risk of malware transmission. At present, the security of IPv6 network is relatively lower than that of IPv4 network, and there are more vulnerabilities and security loopholes, which is the main reason for the increase of security risk of IPv6 network.

4. Unauthorized access risks. The encryption algorithm and encrypted tunnel technology used in IPv6 network are all designed based on IPv4, which makes IPv6 network vulnerable to various attacks. In practical applications, attackers can attack IPv4 networks and use tunnel technology to attack IPv6 networks.

3.3 Security risks on the business side

In the current IPv6 network, there are a lot of services, including: access control, data flow audit, network traffic monitoring, security policy configuration, security protocol verification and so on. These services will be directly exposed to the IPv6 network, and these services are the most vulnerable places in the IPv6 network. On the service side, there are the following attack modes:

1. Route attack: On the service end, attackers can use tunneling and NAT technologies to translate IPv4 addresses into IPv6 addresses, and then spoofing IPv4 addresses to attack services.

2. Traffic attack: On the service end, attackers can analyze service data flows to find security vulnerabilities and attack modes, so as to attack services.

3. Security protocol verification: On the service side, attackers can use encryption algorithms and tunnel technology to translate IPv4 addresses into IPv6 addresses. However, the attacker cannot detect these applications.

4. Countermeasures for IPv6 network security risks in the new era

At present, in the construction of IPv6 networks, there are many security risks. Therefore, a series of security measures should be taken to deal with the possible security problems. In response to current security risks, the following measures should be taken:

4.1 Strengthening IPv6 network infrastructure

In the construction of IPv6 network, various technical means and measures should be adopted to improve the security of IPv6 network infrastructure. The first is to strengthen the security transformation of the existing IP devices and IP protocols, improve the address planning scheme of the IPV6 network, rationally allocate IP address resources, and improve the security of addresses. The second is to strengthen the security transformation of IPv4 network equipment, routers, servers and other equipment to improve the security of the equipment; Finally, it is to deploy the necessary security protection equipment in the IPv4 network, such as firewall, VPN, etc., to ensure the security of IPv6 network data.

4.2 Strengthen management and monitoring of IPv6 network security

In the construction of IPv6 networks, it is necessary to clarify the responsibilities and obligations of IPv6 network security management entities, and establish and improve the IPv6 network security management system. First, a special management system and process should be formulated at the initial stage of IPv6 network construction to regulate the related behaviors in the process of IPv6 network construction, operation and maintenance. The second is to strengthen the supervision of IPv6 network operating units and standardize the behavior of operating units in IPv6 network. Finally, it is to carry out real-time monitoring and management of the completed IPv6 network to discover

and deal with security problems in time.

4.3 Strengthening security protection of IPv6 mobile Internet applications

First, a large number of malicious programs spread and proliferate through the mobile Internet, causing serious harm to users; Second, there are a large number of data eavesdropping, tampering and attack threats on the mobile Internet; Third, there are a lot of malicious programs using the mobile Internet to spread, attack and so on.

First, strengthen the supervision and testing of new media applications such as apps and wechat public accounts; Second, strengthen the supervision and testing of important infrastructure operators and providers such as communication operators, cloud service providers and information service providers; Third, strengthen the protection of users' personal information to ensure that users' personal information is not leaked or abused; Fourth, strengthen the security testing and management of mobile Internet services and applications involving important fields such as national security, national economy and people's livelihood; Fifth, strengthen the security testing and management of mobile Internet services and applications involving important national security and social and public interests; Sixth, strengthen the security testing and management of mobile Internet services and applications involving sensitive information such as state secrets, trade secrets and personal privacy.

4.4 Raise awareness of personal protection

In the construction of IPv6 network, the protection awareness of individual users should be raised in various ways. First, install security protection software on mobile Internet devices; The second is to install security protection software in the mobile operating system; The third is to improve the ability of personal user information security protection through the automatic identification technology of mobile phone terminal and fingerprint recognition technology; The fourth is to set the boot password through the mobile phone terminal to protect the security of personal user information; The fifth is to set up a "blacklist" system to limit the behavior of not resetting the password; Sixth, to protect the security of personal information through legal means.

Epilogue

At present, the development of IPv6 network is still in the early stage, but IPv6 network has become the development trend of future network. Due to many advantages of IPv6 network itself, IPv6 network has a huge advantage in application and promotion in China. However, in the actual application process, there are still many security problems. Therefore, how to solve the problem of IPv6 network security and improve the security of IPv6 network is an important problem to be solved at present. This paper analyzes the current security risks, and puts forward corresponding countermeasures and suggestions. In short, with the continuous development and progress of next generation Internet technology and application, IPv6 network will be more and more secure.

References:

[1] Qiuyan Gao. Research and Implementation of IPv6 Network security based on universities [J. Information Systems Engineering,2021(2):55-56.

[2] Zhen Xu,Yanni Han. Analysis of IPv6 network security risks and countermeasures [J]. Journal of North China Electric Power University (Social Science Edition),2018(7):51-53.

[3] Yu Zhai, Maierdan Ruzi. About IPv6 Security risks brought by networks and countermeasures [J]. Digital Communications World, 2019,22(8):153-154.