Analysis of IPv6 network security risk points and security guarantee countermeasures

Heping Yu[1], Jian Liu[2], Bo Feng[1], Yicong Li[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, the construction of 5G, Internet of Things, cloud computing and data center has been strengthened, and the application of IPv6 has become more and more extensive. New information technology can be developed on the basis of IPv6. In the IPv6 construction, how to ensure the security and stability of the whole network is an important topic worth discussing. In this paper, the IPV6 network protocol and the working principle of IPV6 expansion and analysis, and on this basis, the analysis of IPv6 network may exist security risks, and give the corresponding security countermeasures.

Key words: IPv6; Security risk; safeguards

IPv6 is an internationally recognized solution for the commercial application of the new generation of Internet with a growing user base. Information technology has played a strong role in promoting the construction of IPv6. In fact, IPv6 can be understood as the foundation of the current and future development of information technology. If the security of IPv6 is compromised, then the security and stability of the new infrastructure will be threatened. Therefore, it is necessary to analyze the common security risks in IPv6 network protocol, and create a set of scientific and reasonable security prevention system and countermeasures to avoid affecting the overall network performance and implementation effect, so as to strengthen IPv6 network security protection.

1. IPv6 network protocol

In late 2011, IPv6 began to be enabled on a large scale, and it is a great improvement over IPv4.

(1) Address space

Compared with IPV4, IPV6 address space has been improved, at the same time, IPv6 also has a network prefix, can be calibrated to the subnet, thus expanding its subnet address, can further make up for the IPv4 network address fewer defects, that is to say, IPv6 can be understood as having an approximate infinite address space, Without the need to rely on NAT like IPv4 to expand the address space, at the same time, the huge address space can realize the hierarchical division of the network silk, reduce the scale of the routing table.

(2) Packet structure

Compared with IPv4, the IPv6 message structure is also optimized and the message content is further enriched. For a variety of protocols, IPv6 can be well partitioned, and can be stored independently, so that the protocol header can be processed quickly, and the configuration is flexible, making the packet processing efficiency is higher, and more services are supported. For IPv6 networks, the use of IPsec protocol can achieve end-to-end security, and can effectively ensure security between various ports. In addition, IPv6 enhances the mobility of mobile terminals, reduces the operation difficulty of deploying networks, and effectively realizes the automatic configuration of IP addresses.

(3) Support level

The continuous deepening of IPv6 protocol provides new ways, new ideas and new directions for improving network management and security innovation mechanism, and realizes the accurate management of network addresses, encryption and traceability of data transmission. However, since the transmission characteristics of IPv6 network have not changed, there are still a series of security problems to be solved in its practical application. For example, for the new IPv6 network protocol, the transition evolution technology from IPv4 network to IPv6 network still needs to be further developed, and there are certain security risks in the application management of IPv6 network protocol and the functional support level of equipment.

2. IPv6 service network security risks

(1) Several security risks in IPv6 Internet networks

At present, the IPv6 network protocol has been strengthened in the initial design of security considerations, but still can not completely avoid security risks. First of all, the large address can alleviate the current address tension, but the massive address space will also cause great challenges to the security of the cryptographic algorithm, but also make the large-scale address query work more difficult. Secondly, the flexible expansion of packet contents and new traffic signatures improve the packet processing efficiency and provide personalized services. However, it is also vulnerable to security attacks such as NDP attacks and route redirection attacks, resulting in data interception or tampering.

(2) Several security risks exist when IPv4 and IPv6 coexist in the network

IPv4 and IPv6 network protocols are not compatible, the two can not directly communicate, the current construction of the network protocol uses the evolution of the transition from IPv4 to IPv6, in the transition process of IPv4 to IPv6, there are inevitably some technical vulnerabilities, and once these technical vulnerabilities are used by attackers, They bypass the security monitoring to attack the network.

There are three main types of transition protocols: dual stack protocol, tunnel mechanism protocol, translation mechanism protocol. In the dual-stack environment, the attack caused by the defect of any of the two logical channels of IPv6 and IPv4 will be based on the nodes of the dual-stack network and propagate between the two logical channels, directly affecting the network; In the tunnel mechanism environment, because many existing networks can not be fully upgraded, so it is necessary to establish an automated tunnel to access IPv6 through the client or router, such a tunnel exit router will become the target of the attacker, if its tunnel node is attacked, it will cause a great threat to the security of the entire network. In the Transmission environment, DDOS attack is the most common one, it can create a large amount of NAT data, so that the Transmission node can not be assigned to the normal user of Transmission, thus to the whole network security caused a great threat.

(3) Technical risks and management risks of IPv6 network

In the existing network, a large number of IPv4 users and terminals are still in the IPv4 environment, and IPv6 only occupies a small part, forming an "island" in the local area, and most of the network equipment only support IPv4, even if some network equipment began to introduce IPv6, but the application of IPv6 is relatively weak. The security protection ability is limited. Therefore, the large-scale construction and use of IPv6 is likely to bring a series of security problems. In addition, due to the huge capacity of IPv6, it does not need the help of NAT, and can provide unicast addresses for users around the world without relying on NAT. However, this will make IPv6 unable to provide the security guarantee of NAT, and its huge address space brings great difficulties to user allocation and management. In the actual management of IPv6 network, there is a lack of systematic management mechanism and scientific management mode, so it is impossible to protect the security of IPv6 network through sound and reasonable management measures. In the future, the IPv6 network management mechanism and management mode need to be further developed.

3. Security issues in IPv6 deployment

In the work of accelerating the deployment of IPv6 network, a security risk defense system based on IPv6 network protocol should be effectively built, so as to ensure the security and stability of all aspects in the subsequent network planning and construction process.

1. Optimize the security management system

(1) Equipment upgrading. The current network equipment still has some security problems for some functions of IPv6, therefore, the future technical personnel need to further carry out comprehensive security protection and debugging work for the equipment to enhance the security of network equipment. (2) Functional requirements. When using the firewall, it should be combined with the work needs, adopt feasible transition technology, integrated into the application layer gateway, meet the IPv6 analysis, identification and virus detection and analysis, and create a dual-stack application scenario that supports the coexistence of IPv4 and IPv6. (3) Performance indicators. In the IPv6 packet structure, different IPv6 headers should be encrypted. For packets containing multiple extension headers, more detailed and careful processing should be carried out to enhance the degree of data encryption, especially when the extended header packet is abnormal, it is necessary to update its performance. (4) Strategic requirements. Enhance network security protection through dual-stack configuration, and carry out security demand analysis and control for different logical channels, that is to say, further strengthen the consistency check ability on the basis of mastering security policies. (5) Carry out network security inspection. Attach importance to network security inspection work, apply security detection tools to carry out network security monitoring, correctly understand the scheduling strategy in the use process, and take targeted optimization measures according to the security inspection results. Secondly, when using the relevant special testing tools, it is still necessary to focus on the corresponding testing and analysis of IPv6. (6) Carry out security network monitoring. It is necessary to establish a comprehensive and close correlation between the handling methods and measures of some security problems such as anti-virus and malware in use at this stage and IPv6, and then collect statistics on various risk issues to form a security threat rule base as comprehensive as possible for analysis and summary, so as to conduct future security investigation and hidden danger handling. Better find targeted, scientific and reasonable various types of network security detection and protection technology.

2. Effective strategies to prevent hacker intrusion

At present, there are some security loopholes in the application of IPv6, which have a great impact on the overall security of IPv6 system. Therefore, it is necessary to work out targeted prevention and control strategies according to the characteristics of various network attacks.

(1) Strengthen the protection capability of the network itself, adopt appropriate border protection technology, and repair the security defects in the network protocol in time. Due to the huge number of IP addresses, this paper studies a network security attack defense method based on IP addresses. At the same time, IPv6DNS can enhance the security of DNS according to specific network operation requirements, realize reasonable backup of DNS, and effectively cope with attacks, which provides a good solution for new problems and challenges brought by IPv6 network.

(2) When the IPv6 network and IPv4 network are dual stacks, the firewall system and security attack defense device should be updated. According to the specific performance and positioning characteristics of the firewall, the firewall should be set outside the egress router or between the egress router and the Intranet, and combined with the performance and positioning of the security defense device. So as to play a certain role in protecting the risk of security attacks.

3. Ways to improve data security

As an upgrade of IPv6, privacy protection technology plays a huge role in ensuring user security. When users start using IP headers, it is easy to add a new extension header to extend IPv6. The MAC address in the IP packet may be partially encrypted, hiding the mac address

of the client, which is data encryption at the network layer. At the application level, Microsoft's USA Privacy Extension technology enables certain MAC addresses to be hidden under new operating systems, making upgrading easier.

4.FieldGuide

When IPv6CryptedCriteria is used, the data will be encrypted. Because IPSec's cryptographic mechanism can serialize FIM protection, and the password is freely selected, the password is not disclosed, so the firewall cannot obtain the TCP/UDP port number. If the firewall exposes all encrypted packets, it cannot prevent external users from accessing services that should not be provided. In this way, when a host in the network accesses an external node from the network, the data can be anonymously tracked and intercepted. When the external data enters the firewall, the original data will still be retained.

5.FBI

Some intruders may exploit vulnerabilities in the protocol itself to attack it. To prevent such attacks, it is necessary to strictly control the protocol deployment, IP address extension header, etc., to minimize the number of packets, so as to prevent such attacks. Intrusion detection (InfraredDetectionSetting, IDS) is a new type of firewall function. Since all connection requests cannot be denied, the firewall is only identified by another ID mask. Based on the detected data source, intrusion prevention systems can be divided into two categories, one is network-based intrusion prevention systems, and the other is host-based intrusion prevention systems. The system can directly extract the required audit data from the network data stream and restore the suspicious behavior in it. In the process, interactions with the target system as well as the outside world can be received in real time. There's a very hidden door lock in there, and there's an attempt to steal. In addition, the network intrusion system is not active surveillance, but a form of passive monitoring, making the intruder difficult to detect. The audit data collected will not be compromised or affect the performance of the protected system. When a suspected attack is detected, the firewall will be monitored according to the danger level, or the firewall will be denied.

In short, IPv6 network protocol is more secure than IPv4 in security, but the current IPv6 network protocol development is not perfect, there are still some security problems, the future from the security management, products, technology, training and other aspects of IPV6 network security issues to effectively prevent, improve the overall security and stability of IPv6 network. Lay a solid foundation for the further development of information technology.

References:

[1] Ran Zhang. Risks and Countermeasures of IPv6 Network security in universities [J]. Network Security Technology and Application,2022 (05) :100-101.

[2] Tingting Song. Exploration of Network security risks and Countermeasures in IPv6 era [J]. Computer Programming Skills and Maintenance,2021 (11) :151-153.

[3] Hui Zhu. Research on IPv6 Network security risks and Countermeasures in universities [J]. Network Security Technology and Application,2021 (07) :98-100.

[4] Shuling He,Shiqing Chen. Network security risk prevention under IPv6 scale deployment [J]. Financial Technology Times, 2019,29 (04) :64-67.