Original Research Article

Discussion on the Security Protection of Telecommunication Network

Chen Chen[*]

Guangwan Dexin Technology Co., Ltd. E-mail: chenc@sina.com

Abstract: This article first studies the telecommunication network security according to industry standards, then discusses the current situation of network security protection of domestic telecommunication enterprises. It also sorts out the technical means of telecommunication network security protection, and finally puts forwards the prospect and suggestions of telecommunication network security protection.

Keywords: Telecommunications Network Security; Security Protection of Telecommunications Network; Telecommunications Network Security Standards

As a social public information system, telecommunication network is an important national infrastructure. The security of telecommunication network plays a decisive role in the continuity and reliability of telecommunication services, and also important in the development of economy and society.

1. Overview of telecommunications industry security standards

1.1 ISO security architecture

The framework of open systems interconnection is described in *ISO 7498-2-1989 Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. The purpose of open systems interconnection is to enable heterogeneous computer systems to interconnect to realize effective communication. Security of Open Systems Interconnection (OSI) includes two levels: secure communication and management security.

The hierarchy of open systems interconnection shows that there should be security mechanism and service in the secure channel in order to realize end-to-end communication, in which the security measures of the terminal are not considered. OSI security management manages secure communication from three different dimensions: system, service and mechanism. System security management plans and maintains secure communication from the level of secure communication strategy. Security service management is to manage specific services, which provide various security services necessary for secure communication in a layered manner. Security mechanism realizes security functions from the perspective of concrete technology realization, and provides the foundation for security services. Security mechanism involves access control, key management, route authentication, data integrity technology and so on.

OSI is a framework of system interconnection, and its security mechanism should be deployed in various occasions, so that the time and space cost of stealing data is far greater than the value of data itself, thus ensuring information security.

1.2 Standards for telecommunications industry security protection system in China

doi: 10.18282/jnt.v2i3.1364

YD/T 2386-2011 Data Network and Open System Communication Security End-to-end Communication System Security Architecture is an industry label issued by China in order to realize security integration and security interoperability in multi-operator environment. This standard establishes a general security architecture composed of three elements: security dimension, security layer and security plane, and gives the security threats that this security architecture can resist and the security goals that can be achieved. This standard is applicable to all kinds of end-to-end communication systems.

Security dimension is the security measure to solve a certain network security problem. Security dimensions mainly include access control, authentication, non-repudiation, data confidentiality, integrity, availability, communication security and privacy.

From the perspective of security, the security layer divides the network into three levels: infrastructure security, service security and application security. Infrastructure security layer involves the security of equipment and communication links. Service security layer involves transport services and security services, such as DHCP services and AAA services. User application security is realized through application security layer, and related applications such as FTP, Web, Email, e-commerce, and video conference.

Security plane divides the end-to-end communication system into management security plane, control security plane and user security plane. Each plane is composed of the above three security levels, and multiple required security dimensions can be applied to the plane.

2. State quo of network security protection of telecom enterprises in China

Telecom enterprises in China attach great importance to network security protection, and have formulated relevant technical standards and management norms.

China Mobile has formulated the enterprise internal standard "General Technical Requirements for China Mobile Network Security", which is a technical document constantly revised with the development of technical level. Starting from the nature of the network and based on moderate security, whole process security and dynamic security, this requirement studies the vulnerability and threat of each network through the security assessment process, so as to find a reasonable defense plan, recovery plan and traceability method. The technical requirements mainly include technical guidelines, wireless access security technical requirements, core network security technical requirements, business platform security technical requirements, terminal and SIM card security technical requirements and information technology support system security technical requirements.

Since 2010, China Telecom has published the *White Paper on Network Security Technology of China Telecom* every year, analyzing the current network security situation and trends, and proposing countermeasures. The continuously published white papers help China Telecom to grasp the overall situation of network security more accurately, focus on related hot technologies such as 5G security, mobile Internet security, IPv6 network security, cloud security, and Internet of Things security, and strengthen network protection in a targeted manner in combination with its own characteristics. China Telecom has developed a series of security protection products to provide security services for different user groups, and Yundi is a representative network security protection platform.

China Unicom has formulated a series of internal network security standards, including *Technical Specifications for IMS Network Security of China Unicom*, *General Strategy for Intranet Information Security of China United Network Communications Group Co., Ltd.*, and *Technical Specifications for Data Center of China Unicom—Data Center Network Security*.

3. Introduction to technical means of telecommunication network security protection

The security architecture developed by ISO and the end-to-end communication system architecture in China are essentially divided into several small systems that are easy to handle by layering, and each layer realizes a single function. Telecommunication network covers both computer system and communication system. Comparatively speaking, the computer system has clear topology, similar asset types and single protocol, while the communication system has large scale, diverse assets, complex topology and diverse protocols. The main trend of telecommunication network development is IP. The openness of Internet makes telecommunication network face more threats.

Under the trend of diversified network threats, telecommunication network security protection measures are also developing and evolving rapidly. This article mainly introduces anti-DDoS attack, anti-phishing, website security monitoring and website security protection.

3.1 DDoS

DDoS attack is a common attack method that affects government and enterprise customers in telecommunication network. Attackers control botnets and attack key nodes of enterprise network servers, IDC or telecommunication networks, which will cause bandwidth congestion, resulting in unreachable services and loss of services. In e-commerce, government, finance and other industries, the inability to provide services to the outside world will bring great economic losses and political influence. In case of DDoS attack, it can ensure the normal communication within the network by deploying devices like firewall, IDS, IPS at key nodes of the enterprise network, but it cannot guarantee that the access circuit will not be congested. In order to ensure the normal business, it is necessary to deploy effective anti-DDoS attack measures in the operator network connected to the enterprise network.

Traffic cleaning and traffic suppression are commonly used methods, that is, traffic cleaning equipment is deployed at key nodes of telecommunication network, and network traffic is drawn, cleaned, suppressed and then re-injected into customer network.

Telecom operators can deploy large-capacity traffic cleaning equipment at IDC and MAN outlets and backbone networks. The earlier DDoS is discovered, the easier it is to reduce the impact of attack. Therefore, in terms of attack traffic detection, telecom operators should open self-service monitoring interfaces to users while providing telecom monitoring services, so that users can start the traffic cleaning function when they find abnormal traffic.

Traffic suppression means that telecom operators use the traffic scheduling capability of the Internet to publish black hole routes to customers' IP addresses or network segments in IP networks according to user customization, and discard traffic from specific directions of the network including attacks. Operators can block IP traffic from international operators, other domestic operators or to specific enterprise networks as needed.

3.2 Anti-phishing

The mechanism of phishing is to send illegal links to potential victims by e-mail or short messages, and trick them into using fake websites. In the process, the victims may reveal their personal identity and financial information. Phishing websites cause both economic and reputation losses to enterprises that have been counterfeited, and also cause great losses to netizens. The timeliness of phishing website interception is very important. And telecom operators have great advantages in managing phishing websites. They can find phishing websites comprehensively, timely and accurately, intercept and dispose them in real time, and provide customers with strong anti-phishing ability by relying on the control ability of telecom backbone network, the advantages of big data resources and the unique network intelligent pipeline ability of operators.

3.3 Website security monitoring

Website security monitoring includes website usability monitoring, website content security monitoring and website vulnerability detection.

Website usability monitoring is to monitor the customer's website for 7*24 hours, and timely alert users by short messages and emails when there is abnormal access interruption and slow access response, so as to quickly start abnormal investigation and handling. The realization of website usability monitoring is to deploy multiple distributed monitoring points in the network, and multiple operators can plan and deploy monitoring points cooperatively. More monitoring points can improve the accuracy of monitoring results and eliminate false alarms caused by problems such as monitoring lines and operators.

Website content security is extremely important for government and enterprise customers. Website content monitoring includes tampering monitoring, sensitive keyword monitoring and dark chain monitoring. The operator monitors the changes of the content and structure of the user-specified page, and gives an alarm to the webmaster, who verifies and handles it. In the monitoring of sensitive keywords, operators should be able to customize the keyword library, monitor the sensitive information of web pages in real time, and notify the webmaster when keywords match. If there are hidden links in the customer's website, such as online games, gambling, pornography and other advertising links, the operator should identify the harm degree in time, alarm the hidden links in time, and make necessary treatment.

When a website has high-risk vulnerabilities, it is easy to be exploited by attackers, which leads to data leakage, tampering or suspension of the website, and even paralysis of the website. In order to ensure network security, operators should scan users' websites for deep vulnerabilities, and find out whether there are SQL injection vulnerabilities, XSS vulnerabilities, CSRF vulnerabilities, Web application vulnerabilities, CGI vulnerabilities, form bypass vulnerabilities, etc., and provide reinforcement suggestions. Operators should update and maintain the vulnerability database in time to ensure its timeliness.

3.4 Website security protection

Operators deploy Web Application Firewall (WAF) to ensure website security. Visits to the user's website initiated by visitors first pass through the website security protection service node of the operator. By analyzing, auditing and filtering the access requirements, the protection node forwards the access that meets the security requirements to the server, while the access that does not meet the requirements is filtered out. In addition to the Web intrusion prevention function, WAF deployed by operators should also meet the specific needs of operators, such as intelligent IP address filtering, IP blocking based on geographical location, access filtering and virtual patch. Operators mainly deploy cloud WAF, and hardware WAF or software WAF in specific occasions.

Web intrusion prevention detects and filters specific Web traffic through set security policies, and can prevent Web attacks such as SQL injection, XSS cross-site attack, CC attack, cross-site request forgery, parameter pollution, cache overflow attack, cookie modification, XML injection, parsing vulnerability, remote command execution, file inclusion, multi-layer compilation attack, and dynamic application confusion attack.

Network operators have many requirements for IP address control. Operators customize the IP address filtering strategy, and the system automatically blocks malicious IP addresses according to the configured strategy. Operators can also configure IP ban policies based on countries and regions according to specific needs, and intelligently block IP access in specific countries and regions. They can also set that the specified address cannot access the website, or set the specified IP, URL, UserAgent and Referer to allow or block, so as to realize access control.

4. Conclusion

With the development of 5G networks and the application of new technologies in recent years, such as big data and cloud services, telecommunications networks are facing new challenges. Telecom network security protection is the key point of national important infrastructure protection. Operators and security agencies should strengthen cooperation, promote the standardization of management system, and promote the development of telecom network security.

References

1. Deng L. Network security protection system design of telecom big data platform (in Chinese). Wireless Internet Technology 2020; 17(1): 58–61.
2. Xiong Q, Wang F, Zhang B, *et al*. Telecom network security risks and protection framework (in Chinese). Information and Communication Technology 2016; 10(6): 31–36.