An Intelligent Network Security Protection Solution

Jinxiong Zhao [a], Zhiru Li, Xun Zhang, Xiaoqin Zhu, Yong Zhi

Grid Technology Center, State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China.

[a]18352449382@163.com

Abstract. The network security monitoring device (ZJXD) designed is a network security monitor based on threat intelligence and anti-attack chain intrusion technology. The measurement system has the functions of data monitoring, automatic analysis, safety detection, event correlation and situation analysis, which can be extended to realize micro applications by customizing according to the requirements, so as to achieve the purpose of building a platform with multiple applications.

Keywords: Network Security Monitor, Threat Intelligence, Anti-Attack Chain Intrusion.

1. Introduction

The network security detection system (ZJXD-S), known as the network information detection system [1-4], mainly carries out work through the Internet and manages the computers connected with the interconnection network safely [5-8], so as to avoid computer users from accessing illegal websites [9-12], transmitting and publishing illegal information [13-15]. To prevent the abuse of network resources, leakage of sensitive information and other violations from happening in the future, it is also a necessary approach to detect Behavior and content of computer users.

The current network detection system functions is mainly as follows: It can timely prevent the sensitive information leakage of internal computers through the Internet, quickly locate and trace the source, and prevent the occurrence of violations by analyzing all network contents; It can monitor the network behavior and network traffic of the entire computer users, help the network to operate efficiently, and provide effective technical support for information construction and management; The network information monitoring system is a B/S architecture product integrated with software and hardware, which is specially designed to prevent the malicious dissemination of illegal information and the leakage of confidential information, commercial information and scientific research results; It can also monitor the compliance of transmission content in real time and manage employees' online behavior; It can determine whether the current packet is transmitted based on the information from the monitoring configuration module and the results from the traffic statistics module.

2. Methodology

The basic architecture of ZJXD-S consists of one framework and six modules: The main function of the 1 frame is to realize full data collection based on full traffic, and detect attack that fully monitored at the network level; The six modules are respectively to realize the management of security situation, security event, asset monitoring, advanced analysis, intelligence warning and micro-application. Similarly, there are six modules in ZJXD, Web attack monitoring.

ZJXD is connected with the micro-application module in the information security management framework. If one of the following situations occurs, such as web attack, port scanning, webpage tampering, webshell detection, suspicious file detection and other illegal behaviors, micro-application management will issue instructions to ZJXD calling one of the functional modules to intercept and block the illegal behaviors. Another key role of ZJXD-S is to actively defend the flow, log and assets of the entire system collected by detecting sensors, and to isolate suspicious and illegal behaviors in the first. In essence, the protection is implemented from the perspective of full traffic, full log and full asset.

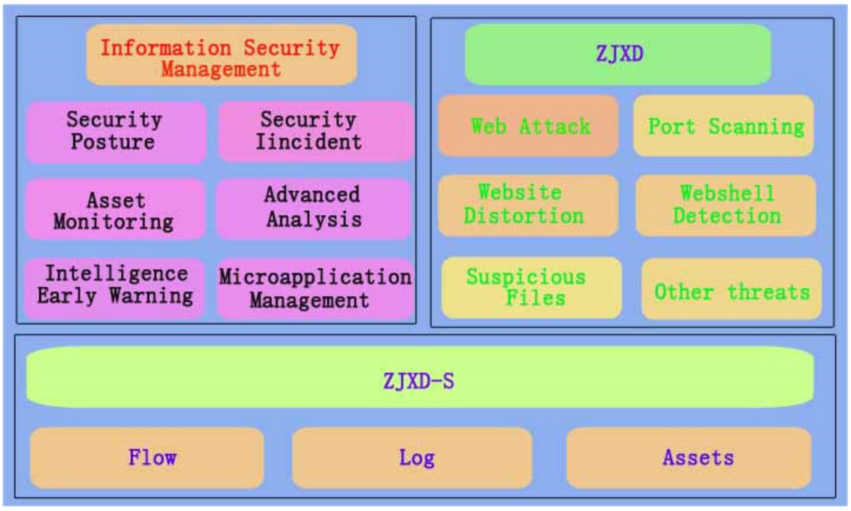

Fig. 1 Principle design framework of ZJXD-S

2.1 Safety Micro Application

Each successful attack requires seven steps: detection, weapon construction, payload delivery, attack utilization, placement, communications control, and target completion. These seven steps obtain the protection advantage at the key nodes, and realize the omni-directional active defense purpose of "discovery, positioning, tracking and strike" respectively. The defensive confrontation model is as follows:

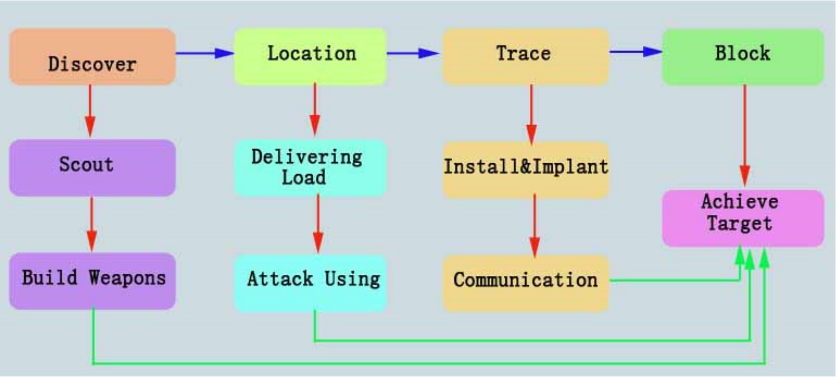

Fig. 2 The defensive confrontation model

The discovery stage mainly includes eight aspects: web attack port scanning, vulnerability information intrusion detection, suspicious program detection, suspicious file detection, abnormal behavior detection, malicious program detection, external threat detection, log audit detection, etc.; The positioning stage mainly involves five aspects: webpage tampering intrusion, webshell, abnormal behavior, malicious program, abnormal behavior alarm, etc.; The tracking stage includes flow analysis, log analysis, reverse analysis, attack tracing, expert analysis and honeypot network; The strike phase consists of eight parts: black and white list, vulnerability repair, intrusion protection, sandbox, vulnerability repair, malicious code detection, DNS redirection and forensic analysis.

2.2 Network Security Threat Monitoring

ZJXD is deployed at the boundary of the information outer network. The mirror flow of the outer network boundary switch is used to analyze and detect the outer network boundary flow. The honeypot system is a separate server system (both physical and virtual) deployed in the DMZ area of the outer net, mainly used to simulate the user's outer net service, and controlled by ZJXD.

ZJXD-S carries out real-time monitoring and warning of security events by means of adopting the system to submit data and vulnerability scanning, etc. Real-time monitoring and warning of network security events is conducted through the collection of station control layer switch, network analyzer and safety protection equipment safety event data. The host of the factory station can realize the alarm of user's illegal operation, U disk plug and plug, serial port equipment access, network equipment access, network attack, abnormal traffic, etc. For the host of the factory station, ZJXD-S can launch warning alerts to the user's illegal operation, U disk plug and unplug, serial port equipment access, network equipment access, network attack, abnormal traffic, etc., to help the administrator to find the violator in the first time. At the same time, ZJXD-S integrates the security event monitoring, security vulnerability scanning, network traffic protocol security analysis, operation and maintenance operation behavior control (realizing the joint alarm with the work ticket) and other functions to strengthen the safety protection capacity of the plant.

3. Summary

In summary, as an upgrade product of the original power secondary system network security monitoring platform, the safety supervision platform has been greatly improved in terms of "breadth", "depth" and "accuracy". Monitoring objects include special security equipment, general safety equipment, host operating system, database, network equipment, monitoring scope includes main station, substation and power plant (part of the network). And the monitoring content also involves the equipment state, the security state, the security event.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61762058) and State Grid Science and Technology Projects (522722180007).

References

[1]. Hao Wu, Wei Wang, Changyun Wen, Zhengguo Li. Game Theoretical Security Detection Strategy for Networked Systems. Information Sciences. Vol.453(2018), p. 346-363.

[2]. Vadursi Michelel, Ceccarelli Andrea, Duarte Elias P., Mahanti Aniket. System and Network Security: Anomaly Detection and Monitoring, Journal of Electrical and Computer Engineering. Vol.2016.

[3]. Min-Joo Kang, Je-Won Kang. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. PLOS ONE, 2016.

[4]. Fimpel Heiko, Lindner Falk, Winncki Alexander. Methods and Detection of Attack Security for the integration of open Network Connections in Vehicle Systems. AUTOMOTIVE SECURITY. Vol.2310(2017), p. 97-112.

[5]. Mohsen Jahanshahi, Fathollah Bistouni. Interconnection Networks. Crossbar-Based Interconnection Networks. 2018, p.9-39.

[6]. Jingjian Li, Bo Ling. Symmetric graphs and interconnection networks. Future Generation Computer Systems. Vol.83(2018), pp.461-467.

[7]. Rachel Alemu. Regulation of Network Interconnection and Network Access. The Liberalisation of the Telecommunications Sector in Sub-Saharan Africa and Fostering Competition in Telecommunications Services Markets, Vol.6(2018), p.211-256.

[8]. Vitor H. P. Louzada, Nuno A. M. Araújo, José S. AndradeJr., Hans J. Herrmann. The Cacophony of Interconnected Networks. Interconnected Networks. 2016, p.141-148.

[9]. Harry Leech. Website offers steroids illegally, Sunday Times. 2016, p. 4.

[10]. HAWRYLUK, KAREN. Mastermind behind biggest illegal website in history is from Quebec, CBC Radio, 2017.

[11]. Laurie McGinley. FDA targets hundreds of websites illegally selling prescription drugs. Washington Post, 2017.

[12]. Helen Bruce. Court orders block on illegal music download website. Daily Mail. 2013, p. 11.

[13]. Miller KE, Ruiz DE, Graves JC. Update on the prevention and treatment of sexually transmitted diseases. American Family Physician. Vol.67(2003) No.9, p. 1915-1922.

[14]. Florence Hartmann-Vareilles. Achievements in civil intellectual property enforcement and recent initiatives within the Digital Single Market Strategy on the regulatory environment for platforms and online intermediaries. ERA Forum. Vol.18(2017) No.1, p. 1-6.

[15]. Robert Mathews. Interrogating “privacy” in a world brimming with high political entanglements, surveillance, interdependence & interconnections. Health and Technology. Vol.7(2017) No.4, p. 265-324.