Design and Implementation of a Lightweight Intrusion Detection and Prevention System

Xiaogang Wei(✉)

NARI Group Corporation/State Grid Electric Power Research Institute, Nanjing 210003, China
andrew_wee@163.com

Abstract. While mobile internet brings convenience to people, it also introduces many security risks. For security protection of specific business, the technical means such as traffic analysis and illegal protocol identification can effectively detect network attacks, because of the simple business protocol and small business access. This paper proposes a lightweight intrusion detection and prevention method, based on nDPI, adopting common network packet capture means for design and implementation of a lightweight intrusion detection and prevention system. The test results show that the system can detect the abnormal protocol through the traffic and trace back to the corresponding terminal, so as to handle the abnormal terminal response and block the abnormal connection initiated from the terminal, thereby achieving the purpose of intrusion prevention.

Keywords: Intrusion detection · Intrusion prevention · Traffic analysis · Protocol identification

1 Introduction

With the wide application of mobile informationization technology, the number of mobile terminals is growing rapidly, and various mobile applications are emerging one after another, providing many conveniences for people's production and life. However, while providing convenience, mobile informationization technology also brings a lot of security risks, such as the risk of illegal terminals accessing the intranet. Attackers use legitimate terminals to carry out network attacks on the intranet system. There are many forms of cyber attacks, such as DOS attacks and port scan attacks. Such attacks can cause service rejection or service response delays. Abnormal traffic or excessive traffic will appear in the network data transmission. Therefore, through the analysis of network traffic and the intrusion detection and prevention, the network environment can be effectively managed [1], which is essential for the safe operation of mobile informationization business.

At present, the traffic and protocols of the power mobile business connected to the intranet are relatively simple, which is different from mobile internet business, using many and complex protocols. In view of this situation, this paper proposes lightweight intrusion detection and prevention method, based on nDPI (network Deep Packet Inspection) [2, 3], which analyze network traffic, identify the network protocol, and distinguish the abnormal network protocol of the power mobile business connected to the internal network, and on this basis, perform network redirection on the connection

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 433–439, 2019.
https://doi.org/10.1007/978-3-030-21373-2_34

with the abnormal network protocol. The lightweight intrusion detection and prevention system is described in detail below.

2 System Design

2.1 Software Process Design

The lightweight intrusion detection and prevention system designed in this paper is mainly composed of three parts, which are composed of network traffic capture

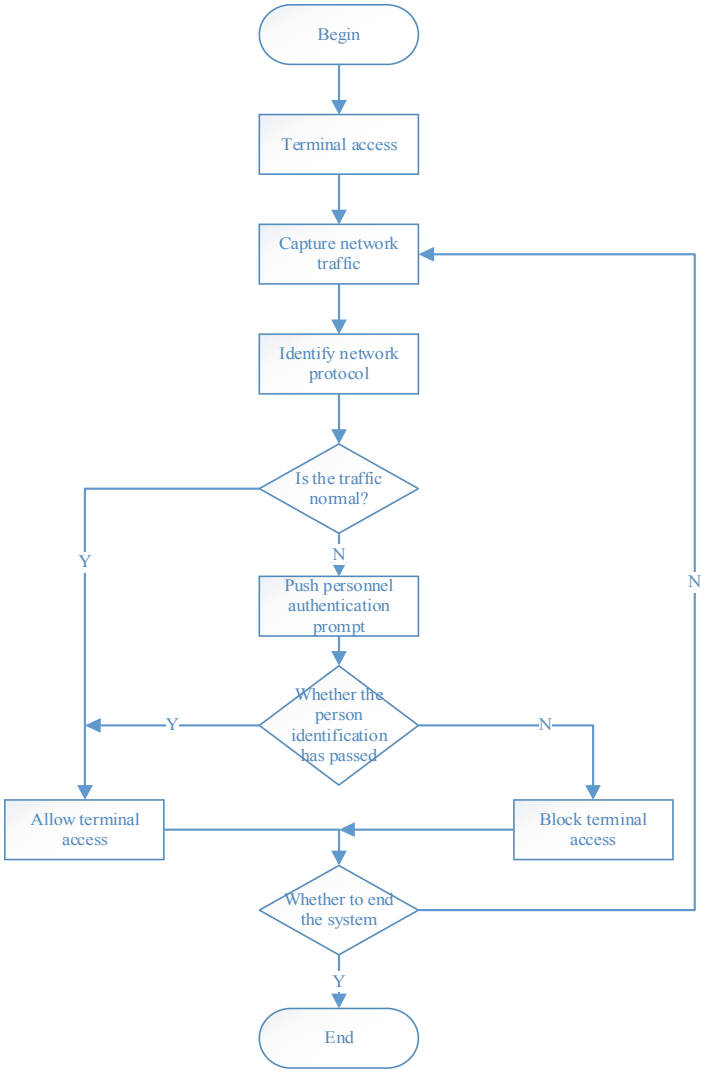

Fig. 1. Basic software flow for lightweight intrusion detection and prevention systems

module, protocol identification engine and response processing module. The basic software flow chart is shown in Fig. 1.

The capture module of network traffic captures the traffic generated after the terminal accesses the network according to certain rules. And the protocol analysis engine performs protocol analysis on the captured network traffic, and can distinguish the abnormal protocol in the business running process according to the established protocol. This method is especially effective for a single protocol and a simple process. After that the response handling module operates on network traffic with an abnormal protocol, and determines whether to allow the terminal to access the network according to the authentication result.

2.2 Deployment Architecture Design

The deployment architecture is shown in Fig. 2. All types of terminals, such as PCs, laptops, tablets, and mobile phones, access the application server deployed on the internal network by wireless network (such as a carrier network or a self-built WIFI network), passing through routers, application firewalls, access switches, and other network devices. Because the wireless network itself has a large number of security risks, in order to ensure that the internal network resources are not damaged or sniffed by attackers, network traffic passing through the terminal access process needs to be detected. The port mirroring function of the switch mirrors the traffic entering the application server to an idle port of the intrusion detection and prevention system for analysis.

Different from the general intrusion prevention system in the critical network path, the intrusion detection and prevention system designed in this paper adopts bypass work, which not only does not affect the data forwarding performance when the terminal accesses the application server, but also avoids node failure because of software defect. That directly causes the terminal to fail to access the application server.

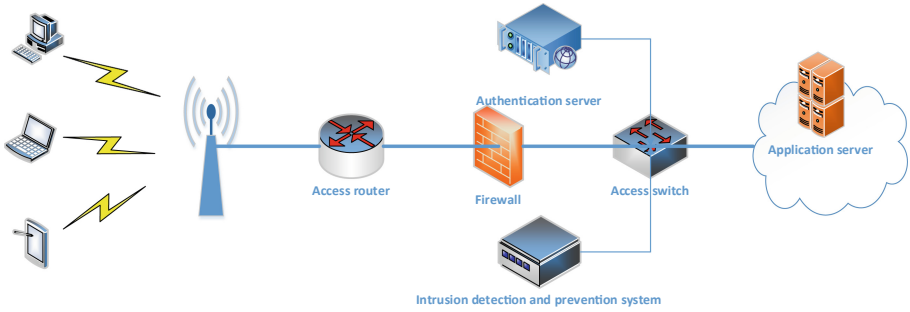

Fig. 2. Overall deployment architecture

3 System Implementation

3.1 Capture Module of Network Traffic

Network traffic capturing is a prerequisite for traffic monitoring [4–6], and there are many ways to capture traffic. This article uses the libpcap library on Linux. Libpcap (Packet Capture Library) is a packet capture function library. It is a network packet capture function library under Unix/Linux platform. It is a system-independent user layer packet capture API interface, which provides a layer for network monitoring. Tcpdump, developed based on libpcap, is capture tool on Linux. The process of using libpcap in this paper is as follows.

(i) Get network interface. Determine the network interface that needs to be monitored on the intrusion detection and prevention system. The interface can be specified or automatically selected by libpcap and he specific function is pcap_lookupdev().
(ii) Open the network interface. After determining the network interface to be monitored, the interface need to be initialized and the specific function is pcap_open_live().
(iii) Get the data packet. After opening the network interface, the interface has started to be listened. This is the core part of used process of the libpcap. The function pcap_dispatch() can be used to complete the task of obtaining the data packet.
(iv) Release network interface. This function releases the interface after the completion of operation. The specific function is pcap_close().

3.2 Recognition Engine of Network Protocol

The purpose of capturing network traffic is to identify the network protocol, distinguish the abnormal protocol, and facilitate the subsequent response processing. This paper implements network anomaly protocol identification based on nDPI technology. nDPI is an extension library of OpenDPI [7–9] maintained by ntop. It has been developed from OpenDPI, solves many problems of OpenDPI, and has quite perfect application layer protocol recognition function [10–12], almost becoming the only choice in the DPI field. This system performs secondary development of the nDPI source code, and adds an identifiable protocol type to the power-specific service, and alerts the abnormal protocol, and notifies the subsequent response processing module to timely process the connection that generates the abnormal protocol. The specific process is shown as follows.

(i) Initialize recognition engine. Call ndpi_init_detection_module() to initialize the detection module of the recognition engine.
(ii) Set the protocol to be identified. Call ndpi_protocol_detection_bitmask2() to set the protocol mask, call ndpi_load_protocols_file() to load the protocol file, and specify which protocols are specifically identified by the protocol file.
(iii) Identify protocol. ndpi_detection_process_packet() is used to obtain the specific information of the packet, including the protocol stream and the detailed information of the packet. During the running of the business, the system

performs protocol matching according to the specified protocol. If the matching cannot be completed, the protocol is abnormal. For abnormal protocols, it can be traced back to specific terminals to facilitate subsequent response processing.

(iv) Statistics and analysis: The system performs statistics on the protocols identified during the operation of the business and visualizes the processing of the abnormal protocols.

3.3 Response Handling Module

The system response for the terminal (PC, notebook, tablet, mobile phone, etc.) that initiates the abnormal protocol is shown in Fig. 3. After the terminal initiates an access request to the application service, the intrusion detection and prevention system designed in this paper obtains and monitors the traffic on the network through the capture module of network traffic, and traces the terminal initiated by the abnormal protocol after the recognition engine detects the abnormal protocol. And the network redirection packet is sent to the terminal, then the access of the terminal is redirected to the authentication service. After the authentication service receives the request of the terminal, the authentication prompt is pushed for the terminal. And only the authenticated terminal is allowed to access the network.

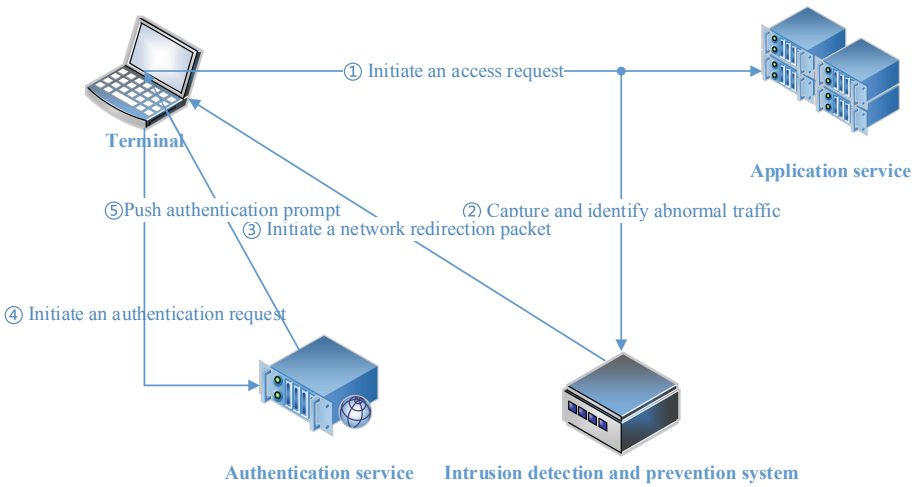

Fig. 3. Flow diagram of response and processing

4 System Tests

When setting the protocol file, you can specify the specific network protocol and port, or specify the IP address included in the specified protocol, or even specify the specific website name. The system can identify the corresponding protocol by string matching. Figure 4 shows one of the statistical analysis results after system detection. HTTP and

ICMP are the protocols specified in the protocol file, and 13.9% are unspecified protocols in the protocol file, then further analysis is required. Finally, 13.5% of the traffic is considered abnormal by the system, which should processed for subsequent response. In the actual power business, the protocol type is single. So it is easier to distinguish other protocols unrelated to the business through the system designed in this paper. The traffic carrying these unrelated protocols will be redirected by the system to further check whether the terminal users have Aggressive behavior.

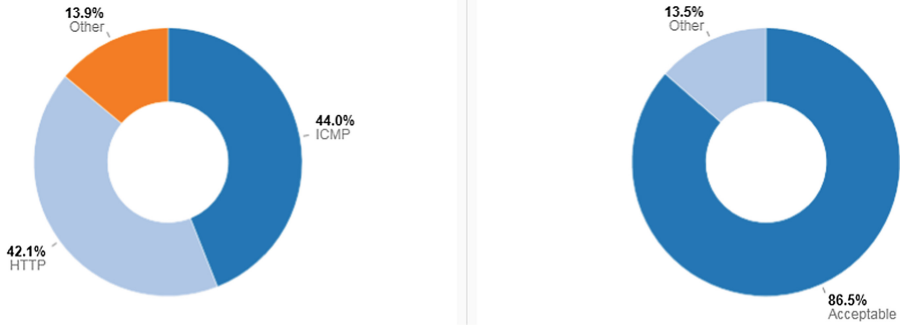

Fig. 4. Preliminary statistical analysis results

5 Conclusion

This paper considers the complexity of deployment for existing intrusion detection and prevention system. For the power business, the intrusion detection and prevention functions are combined into one, and a lightweight intrusion detection and prevention system is proposed. The design schemes, implementation schemes and test results are given in this paper. Experiments done by authoritative organization show that the schemes proposed can reduce false positive rate and false negative rate compared existing methods. That has relatively high reference value for network traffic monitoring, protocol analysis and response handling of abnormal terminals.

References

1. Zhou, Y.: Application of protocol analysis technology in intrusion detection system. Comput. Syst. Appl. **20**(6), 161–164 (2011)
2. Yuan, C.-L., Ouyang, Z.-Y.: Research on experimental platform of traffic monitoring and analysis based on nDPI. Exp. Technol. Manag. **32**(3), 97–100 (2015)
3. Deri, L., Martinelli, M.: nDPI: open-source high-speed deep packet in spection. In: IWCMC 2014 (2014)
4. Su, J.-F.: Research and implementation of topology visualization in network measuring instrument. Xidian University (2012)
5. PCAP Next Generation Dump File Format [OL], May 2014. http://www.tcpdump.org/pcap/pcap.html

6. Song, X.-Y.: Research and design of an application layer network traffic monitoring system. Xi'an University of Science and Technology (2016)
7. Wei, Y., Zhou, Y.-F.: Analysis of message identification for OpenDPI. Comput. Eng. Supplement(1), 98–100 (2011)
8. L, Y.-M., W, Y.: Illegal business identification technology based on DPI and DFI. In: Software Guide, vol. 14, no. 12, pp. 177–179 (2015)
9. Zhuo, W.-H.: An improvement of NBOS S traffic identification module. Southeast University (2014)
10. Liu, A.X., Meiners, C.R., Norige, E., et al.: High-speed application protocol parsing and extraction for deep flow inspection. IEEE J. Sel. Areas Commun. **32**(10), 1864–1880 (2014)
11. Zhuo, Z.-L.: Research on the key technologies of network tracing in the anonymous network. University of Electronic Science and Technology (2018)
12. Jing, P.: Implementation of deep packet inspection in integrated space and ground network. Beijing Jiaotong University (2017)