A Brief Analysis of the Key Technologies of Power Enterprise Network Perimeter Information Interactive Security Audit

YANG Hao LIN Nan XIAO Yongcai ZHANG Lingling

State Grid Electric Power Research Institute of Jiangxi, Nanchang 330096, China

Keywords: Network perimeter; massive information; interaction; security audit; key technologies

Abstract: According to the structures of internal and external information networks of power enterprises and the characteristics of enterprise network perimeter information interactions, the paper designs a security audit model and a security assessment framework based on state graph perception, proposes related technologies of perimeter massive log analysis and deep mining, and gives a specific research direction and research methods, thus providing guidance for the construction of a network perimeter information interactive security audit platform for power enterprises.

Introduction

Nowadays most companies of state grid have implemented SG186 and SG-ERP projects for information system and established internal and external enterprise networks for information. Their information system has been deeply integrated with the enterprise smart power grid’s six links including power generation, transmission, transformation, distribution, utilization and dispatch, to ensure the massive information interactions between the internal and external networks of enterprise. As a state energy sector, how to ensure information interactive security has become an important research field needing long-term and in-depth research of enterprise informatization management, operation and maintenance staffs.

In the time when information technologies develop rapidly, network attack technologies also develop fast and show the trends of upgrading, systematization and continuous development. The paper discusses the security audit model and security assessment framework of massive information interactions of internal and external network perimeter, and proposes the key technologies to construct a security audit platform for internal-external-network perimeter massive information interactions (hereinafter referred to as the security audit platform), thus providing the general guidance for the perimeter security monitoring, collection and assessment of internal and external information networks of power enterprises.

Review of Research Status

TCSEC (Trusted Computer System Evaluation Criteria) issued by United States Department of Defense in 1985 is the earliest criteria with the widest range of influence in security information architecture. The Criteria divides security into four aspects which are security policy, accountability, security assurance and document, and divides the security level of computer operation system into four grades (A,B,C and D) and seven levels (A1, B3, B2, B1, C2, C1 and D), of which A1 is the highest security level and D is the lowest level. TCSEC requires the operation system to have the audit function from C2 and the full audit functions from B3 [1].

In China, related laws and regulations, such as the *Basic Requirements of Information System Security Classified Protection* (GB/T22239-2008)[2]and the *Information Security Management System Requirements* (GB/T22080-2008 IDT ISO/IEC27001:2005)[3], also explicitly specify the technical requirements for information security audit.

Currently, the information system audit based on the bypass packet capture technology has become the mainstream technology, of which the types include host audit, network audit and log audit [4] [5]. In recent years, with the development of cloud computing technology, the information interactive security audit technology based on cloud computing has become a research focus in the field[6].

Processing, applied mining algorithm and pattern analysis are three major stages of log analysis mining. Robert Cooley, et. al., designed and realized the WebMiner system based on Web log data processing, and the log analysis scheme has been applied widely. In fact, the essential point of the key technology used in massive log data analysis is to realize the compression and merging of log data.

The Hadoop developed by Apache Software Foundation has been very mature after years of development, especially the HDFS and MapReduce components of computing framework [7]. It has been proved that the cluster of several hundreds of computers is available and can bear data at PB level. Although using Hadoop for log analysis will generate extra learning and operation & maintenance costs, the application makes it possible to analyze the massive security logs of internal and external networks.

Analysis on Enterprise Status

The information system of power enterprise belongs to the secondary system, which is divided into areas I-IV according to its relationship with the production system. Area I is the real time monitoring area, area II is the noncontrolled production area, area III is the production management area, and area IV is the management information area.

Areas I-III are closely related to the production of power enterprise. Currently the secondary system security protection framework of the three areas has been completed. Measures, such as power secondary system security analysis and lateral isolation, of power enterprises at different levels can be fully implemented. The perimeter security protection deployment between power generation control area and management information area is increasingly improved. Dispatch technology support system, electricity trading system, power collection system and marketing management system all can make secure information interactions [8].

In 2007, as a mainstay enterprise of state energy, State Grid classified areas I-IV into the internal information network and established an independent external information network interconnecting with the Internet, and tightly prescribed that areas I-III could not interconnect with the external information network, and all information should be exchanged through area IV's network which exchanged data with the external information network through the security isolation device. The isolation device can find and block malicious information interactions, but can't audit interactive information and lacks security audit abilities like tracking or tracing back [5]. As State Grid promotes the construction of smart power grid, the internal-external-network information interaction is developing towards the massive pattern, so researching the key technologies of internal-external-network perimeter information interactive security audit and establishing an integrated security audit platform have become matters of great urgency.

Internal-external-network Perimeter Massive Interactive Information Security Audit Model and Assessment Framework

The design of model and assessment framework is the theoretical basis to realize the security audit platform. According to the practical operation situation of internal and external information networks of power enterprises, the paper designs the information security audit model and assessment framework as Figure 1.

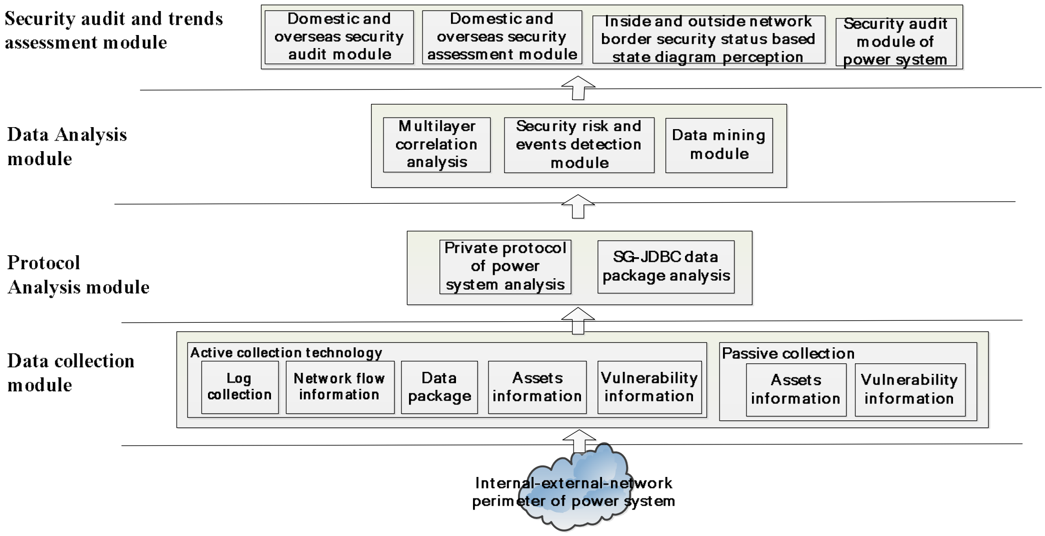
Security audit and trends assessment module
Domestic and overseas security audit module
Domestic and overseas security assessment module
Inside and outside network border security status based state diagram perception
Security audit module of power system
Data Analysis module
Multilayer correlation analysis
Security risk and events detection module
Data mining module
Protocol Analysis module
Private protocol of power system analysis
SG-JDBC data package analysis
Data collection module
Active collection technology
Log collection
Network flow information
Data package
Assets information
Vulnerability information
Passive collection
Assets information
Vulnerability information
Internal-external-network perimeter of power system

Figure 1 Internal-external-network Perimeter Massive Interactive Information Security Audit Model and Assessment Framework

Data Collection

Include the active collection and the passive collection, and establish internal-external-network perimeter security risk identification and event description methods based on the attack & defense state graph method. Build the specific description language according to the characteristics of power enterprise and build the security risk & event description model on the basis; describe the identification rules of internal-external-network perimeter security risks and events in the form of attack & defense state graph in a visual way; adopt the detection algorithm based on classical algorithms like Apriori to identify internal-external-network perimeter security risks and events fast; use the asset information and vulnerability collection method based on active detection and bypass to identify the vulnerability information of system and build the basic model of audit object.

Protocol Analysis

Include the data packets based on SG-JDBC driver, Modbus protocol data packets, CDT protocol, DLT645 protocol, DNP3.0 protocol, IEC101/102/103/104 protocol and so on, and focus on the data communication packet analysis and the precise restoration of users' practical network operations and database operations based on the power sector's SG-JDBC driver and the business system's private communication protocol.

Data Analysis

Realize end-to-end and net-to-net data collection and the identification record of individualized power control instructions according to the characteristics of power enterprise based on improved power protocol analysis and power instruction control, to make power control data network get the security audit record for the analysis and restortion assurance of data collected, and analyze restored data based on the multilevel association analysis model to realize the multilevel association analysis on user operation and database access and realize the multi-level association of audit system.

Security Audit Model and Security Situation Assessment

Build a security audit model applicable to electric power system according to the characteristics of power enterprises' internal-external-network perimeter data and users' access behaviors; identify the security risks and events of power system and assess the internal and external networks' perimeter security situation of power system according to the asset information and vulnerability information of internal and external networks. The essence is the security audit and situation assessment model based on state graph perception, which is integrated with other mature security audit models at home and abroad.

Internal-external-network Perimeter Massive Security Log Analysis and Deep Mining

Massive security log analysis and deep mining, essentially, is to complete the collection of basic analysis data of security audit platform, which is the core of hardware support part of platform. The design idea in the paper is to use technologies, including flow analysis, compliance analysis, data mining, OLAP association analysis and so on, assisted by the machine learning and statistical methods to realize a multi-dimension association analysis on logs, including developing the flow data analysis technology combining deep packet analysis with dynamic flow detection, building a database-access-oriented standardized behavior audit pattern library, and developing a massive security audit log data mining technology based on Markov time-varying model. Figure 2 shows the technical framework diagram.

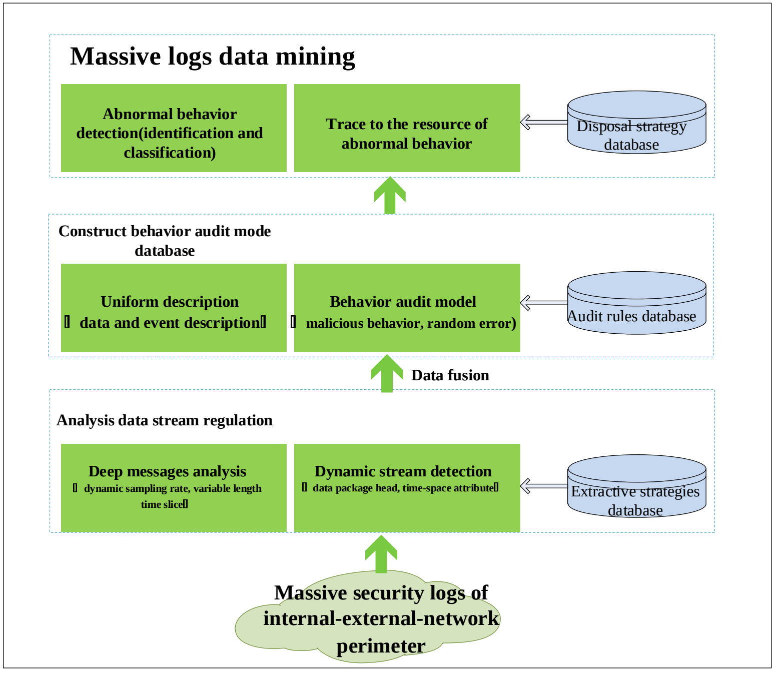
Massive logs data mining
Abnormal behavior detection(identification and classification)
Trace to the resource of abnormal behavior
Disposal strategy database
Construct behavior audit mode database
Uniform description
▯ data and event description▯
Behavior audit model
▯ malicious behavior, random error)
Audit rules database
Data fusion
Analysis data stream regulation
Deep messages analysis
▯ dynamic sampling rate, variable length time slice▯
Dynamic stream detection
▯ data package head, time-space attribute▯
Extractive strategies database
Massive security logs of internal-external-network perimeter

Figure 2 Design Framework of the Analysis and Deep Mining System of Massive Security Logs

One key point of the framework is to realize the flow data analysis technology combining deep packet analysis with dynamic flow detection. The strategy is to develop an adaptive deep flow packet analysis method based on dynamic sampling rate and variable-length time slice, and research the practical situation of packet arrival rate and router load by analyzing the mutual restriction relationships of packet arrival rate, router load, sampling rate and statistic time slice, and then dynamically adjust the optimization model of sampling rate and use the model to find the generation and flowing laws of dynamic data flows; on the other hand, develop a dynamic data business flow analysis method based on data packet headers and space-time attributes to analyze the difference of different data business flows in data packet header and space-time attribute, such as data packet flow direction, packet interval time and mean packet length, during protocol interactions, in order to realize the real time data flow sorting algorithm.

The second point of the framework is to build a database-access-oriented standardized behavior audit pattern library. First, build the unified description model of massive data of internal-external-network information system and the unified feature description model of security events according to the characteristic of power enterprise. Get and collect samples of malicious attack and random fault and use the machine learning method for training samples to analyze the data flow characteristics and behavior characteristics when the network suffers malicious attacks, and then build an association model using the association analysis method. Next, analyze the data flow characteristics and behavior characteristics under random faults to build the behavior pattern library for different network security events, the audit rule pattern library of characteristics & behaviors in the uniform format of network security events, and the fine audit strategy library. Finally, on the basis of fully grasping the cause of traditional single feature library, modify and extend behavior characteristic attributes and also improve characteristic engine correspondingly. Check the effect of characteristics in uniform format with a practical test to optimize the description model of security event characteristics in uniform format established earlier. In this way, solve the low matching efficiency problem of traditional security event characteristic classified description method in unified security event monitoring.

The third point of framework is how to realize the massive security audit log data mining technology based on the Markov time-varying model. First, develop the mining algorithm of network abnormal behavior patterns based on the Markov time-varying model of time series by analyzing the behavior characteristics and distribution laws of data packets and data business flows in time and space, and build the corresponding detection model. Second, extract typical large-scale network security events or threat behaviors from massive log data, analyze the attributive characteristics and distribution laws of data packet header, and build the classification model and develop the detection algorithm of abnormal network behaviors in large-scale security events. Third, develop a precise behavior tracking method. Basing on the object-level audit data trading consistency technology, analyze network security events and tract the source of events to realize the precise audit to tack and trace to the source of abnormal data behaviors, in order to achieve the objective of all-around information risk control of internal and external networks and ensure the traceability of data between internal and external networks.

Conclusion

Basing on years of experience in electric power informatization and information security field, with the objective of realizing secure information interactions of internal and external networks of power enterprises, the paper proposes some key technologies and research methods of internal-external-network information interactive security audit platform but doesn’t involve specific design or implementation plan. To build such as security audit platform, it’s necessary to use the key technologies proposed in the paper, such as the design model, assessment framework, and log analysis & mining, and design corresponding scan hardware and supporting software.

In fact, the power enterprise, as the large state energy enterprise, has a highly complicated information system and massive interactive information between internal and external networks, so its information interactive security audit is a long-term task needing continuous exploration and research.

References

[1] United States Department of Defense, Trusted Computer System Evaluation Criteria[Z],1985

[2] The State Standard of the People’s Republic of China, The Basic Requirements of Information System Security Classified Protection(GB/T22239-2008)[Z], 2008

[3] The State Standard of the People’s Republic of China, Information Security Management System Requirements (GB/T22080-2008 IDT ISO/IEC27001:2005)[Z], 2008

[4] Chen Zhuang, Huang Yong, Zou Hang. Analysis and Design of ICS Information Security Audit System, Computer Science, 2013,6,(40): 340-343

[5] IEC. Industrial Communication Networks-Network and System Security-Part2-1:Establishing an Industrial Automation and Control System Security Program. IEC62443-2-1 . 2010

[6] QIN Rong-sheng. On the Development of Cloud Computing and Its Challenges to Accounting and Auditing, Comtempory Finance & Economics, 2013.1(338): 111-115

[7] Patrick D M. POlley Management In secure Group Communication[A]. The elghth ACNsymposlum on Acess Control models and technologles,2004

[8] State Electricity Regulatory Commission. Electric power secondary system safety protection regulations[Z], 2005.