Advances in Engineering Research, volume 150

4th International Conference on Machinery, Materials and Computer (MACMC 2017)

An Information Security Situation Analysis Model of Intelligent Electric Grid based on Large Data

Yang Ying, Meng Huiping[a], Dang Fangfang[b], Yan Lijing

Information & Telecommunication Co. of State Grid Henan Electric Power Company, Zhengzhou, 450052, China

[a]email:iemengping@126.com, [b]email: 1365351078@qq.com

Keywords: Infiltration technology, Security situation analysis, Early warning ability

Abstract. With the development of the electric power enterprise, the security of information and communication has been pay more attention than before. In recent years, the information security event aiming at the electric system has occur frequently. The infiltration technology and attack methods has been diversification and more purpose, persistent and complicated. It is urgent affairs to promote the ability of security situation analysis, perception and early warning. On the basis of the network flow collection and analysis system, this paper has realized automatic behavior analysis for the existing three-level network, information security equipment, basic soft and so ware and hardware, recognized the source of security problems, located the security threats accurately to improve the information security defense ability.

Introduction

In recent years, the information security event aiming at the electric system has occur frequently. The infiltration technology and attack methods has been diversification and more purpose, persistent and complicated. With the rapid development of the intelligent electric grid, the framework and network condition of electric business system has become more and more complicated. Henan company has put the whole information assets of 100 county companies into its management and operation system. It will face many challenges to guarantee the safe operation of this complicate and huge information system. The existing conventional information detection methods are uncertain when they are used to recognize the characteristics of complicate attacks, threats situation, risks early warning. If these security threats can not be discovered, controlled and disposed in time, they are possible to diffuse into the other key links of the regulation system to cause the fatal harms. Therefore, it is urgent affairs to promote the ability of security situation analysis, perception and early warning [1]. On the basis of the network flow collection and analysis system, this paper has realized automatic behavior analysis for the existing three-level network, information security equipment, basic soft and so ware and hardware, recognized the source of security problems, located the security threats accurately to improve the information security defense ability [2].

Deploy the Distributed Network Flow Collection and Analysis System, Realize the Complete Coverage Data Collection

Henan company has put the whole information assets of 100 county companies into its management and operation system, it has become a difficult problem of information security management that how to get the real-time and effective data. On the basic of the existing distributed network flow collection and analysis system, deploy it at the location of aggregation switch of county company to realize the collection and analysis of network flow, violation behaviors, information security attack and so on[3][4]. Judge the security situation of the network and upload the results of collection and analysis to the superior network security situation perception and analysis center to lay an accurate data foundation of the subsequent analysis.

Construct the Information Security Behavior Analysis Platform, Realize the Graded Network Security Situation Perception and Analysis

The information security behavior analysis platform can realize an accurate analysis on network security, it is a necessary premise of carrying out the effective network security supervise and management. On the basis of enterprise asset data, get the analysis results of the security threats situation through effective obtaining the large-scale network security events data and associate analyze on regulation, situation and behavior [5]. The information security behavior analysis platform conducts the security behavior analysis through the following methods.

(1)Automatic behavior analysis. Introduce the analysis sample into the controllable virtual environment, analyze or operate the sample. Judge whether the sample exists malicious codes by analyzing the automatic process of the sample.

(2)Abnormal flow detection. Build model for the normal behavior of the network. Recognize the abnormal flow through analyzing the flow offset to the normal behavior model.

(3)Trojan character analysis. Recognize the network flow according to the trojan character library.

(4)Network flow analysis. Include blacklist analysis, protocol analysis, network status analysis, network behavior analysis and so on.

(5)Terminal behavior analysis. Include terminal network model detection, vulnerability scanning and analysis, trojan character analysis, attack behavior analysis, customized behavior analysis.

(6)Vulnerability library attack analysis.

(7)Complicate and continuous threat detection, analysis and early warning.

After the associate analysis on the security behaviors according to the time period, conduct the associate analysis on the comprehensive clues to complete the security behavior evaluation. Combined with the recent network security situation, analyze the security level according to the security behavior perception. The security level can be specified according to the demand.

Build the Intelligent Alarm and Analysis Engine System, Realize the Real-time Alarm and Problem Location

Take the security events as the sample pool, conduct the intelligent self-study statistical analysis based on security events dimension index. Put the variety of security events into the alarm and analysis engine knowledge library to realize the comprehensive process on the different security events from different manufactures. Aiming at the security events and alarm related analysis, build the alarm analysis system. This system can analyze the security events layer by layer, transfer the alarm and locate the problem quickly, avoid the repeated alarms and useless alarms. Recognize the source of security clearly, locate the root reason of problem accurately. Collect the data flow of the backbone network switches through the high speed network receiving device to analyze the network attack. Discover the variety of information assets through the asset management system to provide the data basis for the analysis on the network attack. Scan the security vulnerability of the information assets through the vulnerability scan and management system to provide a multi-dimensional data source.

This system is deployed through the method of functional module cluster. The data collection cluster includes:

(1)Data flow collection cluster: conduct the full traffic mirror collection to the backbone network data.

(2)Security log collection cluster: collect the security logs of the internal network and information security devices.

Conduct the targeted analysis on the corresponding security data through data collection cluster. Send the flow event to the Hadoop big data cluster to realize the quick log search on the level of TB.

At the same time, send the result of the targeted analysis to the center database. Send the flow data and original events to the message process center. The message process center will dispatch

these information to the associated analysis engine cluster to conduct the security analysis on the information. The result of analysis will be returned to the message process center to use the pre-setting regulation to conduct the task and find the vulnerability. Users can inquire the security event, security alarm, assets information though the management center.

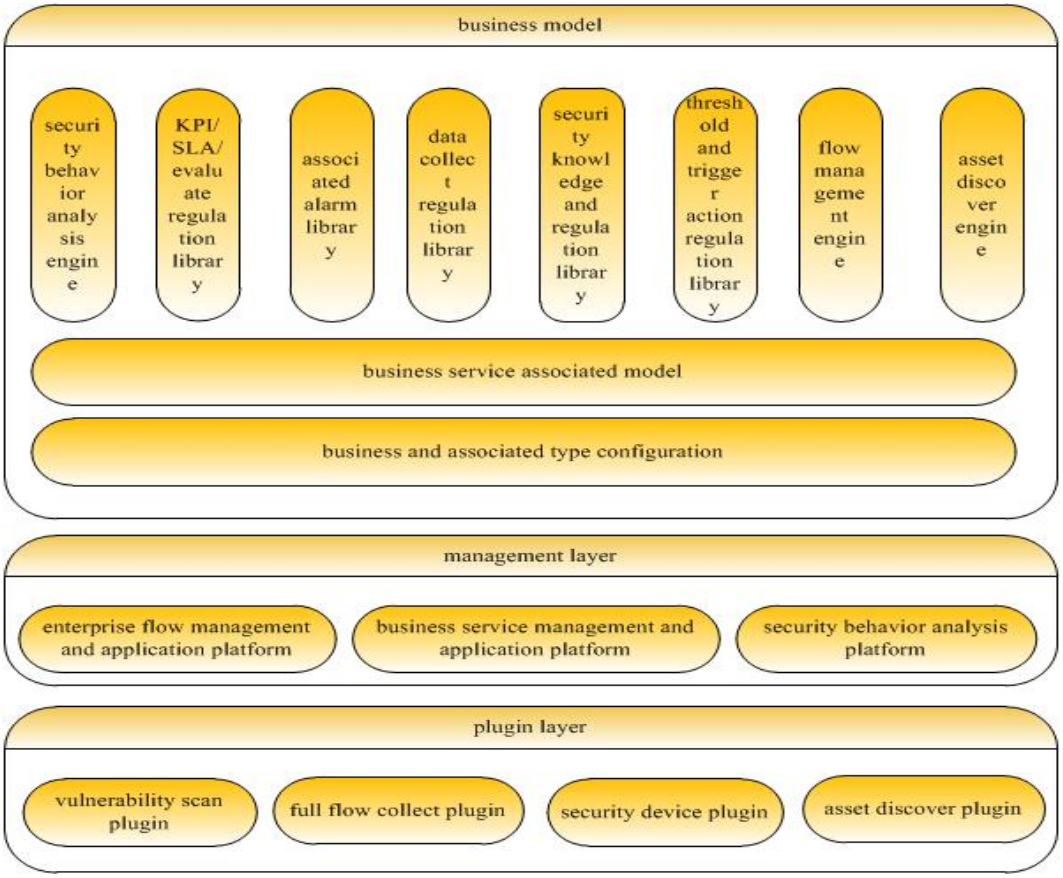

Figure 1.The security management model

This system is made up of three layers. The lowest layer is plugin layer. It includes vulnerability scan plugin, full flow collect plugin, security device plugin and asset discover plugin. Above the plugin layer, there is management layer. This layer includes enterprise flow management and application platform, business service management and application platform and security behavior analysis platform. Above this layer, there is business and associated type configuration, business service associated model. They realize the security behavior analysis engine, KPI/SLA/ evaluate regulation library, associated alarm library, data collect regulation library, security knowledge and regulation library, threshold and trigger action regulation library, flow management engine and asset discover engine. Based on the above models, it has realized the full flow collection, information assets discover, vulnerability detection, security attack analysis and so on.

Conclusion

This project has realized the panoramic monitor on the information assets and business network data communication and formed a real-time automatic defense system. The system can recognize the continuous, coordinated, complicated and concealed security attacks automatically and provide an effective support for the security maintenance staff to implement the more accurate protective measures and conduct a precise judgement and response. It can improve the real-time security defense level of the business network operation system powerfully.

References

[1] Zhu Ting, Research on The Intelligent Electric Grid Information Security Standardized Wor [J].

Enterprise Reformation and Management, 2017.

[2] Yang Bin, Zhang Dahua, Xie Yingjun, Research on The Intelligent Electric Grid Information and Communication Management System[J]. Information Technology, 2011.

[3] Zhang Zhou-feng, Security Analysis and Architecture of Intelligent Inspection System Based on RFID. Zhengzhou University,2011.

[4] Li Mengxing, Chi Chengzhe, Wang Haiyan, Research on The Electric Grid Enterprise Information Security Situation and Defense Measure[J]. Information and Communication, 2010.

[5]Yin Zhi-qing. The Analysis and Practice of Electric Power Enterprise Network Security Construction[J]. Power Information, 2009.