IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 4, Aug - Sept, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

ICS BEHAVIOR AUDITING SYSTEM FOR ELECTRICAL, PETROCHEMICAL INDUSTRY

Yuan Huang

ZTEsoft; Kai Chen, Institute of Information Engineering of Chinese Academy of Sciences

Abstract

The threats of industrial control system have increased. Traditional security audit technology can`t meet the security needs of the petrochemical, power and other industrial control systems. We design a behavior auditing system. The product supports collecting the security events about the power, petrochemical typical industrial control system. It can analysis the correlation, as well as do the safety assessment and positioning the safety incidents. The product supports data analysis and visualization of the results. It can also provide multi-dimensional security reports for managers.

1. Introduction

Security incidents on industrial control system occur frequently. It attracts the attention of people around the world. Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). ICS are typically used in industries such as electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical and pulp and paper. These control systems are critical to the operation of the country. Its operation related to the strategic security of the country [1].

Traditional network and information system is based on TCP/IP. Many industrial control systems have specific protocols. These protocols have a high efficiency and real-time performance, but with lower security. With the rapid development of industrialization and information technology, industrial control systems products are increasingly using information technology (IT) based on common protocols, common hardware and software. While promoting the development of industrial production, it also has security problems of industrial control systems. Meanwhile, in order to improve the operating efficiency of the plant or company management, industrial control systems connect to public network such as Internet through a variety of ways. Trojans, viruses and other threats are spreading to industrial control systems.

Industrial control and information security has just gone through more than a decade. It is still in development. How to build a comprehensive knowledge and practical application of the system is the starting point of our top priority and that the audit system design. The rest of this paper is structured as follows. Section 2 describes the industrial control system security situation and threats of the ICS.

Section 3 presents the behavior auditing system products. Finally, we outline items for the future work in section 4.

2. Safety Status of ICS

Since 2001, the development of common standards and Internet technology is widely used in industrial control systems. Industrial control system security is becoming increasingly serious. The "Stuxnet" incident in 2010 fully reflects the grim situation facing the industrial control systems of information security [2].

The Repository of Industrial Security Incidents (RISI) shows that the world has more than 200 attacks on industrial control systems till October 2011[3]. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) showed that there are 295 incidents in 2015. The key manufacturing sector accounted for 97 of these events. There are 46 from the energy industry. And 25 events are from the water and wastewater systems [4].

Ministry of Industry issued "The notice on the strengthening of industrial control systems for information security management" in October 2011. The notice requirements of various departments and enterprises need to fully understand the importance of industrial control systems for information security management. It aims to guarantee the security operation of SCADA, DCS and PLC in the industrial field [5].

Currently, the main security threats facing the industrial control systems are in the following areas:

(1) Industrial control security threats on specific protocols

Industrial control systems have a large number of specific protocols, such as OPS, Modbus, etc. These protocols are closed. These protocols are regarded as safety protocols in mistake. The primary purpose of these protocols is to ensure high availability and business continuity. Due to lack of security considerations, they are likely to cause major security incidents. With the development of industrial control systems, the systems use a large number of terminals and PC servers. There are also general operating systems and databases in the systems. ICS are suffering attacks from the Internet Trojans and hackers.

(2) Network security threats

Initially, industrial control systems and enterprise management systems are not connected. Both systems run separately. But in recent years, in order to achieve real-time data acquisition and transmission, industrial control systems and enterprise management systems connected by way of logical isolation. So the two systems can communicate with each other. Enterprise management systems are generally connected to Internet. In this case, involving a range of industrial control systems further expanded. It is vulnerable to attacks and threats from the Internet. In the case of mixing private and public networks, the security status of industrial control systems will become more complex.

(3) Risk on security policy

In order to pursue the availability, many industrial control systems ignore safety. The lack of a complete and effective security policy and management process is the biggest problem of industrial control systems [6]. Although many security measures have been implemented, the system is in threats because of operational errors or management.

(4) Operating system security threats

There are various different operating systems (Windows, Linux) in ICS. Lots of operating systems are too old without updating. After updating the operating system patches, industrial control software may not be compatible with the new patch. Therefore, the general system will not run on Windows platform patch, causing the system security risk.

(5) Terminal and application security risks

Checking the application at the terminal before loading is a traditional way to prevent malicious software. But such measures have not enough strength to cope with the increasing attacks such as a rootkit would undermine the system services and operating system code.

3. Design of ICS Behavior Auditing System

3.1 Goals of the System

Industrial control system security threats continue to increase. The ICS behavior auditing system is an abnormal behavior for industrial control systems audit products. The system is to address the nation's critical industrial infrastructure-related security threats. Through a comprehensive monitoring system in a variety of sessions and events, to analysis the related information in intelligent control system, safety assessment and position safety incidents accurate. The auditing system can detect ICS abnormal behavior. It can also do business process behavior auditing, content monitoring and other related technologies. The auditing system can be applied to different industrial control network scenarios.

3.2 Technology Introduction

3.2.1 Proprietary Protocol Identify and Anomaly Analysis Techniques

Currently in the field of industrial control, there are many types of communication protocols. In particular, there are a large number of industrial control system proprietary protocols. These proprietary protocols have big differences to common network protocols. Existing security equipment and software can’t solve these security problems. The behavior auditing system aims to study the intelligent protocol identification and analysis technology for industrial control systems’ proprietary protocols. A variety of common protocols can be identified by the auditing system. The system analyzes the semantics of the protocol data after restructuring the data communication, to identify various communication sessions and system events. And ultimately achieve the purpose of the audit. Protocol identification technology is the core model. The system combines protocol analysis, environmental analysis, status tracking and pattern recognition technology, to intelligent identify and analysis upper layer protocol.

3.2.2 Vulnerability of Core Components and Vulnerability Mining Technology

We will focus on the core components of vulnerability mining technology based on Fuzzing. The study includes the vulnerability of its core industrial control components and vulnerability of industrial control software and hardware tap based on Fuzzing. Fuzzing is a technology through input a group of random test data. Then monitor procedures during the operation of any exception. The random data which cause exception will be recorded. Finally it further positioning the defects [7].

3.2.3 Technology on Abnormal Behavior Detection

Abnormal behavior detection analysis can discover the event and normal behavior inconsistent. It is helpful for administrators to control the influence of abnormal behavior and to prevent them. The abnormal behavior is avoided to network security. By simultaneously monitoring the abnormal behavior, it can find differences between behavior and usual behavior that the executor usually done. It is able to provide timely security for acts performer.

(1) Through establishing the normal behavior model of ICS, check the deviation of the current activities of the model. It can confirm the invasion behavior and security events.

(2) Real-time online analysis technology can shorten the time of behavior analysis.

(3) Network layer anomaly behavior detection analysis is based on DPI. The technology enables real-time/off-line deep packet analysis based on massive data processing platform. So that it can monitor the abnormal traffic devices effectively.

(4) Application layer software to detect abnormal behavior around the ICS applications. This feature collects the results based on the application layer data. It supports running state analysis, analysis of instruction tamper detection, anomaly detection analysis of configuration changes.

(5)Operating system different behavior detection based on security events often massive log analysis techniques. This technology can detect the security status of the entire system. Analysis unearthed a variety of information contrary to the normal operation of the system at the same time.

(6)Abnormal behavior-based network security forensics security event data, which is multi-period safety testing platform provided a detailed multi-dimensional. It supports a single point of access to security incidents.

3.2.4 Intelligent analysis of security events

Auditing system established a detecting abnormal behavior for industrial control system mechanisms. Correlation analysis focuses on the behavior of massive amounts of data and long-term attack. Smart industrial control systems related to the massive security event analysis, safety assessment, location and back related analytical techniques. The massive security events are from multiple regions, multi-terminal, multi-type, and history across all types of long-period event data collection.

3.2.5 Security Visualization

After analysis of the data, how to treat these data effectively, so that managers can be quickly and intuitively absorbed and exploited, has become a key issue to be solved. The system provides users with a global view of security event auditing through visualization technology. It supports security status tracking, monitoring and feedback. To provide accurate and effective reference information for decision-makers. And to some extent reduce the development time and effort it takes decisions. Minimize human errors. So that to improve management efficiency.

3.3 Structure of the System

As for industrial control system behavior auditing system of electric and petrochemical industry, the main function is to collect various ICS security event information and take intelligent correlation and analysis, as well as hardware and software vulnerability discovery, that enabling industrial control system reaches the goal of security assessment and security incidents accurate positioning.

Our auditing system design lying on four-layers structure which namely data collection, information and data management, intelligent analysis of security incidents and security of visual display, as shown in figure 1. Where in the data collection terminal monitor the industrial network system service logs, communication sessions and security events by security agents, flow mirroring crawl detection, etc. In the multi-layer implement environment, the use of relay isolation mode unidirectional reported collecting information can adapt to a variety of network environments better. Management information data parsing such as MODBUS, OPC, Ethernet / IP, DNP3, ICCP and other proprietary protocols, can storage distributed mass data, optimize structure and query efficiency, and achieve data plane system scalability. By heterogeneous data analysis, intelligent analysis layer can do preprocessing for the analysis result. By using security event correlation analysis and safety data mining technology, industrial audit system application process can find protocols and behavioral abnormalities.

Comprehensive presentation layer security can take security audit results visualization, render industrial control system security events, identify security threats and security trends in industrial control systems as well as give pre-judgment.

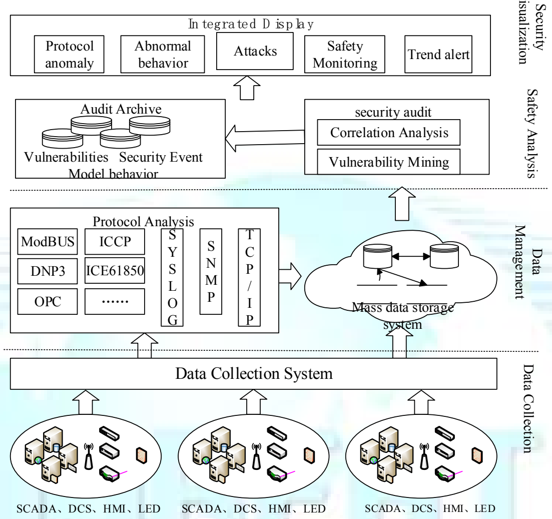

Figure 1: ICS auditing system architecture

Data acquisition need to get raw data necessary conversion, make the data more standardized, meanwhile make the data preprocessing and the uploaded data integration. Since the data collection involves various types of equipment, collection points need to be deployed in each node of the network, it is necessary for our system to adopt a standard framework for data collection. Based on the Open Agent Architecture Framework which using Agent technology for data collection ， on the one hand ， it has compatible with existing sources of data collection protocol, on the other hand ， can be easily extended for possible future source data acquisition protocols. The main part of the acquisition target can be divided into three parts, one is the network or host a variety of log files generated by the equipment and device status information, and the second is a network packet, the third is the operation of the industrial control terminal, configuration information and protocol data flow.

Data management is responsible for receiving data extraction and data acquisition from data layer, as well as the data necessary preprocess. In view of the electric power, petrochemical and other industrial control network and system size, the amount of the information collected will be formed between GB and possible to reach PB, traditional file systems and relational databases can’t afford such a large data load. Therefore, in the data management framework rely on the mass data storage system can achieve data cloud platform. Combination of HDFS and HBase programs as the basis for data management platform [8], thus ensuring TB or even PB-level data storage and management capabilities. Figure 2 shows the hierarchy of the module.

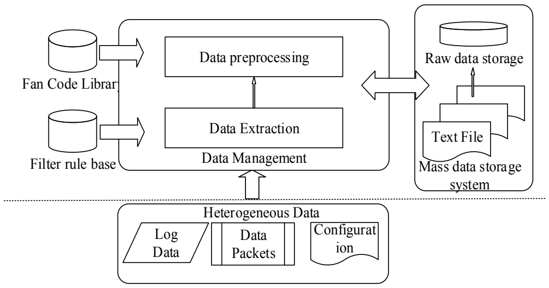

Figure 2: Hierarchical data reception and storage module schematic

Data analysis played a key role in the entire system, it brought forward that the link to the data received and stored after the conduct reduction integrated processing. The main aim of the event information for the same device generates the same object integration, at the same event in a time sequence of the same object in different devices produced in accordance with the sequence of events for integration. This is make use of taking organize and process information for twice, from a logical analysis of the level of correlation between the data [9]. That latter is the data of portion can reduce and be integrated after the subsequent safety applications and even visual display, which provides an important basis for analysis. Hierarchical data analysis section is shown in Figure 3.

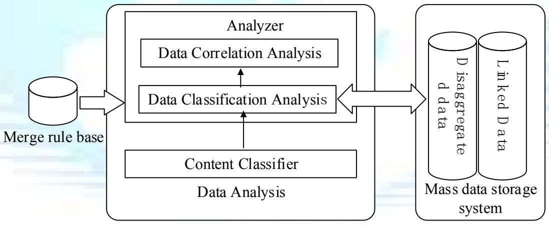

Figure 3: Data analysis schematic

Visualization is the interface between the user and the system, which achieve the safe state visualization, interaction analysis, tracking, monitoring and feedback. From the use of perspective, security visualization including reporting, historical analysis, real-time monitoring, security events, security model five categories. Among them, the historical analysis including time series analysis, correlation diagram, interaction analysis and forensic analysis.

3.4 Promote this application

Ultimately, Industrial control systems will formation behavior auditing system products for the power industry, the petrochemical industry, the formation of large-scale application. Therefore, the product will be developed with the power, petrochemical industry characteristics program of industrialization, construction of industrial control system behavior auditing system. Transition Center implement product engineering, and construction product promotion center for marketing and solutions planning, construction of service centers to provide customers with the sale and so before, after-sales service and training. Finally, culminate in a full range of industrial control system behavior auditing system products industrial capacity.

In order to make largest safety value of industrial control systems behavior auditing system for power, petrochemical industry, the Ministry of Planning for the majority of system integrators and end users. Based on industrial control the behavior of the various auditing system provide solutions developing, porting, testing, optimization, selection, training, consulting and implementation services. What's more, there will be highly available, scalable and high performance solutions for customers.

4. Conclusion

This paper analyses threats in the industrial control system currently, combined with the current needs of industrial control systems. Then design the ICS behavior auditing system. The auditing system support protocol analysis, vulnerability discovery, behavioral monitoring, visualization and other methods to achieve the purpose of the industrial system security assessment and security incidents targeting. The ICS auditing system consists of four-tier structure, namely data collection, data management, security event analysis and security visualization. It can monitor system capable of sessions and events. So that it has the ability to improve the security of industrial control systems.

Acknowledgments

The project was built by the fiscal [2013] No.757 of China to provide support.

References

[1] CM Xia, T Liu, HZ Wang, Q Wu. Industrial Control System Security Analysis [J]. Information Security and Technology,2013,02:13-18.

[2] QZ Wei. Industrial Network Control System Security and Management. Measurement & Control Technology,2013,32(2):87-92.

[3] 肖建荣.工业控制系统信息安全[M].北京:电子工业出版社,2015:1-4.

[4] Industrial Control Systems Cyber Emergency Response Team. NCCIC/ICS-CERT 2015 Year in Review[OL]. https://icscert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

[5] 工信部.关于加强工业控制系统信息安全管理的通知—工信部协[2011]451 号[J].计算机安全,2012,2012(1):2-3.

[6] 张帅.工业控制系统安全风险分析[J].信息安全与通信保密,2012,2012(3):15-19.

[7] ZY Wu, HC Wang, LC Sun, ZL Pan, JJ Liu. Fuzzing. Application Research of Computers，2010,27(03):829-832.

[8] Priyanka D. Harish, Swapnoneel Roy. Energy Oriented Vulnerability Analysis on Authentication Protocols for CPS [C]// Proceedings of the 10th IEEE International Conference on Distributed Computing in Sensor Systems. Marina Del Rey, CA: IEEE, 2014.

[9] DD Lin, JG Zhang, JY Li, et al. Identifying Genetic Connections with Brain Functions in Schizophrenia using Group Sparse Canonical Correlation Analysis[C]// Proceedings of the 10th IEEE International Symposium on Biomedical Imaging. San Francisco, CA: IEEE, 2013.