An overall design of network security situation assessment system

Yuxin Zhao[1] Yuan Hu[2]

Professional Department,Beijing Information Technology College,Beijing，China

Computer Science Department,Beijing University of Technology, Beijing，China

zhaoyx402@126.com,ichigo517@126.com

Keywords: Network security; overall design; Logical structure; Physical structure; Distributed deployment model

Abstract. In order to help network managers better grasp the situation of network security, and timely respond to major network security incidents, as well as reduce the loss of network attacks bring to the target network, network security situation analysis system has been studied and the overall design is proposed, whose logical and physical structure has been designed in detail. At the same time, for the purpose of meet the application requirements, a cascade distributed deployment module is proposed, which would laid a solid foundation for the promotion and application for the system.

Introduction

With the development of science and technology, all kinds of network security has become an inevitable event in our country, such as the network of economic crimes, large-scale network attacks, theft and other problems. All these have become key factors threatening social stability, national security and restricting economic development of our country. Therefore, network security situation analysis has become an inevitable development trend of future network management, and theoretical research and application deployment for it has become a research focus. Fortunately, our country has realized the urgency of protecting our information systems; Supported by the National High Technology Research and Development Program, Our research carried out a systematic and practical exploration on network situation analysis system, the overall design of the system has been researched. Details are as follows:

Architecture of network security situation analysis system

Architecture of network security situation analysis system is shown in Figure 1.Divided into data integration module, system functions module and system interface module. The function of each module is as follows:

A. Data Integration Module

Network security situation analysis system input data from different sources, including diversity deployed in the network security devices and data sources of different types of users, such as caused by the reported data. Data collection network security event format was diversity, so the first step in network security situation analysis is to preprocess the data and integration. Some expert knowledge provided by the upper layer application, the collected are stored to the corresponding database (library network security incidents, vulnerabilities library equipment, equipment operation information database, information flow statistics library, etc.). This module mainly uses a scalable data integration technology based on Agent, which is based on schema mapping technology to overcome, XML, intermediate representation and other traditional techniques in data source dynamic and strong, massive lack of real-time integration environment. Dynamically join and withdraw support data sources, a high degree of scalability. This technology not only theoretically support any data source integration, and can also effectively support data collection across the administrator, it can meet the network environment for large-scale needs.

B. System function module layer

System function module layer includes two core functions: network security situation assessment and network security situation prediction.

- Network security situation assessment is mainly based on multi-dimensional, configurable system quantifiable indicators to describe the macroscopic overall security posture of the network. Model based on pre-defined indicators Knowledge user, based on the acquisition of network security incidents come to quantify network security index value is calculated.
- Network security situation prediction is based on historical data of statistical laws, through the relevant trend forecasting model to predict changes in network security, providing early warning network for network administrators, network managers to facilitate network protective measures taken in advance, thereby reducing network attacks carried to risk.

C. System interface presentation layer

System interface presentation layer mainly responsible for providing a variety of calculations to the user interface and interactive display of network security posture of the system. Mainly includes two aspects: First, through an intuitive graphical mode image of the results calculated by the system function module displayed, such as the situation in real-time display interface, security event viewer interface, network topology view interface, statistics, query interface, trend forecasting View interface. The second is to provide the user interface to interact with the system, to facilitate the management of the underlying knowledge base, such as the index system configuration interface, user preferences, search interface, network security alarm sorting feedback interface, configuration interface, such as association rules.

D. Data Acquisition Module

Data acquisition module mainly includes the following four aspects:

- Network security events collected from a variety of network security devices, such as the target network vulnerability information, traffic characteristics, and network attacks, etc.
- Network security alarm events obtained by the correlation analysis of the original event in analysis module;
- Network security posture index and major network security incidents reported by lower-level network security situation analysis of network security situation systems. Its output is used to reflect the network security situation index value.
- Network security issues detected by low-level network probe.

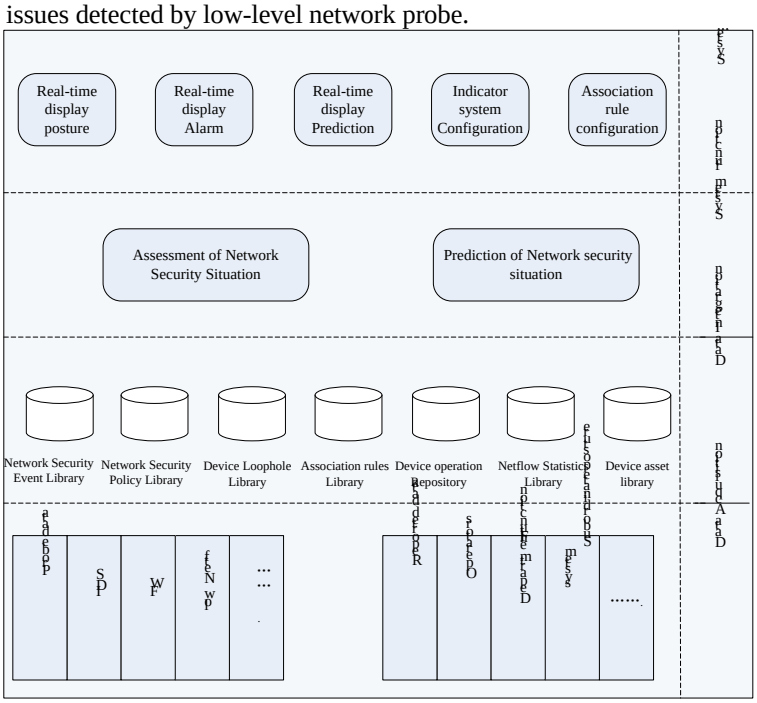

Fig1.Architecture of the system

Physical structure of network security situation analysis system

Single network security situation physical structure of network security situation analysis system

is shown as follows:

Figure 2 shows the physical structure of network security situation analysis system. Target network information flow monitoring and network security testing provide the agent. These network security devices get into the network security situation analysis system in the past. The collected data are over the network integration and the associated servers centrally. After processing is complete storage to network security situation analysis database server system above. Network security situation assessment server for real-time assessment is decided by reading the data in the database. Final results by showing the relevant server network security situation analysis system presented to the user.

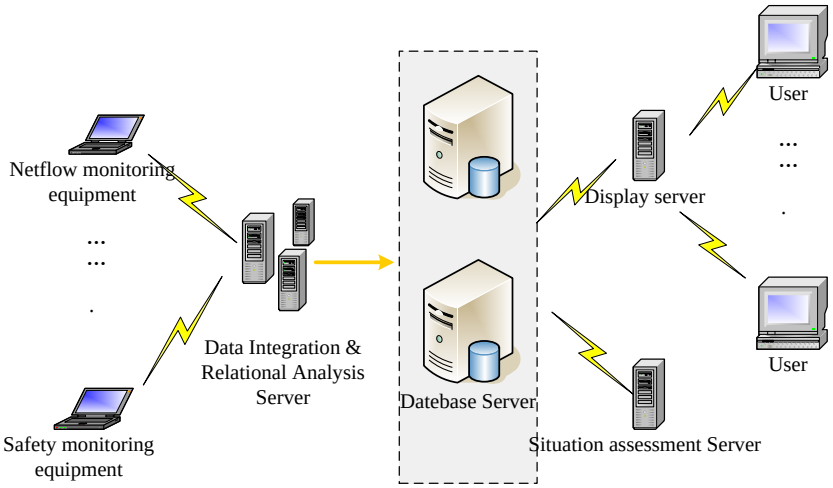

Fig2.Physical structure of the system

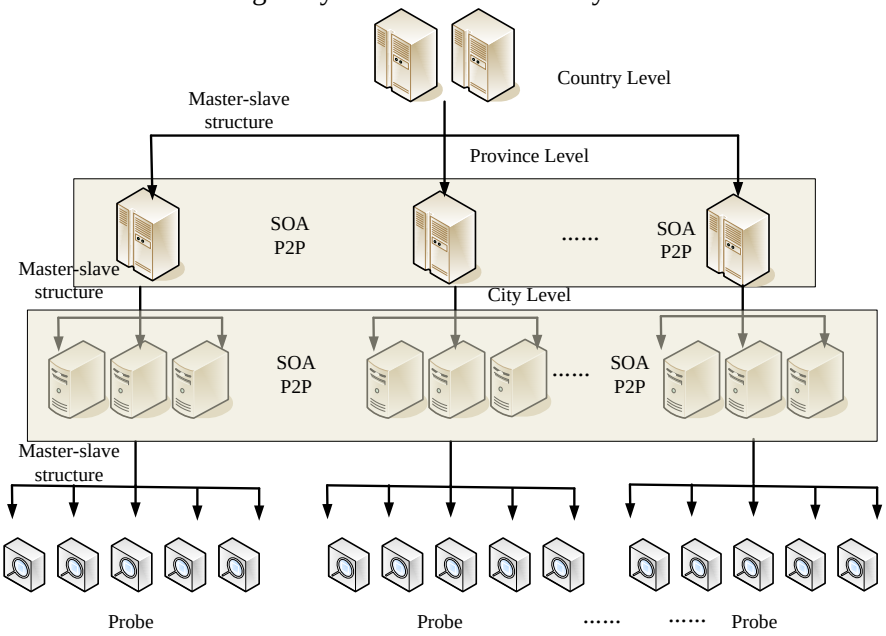

Fig3.Deployment structure of the system

Distributed deployment of network security situation analysis system

Single network security situation physical structure of Demand for the use of the national backbone network security situation analysis, this section gives a multi-level network security situation deployment structure analysis system. As shown in Figure 3, the structure can be seen from the deployment, the system supports three levels of cascading deployment linkage analysis and other levels:

E. first level

The first level is the national security situation analysis server deployment;

F. second level

The second level is the provincial security situation analysis server;

G. third level

The third level is the municipal security situation analysis server. Between the upper and lower levels of network security situation analysis system, using the "master-slave" type of cascade, lower network security situation analysis system will calculate its network security situation and major network security incidents reported to the higher level network security situation analysis system, facilitate superior network security situation analysis system to achieve the overall network security situational awareness.

The entire deployment program uses "distributed sensing plus distributed processing plus distributed storage" and "divide and conquer integrated" approach, the network security situation integrated computing tasks into parallel analysis on different computing and storage nodes, each node local computation results through the "master-slave" cascade summary comprehensive and effective implementation of the security situation on the whole network of global cross-domain control.

Process of Network Situation Assessment

In order to free the network administrator from the massive network security logs, and facilitate the management to master the target network security from the macro.

First, we establish the index system through configuration subsystem index system. There are a variety of properties which can affect the network security situation, and each of them has different importance, and the decision situation in different networks or the same network at different times of factors is evolving. Therefore, we need to establish evaluation index system for specific applications under the index system can be configured by the subsystem, and then stores the index system to index system library database.

When the system is running, the index is calculated by reading the index system database subsystem, the role of the index system analysis module of the user pre-defined indicator system loaded into the system as an index system model of the current network security situation assessment

Then, based on the index system, the network security situation is calculated using the network security data detected by low-level Data acquisition module, As the network security posture by multiple underlying factors comprehensive evaluation of network security situation gets so involved in the issue of the importance of each factor in the overall trend of network security situation assessment. Generally in different application environments, network manager focus on network security will be different, such as a service provider for the purposes of denial of service attacks that may affect the service than the impact of the availability of data confidentiality Trojan attacks more serious. Hence the need to assess the situation on the basis of a given factor, the use of network-based security index weights interactive search methods to mine user rights situation in each weight factor above.

Finally, the results of the situation calculation are written back to the database, and display to the user through index visual display subsystem.

Conclusion

In this paper, an overall design of network security situation analysis system is proposed, which consists of data acquisition subsystem, data integration subsystem, association analysis subsystem, situation assessment subsystem, the trend prediction subsystem and the front display subsystems. The system has a customizable, adaptive, self-feedback, quantifiable indicators, which can describe the current macroscopic security posture of the national Internet, and well reflect the underlying network operation, as well as adaptive adjust network security index system depending on the application requirements.

References

[1] LIN C, PENG X.H. "Research on network architecture with trustworthiness and controllability",Journal of Computer Science and Technology,Volume 21- No. 5, May 2006,pp. 732-739.

[2] Dhanakoti M, Nedunchezhian R, "Correlated Alerts and Non-Intrusive Alerts", Journal of Control Engineering and Applied Informatics,Volume14- No. 4, April 2012,pp. 3-9.

[3] Panagiotis V, Ioannis G, "Karafyllidis. Simulation of quantum key expansion using quantum cellular automata", Computer Physics Communications,Volume180- No.2, February 2009,pp. 251-255.

[4] Haslum K, Arues A, "Multi-sensor real-time risk assessment using continuous-time hidden Markov models", Computational Intelligence and Security, May 2007,pp. 694-703.

[5] LIN C, PENG X.H, "Research on network architecture with trustworthiness and controllability", Journal of Computer Science and Technology,Volume21- No.5, May 2006,pp. 732-739.

[6] Kizza J M, "Computer Network Vulnerabilities", Kizza J M. Guide to Computer Network Security. Springer, 2013: pp.89-105.

[7] Wei S, Jin N, Hui X, et al, "A situation assessment model and its application based on data mining", In Proceedings of the 9th International Conference on Information Fusion(ICIF 2006), Springer, 2006,pp. 1-7.

[8] Soliman M A, Ryas I F, Martinenghi D, et al, "Ranking with uncertain scoring functions: semantics and sensitivity measures", In Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD 2011), ACM press,. 2011,pp.805-816.