A Network Security Situation Awareness Method Based on Multi-source Information Fusion

Yue Gao[a], Shuying Zhang[*, b]

College of Computer Science and Technology,Beihua University

Jilin, Jilin, 132021, China

*Corresponding author

[a]lunagao@126.com, [b]jlzhangsy@126.com

Keywords: Multi-source Information; Network Security; Information Fusion; Situation Awareness

Abstract. This paper introduces the situational awareness theory and classical model, and proposed a network security situation awareness model based on multi-source information fusion. The model makes a situation awareness through the collection, extraction, pretreatment, normalization and situation calculation of the information of network multi-source data elements. Compared with the existing safety situation assessment and awareness method, the structure of the model is more complete and the results are more accurate and effective.

Introduction

With the rapid development of computer network, various kinds of cyber attacks have been happening, and the issue of network security has become the focus of attention. Firewall, intrusion detection system, and other safety equipment deluge alarm information every day, so that network administrator is very difficult to understand the security situation in the system in the face of a large number of alarm information, and they can’t take appropriate response measures in a timely manner. Therefore, how to accurately and accurately predict the network security situation has become a research hotspot in the field of cyber security. In recent years, situational assessment techniques have been applied in the field of computer networking. There's a lot of research done by experts at home and abroad. The United States, Canada and other western countries have established the situational forecasting system and developed the situational forecasting software. Tim Bass's data fusion model gives a methodology guidance [1] . In our country, it's late to start the situational awareness, but there are a lot of research and exploration. Y. D. Chen et al. established a conceptual model and architecture of network security situational awareness [2]. D. P. Liu et al. designed a multi-granularity network security situational awareness model based on knowledge base [3]. Y. Wei et al. proposed an evaluation framework for the network security posture assessment model[4].

This paper draws on the existing achievements and experience[5-7], presented a method of network security situation prediction based on multi-source information fusion.

In the second section of this paper, author introduces the theoretical model of situational awareness. In the 3rd section, author introduces a typical network security situational awareness model. In the fourth section, author introduces network security situational awareness model based on multi-source information fusion. The last section is conclusion.

The Theoretical Model of Situational Awareness

In the late 1990s, situational awareness was introduced into the field of information technology security and was first used to study the next generation intrusion detection system. Then there is the concept of network situational awareness. The situational awareness in this paper refers to the situational awareness of network security. At present, there is no unified definition of security situation perception, and a descriptive definition is given below:

Network security situational awareness, which refers to use technical means to obtain the whole network security element, such as various network equipment operation status, network behavior and user behavior and so on from the latitude of time and space in the large-scale network environment. And determine the network security situation and predict its future development trend by the integration analysis of the obtained multi-source data information.

Endsley conducted systematic research on the evaluation method of situational awareness and situational awareness, and built the theory foundation of situational awareness, The theoretical model of situational awareness [8] is shown in Fig. 1:

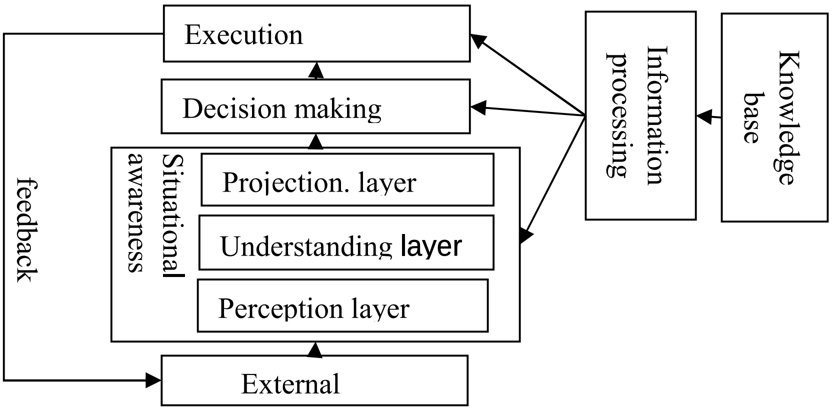

Fig. 1. The Theoretical Model of Situational Awareness

Situational awareness includes three levels: Perception, Comprehension and Projection.

Perception layer: it is responsible for the perception of various elements in the environment, including the state of the environment, properties and dynamic changes of the environment. This level of activity is done by people's senses such as vision, hearing, and touch.

Comprehension *layer.* it is based on the perception layer, measuring the importance of environmental elements to achieving goals, and synthesizing all the elements together to understand.

*Prediction layer.*The highest level of situational awareness is based on the perception layer and the understanding layer, predicting the next state and behavior of each element in the environment.

A Typical Network Security Situational Awareness Model

In order to evaluate the operation situation of a network comprehensively, accurately and objectively, scholars have studied many perceptual models. As shown in Fig. 2, a typical network security situational awareness model is presented.

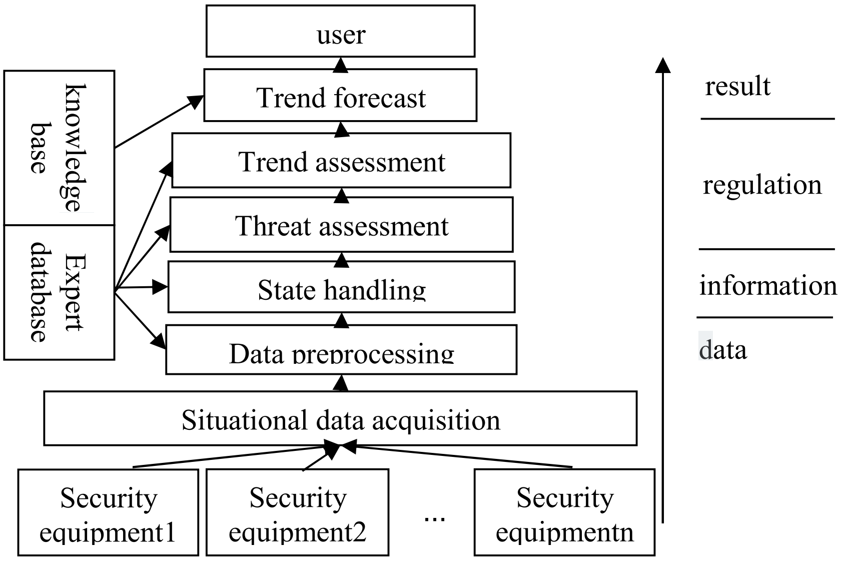

Fig. 2. A Typical Network Security Situational Awareness Model

In this situational awareness model, the realization of situational awareness is divided into 5 levels (stage).Firstly, IT resources are collected and then processed through different levels of processing and feedback, finally realizing human-computer interaction through situational visualization. The five processing levels are:

Data preprocessing: it is an optional level, preprocessing for some unstructured data, such as user distributed processing, impurity filtering, etc.

Event extraction. It refers to the standardization and revision of events after information collection, and an extension of the basic characteristics of the event.

Situation assessment: including correlation analysis and situation analysis. The result of situation assessment is to form the situation analysis report and the network comprehensive situation map, and provide support decision information for network administrators.

Impact assessment: it will map the current situation to the future and assess the impact of the participants' assumptions or prediction behaviors;

Resource management, process control and optimization: through establishing certain optimization indicators, real-time monitoring and evaluation of the whole integration process, and achieve optimal allocation of related resources.

Network Security Situational Awareness Model Based on Multi-source Information Fusion

The network security situational awareness model based on multi-source information fusion is shown in Fig. 3.

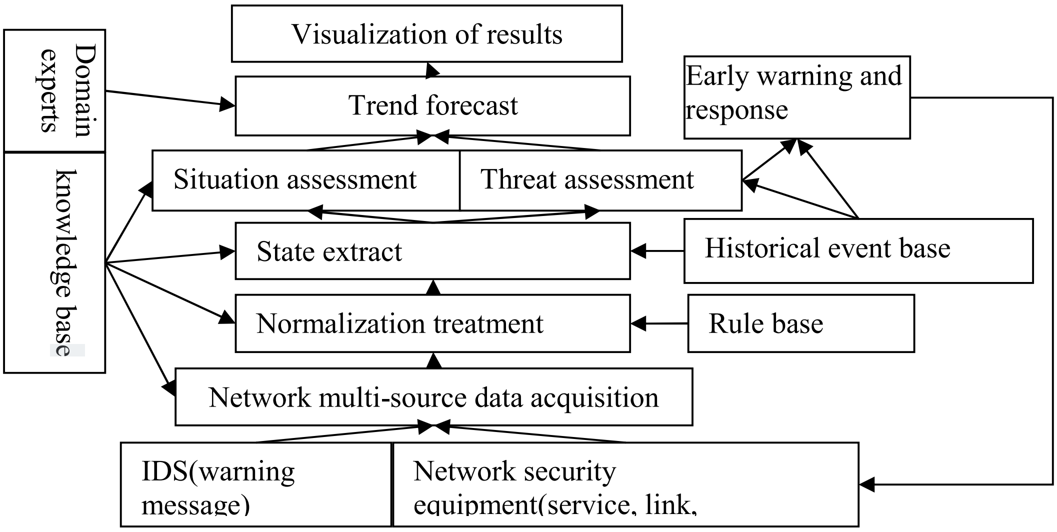

Fig. 3. Network Security Situational Awareness Model Based on Multi-source Information Fusion

The model can be divided into three levels from the bottom up, namely, multi-source information layer, network security posture assessment layer, and network security situation prediction layer, which can be divided into the following main parts.

Network data collection. Network data collection includes data collection of several aspects such as network threat information, service status information, link status information, network configuration information and network traffic information. Different information corresponds to different methods of collection, such as traffic information using netflow software, threat information using Snort and other software and so on.

Data normalization processing. All the raw data collected is normalized according to certain rules. The main function of normalization is to extract the valid information of the data. After normalization, the data can be analyzed and processed by expert system.

Extraction of state information. Based on the knowledge of the expert knowledge library and the history event library, analyze the normalized data, process, extract useful network status information.

Situation assessment. It includes correlation, situation analysis and situation evaluation. The core of the situation assessment is the correlation analysis. Correlation analysis is to use data fusion technology to correlate and identify multi-source heterogeneous data from time, space, protocol, etc.

Dangerous assessment. Analyze the network data according to historical event database. Event features in historical event libraries can be updated and supplemented in real time. Because the dangerous assessment is accurate and fast based on the historical event library, once the danger is assessed, the danger is immediately sent to the upper level for security situation prediction, and send alerts and responses to users. But the dangerous assessment is impotent against uncharted or unformed attacks. Therefore, it is necessary to carry out an abnormal situation assessment of this data while conducting a dangerous assessment of network data.

Situation prediction. Based on the results of situational assessment and risk assessment, assess the current security situation of the network and predict the future security status, and provides a reasonable basis for users to make rational decisions about network status security.

Early warning and response. The results of situational assessment and hazard assessment can be put into early warning and response modules. On the one hand, it can be used to visualize the situation. On the other hand, the process processing module is sent to the process processing module to process the response and security dangerous operation.

Conclusion

This paper presents a network security situational awareness model based on multi-source information fusion, which is based on analyzing the theoretical model of network security situation perception and current research situation at home and abroad. This model comprehensively considers multi-source network security information, using rules library, knowledge base, historical event library and other domain knowledge, and preprocessing multi-source information, state extraction. And then, it can realize the threat assessment, situation assessment and situation prediction of network security state. The software architecture of this model has been built, and have implemented some of these key technologies. Next step, we will delve into data fusion technology to make situational awareness more accurate and timely.

Acknowledgment

The research work is supported by "Internet+ education model of Linux curriculum group construction and teaching mode research (GH16061) and "research on Java series teaching mode based on education concept of CDIO engineering (GH170128)" of the 13th five-year plan project of education science in Jilin province.

References

[1] T. Bass, Intrusion Detection Systems and Multi sensor Data Fusion, Communications of the ACM, Vol.43(4) (2000), p. 99-105.

[2] Y. D. Chen, L. W. Zhao, etc. Research on network security situational awareness system structure [J], Computer engineering and application, Vol.44(1) (2008), p. 100-102.

[3] D. P. Liu, X. H. dong et al., the cloud method of multi-granularity analysis of network security situation computer application, Vol.2(2009), p. 370-373..

[4] Y. Wei, Y. F. Lian, etc. A network security situational awareness model based on information fusion.Journal of Computer Research and Development, Vol.46(3)(2009, p. 353-362.

[5] Z. C. Wen, C. L. Cao, Network security situation awareness based on weighted factor, Journal of Computer Applications, Vol.35(5) (2015), p.1393-1398

[6] C. L. Wang, L. Fang, D.X. Wang, et al. Network security situation awareness system based on knowledge discovery, Computer Science, Vol.39(7),(2012), p.11-24.

[7] Y. Dong, Research on Key Technologies of Large-scale Network Security Situation Awareness Based on Network Traffic, PLA Information Engineering University,(2013)

[8] M. R. Endsley , Toward a theory of situation awareness. Human Factors, Vol. 37(1) (1995), p. 32-64