International Journal of Computer Networks and Communications Security

VOL. 5, NO. 4, APRIL 2017, 71–75
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Multi-Perspective and Multi-Level Analysis Framework in Network Security Situational Awareness

M.Azhagiri, Dr A.Rajesh and Dr S.Karthik

[1] Research Scholar, St.Peter's University, Avadi, Chennai-600054

[2] Professor/CSE, C Abdul Hakeem College of Engineering and Technology, Melvisharam, Tamil Nadu 632509

[3] Associate Professor/IT, V.M.K.V Engineering College, Salem, Tamil Nadu 636308

[1]*azhagiri1687@gmail.com*

ABSTRACT

Network Security Situation Awareness (NSSA) knowledge has been comprehensively studied in multi-data analyzing research these years. NSSA is a conception pertinent to assessing and showing the global and comprehensive situation of network security, so it requires people to collect all kinds of data and analysis for as many dimensions as possible in order to reflect the macroscopic pictures. For network security situation evaluation method has been provided, and it represent's how to apply this method to NSSA. A multi-perspective and multi-level analysis framework for NSSA is presented to demonstrate the advantages and effectiveness by using this method.

Keywords: *Situation Awareness, Multi-Level Analysis, Multi-Perspective Analysis, NSSA.*

1 INTRODUCTION

The idea of Situation Awareness (SA) comes from the research on human factors in the domain of aerospace and aviation. The concept of Situational Awareness is an extremely important one in information security cyber security operations. Situational Awareness is defined as: "Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future." Also, it is stated that Continuous monitoring is ongoing observance with intent to provide warning. A continuous monitoring capability is the ongoing observance and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations.

Research of Network security situational awareness (NSSA) is based on the integration of all kinds of network security elements of the assessment from the macroscopic angle of real-time network security situation. Also it predicts the development trend of network security situation in certain condition.

The definition of the conceptual model is shown in Figure 1. However, the traditional concept of situational awareness is mainly used in the field of aviation human factors considerations, and not introduced into the field of network security. [1][2][3]

NSSA contains two meanings:

- According to the network security devices in real-time alarm information and other information, the association merge, data fusion, etc, reflect real-time operational status of the network;
- According to some historical data offline analysis, use the certain means to predict potential threats.

Based on the basic functions, NSSA will be divided into three stages: Network Security Situation Recognition (include Extraction of situational factors, Data preprocessing), situation understanding and situation prediction.

In the Situation Recognition, the most significant working is Extraction of situational factors. Accurately and comprehensively extracting the situational factors is the fundamental of NSSA. But the net have to been a huge nonlinear complex systems, it has immense flexibility, so extraction of situational factors is very complex. [4]

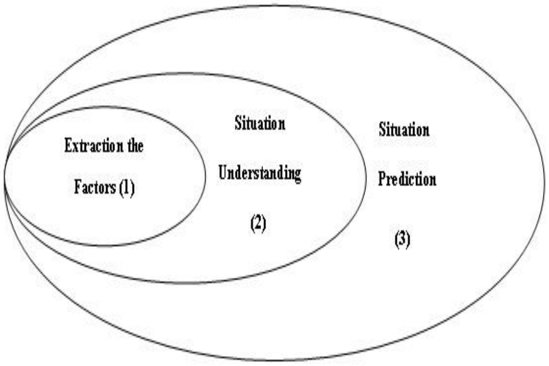

Fig. 1. Three level model of Situational awareness

This paper is organized as follows. Section 2, we discuss the conceptual model of NSSA system framework. Section 3, we suggest a method of situation evaluation Based on Multi- Perspective Analysis in NSSA. Section 4, we establish the model of Design of a Multi-Level Analysis Framework of NSSA. Section 5 gives a conclusion of the paper.

This paper is organized as follows. Section 2, we discuss the conceptual model of NSSA system framework. Section 3, we suggest a method of situation evaluation Based on Multi- Perspective Analysis in NSSA. Section 4, we establish the model of Design of a Multi-Level Analysis Framework of NSSA. Section 5 gives a conclusion of the paper.

2 NSSA SYSTEM FRAMEWORK

2.1 Hierarchy of NSSA

Modeling is the basis of NSSA. There are many researches about NSSA models [5] [6] [7]. According to Tim's idea, it's to construct the network security situation infrastructure with the application of multisensors data fusion. Tim Bass gave a primary framework which provides conceptual analysis of Network Situation Awareness (NetSA).

It is the basis of other models. But it can't solve the actual security problems and has many shortages. As networks evolve in complexity, the number of objects, threats, sensors and data streams dramatically increase [1]. After investigating many other NSSA models, we give a conceptual model of NSSA. It is a hierarchical model, illustrated Figure 2.

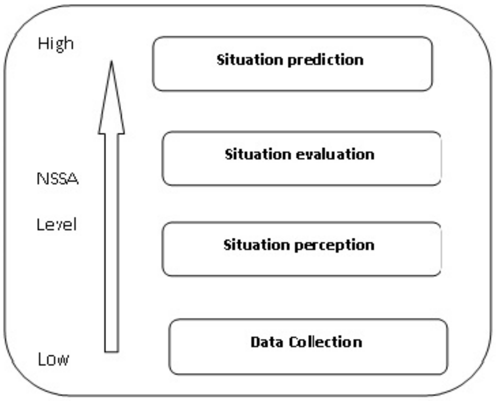

Fig. 2. Conceptual model of NSSA

2.2 A Novel Design Approach to NSSA System

Based on above conceptual model of NSSA, we suggest a novel design approach to NSSA system, illustrated in Figure 3. This framework gives precise mathematical model to describe network security situation and its trend. Especially, it gives a practical security reinforcement scheme used to guide people to improve network security. It is composed of five modules, except security reinforcement scheme module, four of them correspond to the four levels of conceptual model.

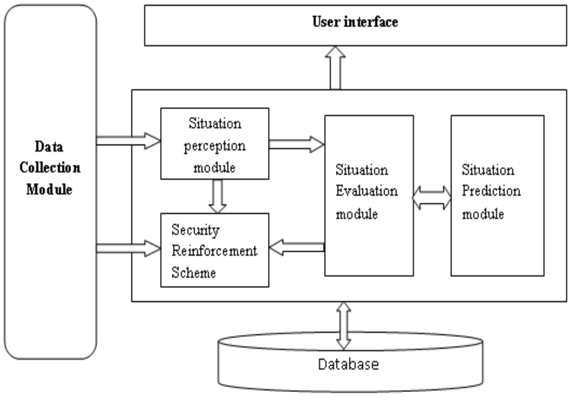
User interface
Data Collection Module
Situation perception module
Security Reinforcement Scheme
Situation Evaluation module
Situation Prediction module
Database

Fig.3. The framework of NSSA

- **Data collection module:** It observes information in cyberspace and captures metadata by multi-sensors. The output of this module is tremendous original data. **Situation perception module:** It analyzes the original data, then categorizes them and transforms into a unified format of XML. This module prepares for situation evaluation, and it is the basis of situation awareness.

- **Situation evaluation module:** Analyzing the input of security incidents with precise mathematics model. This module gives a comprehensive and quantitative description of current situation. It is the core of situation awareness and will be discussed in section 3.
- **Situation prediction module:** Comprehending all historical situation values this module plots situation map. It forecasts the future situation using time series model.
- **Security Reinforcement Scheme module:** Using the data input from other modules, this module gives a practical security reinforcement scheme to guide managers to improve network security.

2.3 Evaluation methodology in Network Security Situation Awareness

To assess the situation we need to clear the important points as following:

- **Evaluation standard**: situations always have its two sides for us, good side and bad side, and we need to clarify the core strength of the two sides, and the comparison of these two strengths mainly compose the evaluation standard.
- **Main factors**: there are many factors that have important impact on the evaluation standard contained in the enemy side, our side and also environment. Some of the factors can scale up the power to be played out, some may play a restricting role.
- **Evaluation rules**: these rules reflect the relation between each evaluation factor and the evaluation results and even describe how to combine multi-factors together to raise effect on the final results. These rules generally direct the calculation of the situation exponent which represents the comprehensive stat of the specified situation.

While all these three points have been identified and investigated, it is feasible to gain the comprehension of any kinds of situations by evaluating the current factors and forecast the changes of situations by evaluating the possible factors in the near future. Hence, we can regard the data generated by Perception as the input of evaluation, and regard the output of evaluation as the measure of Comprehension and Projection result.

Internet is a huge device for people to transfer information. It connects all types of computing equipment together by forming a virtual space which is named cyber space. The security situation in this virtual world is called Cyberspace Situation or Network Security Situation. We are dedicated to evaluate the security situation of cyberspace by the methodology aforementioned. Before evaluation we have to clear and define the environment and the working principle in the cyberspace. Then we explore through this virtual environment to find out the contrary strengths that can be chosen as the evaluation exponent, the factors that could affect situation notably, and the rules that every factors comply with in cyberspace.

This theoretical method is a direction of getting comprehensive knowledge of Network Security Situation. It emphasizes the importance to form logical relation among the situation factors other than mixing all the low level data together via variety of analysis methods. As we do evaluation based on a higher level knowledge, we encounter new challenges as following:

- **Identification**: situation factors is a virtual object to be identified, so there have to be some specific identification methods for every kinds of low-level data to assign data to the right factor objects;
- **Relation rules**: Network environment is a virtual space that we can’t gain awareness directly by our sense organ, we can’t see it neither hear it, but by using sensor tools in the network, so it is hard work to work out the relation among the factors manually.

3 SITUATION EVALUATION BASED ON MULTI- PERSPECTIVE ANALYSIS

Situation evaluation is a quantitative analysis about security, and it is the basis of situation prediction. There are many mature models for use to evaluate situation, but most of them have drawbacks. In this section we give a situation evaluation model using multi-perspective analysis. In data collection module, we use six detection subsystems to all-round monitoring network, including Malware Detection, IDS and Firewall, Vulnerability Scan, Penetration Testing, Online Testing and Security Service Detection. the multi-perspective analysis framework is shown in Figure 4.

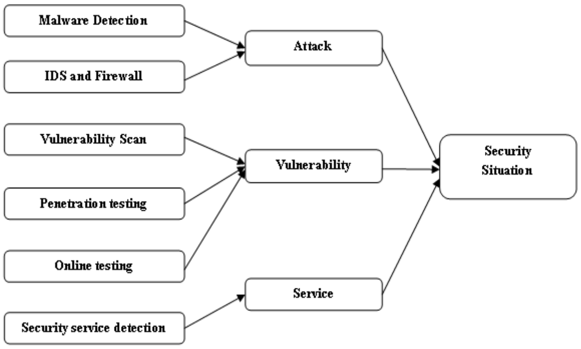

Fig. 4. Multi-perspective analysis

In situation perception and evaluation modules, because of topology of network and distinctness of hosts, we must distinguish different networks. Firstly, we consider a single computer security situation evaluation. According to the security situation of each host, we adopt additive weight method to compute security situation of entire network. Supposing a network contains N hosts, for security situation evaluation of a single host, we consider three types of security factor: security attacks, vulnerabilities and security services.

4 DESIGN OF A MULTI-LEVEL ANALYSIS FRAMEWORK OF NSSA

We derive a multi-level analysis framework of NSSA is shown in Figure 5, which make a little change from Endsley [8] three level model of situation awareness. First it proposes that every kind of data should have a corresponding process engine for identifying the data belong to a particular factor. Second, it divides the perception into two parts, factor identification and relation rules, because the purpose of perception is to get knowledge of who will take part in the activities and how they act.

Last, it clarifies that the core process of NSSA is situation evaluation, and this process will generate the knowledge of current situation and then forecast the situation in two days or a week time. The accuracy of evaluation and forecast mainly depends on the integrity of information we get, so we should make it a scalable framework to extend new data acquisition capabilities.

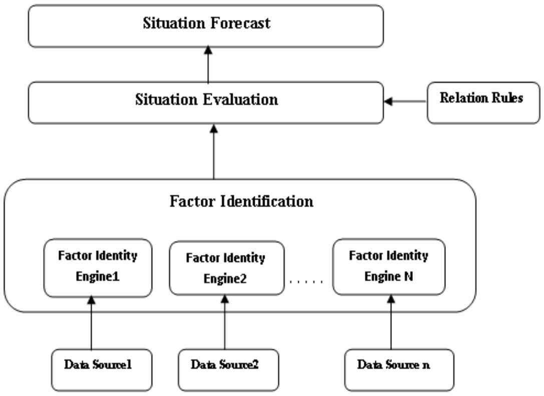

Fig. 5. NSSA Multi-level analysis Framework

5 CONCLUSION

This paper displays the challenges of Network Security Situation Awareness, and tries to give the corresponding resolutions. We point out that the relationship between the situation evaluation and the situation awareness, and then propose a method for situation evaluation. The situation evaluation model adopting multi-perspective analysis is more comprehensive than simple hierarchical model. At last, we introduce the multi-level analysis framework for Network Security Situation Awareness. While there are still some detail methods should be studied deeply, and we will give a further discussion in the future work.

6 REFERENCES

[1] XI Rongrong YUN Xiaohun JIN Shuyuan□ZHANG Yongzheng,“Research survey of network security situation awareness”, Journal of Computer Applications, 2012,32(1), pp. 1-4,59, 2012-1-1

[2] LI Shuo, DAI Xin, ZHOU Yuxia, “Research progress of network security situation awareness”. Application Research of Computers, Vol. 27, No. 9, 2010.9, pp. 3227-3232.

[3] WANG HuiQiang, LAI JiBao, ZHU Liang, LIANG Ying, “Survey of Network Situation Awareness System”. Computer science. 2006, Vol 33 No 10, pp. 5-10.

[4] ZHOU Changjian, SI Zhenyu, XING Jinge, LIU Haibo, “Study on cyberspace situation awareness modeling method based on Deep Learning”, Journal of Northeast Agricultural University, 44(5), pp.144-149, 2013.5

[5] Bass T, "Intrusion Detection Systems and Multi-sensor Data Fusion: Creating Cyberspace Situation Awareness", Communications of the ACM, 2000, 43(4): pp.99-105.

[6] Chen XZ etc., "Quantitative hierarchical threat evaluation model for network security", Journal of Software, 2006, 17(4): pp.885-897.

[7] Lai jibao etc., "Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory", IEEE, 2006.

[8] Endsley M R, "Design and evaluation for situation awareness enhancement", Human Factors Society, 32nd Annual Meeting, Santa Monica, CA, 1988.