*International Journal of Intelligent Information and Management Science*
*ISSN: 2307-0692, Volume 8, Issue 3, June, 2019*

# A Brief Analysis of the Application of Network Security

Jianjun Wu
Hunan City University, Yiyang, 413000, China

**Abstract:** With the rapid development of network technology, more and more places are used. In order to ensure the security of network data, the research on network security is put forward. The importance of network security is further illustrated by the perception and model classification of network security.

**Keywords:** Network security; Model; Perception; Research

## 1. Introduction

With the continuous expansion of the scale of the network, there are many vulnerabilities in the network, which are very easy to be attacked by attackers. Even now there are some corresponding defensive means, the attackers' means of attack still show complex and diversified forms. Therefore, this situation challenges the security of the network to a great extent. On the issue of how to deal with cyberspace security, with the introduction of relevant laws and regulations on cyber security, cyber security situational awareness has been upgraded to a strategic level, which represents the latest trend of attack-defense confrontation. General Secretary Xi Jinping proposed that we should set up a correct concept of network security to perceive the situation of network security all-round and enhance the ability of network security defense and deterrence [1-3]. Therefore, this chapter puts forward the in-depth study of network security situational awareness, mainly introduces the basic theory and key technologies of network security situational awareness in detail, and points out some drawbacks in its key technologies.

Network security situation is the current overall state of the network and the future trend of change, which is composed of various factors, such as user behavior in the Internet, the operation status of Internet equipment and so on. In large-scale network environment, network security situational awareness (NSSA) is the process of acquiring, understanding and displaying various security elements that cause changes in network security situation, and predicting the future development trend. As a state of network security and a trend of network security, "situation" is a global concept and no single state can be called situation [4-5].

Network security situation visualization is to provide a visual situational awareness platform for network security managers, so as to facilitate security managers to manage the security situation and have an intuitive perception of the overall security situation of the network.

## 2. Network Security Situational Awareness

The earliest situational awareness was put forward by Endsley. Situational awareness consists of three aspects: extraction, understanding and prediction of situational factors. In a certain time and space, situational awareness perceives and understands environmental factors, and predicts the future state of development. With the rise of the Internet era and the boom, the research on network security is increasing day by day. Through research and analysis, it is found that the content of situational awareness research can correspond to the content of network security. Therefore, research experts put forward the research on network security situational awareness, which means that in large-scale network environment, active detection, information identification, aggregation storage, vulnerability utilization and verification can be carried out to obtain the current network security situation and future development and changes. Usually, we use a variety of detection tools to collect and extract the elements that affect the security of the system. Secondly, the data of various network security elements are collated and analyzed to form multi-source data. Then, through data fusion, the current network security status and unsafe factors are further analyzed qualitatively and quantitatively, so as to establish a situation recognition and prediction system based on network security. Finally, the actual situation of network security can be identified by the output data of situation assessment, and according to the output results of situation prediction, the change situation of network security situation in the next stage can be obtained.

Situational awareness has been used in the early research of the US military in military confrontation. In the military field, situational awareness is to better understand the situation of the enemy and ourselves, including com-

bat capability, military status and location, so as to make quick and correct decisions, so as to achieve the goal of knowing one's own enemy and knowing the other, and not endangering all wars. In the field of data, the term state is called potential assessment, which refers to the perception of environmental elements and events that can cause changes in time and space, including the understanding of their meaning, and the state measurement after changes in some variables (such as time or predetermined events).

Endsley proposes a situational awareness process suitable for automation and human-computer interface systems, and divides the information processing process of situational awareness into three stages:

Situational awareness: As the basis of situational awareness, situational awareness prepares for the next situational understanding by extracting effective information from a large amount of information and making correlation analysis of the extracted information.

Situation understanding: It is the core of situation awareness and a process of dynamic understanding of current security situation. Based on the analysis of the detection stage and the related understanding of it, the corresponding security situation map is generated according to the degree of threat to show the network security situation.

Situation prediction: It is the application of situational awareness technology itself. Through the understanding of the history and current network security situation, the future security trend of the network is predicted, so as to better grasp the situation of network security situation.

## 3. Network Security Situational Awareness Model

In the analysis process of network security situational awareness, most of them will be applied to very mature analysis models.

Although the analysis methods of type A are different, they basically include three elements: perception, understanding and prediction. At present, most of them are Several research experts have put forward their own framework models of network situational awareness in their respective research fields.

The following four models are more extensive models proposed by research experts. Next, this chapter will introduce the four models separately.

Endsley model: Situational awareness in Endsley model focuses on perception, which is the process of sorting out the status, attributes and dynamics of the important elements in the network environment. The understanding of Endsley model is to fuse and analyze the important elements of information in these network environments. It is not only to judge and analyze the single elements of network security, but also to fuse and sort out the related elements of network security. At the same time, the understanding in Endsley model will change with the change of situation, and new understanding will be formed by integrating new elements of network security. Endsley model is based on the understanding of the state and changes of situation elements, and predicts the changes of network security state that will appear soon.

OODA model: The OODA model is a continuous process of observation, evaluation, decision-making and action, as shown in Figure 2.1. It has the characteristics of circular confrontation. Applying OODA cycle to network security situational awareness, both attackers and defenders will face such a cycle: perceiving the attack or attack process in observation, adjusting and deciding the attack or defense method in understanding, and predicting the next action of the attacker or defender, thus launching an attack or defense action, and then going into the next round of observation. For example, if the defender's OODA cycle is faster than the attacker's, the defender can predict the next action the attacker will take by focusing on what the attacker is doing or analyzing what the attacker may do, that is, analyzing the attacker's OODA loop, and then taking defensive action before the attacker, and finally gaining the advantage.

## 4. Distribution Matrix of Network Security

When 1E attack occurs in the network, if only 1R protection measures are deployed in the network, then the attack can be monitored through this protection measures. However, because the protection measures are only responsible for monitoring and cannot respond to the attack, the network state will still be in a high state at this time; when other arbitrary protection measures are deployed in the network, the attack cannot be monitored, and will not affect the current network, then the current network state will still be in a high state.

When 2E attacks occur in the network, if only 2R protection measures are deployed in the network, then the attack can be monitored through this protection measures. However, because the protection measures are only responsible for monitoring, and cannot respond to the attack, the network state will still be in a medium-high state at this time; when other arbitrary protection measures are deployed in the network, the attack cannot be monitored, and will not affect the current network, then the current network state will still be in a medium-high state. When 3E attacks occur in the network, if only 3R protective measures are deployed in the network, then the attack can be prevented by this protective measure, so that the attack does not cause any loss to the current network, then it can be judged that the current network state is still in a high state; when other arbitrary protective measures are deployed in the network, these protective measures are against the attack. The attack cannot play any protective role, so the attack will seriously affect the current network security status, leading to the current network state to appear in the middle state.

When 4E attacks occur in the network, if only 4R protective measures are deployed in the network, then the attack can be prevented by this protective measure, so that the attack does not cause any loss to the current network, it can be judged that the current network state is still in a high state; when other arbitrary protective measures are deployed in the network, these protective measures are against the attack. The attack cannot play any protective role, so the attack will seriously affect the current network security status, resulting in the current network status is in a low state.

When 5E attacks occur in the network, if only 5R protective measures are deployed in the network, then the attack can be prevented by this protective measure, so that the attack does not cause any loss to the current network, it can be judged that the current network state is still in a high state; when other arbitrary protective measures are deployed in the network, these protective measures are against the attack. The attack cannot play any protective role, so the attack will seriously affect the current network security state, resulting in the current network state showing a low state.

## 5. Concluding Remarks

Internet security management platform is the inevitable product of the development of Internet technology. It integrates various information resources, strengthens intelligent means of detection and analysis, takes security incident management as the starting point, intellectualized analysis technology as the means, knowledge management as the support, system integration as the goal, eliminates security risks to the greatest extent, and ensures information security.

## References

[1] Evans A., Kantrowitz W.A. User authentication scheme for requiring secrecy in the computer. ACM. 1974, 17, 8.

[2] Helmut K., Yan L., David O., Fiona P., Li Z. Common criteria certification in China: A comparison with the schemes of the ccra. Cryptographic authentication of time invariants. 2006.

[3] Monica J., Garfield P.G., MC K. Information systems management. Planning for Internet Security. 1997, 14, 1.

[4] Durso F.T., Gronlund S.D. Situation awareness: Handbook of applied cognition. New York: John Wiley & Sons. 1999, 283-314.