Research of cyberspace situational factors organization criterion

Luo zi juan [1, a], Wang cong lin[2,b]

[1]Science and Technology on Information Systems Engineering Laboratory,

NanJing,China

[a]48688489@qq.com [b]xxkywcl@126.com

Keywords: cyberspace ; organization criterion; situational factors，situational awareness

Abstract. This paper proposes a cyberspace situational factors organizational methods, provide a unified framework for data organization, so that information from different sources can be organized between the host status information to be consolidated, abnormal event information, traffic information, topology scan results and other data.

Introduction

With the rapid development and wide application of information technology network, in economic and social life of the great changes brought about development, network information in the field of virus attacks and malicious harm, but also for the development of the network running applications and socio-economic environment to bring extremely harmful effects, causing great loss of social and economic development. Especially in recent years, the network information technology application in social and economic development is more and more widespread and common cyberspace situational elements of the collection, extraction, processing network has also become a technical difficulty cyberspace posture[1-4].

With the growing capability of technological means and, consequently, increasing the speed of military operations, information on the battlefield has become a valuable target for the military officers.

In this context, the Situational Awareness of modern combat aims to meet the needs of the Command and Control. In order to lead their military organizations, the commander would require concise information about his and the enemy troops. For example: What are the logistical needs? How to carry out an attack? What is the intention of the enemy?

Cyberspace situational factors

According to the requirements of cyberspace situational awareness，, situational factors include environmental factors and elements of the activity, and the activities involved in three aspects: goals, relationships, and events,, and activities related to the situation and therefore the elements from the target elements of the relationship between the elements and the event features three terms of extraction[5]. Among them, the environmental factors including geographical environment, network environment and electromagnetic environment; target elements include information systems, information flow, cyberspace weapons and combat personnel; factors include the physical connection between the relationship[6], information exchange relations and social relations; event elements including other acts, events and results, including the four major data host status information, exception event information, traffic information, topology scan results and the like. In the handling and use of existing networks in cyberspace situational following questions: (1) data format is not unified, different types of trend data is difficult to compatible; (2) the user or system-demand, publishing, low ability to receive data (3) Process cumbersome storage, transport and use of trend data[7].·

Cyberspace situational factors organizational methods

A common cyberspace situational factors of organization method includes the following four steps

First of all, according to user requirements extracted cyberspace situational factors (including the host state information, abnormal event information, traffic information, topological scans)[8], these data packets of tissue specific elements of the organization in accordance with uniform methods. The paper is divided into five segments, respectively is: the main file header, host state information, abnormal event information, traffic information, topological scan results.

In the main file contained in the header fileid, version number, title, categories, packet length, the length of the message header[9], the host state information description, abnormal event information description, scanning traffic information description, topology information description, etc. Master file header of each item of data are shown in table 1[10].

Table 1 main file header

Structure	type of data item meaning	length (characters)	Type
File begin information	File identification information.	4	char[]
	Version	5	char[]
	Generated by the date and time. Format: CCYYMMDD hhmmss. Which CC said century (00 to 99), YY is said in the last two years (00 to 99), the MM is in (01 to 12), the DD is date (01 to 31), hh is hours (00 to 23), the MM is minutes (00 to 59), ss (00 to 59) is the second	14	char[]
	The title	80	char[]
Security information	security	1	char[]
File length	The length of the message	12	UINT
	The length of the message header	6	UINT
The host state information	The main machine shape state	3	UINT
	The length of the first host status information	10	UINT
	N the length of a host state information	10	UINT
Abnormal event information	The number of abnormal event information	3	UINT
	The length of the abnormal event information	6	UINT
	The first n the length of the abnormal event information	6	UINT
Traffic information	The number of traffic information	3	UINT
	The length of the flow of information	5	UINT
	The first n the length of the flow of information	5	UINT
Topology scans of data	Above topology scanning information quantity	3	UINT
	The length of the scanning first topology information	2	UINT
	The length of the first data extension jokes head	2	UINT

The host state information of data items such as table 2.

Table2 host state information of data items

Data item meaning	length (bytes)	describe	types
The port number	4	service port	UINT
Service agreement	64	Service agreement	char[]
Service name	64	Service agreement	char[]
Service object	64	Service object	char[]
service function	64	service function	char[]
Service type	32	Service type	char[]
Vulnerability port number	4	port	UINT
Vulnerability names	64	Vulnerability names	char[]
Vulnerability describes	64	Vulnerability describes	char[]
Hole type	32	Hole type	char[]
CPU information	8	CPU percentage	FLOAT
Memory information	8	Memory usage percentage	FLOAT
information of abnormal process	32	abnormal process	char[]
Other	32	other exception information	char[]

Abnormal event information of data items are shown in table 3.

Table3 Abnormal event information of data items

Data item meaning	length (bytes)	describe	types
security incident ID	8	event ID	ULONG
Event time	8	safety incident	ULONG
Event name	64	security event name	char[]
Describe	64	security events description	char[]
source IP	4	event source IP	UINT32
Source port	4	event source port	UINT32
Destination IP	4	Event Destination IP	UINT32
Destination port	4	Event Destination port	UINT32

Traffic information of data items are shown in table 4.

Table4 Traffic information of data items

Data item meaning	length (bytes)	describe	types
Source IP	4	data flow transmission	UINT32
source port	4	data flow transmission source port	UINT32
Destination IP	4	data flow transmission purposes	UINT32
Destination port	4	data flow transmission purposes	UINT32
Flow	4	data flow	UINT32
Protocol application	64	layer protocol for the data flow	char[]
Features	64	destination IP	char[]

Topology scans of data items in table 5.

Table5 Topology scans of data items

Data item meaning	length (bytes)	describe	types
The main object of type	4	identified main type	UNIT
Subtype	4	identified object subtype	UNIT
Node ID	4	identified node ID	UNIT
node name	32	node name	string
node description	64	node description	string
The parent node ID	4	The parent node ID	Unit
The unit	64	nodes belong name	string
Topology position	4	topology view the location	double
geographical position	4	geographical position	double

Situation transmission element method

Cyberspace situational intelligence data packaged into a common message format main steps include:

1) The format of the host state information as defined in Table 2 are sequentially written messages;

2) abnormal event information in accordance with the format defined in Table 3 are sequentially written messages;

3) The format of the topology scan result information defined in Table 4 are sequentially written messages;

4) the corresponding information file format in Table 1 are sequentially written into the main file header packets in.

After the user receives the packet, the first packet network in accordance with specification is converted into cyberspace situational intelligence data. The main steps include:

1) Read from the message out situational intelligence data master file header;

2) Read from the message out host status information;

3) Read the abnormal event information from the packet;

4) to read out the topology scan results from the packet;

5) Read out traffic information from the packet;

From the foregoing, Universal Cyberspace situational factors organizational methods of the present invention to meet the different departments, users and system "on-demand package" and "on-demand extraction of" relevant situation requires unusual events and elements for cyberspace situational network release and use of the feature.

Conclusion

Compared with the prior art, the significant advantages: 1) Cyberspace situational elements of the organization process of the present invention, can be packaged into a unified multi-class elements of a particular form of packets, applicable to many types of trend products; 2) The present invention realizes transmission diversity of content, the use of many types of data (host status information, exception event information, traffic information, topology scan results information), integrated express network electromagnetic spatial elements; 3) The present invention enables flexible transmission nature: for different user needs, users can "demand package", "on-demand extract" interesting intelligence data; 4) the invention achieves the transmission of simplicity: a small data formatting processing cost, the user can in the limited bandwidth conditions By handling and use of intelligence products.

Reference

[1] Xu Bo quan,WangHeng,Zhou Guangxia. Understanding and studying Cyberspace [J].Command Information System and Technology ,2010,1(1):23-26.(inChinese)

[2] Zhou Guangxia Wang Jing Zhao Xi. Development Trend of U.S.Military Cyberspace and Its Enlightenment[J] Command Information System and Technology,2015,6(1):1-5.(in Chinese)

[3] U.S. Army Capabilities Integration Center.Cyberspace operations concept capability plan 2016-2028[R].Washington D.C.: Department of the Army,2010.

[4] Naval Operations for Information Dominance, U.S. fleet Cyber command.Navy Cyber power 2020[R].Washington D.C.: Department of the Navy,2012.

[5] Office of the USAF Chief Scientist. Cyber vision 2025[R]. Washington D.C.: Department of the AirForce,2012.

[6] Zhuo Y, Zhang Q, Gong ZH. Research and implementation of network transmission situation awareness. In: Proc. of the CSIE. Los Angeles, 2009. 210−214. http://ieeexplore.ieee.org/

[7] Sun JG, Liu J, Zhao LY. Clustering algorithms research. Journal of Software, 2008,19(1):48−61 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/48.htm [doi: 10.3724/ SP. J.10 01. 2008 .00048]

[8] Bass T, Robichaux R. Defense-in-Depth revisited: Qualitative risk analysis methodology for complex network-centric operations.In: Proc. of the Communications for Network-Centric Operations: Creating the Information Force (MILCOM). IEEE, 2001. 64−70. http: // citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.5445&rep=rep1&type=pd

[9] Wei Y, Lian YF, Feng GD. A network security situational awareness model based on information fusion. Journal of Computer Research and Development, 2009,46(3):353−362 (in Chinese with English abstract).

[10]Wei Y, Lian YF. A network security situational awareness model based on log audit and performance correction. Chinese Journal of Computers, 2009,32(4):763−772 (in Chinese with English abstract).