A Distributed Security Situation Evaluation Model for Global Network

Weiwei Zhang

School of Cyber-Physical Systems and Control, Peter the Great St. Petersburg Polytechnic University, RUSSIA, St. Petersburg, 29 Polytechnicheskaya str., email: carlchueng@outlook.com

Abstract: **Global network security assessment under distributed environment is extremely urgent. We try to design a distributed security situation quantitative evaluation model, and simulate the distributed security evaluation of the service subnet by building the LAN experimental platform. The result shows that this model has high practical value for vulnerability and attack means analysis of global network.**

Keywords: **network security, distributed security evaluation, centralized environment, appraisal procedure, global network**

I. INTRODUCTION

With the rapid growth of global trade, more and more economic investment has flowed into Central and Eastern Europe and the BRICS countries. Multinational corporations have set up branches or joint venture companies in these areas, which has also brought about certain cyber security risks while helping local governments increase the income and improve the employment rates. Large international groups and R&D institutions have a wide range of branch offices, as well as a complex network environment and ragged levels of security policies, so they tend to be targeted by hacking organizations. How to conduct a security assessment of a company's network from a global perspective is crucial for setting up an effective security strategy in the next step.

As J. McCumber said [1], the evolution of cybersecurity assessment method has gone from an artificial, local, single stage to an automated, global, and widely distributed situation. It is particularly noteworthy that the security of a host in a network depends not only on its own security status, but also the security of other ones in the global network. Therefore, assessing from the entire network is of great significance for discovering weaknesses in global network. F.B. Shaikh, and S. Haider [2], after analyzing the security threats of cloud computing, believe that the identification and analysis of distributed vulnerability are very important in the global environment, especially big data and cloud platform. Vulnerability is the direct premise of the security threat. No matter how advanced the attacker uses, if the protected assets have no weakness or only a slight vulnerability, it is difficult for the attackers to make use of their tools to damage assets [3,4,5]. Therefore, by identifying and analyzing the loopholes and security conditions of the services running on the network system, it is helpful to improve the level of network security protection and provide effective support measures for the integrated security management of the system.

However, the development of efficiency and security issues are often a pair of brothers who go hand in hand, and the whole is usually not a simple sum of parts. With the rapid development of the Internet in today's information society, cross-domain collaboration and sharing between different branches of enterprises have become necessary tools for enterprises to improve their competitiveness and expansion [6]. Undoubtedly, this will expand the company's own virtualized network boundaries, making it easier for attackers to exploit various security vulnerabilities to implement distributed [7], springboard attacks, or to achieve successful intrusion through application layer trust relationships between security domains [8]. Therefore, the security problem of distributed systems is not a synthesis of the security problems of distributed nodes. Local intrusion detection and auditing are not enough to deal with the security threats brought about by the virtualization of the organizational structure [9]. The security policies between subsystems cannot be simply added. It is difficult to implement uniform security standards in different branches. From the perspective of the global network, different branches often combine into different subnets because of the need for information exchange. Subnets also need to interact with the outside world, such as the CRM system we are familiar with. Sales consultants need to be allowed to access the company's CRM system and get analytical support to conduct business with customer companies. Because this process takes place outside the company and lacks strong supervision, the service port of the system network can easily be abused or even hacked during this process. It can be said that the cross-domain collaboration and sharing between enterprises has raised higher and more specific requirements for enterprise security assessment and protection.

Therefore, it is necessary to analyze the problems of the existing network security assessment methods based on the actual needs of cross-domain situation, and design a distributed network security situation assessment model.

II. THEORETICAL ANALYSIS

Under the actual demand of cross domain sharing, collaboration and defense of enterprise network, the existing network security assessment methods are faced with the following difficult problems:

1) The assessment of the security threat status of the network system usually focuses on the impact of the attack in a single network domain [10], which is difficult to reflect the global security threat situation, and is not conducive to the formulation and correction of the system security strategy.

2) When the enterprise has multiple different branches, in order to realize the security assessment of the business system from the whole point of view, the estimated business network

inevitably transfers private data to other sub network participating in the evaluation of the business, and this has become a privacy security problem [11].

Under the above background, based on the massive alarm information of IDS, the importance of service, the frequency of alarms, and the severity of security threats, we try to design a quantitative assessment model.

We use the centralized service security index $F_{S_{jm}}$to start the derivation of the model framework. Security index for service S_j in network *m* refers to the evaluation index of the losses caused by the intrusion using the vulnerable points. $F_{S_{jm}}$is derived from the importance of the service, the number of attacks C_{jtim} on the service S_j , and the severity of the attack P_{ji}. Based on the analysis method of literature [12], according to the characteristics of service operation in the network system, the importance of the service θ_{jtm} is measured by the normal access of the system service in different time periods. Eq. (1) gives the calculation method for the service security index $F_{S_{jm}}$ of the network *m*:

$$F_{S_{jm}} = \sum_{t=1}^{h} \theta_{jtm} \sum_{i=1}^{k_m} 10^{p_{ji}} C_{jtim} \tag{1}$$

More explanations for the formula:

1) Normal access θ_{jtm}

The number of normal access θ_{jtm} about service S_j varies from time to time during different time periods. Therefore, the same attack event has different influences and losses on services during different time periods. We can define the number of divided periods *h=3*, and divide the time of the day into three periods: Δ_{t_1}=*Night*, which represents the time range of 0:00-8:00, Δ_{t_2} =*OfficeHour* describes 8:00-18:00, and Δ_{t_3}=*Evening* indicates the time interval from 18:00 to 24:00. θ_{jtm} is assigned by the system administrator according to the normal average visit amount A_{jtm} ($t \in [1 \dots h]$) of the service S_j in each period of the network *m*. The visit amount is represented by 1, 2, 3, 4, and 5 respectively: very low, low, medium, high, very high. The larger the value, the greater the average traffic. Then, we will obtain θ_{jtm} in Eq. (2):

$$\theta_{jtm} = \frac{A_{jtm}}{\sum_{t=1}^{h} A_{jtm}} \tag{2}$$

2) Number of attacks C_{jtim}

We define the total number of types of services running in network *m* as d_m, count the number of alarms for different attack event types *i* ($\boldsymbol{i} \in [1, k_m]$, k_m is the total number of attack types for the corresponding service) of service S_j ($j \in [1, d_m]$) according to the alarm data set generated by the IDS in the network. After generating the number of alarms, we can get C_{jtim}.

3) Security threat severity P_{ji}

After setting service S_j which suffers from different types of attacks *i* with severity P_{ji} during time period Δ_t, we use the attack classification and prioritization of the SNORT user manual [13] to determine the threat severity of each attack. Respectively, 1, 2, and 3 indicate the three severity levels: low, medium, and high. Table I is a partial attack category extracted from the SNORT user manual and its corresponding severity.

TABLE 1. ATTACK TYPE AND SEVERITY

Attack category	Description	Severity
Attempted-admin	Attempt to obtain administrator privileges	High
Shellcode-detect	Executable code detected	High
Successful-admin	Successfully acquired administrator rights	High
Attempted-dos	Attempt to cause a denial of service	Medium
Attempted-recon	Attempt to cause Information disclosure	Medium
Network-scan	Detected Network scan	Low
String-detect	Detected Suspicious string	Low
Attempted-user	Attempt to obtain User Rights	High
Trojan-activity	Detected Internet Trojan	High
Successful-user	Successfully acquired User Rights	High
Misc-attack	Mixed attack	Medium
Suspicious-login	Suspicious user login	Medium
Unknown	Unknown traffic	Low
Icmp-event	General ICMP events	Low

III. MODEL DESIGN

Expanding to a distributed environment, we assume that *l* (*l* ⩾ 3) service subnets participate in the overall security assessment analysis, and there is no trusted third-party computing provider. Based on the historical alarm information collected by these subnets, the overall network service security index F_{S_j} can be calculated statistically. Because each evaluation participant has similar network services, by sharing the attack conditions of each service in its own network environment, under the distributed service assessment model, it obtains a more general and global security situation analysis result.

Suppose that the time division of the parties involved in the assessment is the same (day time is divided into three time periods: *Night*, *Office Hour*, and *Evening*), the same type of attack has the same security threat severity, and the total number of types of services running in the overall network is $d(d \leq \sum_{m=1}^{l} d_m)$. If the *m*-th party ($m \in [1 \dots l]$) does not have an attack on a certain service type, the corresponding service $C_{jtim} = 0$. According to their respective IDS alarm data sets, the parties count the F_{S_j} value of the entire network by sharing the service security index $F_{S_{jm}}$ in their respective networks, so that we can get a globalized security posture result. The calculation method of the overall network service security index F_{S_j} is shown in Eq. (3):

$$F_{S_j} = \sum_{m=1}^{l} F_{S_{jm}} = \sum_{m=1}^{l}\left(\sum_{t=1}^{h} \theta_{jtm}\left(\sum_{i=1}^{k_m} 10^{P_{ji}} C_{jtim}\right)\right) \quad (3)$$

Based on the above methods, we present a quantitative assessment model (Fig.1) for distributed security posture.

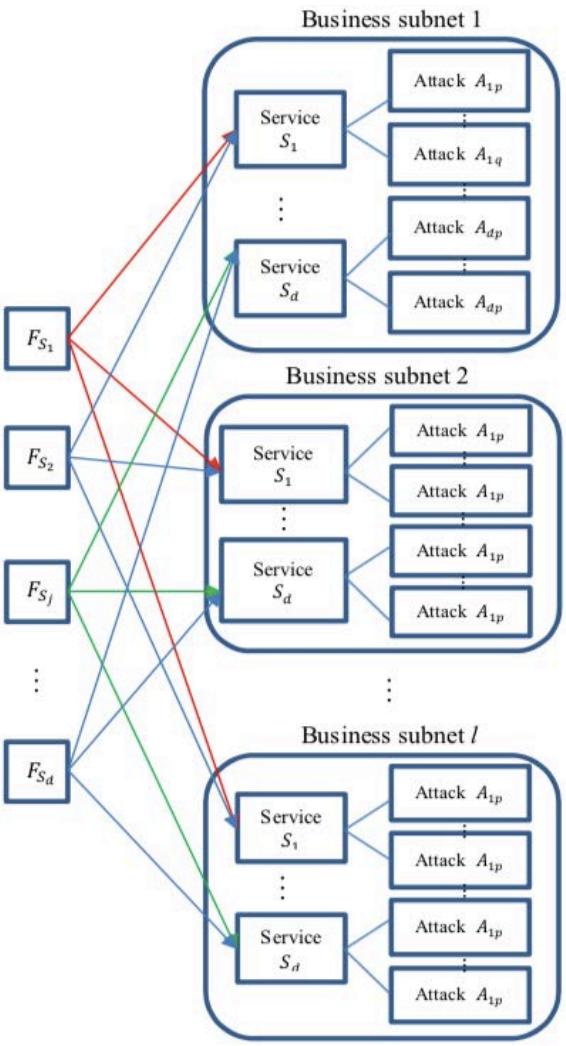

Fig.1. Distributed Security Situation Evaluation Model.

We can draw a conclusion that the greater the value of the service security index F_{S_j}, the higher the degree of security threat caused by exploiting the vulnerability of service S_j, which should be highly valued and prevented. Moreover, F_{S_j} also describes the security threat values for successive periods of time. The security threat trend of service S_j can be derived by comparing these values.

IV. Model Constraints

In the process of computing the distributed security assessment, in order to statistics the multi-party analysis data, the participants will inevitably transfer the private data to other participants to complete the distributed statistical process, resulting in privacy problems. $F_{S_{jm}}$ describes an intrusion event that exploits the vulnerability of service S_j to attack a system. Therefore, network service information that is running or open in a network system is sensitive privacy information. The leakage of this kind of information may lead to the leakage and utilization of the system vulnerability information, which seriously affects the security of the service network.

At the same time, each business network participating in the evaluation needs to interact $(l-1) \times d$ times, when there are more participants or more types of services, the number of interactions will increase linearly.

V. Model Validation

In order to verify the effectiveness of the proposed model in quantitative assessment of distributed security posture, we set up a LAN environment as an experimental platform to simulate the scenario of distributed comprehensive security assessment for three business subnets (l = 3). Each subnet shares a class C address to connect to the Internet. Effective attacks on servers in each subnet are performed using intrusion methods such as buffer overflow and denial of service (DoS) attacks. In the experimental platform, the overall network service type number d = 5. SNORT is deployed on each server in the subnet, and the alarm information generated by it is used as the data source for security assessment. The network services running on the three subnets, as well as the distributed comprehensive service security index obtained from the statistics of one day's data, are shown in Table 2.

TABLE 2. Service status and integrated service security index(example)

Net	Service	Service Importance (A_{t1}, A_{t2}, A_{t3})	Service Importance Weights (3 periods) $\theta_{t1}\ \theta_{t2}, \theta_{t3}$	Distributed Integrated Service Security Index
A	FTP	(1,4,3)	(0.125,0.5,0.375)	F_{FTP} = 647.5
	MAIL	(2,5,4)	(0.182,0.455,0.364)	F_{MAIL} = 565
	DNS	(1,3,2)	(0.167,0.5,0.333)	F_{DNS} = 337.6
	TELNET	(1,2,1)	(0.25,0.5,0.25)	
B	MAIL	(1,3,3)	(0.143,0.429,0.429)	F_{TELNET} = 419.2
	FTP	(1,2,1)	(0.25,0.5,0.25)	
C	WWW	(4,2,5)	(0.364,0.182,0.455)	F_{WWW} = 863
	TELNET	(1,1,1)	(0.333,0.333,0.333)	

The security threats of the five network services in the experimental platform within two weeks are shown in Fig.2. In our example, we can see that under the global conditions, the Internet, FTP, and MAIL are the more frequent attacks. Based on this, enterprise personnel can set corresponding policies, monitor FTP ports, set firewalls on external networks, and do a good job of Mail Anti-Phishing measures to improve the safety of the organization. It can be seen that the global security threat posture map provides intuitive and quantitative data for the overall network security assessment. This method has high practical value for analyzing vulnerability, attack behavior and means of the whole network.

The parameters in the index are set in days. If the production system environment equipment is excellent, it is recommended that the enterprise security personnel set hours or even minutes.

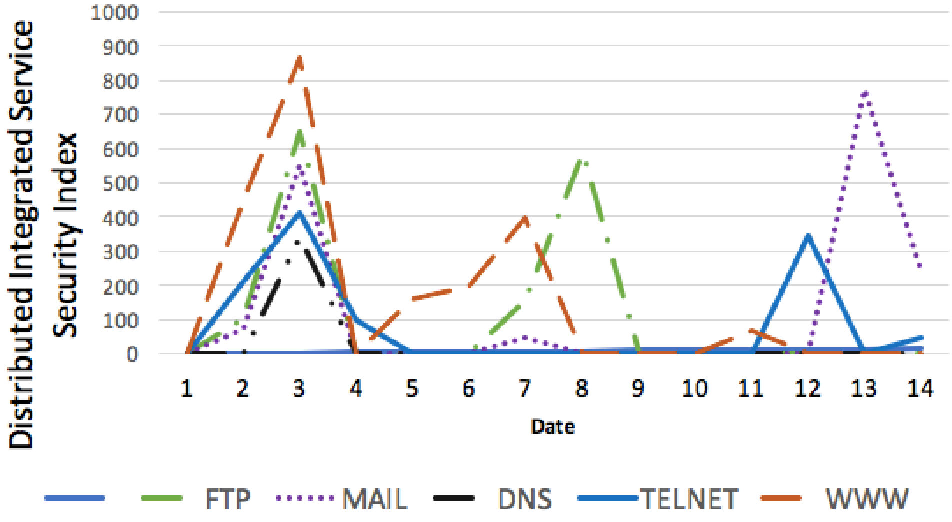

Fig.2. Global security threat Posture.

VI. Conclusion

In order to solve the problem that it is difficult to use the massive and complex alarm information in the field of security assessment to effectively model the overall security situation, we combined the importance of services, the frequency of alarms, the level of security threats, and other factors, studied and proposed a distributed security quantitative assessment model, and verified the model at the same time based on massive alarm information. The results show that this model can perform distributed quantitative assessment under the condition of global security threats.

Secure distributed statistical model is a key issue for implementing network security assessment models in peer-to-peer environments. In the next research, we will try to analyze the privacy issues in distributed assessment, establish a distributed statistical model under the protection of privacy, and combine with different security assessment methods to support a wider range of application scenarios. Random number distribution and sane path methods are worth considering.

References

[1] J. McCumber, " Assessing and Managing Security Risk in IT Systems: A Structured Methodology", *IEEE Trans. CRC Press*, pp.87-101, Apr. 2004.

[2] F.B. Shaikh, and S. Haider, " Security threats in cloud computing", *ICITST*, 2011.

[3] R. Raghavendra, K.B. Raja, S. Venkatesh, F.A. Cheikh and C. Busch, " On the vulnerability of extended Multispectral face recognition systems towards presentation attacks ", *ISBA*, 2017.

[4] M. Almutairi and S. Riddle, "Security threat classification for outsourced IT Projects", *RCIS*, 2017, pp.447-448.

[5] H.H. Wang, L.B. Shi and Y. Ni, "Distribution system planning incorporating distributed generation and cyber system vulnerability", *The Journal of Engineering*, pp.2189-2202, 2017.

[6] K.W. Kongsgard, N.A. Nordbotten, F. Mancini, R. Haakseth and Paal E. Engelstad, "Data Leakage Prevention for Secure Cross-Domain Information Exchange", *IEEE Communication Magazine*, pp.37-43, 2017.

[7] F. Hohl, "Automatically protecting computer system from attacks exploit security vulnerabilities", *Sony Corporation (Minato-ku, JP)*, 2007.

[8] L. Zhou, Dan Wu, B. Zheng and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery", *IEEE Communications Magazine, Issue:3*, pp.66-72, 2014.

[9] Jiming Chen, Junkun and Ten H. Lai, "Energy-Efficient Intrusion Detection with a Barrier of Probailistic Sensors: Global and Local", *IEEE Transaction on Wireless Communications, Volume:12, Issue:9*, pp.4742-4755, 2013.

[10] M. Gharbaoui, F. Paolucci, A. Giorgetti, B. Martini and P. Castoldi, "Effective Sttatistical Detection of Smart Confidentiality Attacks in Multi-Domain Networks", *IEEE Transactions on Network and Service Management, Volume:10, Issue:4*, pp.383-397, 2013.

[11] J. Giraldo, A. Cardenas and M. Kantarcioglu, "Security vs. privacy: How integrity attacks can be masked by the noise of differential privacy", *American Control Conference(ACC)*, 2017, pp.1679-1684.

[12] X. Z. Chen, Q. H. Zhen, and X. H. Guan, "Research on Security Situation assessment of networked systems", *Journal of Xi'an Jiaotong University, vol. 38, no. 04*, pp. 404-408, 2004.

[13] "SNORT", 2010; http://www.snort.org/.