International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.153-164
http://dx.doi.org/10.14257/ijsia.2016.10.11.14

Multi-dimensional Network Security Situation Assessment

Lina Zhu[1,2a], Guoen Xia[2b], Zuochang Zhang[2a], Jianhua Li[1] and Renjie Zhou[3]

[1] School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China
[2a]School of Information and Statistics, [2b]Department of Academic Affairs Guangxi University of Finance and Economics, Nanning, China
[3]Key Laboratory of Complex Systems Modeling and Simulation, School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China
zhulina81@gmail.com

Abstract

Network security situation awareness is vital important for network security supervision. In order to obtain the network security situation effectively, a multi-dimensional assessment method is proposed in this paper. The method is composed of three dimensions at different levels, namely vulnerability, threat and basic operation, with quantitative calculation method for each index. In the service layer, CVSS standard is adopted to assess the vulnerability situation, and simplified DREAD model is chosen for the threat situation. In the node layer, the vulnerability situation in the service layer is added with a weight, the threat situation in the service layer is accumulated according to attack paths based on Markov model, and the basic operation situation is evaluated by D-S evidence fusion of several host and network performance index. In the network layer, each situation equals to weighted summation of corresponding situation in the node layer. Experimental results show the ease of use of this method, and multi-dimensional situation depicts the overall safety evolution process of network system accurately and intuitively.

Keywords*: network security, situation assessment, vulnerability, network attack, threat*

1. Introduction

With the rapid development of information technology and the Internet, network security events happen endlessly, and potential risk exists in network infrastructure. Traditional threats such as Trojan, Botnet and phishing sites are increasing; novel network attacks such as APT (advanced persistent threats) emerge, and the situation is intensifying. Global malicious code samples are growing at a rate of 3 million per day, with cloud malicious code samples having grown from 400 thousand in 2005 to the current 6 billion. Following the Stuxnet and the PRISM event, network infrastructure is faced with global high risk vulnerabilities. The bleeding heart vulnerability threatens about 33 thousand web servers in China, and Bash vulnerability affects about 500 million servers and other network equipments around the world. Basic communication network and other important information systems (*e.g.* financial, industrial control information systems) are facing serious challenges.

Under this background, it is significant and urgent to ensure the security of the network. In the complex environment of sharp and dynamic changes, modern network management must be able to organize and analyze uncertain network management information effectively, improve administrator's awareness and understanding of the operation state of the whole network, and further assist administrator to make security response.

ISSN: 1738-9976 IJSIA

2. Related Work

Network security awareness needs detailed assessment methods. However, most studies for security assessment focus on specific sub-problems, *e.g.* vulnerability assessment, threat assessment and abnormal traffic assessment. For these methods, assessment object is single, there is a lack of heterogeneous multi-source data correlation, and the evaluation results are just part of the network security situation. They cannot reflect the network running status accurately and comprehensively.

In [2-4], a hierarchical analysis method was adopted to describe the evolution of network security threat. The bottom-up assessment framework was divided into service layer, host layer and network layer. Based on the alarm information, considering the importance of service and host, the security situation index in different layers were calculated by weight summation.

The causal relationship between attack steps was considered in [5-7]. Attack graph was built, and Markov chain model and Bayesian network were chosen to dealt with changes over time (*e.g.* whether attack code or patches available). A dynamic network security model was constructed. Further, in [8] and [9], CVSS (Common Vulnerability Scoring System) standard was adopted for quantitative risk assessment, and attack scenario were reconstructed for risk prediction.

The statistical characteristic of network flow was discussed in [10-13], which was suitable for evaluating threat posed by DoS attacks, worms propagation and Botnet scanning.

A multi-source, multi-level situation information fusion method based on Bayesian network was proposed in [14], which evaluated component and network security status from several aspects (*e.g.* basic operation, vulnerability and threat). The Bayesian network build process was described in detail. But the method was lack of specific quantitative evaluation index.

3. Network Security Situation Assessment from Multiple Dimensions

3.1. Definition of Situation Index

3.1.1. Vulnerability Situation:

This dimension reflects the severity of vulnerabilities in a system.

1) Service-level vulnerability situation (SS_V): This index reflects the severity of single vulnerability.

2) Node-level vulnerability situation (NS_V): This index reflects the severity of all vulnerabilities in a node.

3) LAN-level vulnerability situation (LS_V): This index reflects the severity of all vulnerabilities in a local area network.

3.1.2. Threat Situation:

This dimension reflects the severity of attacks happened in a system.

1) Service-level threat situation (SS_T): This index reflects the severity of atomic attack, namely single attack step.

2) Node-level threat situation (NS_T): This index reflects the severity of attacks happened in a node.

3) LAN-level threat situation (LS_T): This index reflects the severity of attacks happened in a local area network.

3.1.3. Running Situation

This dimension reflects the operation status of a system.

1) Node-level running situation (NS_R): This index reflects the operation status, namely the host or network resources utilization, of a node.

2) LAN-level running situation (LS_R): This index reflects the operation status of a local area network. It is a comprehensive reflection of running status of the node layer.

3.2. Situation Assessment Model

The network system is divided into network layer, node layer and service layer. The node types include servers, clients and network devices. Hierarchical multi-dimension network security situation assessment model is shown in Figure 1. For the vulnerability situation: based on the vulnerability scanning result, CVSS is adopted to evaluate the severity of single vulnerability; considering the importance of service and node, vulnerability situation in node layer and network layer are calculated by weighted summation. For the threat situation: based on vulnerability scanning result, IDS alert and security response (*e.g*. antivirus software kills virus, firewall stops abnormal access), DREAD model [15] evaluates the severity of atomic attack from five aspects, namely damage potential, reproducibility, exploitability, affected users and discoverability; based on the network topology and causal relationship between attack steps, attack scenario is reconstructed, and Markov chain is adopted to assess the threat situation in node layer and network layer. For the running situation: the node performance (*e.g*. CPU and memory utilization) and network performance (*e.g*. bandwidth utilization) are integrated by D-S evidence theory to get the running situation in node layer; further, the running situation in network layer is calculated by weighted summation.

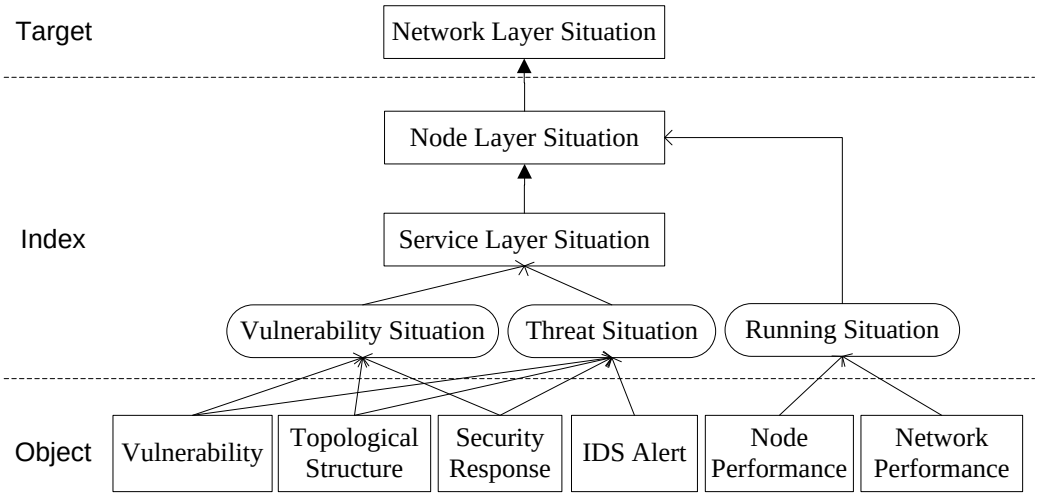

Figure 1. Multi-Dimensional Network Security Situation Assessment Model

3.3. Weighting Parameter Settings

In the process of calculating situation index in each layer, service weight and node weight need determining. Parameter settings is related to service type, specific application and so on. There is no uniform standard. Generally speaking, appropriate evaluation criteria is made by the network security administrator according to specific environment.

3.3.1. Service Importance Weight

Network security administrator determine the weight according to different audience. For public service, according to the number of users and access frequency, method in [2] can be used to set service weight. For private service, this parameter may be determined based on the confidentiality of service content.

3.3.2. Node Importance Weight

The importance of a node is determined by the importance of service that runs on it. The more the number of service with higher importance, the higher status the corresponding node in network, namely the node is more important. Suppose that k nodes are deployed in the network, service is divided into five grades according to its importance, α_j denotes the weight of service in grade j, M_{ij} denotes the number of service in grade j running on node i, then the weight of node i denoted as β_i is calculated as equation (1).

$$\beta_i = \frac{\sum_{j=1}^{5}(\alpha_j M_{ij})}{\sum_{i=1}^{k}\sum_{j=1}^{5}(\alpha_j M_{ij})} \tag{1}$$

3.4. Situation Index Calculation

3.4.1. Vulnerability Situation In Service Layer

The latest version of CVSS (CVSS v3.0) [16] is used to evaluate the severity of single vulnerability, and then get the vulnerability situation in service layer by weighted summation. The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS is composed of three standard groups: Base score, Temporal score and Environment score. Scores range from 0 to 10, with 10 being the most severe. Many utilize only the CVSS Base score for determining severity. Figure 2 illustrates the Base metrics.

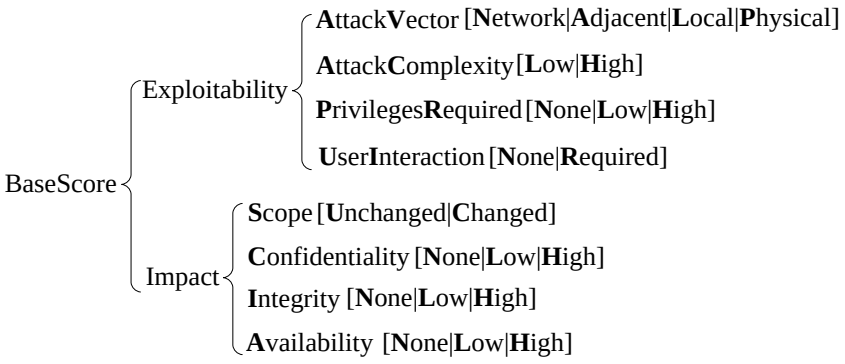

Figure 2. CVSS v3.0 Base Score Group

The CVSS base score is considered as the vulnerability situation in service layer, which is shown in equation (2).

$$SS_V = BaseScore_{CVSS} \tag{2}$$

3.4.2. Vulnerability Situation in Node Layer

Taking node as a unit, this index reflects the severity of all vulnerabilities in a node. Suppose there are k vulnerabilities denoted as vul_i ($i=1,\cdots,k$) in the node, α_i denotes the weight of service corresponding to vul_i, then the vulnerability situation in node layer is calculated as equation (3).

$$NS_V = \sum_{i=1}^{k} \alpha_i SS_V(vul_i) \tag{3}$$

3.4.3. Vulnerability Situation in Network Layer

Suppose there are n nodes denoted as $node_i$ ($i=1,\cdots,n$) in the node, β_i denotes the weight of $node_i$, then the vulnerability situation in network layer is calculated as equation (4).

$$LS_V = \sum_{i=1}^{n} \beta_i NS_V(node_i) \tag{4}$$

3.4.4. Threat Situation in Service Layer

The DEARD model proposed by Microsoft is adopted to evaluate risk after damage potential, reproducibility, exploitability, affected users and discoverability. Specific categories and simplified method of taking value are listed in Table 1. Each category is scored according to IDS alert, vulnerability scanning results and security response. Then the risk caused by atomic attack is calculated by equation (5). Finally, the value of risk is mapped into [0.0, 1.0] as the threat situation in service layer.

Table 1. Simplified DREAD Threat Assessment Model

Symbol	Implication	Value		
		High (3)	*Medium* (2)	*Low* (1)
D	Damage potential	Disrupt system security; gain full trust; perform root privilege	Leak sensitive information	Leak information not important
R	Reproducibility	Repeat easily without a time window	Repeat only at a certain time window and under specific condition	Difficult to repeat
E	Exploitability	Novice can attack in a short time	Experienced programmer can attack and repeat	Programmer with very rich experience and understanding vulnerability can attack
A	Affected users	All users, default configuration	Some users, not default configuration	Very few users, anonymous users
D	Discoverability	Published information about vulnerability and attack; vulnerability exists in frequently used part and obvious	Vulnerability in the little use part; only a few user may find and design a malicious use	Vulnerability is undefined; user is unlikely to find potential threat

$$Risk = Probability \times Impact = (R+E) \times (D+A+D) \tag{5}$$

3.4.5. Threat Situation in Node Layer

Generally, attacker needs to take a series of attack behaviors (atomic attacks) to achieve a specific target. The information and access control privileges of some nodes in the network system are the premise of these attacks. And they happened in turn to alter the information and access control privileges of some nodes, including finding valuable information, enhancing user's privilege, deleting filter rules, and adding trust relationship. All potential attack paths can be discovered by matching the consequence of former attack behavior with the prerequisite of later.

Take node as a unit. Atomic attacks happened on a node are correlated by causal relationship. Markov chain model is adopted to accumulate the severity along attack path. In the reconstructed attack scene, graph node denotes the state of network node, including user's privilege and vulnerability, and directed edge denotes atomic attack. Take the threat situation in service layer as the threat caused by atomic attack. Suppose the prior option of attackers is attack behavior with higher severity. From the initial normal state of target system to the end of attack along attack path, there are two kinds of circumstances to calculate the threat situation in node layer.

Case 1: There is no attack path, but m attack behaviors happened.

$$NS_{\mathrm{T}} = \underset{i=1}{\overset{m}{Max}}\{SS_{\mathrm{T}i}\} \tag{6}$$

Case 2: There is attack path.

$$\begin{cases} NS_{\mathrm{T}-S_j} = \dfrac{\sum\limits_{S_i \in Into(S_j)} [P_{S_iS_j} \times (SS_{\mathrm{T}-S_iS_j} + NS_{\mathrm{T}-S_i})]}{|Into(S_j)|} \\ P_{S_iS_j} = \dfrac{SS_{\mathrm{T}-S_iS_j}}{\sum\limits_{S_k \in Into(S_j)} SS_{\mathrm{T}-S_kS_j}} \end{cases} \tag{7}$$

where $NS_{\mathrm{T}-S_j}$ denotes the threat situation in node layer with node state S_j; $Into(S_j)$ denotes the state set of previous moment when node state switches to S_j; $|Into(S_j)|$ is the number of states in state set; $P_{S_iS_j}$ is the probability of node state transition from S_i to S_j; $SS_{\mathrm{T}-S_iS_j}$ is the threat situation in service layer when node state transforms from S_i to S_j; $NS_{\mathrm{T}-S_0} = 0$ at the initial normal state.

3.4.6. Threat Situation in Network Layer

Causal correlate atomic attacks occurred at different nodes, then the cumulative threat along attack path is gained by using Markov chain.

In the reconstructed attack scenario, graph node represents network node, which has the node layer threat dimension situation; directed edge represents atomic attack; and the threat caused by atomic attack is expressed by the threat situation in service layer. Similar to the node layer threat situation, the attacker is assumed to prefer choosing a more serious attack behavior. From the initial normal state of target system to the end of attack along attack path, there are two kinds of circumstances to calculate the threat situation in network layer.

Case 1: There is no attack path.

$$LS_{\mathrm{T}} = \sum_{i=1}^{m} \beta_i NS_{\mathrm{T}i} \tag{8}$$

where m is the number of nodes in network.

Case 2: There is attack path. The node layer threat dimension situation of each node needs updating, then weighted summation is used.

$$\begin{cases} NS_{\mathrm{T}j} = \dfrac{\sum\limits_{N_i \in Into(N_j)} [P_{N_i N_j} \times (SS_{\mathrm{T}-N_i N_j} + NS_{\mathrm{T}i})]}{|\,Into(N_j)\,|} \\ P_{N_i N_j} = \dfrac{SS_{\mathrm{T}-N_i N_j}}{\sum\limits_{N_k \in Into(N_j)} SS_{\mathrm{T}-N_k N_j}} \\ LS_{\mathrm{T}} = \sum\limits_{i=1}^{m} \beta_i NS_{\mathrm{T}i} \end{cases} \tag{9}$$

where $NS_{\mathrm{T}j}$ denotes the threat situation in node layer of node j; $Into(N_j)$ denotes the node set to attack node j; $|Into(N_j)|$ is the number of nodes in node set; $P_{N_i N_j}$ is the probability of node N_i to attack node N_j; $SS_{\mathrm{T}-N_i N_j}$ is the threat situation in service layer when node N_i attacks node N_j.

3.4.7. Running Situation in Node Layer

Based on the performance parameters, such as CPU utilization C_{CPU}, memory utilization C_{MEM}, and bandwidth utilization C_{BW}, D-S evidence theory is adopted to comprehensively assess the destruction severity of resource availability. C_{CPU}, C_{MEM} and C_{BW} measure the availability of request resources for legitimate users from different aspects, the greater the value of which, the worst the availability of resources. Taking C_{CPU}, C_{MEM} and C_{BW} as three resources available evidence, the evaluation results through D-S evidence theory fusion is more accurate than depending on a single evidence. Define discrimination frame $\Omega = \{Safe, Unsafe\}$ to denote the system's state. The basic probability distribution function is shown as equation (10).

$$\begin{aligned} m_1(\{Safe\},\{Unsafe\}) &= (1 - C_{\mathrm{CPU}}, C_{\mathrm{CPU}}) \\ m_2(\{Safe\},\{Unsafe\}) &= (1 - C_{\mathrm{MEM}}, C_{\mathrm{MEM}}) \\ m_3(\{Safe\},\{Unsafe\}) &= (1 - C_{\mathrm{BW}}, C_{\mathrm{BW}}) \end{aligned} \tag{10}$$

After evidence combination, the function of the local evidence is obtained, such as equation (11).

$$NS_{\mathrm{R}} = m(\{Unsafe\}) = \frac{\sum\limits_{X \cap Y \cap Z = \{Unsafe\}} m_1(X) m_2(Y) m_3(Z)}{\sum\limits_{X \cap Y \cap Z \neq \varnothing} m_1(X) m_2(Y) m_3(Z)} = \frac{C_{\mathrm{CPU}} C_{\mathrm{MEM}} C_{\mathrm{BW}}}{C_{\mathrm{CPU}} C_{\mathrm{MEM}} C_{\mathrm{BW}} + (1 - C_{\mathrm{CPU}})(1 - C_{\mathrm{MEM}})(1 - C_{\mathrm{BW}})} \tag{11}$$

3.4.8. Running Situation in Network Layer

Based on the running situation in node layer, the running situation in network layer is calculated as equation (12).

$$LS_{\mathrm{R}} = \sum_{i=1}^{m} \beta_i NS_{\mathrm{R}i} \tag{12}$$

where $NS_{\mathrm{R}i}$ denotes the running situation in node layer of node i.

4. Experiments and Results

Experiment scenario designed in [9] is reproduced here. The assumed network model is shown in Figure 3, including three servers and one inside host. The database server (DS), file server (FS) and inside host (H1) are deployed on the inside of the internal firewall. The server is marked by a service that external users can access. Other unauthorized access will be blocked by an external firewall. The attacker attempts to attack DS from the host H0. Table 2 lists the initial distribution of vulnerabilities. Figure 4 shows all

possible attack paths that are capable of achieving the attack target. Table 3 lists the evaluation results of atomic attack.

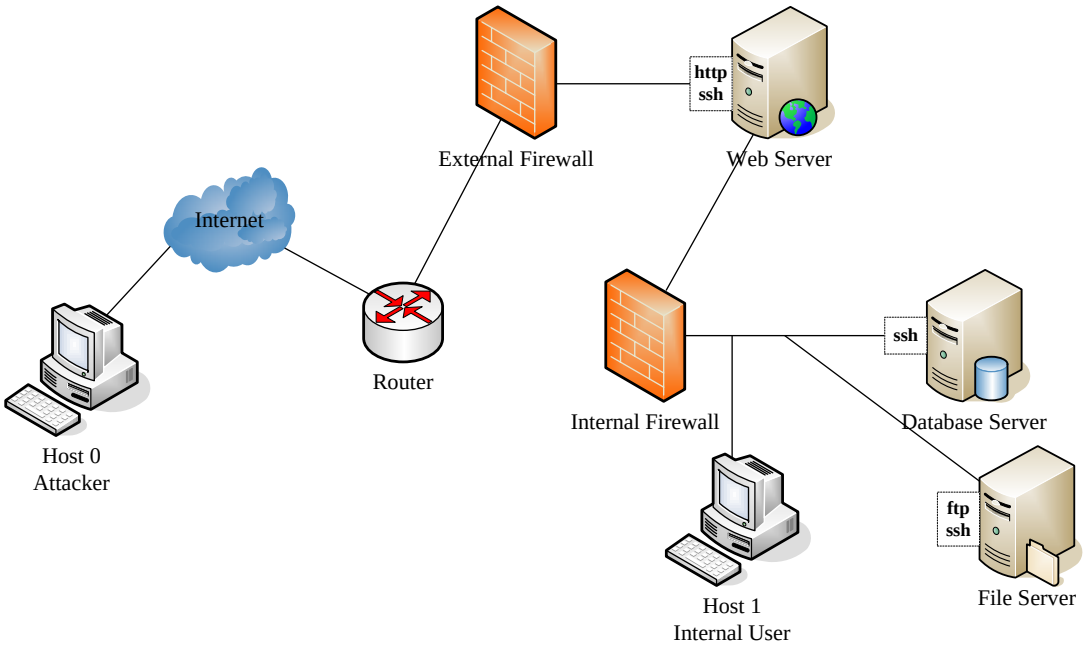

Figure 3. Network model

Table 2. The Initial Distribution of Vulnerabilities

Node	Vulnerability	CVSS severity AV/AC/PR/UI/S/C/I/A	*SS*v	*NS*v
WS	CVE-2011-2688	N/L/N/N/U/L/L/L	7.3	7.3
DS	CVE-2012-2122	N/H/N/N/U/L/L/L	5.6	13.4
	CVE-2010-2693	L/L/L/N/U/H/H/H	7.8	
FS	CVE-2012-6067	N/L/N/N/U/H/H/H	9.8	19.6
	CVE-2011-4130	N/L/N/N/U/H/H/H	9.8	
H1	CVE-2008-3234	N/L/N/N/U/L/L/L	7.3	7.3

Table 3. The Severity of Atomic Attack

Attack	D	R	E	A	D	Risk	SS_T
Att1	2	2	2	2	3	28	0.458
Att2	1	2	2	2	3	24	0.375
Att3	3	3	3	3	3	54	1.000
Att4	3	3	3	3	3	54	1.000
Att5	2	2	2	2	3	28	0.458
Att6	3	3	3	3	3	54	1.000

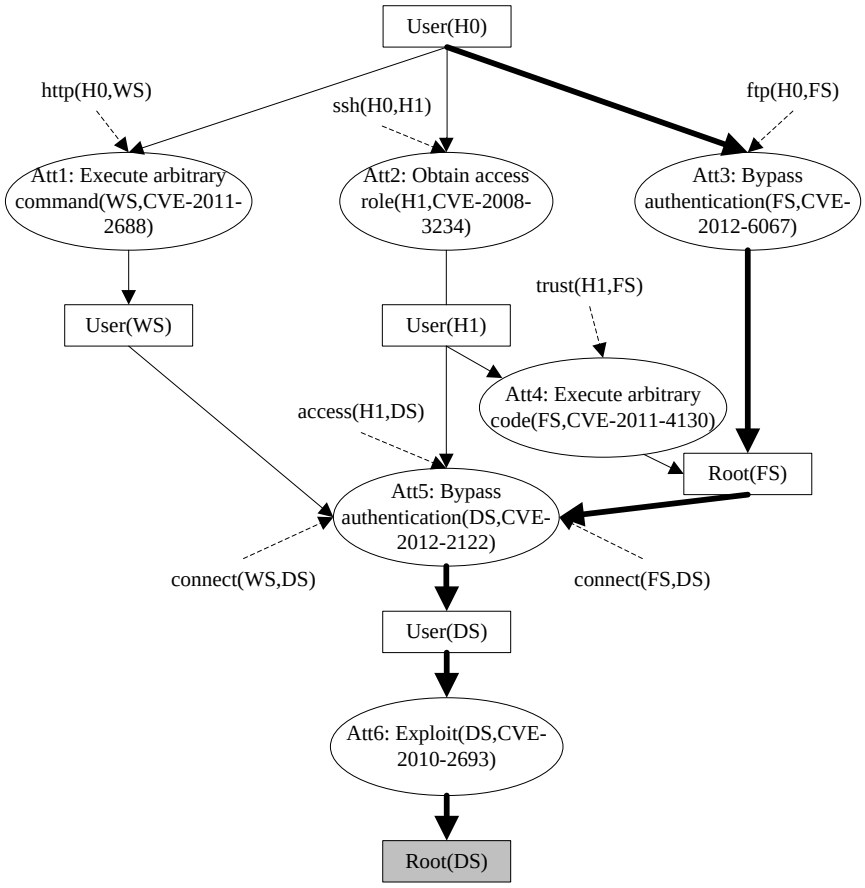

Figure 4. Potential Attack Path

Suppose the attacker prefers implementing attack behavior with higher severity, and the same atomic attack is not repeated after the achievement of specific target. The actual attack path is shown in bold part of Figure 4: Firstly, Att3 was executed from H0 to attack FS, and the FS's super user privilege was obtained; then Att5 was executed to attack DS, and the general user privilege was obtained; further on, Att6 was implemented to promote the privilege to super user privilege. The simplified attack path is shown in Figure 5.

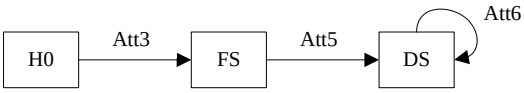

Figure 5. The Real Attack Path

The threat situation in node layer and network layer are shown in Figure 6. The mark 1,4 and 7 on time axis corresponded to the moment when Att3, Att5 and Att6 were executed. Effective remedial measures were not carried out, so the threat situation of node FS remained unchanged. With the evolution of the attack process, the threat situation of node DS and the entire network presented an upward trend. Since the attack behavior does not constitute a significant impact on node resources and network resources, the running situation is not discussed here.

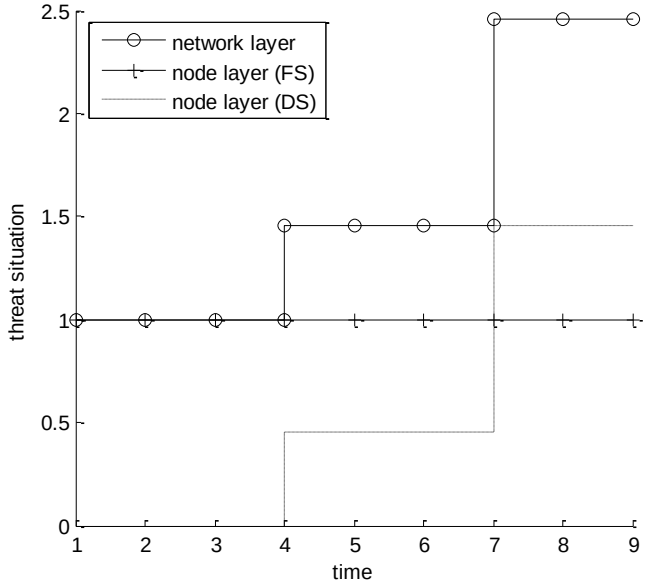

Figure 6. Threat Situation in Node Layer and Network Layer

5. Conclusion

Network security situation awareness needs integrating each specific network management technology (such as vulnerability scanning, intrusion detection, *etc*.) to carry on comprehensive and systematic research about the elements of network security situation, and finally achieve the comprehensive evaluation and display of the overall situation. In this paper, based on multi-source data, a series of hierarchical network security situation assessment indicators from the aspects of vulnerability, threat and basic operation are proposed, followed by quantitative calculation method, and the feasibility of this method is verified by simulation. To make an accurate, comprehensive and detailed description of the network is the premise of the network security situation awareness. In order to improve the practicability of the network security situation assessment technology, we will focus on the effective representation of the knowledge of network security situation.

Acknowledgements

The research presented in this paper was supported in part by the National Natural Science Foundation of China (No.61562004, No. 61300211), the Special Research Fund for the Doctoral Program of Higher Education (No.20130073130006), Guangxi Natural Science Foundation (No.2015GXNSFBA139255), Zhejiang Natural Science Foundation (No. LY17F020030), High Level Innovation Teams and Distinguished Scholars Program Fund of Guangxi Colleges and Universities, the Discipline Construction Fund of School of Management Science and Engineering in Guangxi University of Finance and Economics (No.GK2015002).

References

[1] T. Bass. "Multisensor data fusion for next generation distributed intrusion detection systems", Proceedings of the IRIS National Symposium on Sensor and Data Fusion, Piscataway, NJ, USA, **(1999)** April 28.
[2] X. Chen, Q. Zheng, X. Guan and C. Lin, "Quantitative hierarchical threat evaluation model for network security", Journal of Software, vol.17, no.4, **(2006)**, pp.885-897. (in Chinese)
[3] L. Zhu, Z. Zhang and L. Feng, "Research on hierarchical network security threat situation assessment", Application Research of Computers, vol.28, no.11, (2011), pp.4303-4306, 4310. (in Chinese)
[4] X. Cai, H. Zhang and T. Li, "Network security threats situation assessment and analysis technology study", International Journal of Security and Its Applications, vol.7, no.5, **(2013)**, pp.217-224.
[5] M. Frigault, L. Wang, A. Singhal and S. Jajodia, "Measuring network security using Dynamic Bayesian Networks", Proceedings of the 4th ACM workshop on Quality of protection, Alexandria, VA, USA, **(2008)** October 27-31.
[6] P. Xie, J. H. Li, X. Ou, P. Liu and R. Levy, "Using Bayesian networks for cyber security analysis", Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems & Networks, Chicago, Illinois, USA, **(2010)** June 28-July 1.
[7] N. Poolsappasit, R. Dewri and I. Ray. "Dynamic security risk management using Bayesian Attack Graphs", IEEE Transactions on Dependable and Secure Computing, vol.9, no.1, **(2012)**, pp.61-74.
[8] I. Kotenko and E. Doynikova, "Security assessment of computer networks based on attack graphs and security events", Proceedings of the 2nd IFIP TC5/8 International Conference on Information and Communication Technology, ICT-EurAsia, Bali, Indonesia, **(2014)** April 14-17.
[9] F. Dai, Y. Hu, K. Zheng and B. Wu. "Exploring risk flow attack graph for security risk assessment", IET Information Security, vol.9, no.6, **(2015)**, pp.344-353.
[10] V. Gorodetsky, O. Karsaev and V. Samoilov, "On-line update of situation assessment based on asynchronous data streams", Proceedings of the 8th International Conference on Knowkedge-Based Intelligent Information and Engineering Systems, Wellington, New Zealand, **(2004)** Septemper 20-25.
[11] M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh and G. Varghese, "Network monitoring using traffic dispersion graphs (tdgs)", Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, San Diego, CA, USA, **(2007)** October 23-26.
[12] S. Wang, R. State, M. Ourdane and T. Engel, "RiskRank: Security risk ranking for IP flow records", Proceedings of the 2010 International Conference on Network and Service Management, Niagara Falls, Canada, **(2010)** October 25-29.
[13] M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino and S. Jha. "Interdependent security risk analysis of hosts and flows", IEEE Transactions on Information Forensics & Security, vol.10, no.11, **(2015)**, pp.2325-2339.
[14] Z. Wen, Z. Chen, X. Deng and A. Liu, "Network Security Situation Awareness Method Based on Multi-Source and Multi-Level Information Fusion", Journal of Shanghai Jiaotong University, vol.49, no.8, **(2015)**, pp.1144-1152. (in Chinese)
[15] Tom Olzak, "A practical approach to threat modeling", http://www.infosecwriters.com/text_resources/pdf/, **(2006)**.
[16] CVSS: common vulnerability scoring system version 3.0 calculator, https://www.first.org/cvss/calculator/3.0, **(2015)**.

Authors

Lina Zhu, she received the B.S. degree in computer science and technology from Central China Normal University, Wuhan, China, in 2003, the M.S. degree in pattern recognition and intelligent system from Wuhan University, Wuhan, China, in 2006, and the Ph.D. degree in computer application technology from Harbin Engineering University, Harbin, China, in 2010. She is now an Associate Professor of Guangxi University of Finance and Economics, Nanning, China. She is also a postdoctoral research fellow from October 2014 in Shanghai Jiaotong University. Her research interests include intrusion detection, situation awareness, and WSN key management.

Guoen Xia, he received the B.S., M.S. and Ph.D. degrees from Chongqing University of Technology, Chongqing, China, in 2000, Southwest University, Chongqing, China, in 2004, and Southwest Jiaotong University, Chengdu, China, in 2007. He is a Professor and the Dean of Department of Academic Affairs, Guangxi University of Finance and Economics, Nanning, China, and Master's Supervisor of Guangxi Normal University, Guilin, China. His research interests include business intelligence, logistics management, and network security.

Zuochang Zhang, he received the B.S. and M.S. degrees in cartography and geography information system from Wuhan University, Wuhan, China, in 1999 and 2005. His research interests include GIS and its applications, Internet of Things, and network security. He has published several papers in these areas. He has participated in a number of domestic and foreign research projects, and developed several network security-related projects.

Jianhua Li, he is currently a Professor/Ph.D. Supervisor and the Dean of the College of Information Security, Shanghai Jiao Tong University, Shanghai, China, where he received the B.S., M.S., and Ph.D. degrees, in 1986, 1991, and 1998, respectively. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He is a Committee Member of the information security area of the state tenth five-year plan of China, a Committee Expert of the China State Secrecy Bureau and Shanghai Secrecy Bureau, and a Committee Expert of the Information Technique Standardization Committee of Shanghai, China. He was the Leader of over 30 state/province projects of China, and has authored over 200 papers. He has authored six books and holds about 20 patents. He made three standards and has five software copyrights. He was a recipient of the National Technology Progress Award of China in 2005, the National Technology Progress Award of Shanghai in 2003 and 2004, and two National Technology Progress Awards of Shanghai in 2004. His research interests include information security, signal process, and computer network communication.

Renjie Zhou, he is an assistant professor in Key Laboratory of Complex Systems Modeling and Simulation, School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China. He received Ph.D. degree from Harbin Engineering University, Harbin, China, in 2012. From 2009 to 2011, he was a visiting scholar in the Department of Electrical and Computer Engineering at the University of Massachusetts at Amherst. His research interests include measurement and analysis of online social networks, and network security.

