Advanced Science and Technology Letters
Vol.111 (NGCIT 2015), pp.151-155
http://dx.doi.org/10.14257/astl.2015.111.29

Dynamic awareness method for network threats

Jieyun Xu and Hongzhen Xu

East China Institute of Technology, Jiangxi 330013, china
jyxu@ecit.cn

Abstract. In order to solve the redundancy question in complex network which is caused by similar attack method and similar node object in attack model, the node domain and transition domain of Petri Net are divided into equivalence classes, and then the construction method of rough vulnerability relation model is given. By defining similar degree of path, search for all of the characteristic attack path which can attain attack object by use of ant algorithm, and calculate the maximal threat of object node which is brought by characteristic strategy.

Keywords: Attack and Defense Strategy, Attack Model

1 Introduction

With constant updates of attack technologies, aggrandizing network scale and more complicated structure, the real-time awareness of network threat situations becomes a critical issue to be solved by network administrators[1-2]. But in the face of many nodes (such as user computer, server, security system, network devices) in the complicated network system, vulnerabilities in such nodes, and the intricate connection and access relationship among them, administrators can't figure anything out about how to remove redundant information and extract necessary information and to make timely and comprehensive evaluations of threats by according to the dynamic changes of attack situations [3-4]. So the dynamic threat assessment in the complex network system is an important and very new research topic in today's network security field. It faces great difficulties and moves slowly [5-6].

For the attack strategy generation based on incomplete information, [7] suggested the use of rough attack graph to depict uncertainties for what strategies taken by the attacker. The max-flow analysis algorithm of network risks was developed according to the classification of attack modes [8]. But the rough attack graph's generation method and the related analysis were dependent on the definition and knowledge of the attacker's abilities. In practical analysis, it will meet big challenges, because in the active defending phase, i.e. before the attack happens, the attacker's situation is almost nothing to the defendant. The attacker's power and preference are both uncertain information. So the method is limited in the scope of application [9-10].

ISSN: 2287-1233 ASTL

2 Creation of rough vulnerability correlation model

2.1 Definition of Petri net based on rough objects

In reality, when several vulnerabilities in one node can reach the same attack purpose, different attackers show different preferences for vulnerabilities to be attacked, specifically, attackers decide to choose which vulnerability as breakthrough point as per their familiarity with various attack modes and the attack power. So all predications made by the defending side is of roughness, e.g. evaluating one or more paths which have the biggest threat degree. They are deterministic judgments made based on incomplete information, which can't be completely held by only the attacker's subjective consciousness and experience. They are imperfect.

Professor Tong He and Kaiquan Shi introduced rough set theory to the traditional graph model. Arcs/sides among nodes are used as dividing object in the domain space. After attributes assigned to those arcs/sides, they are categorized to different equivalent classes $[e]_R$ based on the equivalent relation R, discriminating the type of arcs/sides with the same endpoints. On the basis of ideas of rough graph, the paper brings in rough set theory to Petri net modeling to define a new Petri net model. Rough Petri net has descriptive capability to the incomplete information. It represents the in-distinguish ability among attack behaviors in the same node and that among nodes having similar function, position and attack relationship in the domain network. We define it like:

Definition 2.1 the change of space. Given $U = (t_1, t_2, ...t_U)$ to change the domain, t_i is change of Petri network, said an attack behavior. R is the U attribute set, it can form equivalence relation in U. $U / R = \{T_1, T_2, T_3, ..., T_v\}$ said that all the equivalence classes according to the R partition

Definition 2.2 Node space. Given U $U^{'} = \{O_0, O_1, ...O_{|U^{'}|}\}$ is the node domain. O_i is node object of Petri net. $R^{'}$ is attribute set in $U^{'}$. It can form equivalence relation in $U^{'}.U^{'} / R^{'} = \{Obj_1, Obj_2, Obj_3, ..., Obj_c\}$ shows all valence class of $R^{'}$

2.2 The division of the domain class space on Petri

According to definitions 2.1 and 2.2, the node object space and the change of space on Petri net divided equivalence class, formed a class space.

Generation algorithm change class space:

Algorithm：Classpace_generation

Input： $U = (t_1, t_2, ...t_U)$, R

Output: $U/R=\{T_1,T_2,T_3,...,T_v\}$

(1) Initialization. Create set $U/R=\varnothing$ attVal={{Access},{User},{Root, Controlled},{DoS}, {Info-leak}}
(2) for(i=2;i≤m;i++)
(3) { flag=0
(4) for(j=1;j≤class_num; j++)
(5) {if $(I(t_i).Obj == I(T_i).Obj \&\& O(t_i) == O(T_i))$
(6) { $T_j = Obj == I(T_j).Obj \&\& O(t_i) == O(T_j))$
(7) {$T_j = T_j \cup t_i$; flag=1;break;}}
(8) if(flag==0)
(9) Create a new class $T_{++class\_num} \in U/R; T_{class\_num} = \{t_i\}$ }
(10) Output U/R

4 Experiment Design and Discussion

In order to illustrate the establishment and analysis of dynamic network threat perception model, establish the following test network environment, it is shown in Figure 1.

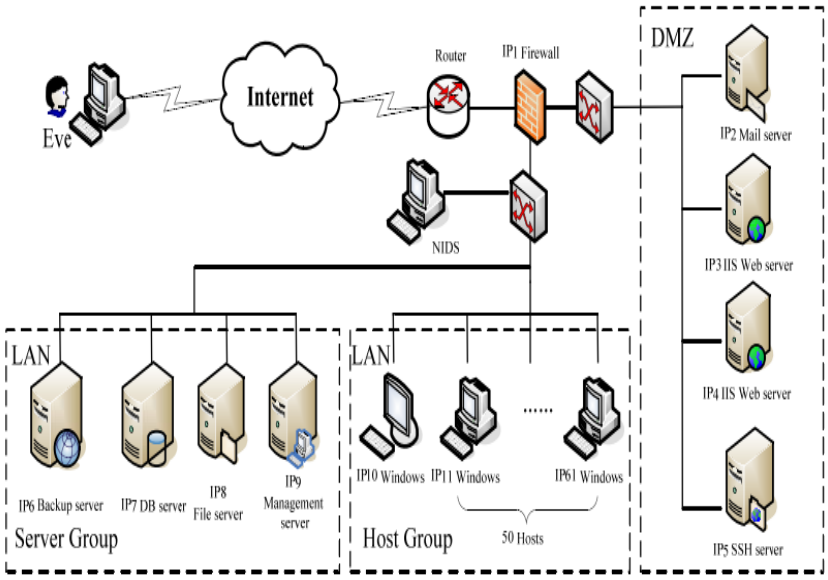

Fig.1. the network topology map

The whole web has 61 host devices, of which 5 hosts running in the DMZ area to provide services to users in the inner and outer net. Two Web servers run simultaneously and are of load balancing configuration. The internal local network includes two parts: server cluster and user cluster. The former consists of backup server, database server, file server and administrator server. The database server stores enterprise private data. Backup server copies important files in IP7 and IP 8 and updates them synchronously. When both database and backup servers break down, they can be automatically shifted as to provide promptly the relevant services. The administration server is responsible for security monitoring tasks. It drives related function modules to generate MD5 abstracts of key data files and regularly monitor and compare abstracts. If application servers in DMZ area and intranet server clusters are attacked, it will send alarms to the administrator and generate relative report. In the user cluster, there are 50 ordinary client computers and one management computer (IP10). With the help of firewall configuration software installed in the management computer and server management software, network administrators can configure firewall and control resource management, performance maintenance and monitoring configuration of each application server system. IP10 will assess punctually the current threat degree of network as per the alarm information sent by NIDS and IP9 and take defending strategies.

Firewall configuration information is in table 1:

Table1. Security policy configuration of the firewall

The source address	The source port	The destination address	The destination port
Extranet	Arbitrarily	LAN	Arbitrarily
Extranet	Arbitrarily	DMZ	Arbitrarily
LAN	Arbitrarily	Extranet and DMZ	Arbitrarily
IP3,IP4	80	IP7	1521
IP3,IP4,IP5	Arbitrarily	IP8	Arbitrarily
IP3,IP4	Arbitrarily	LAN	Arbitrarily
IP2	Arbitrarily	LAN	Arbitrarily

5 Conclusion

It proposed a new dynamic evaluation method for network threats. With IDS alarming information to rectify constantly the previous prediction, the network threat assessment is more practical. Meanwhile for complicated network system, it defined different security monitoring ranges. The rough Petri net was applied to reduce the generated number of attack paths. The adjustment and assessment of threat degree proved more flexible and practicable.

References

1. Zhang Jianfeng. Research on Key Technologies of network security situation assessment. The National Defense University of science and technology, 2013
2. Ma Dong. Research on Key Technologies of network threat detection and situation prediction. The University of national defense science and technology, 2013
3. Chen Chao. Research on technology of network security situation assessment based on knowledge acquisition and fusion rule. The PLA Information Engineering University, 2013
4. Zhang Dan. Research on the credibility of network system based on autonomic computing and self-optimization method. Henan University of Science and Technology, 2013
5. Liu Peng, Meng Yan, Wu Yanyan. Perception and prediction of large-scale network security situation. Computer security, 2013,03:28-35.
6. Ni Pingfu, Wu Zuoshun. Research on analysis method of network vulnerability. Computer technology and development, 2013,04:126-130.
7. Huang Guangqiu, Li Yan. Evaluation model based on rough graph network risk. Computer applications, 2010, 30 (1): 190-195.
8. Liu Xiaowu, Wang Huiqiang, Lv Hongwu, Ann the illumination. Network security situation awareness based on fusion of quantization. Journal of Jilin University (Engineering and Technology Edition), 2013,06:1650-1657.
9. Chen Rongmao. The complex network threat modeling and detection technology research. The University of national defense science and technology, 2013
10. Wang Chunzi, Zhang Bin, Huang Guangqiu. The attack strategy of mining and risk assessment model of attack based on full network. Computer engineering and applications, 2012,04:1-4+53.

