International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.249-256
http://dx.doi.org/10.14257/ijsia.2013.7.5.23

Attack Graph Algorithm in the Application of Intrusion Detection System

Luo Zhiyong[1], You Bo[1], Xu Jiazhong[1], Yu Guixin[1] and Liu Yahui[2]

[1]*Harbin University of Science and Technology, Harbin, China*
[2]*Beijing Information Science and Technology University, Beijing, China*
luozhiyongemail@sina.com

Abstract

In order to discover the network vulnerability timely and solve the very serious problems of network security, this paper puts forward the attack graph which is based on intrusion detection method. The method uses the generation global network attack graph algorithm to build network initial attack graph, and call attack graph optimization algorithm to remove global attack graph unreasonable path, and achieve the goal of simply attack graph. Finally, management personnel get the basis which is computed nodes in each state attack graph algorithms degree of loss to optimize the network security. Experiments show that the intrusion detection method is reasonable and effective, and has the advantages of simple and easy.

Keywords: *Network security; IDS; Attack graph; State node*

1. Introduction

With the further development of network attack and technology, network intrusion are getting more and more complicated, and its form of expression also shows diverse characteristics of network management personnel which brings enormous difficulties [1]-[2]. However, a loophole less network operating system can greatly improve the safety of network [3]. Therefore, we can find the reason of the network state that changes attack sequences early and becomes a key intrusion detection system [4]. Network management researchers found that the attacking sequence which is based on the graph theory model can attack faster, and solve the problems of the network [5].

This paper puts forward a kind of attack graph which is based on intrusion detection system model. Firstly, we optimize the whole generation network attack graph, and then call calculation state node loss degree algorithm to compute attack graph of each node in degree of loss, and form a node key degree. According to the degree of the key size, we optimize network strategy to solve the network vulnerability problems. Through the experiment, we demonstrate that the intrusion detection system and the validity of the model are correct.

The Education Department of Heilongjiang province science and technology research project (NO: 12521108). Harbin university of science and technology university youth fund for scientific research project (NO: 2011YF017)

LUO Zhiyong (1978—), Male, Lecturer, Doctoral students, mainly engaged in network security research

ISSN: 1738-9976 IJSIA

2. Attack Graph Detection Model

2.1. Related Definition

Network management personnel use global attack graph and combine all sorts of attack action between the causal relationship to dig out the network infiltration attack sequence, and grasp attack strategy, discover the network vulnerability, and achieve the goal of enhancement network security [6]. This paper will make invaders intrusion action changes to set for network different state of change so that the relevant defined as follows.

Definition 1, the intruding complexity. The invaders use a loophole to achieve successful invasion of host difficulty degree of numerical measure, this article is the Cd said.

Definition 2, the loophole. It is the network potential weakness, which is expressed as *B*(*Bid*, *Cd*, *deg*). Network potential weakness are among them, the Bid is loophole B in the vulnerability database *ID*, *Deg* uses the holes after a successful invasion to the host in the confidentiality, integrity and availability of bringing harm degree. The quantitative relationship of the *Bid*, *Cd* and *deg* will be expressed in the 7 please referring to literature.

Definition 3, the node degree of loss. The invaders successfully invades one node N_i ($i \neq 0$) of the network, and the node equipment in security is caused by the extent of the losses, this paper recorded as *LD* (N_i).

Definition 4, the key of node degree. The invaders successful invade one node N_i ($i \neq 0$) of the network, the whole network security is caused by the extent of the losses [8], this paper recorded as *KD* (N_i).

Definition 5, the host. A kind of network equipment with H says, its constitute is (*Name*, *SR*, *IDeg*). Among them, the *Name* for host Name; *SR* for security needs degree; *IDeg* is important degree.

Definition 6, the state node. State node is expressed as *N* (*Nid*, *H*, *BS*, *SS*, *SN*, *LD*, *KD*, *P*, *NetD*), in the attack graph with elliptic said. Among them, the state node for *Nid* is *ID*, *H* is the node of the corresponding host or network equipment; *BS* is the host or network equipment the existing loophole set; *SS* is this state host or network equipment by security threats network service set; *SN* is this state node son node set; *LD* and *KD* express the loss of the node degree and key degree; *P* is a network status change to the probability of the state nodes; *NetD* for the network state is the harm degree, which is to the host in confidentiality, integrity and availability [9].

Definition 7, the attack graph. It is a directed graph, and it is the state transition system too, which is expressed as $G = (NS, CS, T, N0, NS_g)$. Among them, the *NS* is the set of the network state nodes; *CS* is the set of network intrusion conditions, every condition in attack graph with pure text said; *T* is the set of state transition relationships; $N0 \in NS$ is initial state node; $NS_g \subseteq NS$ is the set of network intrusion final target state nodes. *G* satisfies the constraints: $t_i(N0, Ns \cup Cs) \rightarrow N_g$. Among them, the $t_i \in T$ is a concrete conversion relation; $Ns \subseteq NS$ is a subset of network state node set; $Cs \subseteq CS$ is a subset of network intrusion conditions set; $N_g \in NS_g$ is a final target state of network intrusion.

Definition 8, the attack path. For the final target state node of the network intrusion $N_g \in NS_g$, if the attack graph consisting of a group of conditions and state nodes which constitute a sequence $L(C_1, C_2, N_0, N_1, \cdots, C_i, N_j, \cdots, C_{n-1}, N_{m-1})$($0<i<n-1, 0<j<m-1$) makes $t_z(N_0, L) \rightarrow N_g$. Among

them, the $t_z \in T$ is a specific conversion relation, the N_0L is an attack path, and this paper records the R.

By defining the 7 and 8 definition can be obtained:

$$KD(H_i) = \sum_{N_j \in NS_i} LD(N_j)$$

Hi for a host of network and $i \neq 0$, NS_i for H_i is a node set in state diagram which affects the state, $N_j \in NS_i$ is any one state node.

2.2. Attack Graph Generating Algorithm

Attack graph is simulation invaders invasion of the whole network which is many kinds of methods of abstract, so the global attack graph plays a very important role [10] for network management personnel manage network security. Combined with the proposed related definition, we give the generating global attack graph steps are as follows:

(1) Collect network information, network topology structure, host loophole, the invasion of conditions of information formalization;

(2) After the formal network security information classification, respectively to join the corresponding queue, construct the network state node initial queue;

(3) According to the network vulnerability information and the use of loopholes penetration of rules, structure against queue;

(4) According to the network node state queue and search attack queue elements, form a new network state node and a new condition node, and join the network state node queue:

(5) Repeat step (4) until successful invades of network and the network state node forms a final state;

(6) To form the global attack graph.

According to the above steps, this paper gives an attack graph generating algorithm which is as follows:

Input: Parameter NS, CS, N_0, MaxStep, P;

Output: Attack Graph G;

Algorithm:

1. State_queue=NULL, N_0.step=0, NS=NULL, G=NULL;

2. ADD(NS,$N_{1\sim n}$); // All state node set to join in the NS

3. Insert(State_queue, N_0); //N_0 to state the queue

4.while(state_queue<>NULL){ S_i=Delete(State_queue);

5.CS_i =Detect(S_i);

6. if((S_i.step-MaxStep)==0) break; else{ for each N_j in NS{

7. g_j= N_j;

8.if((Person(g_j)inCS_i)&&(Result(g_j)notinCS_i)){S_k=NEW();

9.if((i==0)OR(CS_i in N_j.precondition))

10. {if(Probability (N_0, S_k)>P)

11.{if((Exists(S_q,State_queue))and($S_q$likeS_k)and((S_i,S_q)inG))// Judge whether new node in attack graph has already exist

12. {S_q.P=max(S_q.P, S_k.P);// Update invasion

13. e_j=Mark (S_i, CS_i,S_q);Insert(e_j, G);Delete S_k;}

14. else{e_j =Mark ((S_i, CS_i,S_k);Insert(ej, G);

15. k++;S_k.step=S_k.step+1;// Update S_k intrusion steps

16. Insert(State_queue, S_k); // Add S_k to state queue

17.}}}else Delete S_k;}}}}

2.3. Attack Graph Optimize Algorithm

According to a lot of experiments, the Figure 2.2 attack graph generating algorithm in special circumstances produces attack graph, which appears some attack path in actual intrusion process that could not have happened. For example, in Figure 1(a), the attack graph of the attack path *R* (*N_0, C_1, C_3, N_1, N_3, C_6, N_1, C_3, N_3,* the *C_7*, and *N_5*); the actual intrusion process could not have happened. Because the state node N_1 happen, the must invasion condition *C_1* and *C_2*, *C_6* must meet, and conditions of *C_6* are happening in a successful invasion state node *N_1*, so produce paradox. From this example, the global attack graph must be optimization, this paper presents optimization attack graph algorithm, and Figure 1(b) is (a) algorithm to optimize the attack graph.

The secure connection is shown in Figure 2.

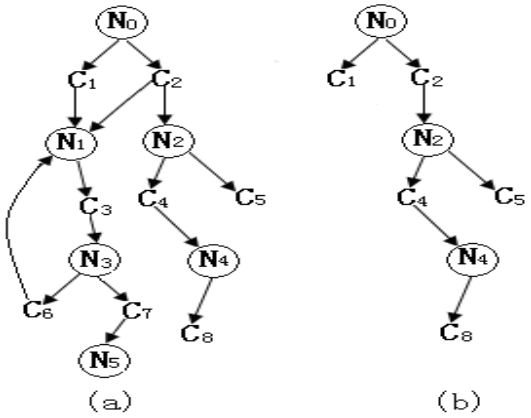

Figure 1. Attack Graph Before and After Optimization Example

Input: before optimization attack graph G

Output: the optimized attack graph G

Algorithm:

1. for each N_i in NS {

2. Sum_i=Count(Pre(N_i)); // N_i is Father node number

3. flag(N_i)=false;}

4. for each C_i in CS Insert(Condition_queue, C_i);

5. for each q in Condition_queue

6. for each N_j in Post(q){

7. num[N_j] = num[N_j]+1;

8. if num[Nj] = Sumj flag(Nj)=true;}

9.for each Ck in Post(N_j) {

10. Insert (Condition_queue, C_k);} // Join condition queue

11. for each N_i in NS if (flag(N_i)==false) Delete(G, N_i);

12. return G;

2.4. Calculate the Loss of State Node Degree Algorithm

When we optimize the attack graph, we should calculate the attack graph in each state node the degree of loss, and then obtain the condition node degree of the key. Network management personnel by getting each state node loss degree and the degree of the key to optimize configuring security, and enhance the network security.

Input: the condition node NS with relevant information

Output: state set each node loss degree LD (NS)

Algorithm:

1. while(NS<>NULL){

2. N_i=Delete(NS,i);// Remove NS set a state node

3. N_j=Pre(N_i);// State node for N_i N_j direct father node

4. N_i.NetD=0,N_i.P=0;// N_j initialization Ni

5. N_i.P=N_i.B.Cd×N_j.P;

6. N_i.NetD=N_i.P×N_i.B.deg;// Calculate Ni harm degree

7. N_i.LD=Ni.H.IDeg×N_i.NetD×N_i.H.SR;

8. i=i+1;}

9. return NS;

3. Network Security Policy Optimization Method

Attack graph is used to simulate the invaders network intrusion methods, so the network management personnel can judge network vulnerability and make the repair in order to enhance the purpose of network security. In this paper, the general method of this process is as follows:

(1) Call algorithm to generate network global attack graph;

(2) Call algorithm to optimize the attack graph;

(3) Call algorithm, calculate state node safety degree of loss;

(4) Put attack graph which can be deleted or repair safety state node in the queue Q;

(5) Compute queue Q element in the key degree;

(6) Queue Q key degree maximum state node out of the team and the whole mend;

(7) Repeated execution (1) to (6) until the queue Q is empty.

4. Experiment

Taking an enterprise network for experimental object, this is verifying with the proposed method to manage their network security effectiveness and correctness. Network environment is: we use 5 host form enterprise network, including that host IP_1 is FTP, IP_2 is MySQL server, IP_3 is Telnet, IP_4 is HTTP, and IP_5 is Oracle server. Enterprise firewall only allows the network access to the Telnet server and the network access. Enterprise network environment host information and vulnerability information are shown in Table 1 and Table 2, and the network topological structure is shown in Figure 2.

Table 1. Host Information

Name	SR	IDeg	Server	Bid	Inv_Cond_ID
IP_1	6	2	FTP	9904,13454	C_2,C_3
IP_2	3	3	MySQL(FTP)	7974	C_4
IP_3	4	2	Telnet	12815	C_1
IP_4	5	1	HTTP	9691	C_6
IP_5	2	3	Oracle	14312	C_5

Table 2. Vulnerability Information

Bid	Cd	Deg	Type
9904	0.5	2	Privilege promotion class
13454	0.7	1.5	Privilege promotion class
7974	0.7	2	Privilege promotion class
12815	0.7	3	Privilege promotion class
9691	0.3	3	Privilege promotion class
14312	0.9	1	Denial of service classes

The Table 1 and Table 2 show the network information. Telnet holes currently has no effective repairing method, and the plus host IP_3 is Telnet server firewall which can't shut down for the network access, so the host IP_3 is the attack graph of initial loophole. The invaders can enter by the server connection, and then ascend the permission. Finally, it gets the purpose of invasion of Oracle server.

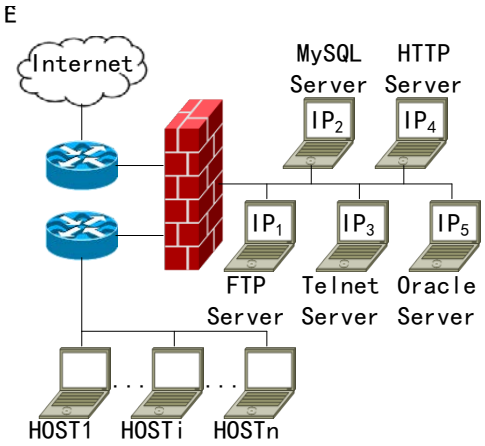

Figure 2. Network Topology

According to the above analysis, we use the attack graph to generate algorithm and optimization algorithm which is concluded that the enterprise network global attack graph is shown in Figure 3(a).

Call calculation state node loss degree algorithm to calculate the Figure 3 (a) state N_1 to N_8 loss degree: $LD(N_1)=16.8$; $LD(N_2)=8.82$; $LD(N_3)=8.82$; $LD(N_4)=3.087$; $LD(N_5)=6.174$; $LD(N_6)=2.205$; $LD(N_7)=0.7718$; $LD(N_8)=1.85$.

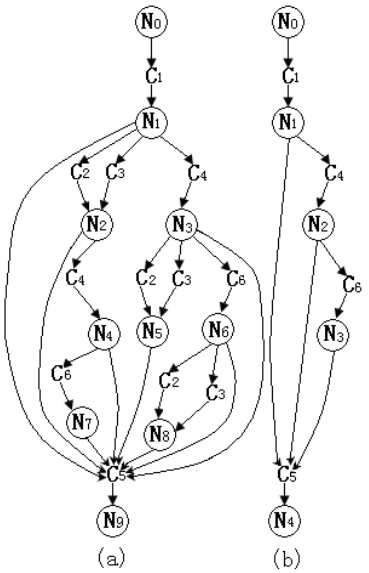

Figure 2. Enterprise Network Attack Graph

Table 2. Vulnerability Information

Name	Bid	Nodes	LD	KD
IP_1	9904,13454	$\{N_2,N_5,N_8\}$	{8.82,6.174,1.852}	16.846
IP_2	7974	$\{N_3,N_4\}$	{8.82,3.087}	11.907
IP_3	12815	$\{N_1\}$	{16.8}	16.8
IP_4	9691	$\{N_6,N_7\}$	{2.205,0.7718}	2.977

In the Table 3, we found that the key to the largest degree IP_1 host and we should priority repair host IP_1 vulnerabilities, namely, leak Numbers for 9904 and 13454 patch. When a host IP_1 leak after the repair, we should call attack graph to generate algorithm and optimization algorithm. The generate enterprise network attack graph is shown in Figure (b).

In order to call calculation state node loss degree algorithm to calculate the Figure 3(b) state node loss degree and repeat the above steps, we obtain the degree of host key for: $KD(IP_2)=8.82$; $KD(IP_3)=16.8$; $KD(IP_4)=2.205$. We can find the key to the largest degree IP_3 host, but as a result of its existing Telnet holes, we can't repair it and can't repair host IP_3 loophole, so take KD (IP_2) and KD (IP_4) maximum for leak repair, then repair the host IP_2 loophole, namely: Leak Numbers for 12815 patches. After having repaired host IP_2 again and repeat the implementation of the above steps, we find attack graph that exist only in a loophole that can repair is host IP_4. We repair host IP_4 loophole to leak Numbers for 9691 patch. Host IP_4 is repaired and prevent host IP_3 visiting the host IP_5 that can achieve the goal that ensure the network security.

5. Conclusions

It is a serious problem for management personnel network to improve the security of network. In order to solve this problem effective and correct, this paper puts forward the attack graph which is based on the intrusion detection method. This method first establishes the global network attack graph, and then carries on the optimization. Finally, we use the calculation state node loss degree algorithm to calculate the degree of the key network equipment. Network management personnel use the key of the network equipment to adjust the network safety strategy and repair the corresponding loophole. Then the management of network becomes more safety.

References

[1] P. Wu, H. Changzheng, Y. Shuping and W. Zhigang, “A Dynamic Intrusive Intention Recognition Method Based on Timed Automata”, Journal of Computer Research and Development, vol. 48, no. 7, **(2011)**, pp. 1288-1297.
[2] M. Bratman, “Intentions, Plans, and Practical Reason”, Massachusetts: Harvard University Press, **(1987)**.
[3] K. A. Tahboub, “Intelligent human-machine interaction based on dynamic bayesian networks probabilistic intention recognition”, Journal of Intelligent and Robotic Systems, vol. 45, no. 1, **(2006)**, pp. 31-52.
[4] S. Guanglu, L. Fei and Y. Mingming, “Traffic measurement system based on Hybrid methods”, Electric Machines and Control, vol. 15, no. 6, **(2011)**, pp. 91-96.
[5] L. Xiaozhe, T. Zhiyong and D. Yiqi, “Safety LAN Host Intrusion Detection System”, Journal of Tsinghua University(natural science edition), vol. 50, no. 1, **(2010)**, pp. 54-57.
[6] X. Xu Jia and L. Chuang, “A Survey of Computer Vulnerability Assessment”, Chinese Journal of Computers, vol. 27, no. 1, **(2004)**, pp. 1-11.
[7] Y. Yun, X. XiShan, J. Yan and J. ZhiChang, “Based on Attack Graph Network Security Probability Calculation Method”, Journal of Computers, vol. 55, no. 10, **(2010)**, pp. 1987-1996.
[8] L. Fang and Z. Sifeng, “New Intelligent Intrusion Detection Model”, Journal of Huazhong University of Science and Technology(natural science edition), vol. 38, no. 1, **(2010)**, pp. 22-24.
[9] M. Dapeng, Y. Wu, Y. Yongtian, Z. Yuan and Z. Bing, “Based on Weakness Relevance and Safety Requirements of the Network Safety Assessment Method”, High Technology Communication, vol. 12, no. 2, **(2009)**, pp. 141-146.
[10] M. Dapeng, Y. Wu and Y. Yongtian, “Method Based on Attack Graph for Network Vulnerability Analysis”, Journal of Nanjing University of Science and Technology(Natural Science), vol. 32, no. 4, **(2008)**, pp. 416-419.

