2010 International Conference on Computer Application and System Modeling (ICCASM 2010)

A Network Security Assessment Model Based on Attack-Defense Game Theory

Baoyi Wang, Jianqiang Cai, Shaomin Zhang, Jun Li
School of Control and Computer Engineering
North China Electric Power University
Baoding, China
Email: wangbaoyi@126.com, jianqiang.cai@gmail.com

Abstract: In this paper a network security assessment model based on game theory is presented to evaluate network security and perform active defense. The model uses the game relationship between attacker and defender to formally describe and quantitatively calculate benefits and costs of both sides. By solving mixed Nash equilibrium of the model, we could obtain the knowledge of possible attack paths of attacker and defender's optimizing strategy. In the end, a simple scenario is presented to illustrate the usage of the proposed model in network security assessment. The results indicate that the model and method is effective and efficient.

Keywords-Game Theory; Network Security; Attack Graph; Optimal Active Defense

I. INTRODUCTION

With the frequent occurrence of events that threaten the network security, how to maintain network security has become an increasingly prominent problem. The existing network security techniques mainly rely on firewalls, intrusion detection and antivirus software. These passive defensive approaches usually respond after an attack is detected, when serious damage to the system may have been caused. Compared with traditional passive defense, the active defensive approaches based on security assessment gradually gain importance, for users could recognize the vulnerability of network and potential threats to security previously by using these approaches [1]. Then users could select active defense strategy content with optimal cost effectiveness to avoid occurrence of dangerous incidents.

In order to objectively analyze and assess the network vulnerability, it is needed to create a systematic attack scene automatically according to the loopholes of target network, network services, physical links and access authority. Therefore the researchers formalize the precondition, process and outcome of network attack, and then put forward the network attack graph model. However, the existing attack graph model just reflects paths that can be up to by exploiting and associating network weaknesses. Generally speaking, the network attackers are intelligent and rational, so they would consider the costs and benefits of an attack. Thus it would be more correspond to the actual to calculate with game theory model when using attack graph to analysis possible attacks.

There is a significant game relationship between the network attackers and defenders [2]. Defenders' optimal defense strategies and attackers' attack strategies are interdependence and interrelationship, thus constitute a network security attack and defense game. Stochastic game model is used to analysis and ratiocinate the relationship between attackers and defenders, and validate the applicability of using game theory to analysis intrusion detection [3]. The authors put forward invasion intentions, objectives and strategy reasoning model based on game theory, and analyze the usage of the model in DDoS defense [4]. By formulating the network intrusion detection as a noncooperative game and performing an in-depth analysis on the Nash equilibrium, the author addresses the intrusion detection problem in heterogeneous networks consisting of nodes with different security assets [5]. Reference [6] combines game theory and network attack-defense to construct defense graph model, then analyzes possible attack behavior the intruder may take from the defender's point of view. While, the defense graph model only reflects state transition of network, it doesn't reflect the paths used by attackers very well. The authors study network security investment issues by using game theory, and establish an attack-defense game model of information security according to the gaming characteristics of information security, so as to analysis the attack-defense game [7].

Different from the works above, in this paper a network attack-defense game model (NADGM) is proposed with the view of network security assessment. The attacker and defender are regarded as two participants in the game. In the model, the attack-defense strategies are formally described and quantitatively calculated. The result of Mixed Nash equilibrium of NADGM is used to predict possible attack paths of attacker and instruct the defender to take optimal defense strategies.

II. THE COMPOSE OF SECURITY ASSESSMENT FRAME

A security assessment frame is proposed in this paper. Through the calculation process we could derive the potential attack paths which could be used by attackers, and optimal defense strategy of the defender. The frame is shown in Figure 1.

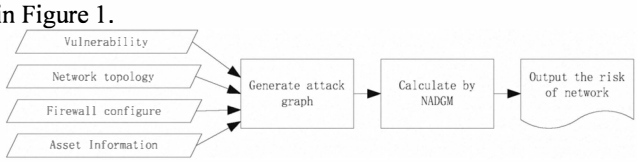

Figure 1. The security assessment frame

As shown in Figure 1, the vulnerability and asset information could be got from the current network, and we could derive the potential attack paths existing in the current

network according to the network topology and firewall rules. Then we use the attack-defense game model to calculate the benefits and costs of the attacker and defender. The model uses proportionality of game theory to calculate optimal behavior strategy of both the attacker and defender separately.

III. THE NETWORK ATTACK-DEFENSE GAME MODEL (NADGM)

A. The Definition of NADGM Model

NADGM is used to compute possible threats. This is the most important part of network security assessment. Based on this need, three basic assumptions are proposed.

1) The ability of every attacker is equal.

Assume that the attacker's ability is equal. This means, to a typical attack, each attacker has the same attack possibility, and every threat on each host has a significant risk.

2) Minimum end-user's ability.

As a participant of NADGM, the defender obviously cannot have fluke mind, that is, there is not a potential attack failure under no defensive act. Therefore, in this paper, assume that the attack will be 100% success if no defensive behavior is practiced.

3) IDS detection is real time.

Once the attacker's attack is found by IDS, it will immediately notify the defender. And, once the defenders are found, attack behavior will be terminated.

The NADGM is a complete information non-cooperative non-zero static game model. Obviously, attacker and defender cannot reach an agreement on cooperative intend, so this game is non-cooperative. After taking their own actions, both attack and defense strategies will have a certain overhead cost, so the utility function cannot simply use the benefits to express, so the game is non-zero sum. Attacker's benefit is transformed by a certain percentage of system's loss. The main objective of NADGM is to calculate the possible attack paths in a certain network region and give defense strategies defenders should select. Two participants separately use their strategies to determine their operations, so their decision order does not affect game results and the game is static.

Definition 1: The general strategy of network attack and defense game form is a triple $G=(\Gamma,S,U)$.

(1) The set $\Gamma=\{1,2,\cdots,n\}$ represents the participants of attackers and defenders side. If the number of attackers is more than one, we call it cooperative attack. If the number of defenders is more than one, we call it cooperative defense.

(2) The strategy space of participants is $S=(S_1,S_2,\cdots,S_n)$. And $\forall i\in\Gamma$, $S_i\neq\Phi$, $S_i=(s_1^i,s_2^i,\cdots,s_m^i)$ is the participant i's strategy set.

(3) The set $U=(U_1,U_2,\cdots,U_n)$ is the utility function of every participant.

Definition 2: The NADGM proposed is a two-player non-zero non-cooperative finite static game model, defined as: $NADGM=(\{a,d\},\{S_a,S_d\},\{U_a,U_d\})$.

Use a to represent attacker and d to represent defender. They are the participants of the game. The strategy space of attacker is $S_a=(s_1^a,s_2^a,\cdots,s_n^a)$, and s_i^a is an attack strategy. The strategy space of defender is $S_d=(s_1^d,s_2^d,\cdots,s_n^d)$, and s_i^d is a defend strategy. U_a and U_d represent the utility function of attacker and defender respectively.

B. The Classification of Attack and Defense

According to the result of attack classification [6], combined with the study of MIT Lincoln Laboratory attacks' classification, the impact each type of attack has on the hosts cannot be expressed accurately with a parameter. Combined with the study of reference [8], we use three properties: integrity, confidentiality, availability to presents the impact every type of attack has on the hosts. This attack classification method combines attack strategic objectives and attack influence as the basis of classification. The three attributes of the attack is represents by a number between 0-1, as shown in Table I.

TABLE I. ATTACK CLASSIFICATION

Category	Description	Integrity	Confidentiality	Availability
Root	Obtain administrator privilege	0.1	1.0	0.1
User	Obtain general user privilege	0.1	0.5	0.1
Data	Unauthorized access or Data read and write	1.0	1.0	0.1
DoS	Denial of Service	0	0	1.0
Probe	Scan attack	0	0.1	0.1

When analyzing the cost of a variety of defensive methods, we propose to divide the variety of defensive strategies into three categories. The following classification is based on the time that system defense consumes and the effect to system normal operation. Each category includes a number of specific defensive measures shown in Table II.

TABLE II. DEFENSE CLASSIFICATION

Category	Description	Features
Elementary	Modify the configuration of the host	Less operating time, no need to stop the machine.
Intermediate	Reboot, use administrator account to reinforce system	Operating time is longer, requires several step by step operations, require professional knowledge, might need to stop the machine.
Advanced	Scan for viruses, back up your system, upgrade the system	Operation time is very long, generally need professional maintenance.

C. The Payoff Matrix Based on Benefit and Cost

Use U_{ij}^a to represent attacker's utility function, and B_{ij}^a to represent attacker's benefit, and C_{ij}^a represents attacker's cost. Subscript i and j represent that the attacker chooses strategy i and defender selects strategy j. Similarly, U_{ij}^d represents defender's utility function, B_{ij}^d represents defender's benefit, and C_{ij}^d represents defender's cost. Subscript i and j represent that the attacker chooses strategy i and defender selects strategy j.

Definition 3: The participant's utility function in NADGM is defined as: $U = B - C$.

So the attacker's utility function is $U_{ij}^a = B_{ij}^a - C_{ij}^a$, the defender's utility function is $U_{ij}^d = B_{ij}^d - C_{ij}^d$.

IV. The Cost-Benefit Analysis of Attack and Defense

The defense cost consists of IDS response cost and damage cost [8]. Defense cost is composed of defensive operations cost, response cost and response negative cost [6].

The attack cost includes not only time and money of the successful attack, which the attacker must pay, but also the punishment that the attacker would suffer when being detected [8].

Attacker's benefits come from part of the defenders' loss. After being attacked, the defenders take defensive measures to restore their losses.

Benefits and costs of the players in NADGM are shown in Table III.

TABLE III. BENEFITS AND COSTS OF ATTACKERS AND DEFINDERS

Defender	***Benefits***	Loss by attack
		Restore
	Costs	Operation costs
		Response costs
		Response nagetive costs
Attacker	***Benefits***	Expected attack benefits
	Costs	Punishment after being detected
		Software and hardware resources

A. The Benefit of Defender

Seen from the classification of attack type, an attack behavior mainly causes damage to integrity, confidentiality and availability of a system. Define P_i, P_c and P_a represent separately the above three kinds of damage level. V_i, V_c and V_a represent separately the hosts' value. Their multiplication is the loss of hosts being attacked.

$R = r_c * V_c + r_i * V_i + r_a * V_a$ is defined as restore of system when defender takes effective defense.

We describe and define benefit of defender as shown in Table IV, where we use the defense strategy s_j^d as the corresponding defense strategies of attack strategy s_j^a, and $\neg s_j^d$ as the other defense strategies which are ineffective to s_j^a. $\neg s_j^a$ represents that the attacker do not attack.

$$B_{ij}^d = (r_c - P_c) * V_c + (r_i - P_i) * V_i + (r_a - P_a) * V_a$$

TABLE IV. THE BENEFIT OF DEFENDER

strategy	benefit
(s_i^a, s_j^d)	$B_{ij}^d = (r_c - P_c) * V_c + (r_i - P_i) * V_i + (r_a - P_a) * V_a$
$(s_i^a, \neg s_j^d)$	$B_{ij}^d = -(P_c * V_c + P_i * V_i + P_a * V_a)$
$(\neg s_i^a, s_j^d)$	$B_{ij}^d = 0$
$(\neg s_i^a, \neg s_j^d)$	$B_{ij}^d = 0$

B. The Benefit of Attacker

The benefit of the attacker is based on the loss of the defense system [9]. Define $k \in [0,1]$ as the conversion rate, which is the percentage of defender's loss which converted into the attacker's benefit in all the defender's loss. Therefore, the attacker's benefit is $B^a = -k * B^d$, as shown in Table V.

TABLE V. THE BENEFIT OF ATTACKER

strategy	benefit
(s_i^a, s_j^d)	$B_{ij}^d = k * ((r_c - P_c) * V_c + (r_i - P_i) * V_i + (r_a - P_a) * V_a)$
$(s_i^a, \neg s_j^d)$	$B_{ij}^d = k * (P_c * V_c + P_i * V_i + P_a * V_a)$
$(\neg s_i^a, s_j^d)$	$B_{ij}^d = 0$
$(\neg s_i^a, \neg s_j^d)$	$B_{ij}^d = 0$

C. The Cost of Defender

The defense cost is composed of Operation Cost (C_O), Response Cost (C_R) and Response Negative Cost (C_{RN}).

Operation cost represents the time consumed and amount of computing resources in defender's defensive operations. According to the complexity level of defensive operations in Table II, operation cost can be divided into three levels.

Response Cost is related to recovery strategies, and this is determined by defense levels and specific network environment.

Some response actions may affect the system availability, which is also determined by specific defense strategy and network environment. Overall, the cost of defense strategy is shown in Table VI.

TABLE VI. THE COST OF DEFENDER

strategy	cost
(s_i^a, s_j^d)	$C_{ij}^d = C_O + C_R + C_{RN}$

$\left(s_i^a, \neg s_j^d\right)$	$C_{ij}^d = 0$
$\left(\neg s_i^a, s_j^d\right)$	$C_{ij}^d = C_O + C_R + C_{RN}$
$\left(\neg s_i^a, \neg s_j^d\right)$	$C_{ij}^d = 0$

D. The Cost of Attacker

To define the cost of the attacker, it's needed to consider the cost of launching an attack and when attacks are detected the punishment which the attacker would suffer. Therefore the relationship of strategy space and the attack cost is shown in Table VII.

TABLE VII. THE COST OF THE ATTACKER

strategy	cost
$\left(s_i^a, s_j^d\right)$	$C_{ij}^a = C_A + C_P$
$\left(s_i^a, \neg s_j^d\right)$	$C_{ij}^a = C_A$
$\left(\neg s_i^a, s_j^d\right)$	$C_{ij}^a = 0$
$\left(\neg s_i^a, \neg s_j^d\right)$	$C_{ij}^a = 0$

E. The Nash Equilibrium of NADGM

According to the existence principle of Nash Equilibrium Theory: any strategy form of limited game at least has one mixed strategy Nash equilibrium. Given an attack-defense game $NADGM = (\{a,d\},\{S_a,S_d\},\{U_a,U_d\})$, in which the probability distribution of the attacker's and defender's strategies $S_a = \left(s_1^a, s_2^a, \cdots, s_m^a\right)$ and $S_d = \left(s_1^d, s_2^d, \cdots, s_n^d\right)$ is respectively $p_a = \left(p_1^a, p_2^a, \cdots, p_m^a\right)$ and $p_d = \left(p_1^d, p_2^d, \cdots, p_n^d\right)$, where $0 \le p_i^a \le 1$, $\sum_{i=1}^m p_i^a = 1$, $\sum_{i=1}^n p_i^d = 1$.

The mixed strategy Nash equilibrium of NADGM could be calculated by the following formulas:

$$V_a(p_a, p_d) = \sum_{i=1}^m p_i^a \left[\sum_{j=1}^n p_j^d U_a\left(s_i^a, s_j^d\right)\right] = \sum_{i=1}^m \sum_{j=1}^n p_i^a p_j^d U_a\left(s_i^a, s_j^d\right) \quad (1)$$

$$V_d(p_a, p_d) = \sum_{j=1}^n p_j^d \left[\sum_{i=1}^m p_i^a U_a\left(s_i^a, s_j^d\right)\right] = \sum_{j=1}^n \sum_{i=1}^m p_j^d p_i^a U_a\left(s_i^a, s_j^d\right) \quad (2)$$

Mixed strategy (p_a^*, p_d^*) is a Nash equilibrium, if and only if the mixed strategy is the optimal mix of both attack and defense strategy, that is to say: for $\forall p_a$, $V_a\left(p_a^*, p_d^*\right) \ge V_a\left(p_a, p_d^*\right)$; for $\forall p_d$, $V_a\left(p_a^*, p_d^*\right) \ge V_a\left(p_a^*, p_d\right)$. Using the above formula we can calculate the mixed strategy Nash equilibrium of both attack and defense sides.

V. THE EXPERIMENT AND NUMERICAL ANALYSIS

We use a simple scenario to introduce the application of NADGM in network security assessment. A small network with multiple operating systems shown in Figure 2 is set to test our model.

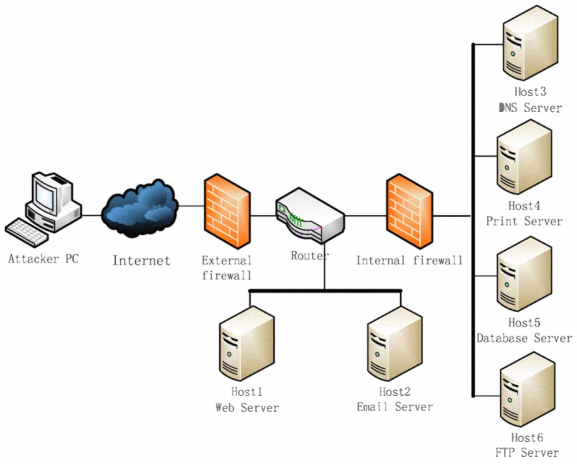

Figure 2. Network topology graph

The external firewall and the internal firewall divide the whole network into three parts: the outer network where the attacker is, the DMZ zone where some application servers are and the inner network where important servers are. Both the DMZ zone and inner network need protection. The attacker launches attacks through Internet from the outer network.

In this experiment, the hosts exist some vulnerabilities, as shown in Table VIII.

TABLE VIII. THE VULNERABILITIES AND HOSTS' VALUES

ID	Host Name & Value	CVE ID	Attack Type
Vul1	Host1(20,20,100)	CVE-2006-0026	Root
Vul2	Host2(30,30,100)	CVE-2009-0410	Root
Vul3	Host3(20,50,50)	CVE-2006-3441	Root
Vul4	Host4(20,20,50)	CVE-2006-6742	Root
Vul5	Host5(100,100,50)	CVE-2006-0260	Data
Vul6	Host6(100,100,50)	CVE-2009-3023	Root

In the network, the significant hosts are host5 and host6. Therefore we mainly protect them by taking proper defense strategies. Through generating network attack graph, five possible attack paths in which the final hosts are host5 or host6 are detected.

AttackPath1: host1→host3→host4→host5.

AttackPath2: host1→host4→host5.

AttackPath3: host1→host3→host4→host6.

AttackPath4: host2→host3→host4→host5.

AttackPath5: host2→host3→host4→host6.

In view of the existing vulnerabilities in network hosts, the corresponding defense strategies are shown in Table IX.

TABLE IX. DEFENSE STRATEGY

ID	Strategy name	C_O	C_R	C_{RN}
Def1	Install patch for web server	10	10	50

Def2	Install patch for Email server	10	10	50
Def3	Shutdown DNS server	10	30	40
Def4	Shutdown Print Server	10	30	40
Def5	Intstall patch for Oracle	50	50	20
Def6	Upgrade FTP service software	50	50	20

In the experiment, some parameters need to be given in the light of experience: $R_c = 1.0$, $R_i = 1.0$, $R_a = 1.0$. NADGM is used to calculate the payoff matrix of the attacker and defender. The results are shown in Table X.

TABLE X. PAYOFF MATRIX

	Def1	**Def2**	**Def3**
Path1	(26, -32)	(0, -24)	(71, -89)
Path2	(26, -32)	(0, -24)	(0, -66)
Path3	(26, -32)	(0, -24)	(71, -89)
Path4	(0, -23)	(34, -43)	(80, -100)
Path5	(0, -23)	(34, -43)	(80, -100)
	Def4	**Def5**	**Def6**
Path1	(93, -116)	(142, -238)	(0, -72)
Path2	(47, -59)	(96, -181)	(0, -72)
Path3	(93, -116)	(0, -81)	(120, -211)
Path4	(102, -127)	(151, -249)	(0, -72)
Path5	(102, -127)	(0, -81)	(129, -222)

According to the existence principle of Nash equilibrium [10, 11], the attack-defense game what we derive is a finite game, therefore there is at least a equilibrium point. We use (1) and (2) to solve mixed Nash Equilibrium when both the attacker and defender adopt mixed strategy. The result of the payoff matrix in Table 10 is as following: $p_a = (0.44, 0, 0.13, 0.43, 0)$ and $p_d = (0, 0, 0, 0, 0.58, 0.42)$. It indicates that the attacker would select strategy1 with probability 0.44, strategy3 0.13, and stategy4 0.43. To the defender, the optimal defense strategy is to play def5 with probability with 0.58, and def6 0.42. In other words, if the defender installs the patch of Oracle and updates the FTP service software, the attacker couldn't implement his attack goal. Thus, the security of the network is greatly strengthened.

VI. CONCLUSION

For the existing active defense methods don't take the benefit and cost of both attacker and defender into account, a new network attack-defense model based on game theory is proposed in order to evaluate the security of a network system, and help the network manager to take optimal defense strategies. It uses the frequently-used game theory in economics to model the relations between the attacker and defender. The defender's optimal response strategies are got through calculating the network's risk. So the network environment would be more safety. This model is more stable and reliable than the model in which the optimal response strategy is generated only from attack's or defense's view.

Nevertheless, there are still some deficiencies in the model proposed in this paper. For example, when we use attack graph to model the strategy of an attacker, it needs much time and memory space to generate attack paths. In our future work, we would improve the attack path generating algorithm.

REFERENCES

[1] D. Feng, Y. Zhang, Y. Zhang, "Survey of Information Security Risk Assessment," Journal of China Institute of Communications, vol. 25, Jul. 2004, pp. 10-18, doi: cnki:ISSN:1000-436X.0.2004-07-001.

[2] M. Bell, "The Use of Game Theory to Measure the Vulnerability of Stochastic Networks," IEEE Transactions on Reliability, vol. 52, Mar. 2003, pp. 63-68, doi:10.1109/TR.2002.808062.

[3] K. Lye, J. M. Wing, "Game Strategies in Network Security," International Journal of Information Security, vol. 4, pp. 71-86, 2005.

[4] P. Liu, W. Zang, "Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies," ACM Transactions on Information and System Security (TISSEC), vol. 8, pp. 78-118, 2005.

[5] L. Chen, J. Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," IEEE Transactions on Information Forensics and Security, vol. 4, Jun. 2009, pp. 165-178, doi: 10.1109/TIFS.2009.2019154.

[6] W. Jiang, B. Fang, Z. Tian, H. Zhang, "Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model," Chinese Journal of Computers, vol. 32, Apr. 2009, pp. 78-118, doi: CNKI:SUN:JSJX.0.2009-04-024.

[7] W. Sun, "Research on Game Analysis of Information Security Investment in Organizations," Dalian: Dalian University of technology, 2008.

[8] W. Lee, W. Fan, M. Mille, S. J Stolfo, E. Zadok, "Toward Cost-Sensitive Modeling for Intrusion Detection and Response," Journal of Computer Security, vol. 10, Jan. 2002, pp. 5-22.

[9] J. Shi, Y. Lu, L. Xie, "Dynamic Intrusion Response Based on Game Theory," Journal of Computer Research and Development, vol. 45, May 2008, pp. 747-757, doi: CNKI:SUN:JFYZ.0.2008-05-001.

[10] G. Li, Basic Course in Game Theory, 1st ed, Beijing: Chemical Industry Press, 2005, pp. 10-37.

[11] Z. Xie, Game theory, 1st ed, Changsha: National Defense University Press, 2004, pp. 31-81.