A Game Theoretic Method for Decision and Analysis of the Optimal Active Defense Strategy

Wei Jiang
Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin, China
jiangwei@pact518.hit.edu.cn

Hong-li Zhang
Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin, China
zhl@pact518.hit.edu.cn

Zhi-hong Tian
Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin, China
tianzhihong@pact518.hit.edu.cn

Xin-fang Song
Beijing Jingbei Vocational Campus,
Beijing, China
xfsong435@yahoo.com.cn

Abstract

This paper presents a game-theoretic method for analyzing the active defense of computer networks. We regard the interactions between an attacker and the defender as a two-player, non-cooperative, zero-sum, finite game and formulate an attack-defense game (ADG) model for the game. An optimal active defense strategy decision (OADSD) algorithm is developed using the ADG and cost-sensitive model. Optimal defense strategies with minimizing costs are used to defend the attack and harden the network in advance. Finally, experiments show that our ADG model and the OADSD algorithm are effective in reducing the overall cost of defense systems and defend attacks that may occur in the future.

1. Introduction

Traditional static protective measures are not sufficient to secure a complex networked system. Intrusion detection (ID) architecture is a passive information processing paradigm. It is a big challenge that making correct optimal proactive real-time defense decisions during an earlier stage of the attack. In such a way that much less harm will be caused without consuming a lot of resources.

Game theoretical analysis is useful for analyzing, modeling, decision, and control processes for network security. Game theory has been recently proposed by several studies for a theoretical analysis of network security [1]-[3]. Lye and Wing use a game theoretic method to analyze the security of computer networks [1]. Peng Liu et al. present a preliminary framework AIOS using game theoretic approach [2]. Alpcan et al. investigated the basic decision processes, as well as possible usage of game theory for developing a formal decision and control framework [3].

Our work is different from the above game theoretic works in several aspects. First, these works are complex and can not proactive defense in real time, while our work focuses on active defense using the simple ADG model. Second, these works focus on interaction between players across the time dimension, while our work focuses on attacker's strategy getting from predefined attack graph. Knowing that a network system is not perfectly secure, we can use automated generation of attack graph [4,5] to discover the potential attack strategies of an attacker. Third, our work systematically identifies cost factors of cost-sensitive model [6,7] and introduces the OADSD algorithm. Instead of passively monitoring, detecting, and reacting to attacks, the relation between the defender and the attacker is modeled as the ADG where the defender may actively take optimal defense actions for attacks that may occur in the future.

The rest of the paper is organized as follows. In section 2, we present formalization definition of the ADG model and discuss the cost-sensitive model. Section 3 presents an algorithm of the OADSD. In Section 4, we use a specific case study to show how defense strategies can be selected in real-world attack

0-7695-3072-9/07 $25.00 © 2007 IEEE
DOI 10.1109/CIS.2007.31

graph. Section 5 includes some concluding remarks and points to future work.

2. The ADG model formalization

2.1. Attack-Defense Game

Definition 1: The strategic form of an attack-defense game is a 3-tuple $G=(N,S,U)$:

The set, $N=(1,2,\ldots,n)$,of players who are attackers and defenders. If the number of attackers is more than one, namely cooperatively attack. And if the number of defenders is more than one, namely cooperatively defend. $S=(S_1,S_2,\ldots S_n)$ is the strategy spaces of the players. $\forall i\in n, S_i\neq\varnothing$, $S_i=(s_1^i,s_2^i,\ldots,s_m^i)$ is strategy set of the player i .The set, $U=(U_1,U_2,\ldots U_n)$, of real-valued is payoff functions of the players.

Definition 2: A strategic form of game is zero-sum if $\sum_{i=1}^{n}U_i(s_1,s_2,\cdots s_n)=0$, for all $s_1\in S_1,\cdots s_n\in S_n$.

The relationship between attackers and defenders is non-cooperative in nature. The attacker wants to maximize its own satisfaction by destroying functionality of a system. On the other hand, the defender wants to minimize the damage of systems.

Definition 3: An ADG is a two-player, zero-sum, non-cooperative, finite game $G=(\{attacker, defender\}, \{S_a,S_d\},\{U_a,U_d\})$ The attacker's strategy space is denoted as $S_a=(s_1^a,s_2^a,\ldots,s_m^a)$, where s_i^a is an attack strategy. The defender's strategy space is denoted as $S_d=(s_1^d,s_2^d,\ldots,s_n^d)$, where s_j^d is a defense strategy. And $U_a(s_i^a,s_j^d)=-U_d(s_i^a,s_j^d)$.

2.2. Strategies for the Two Players

The attacker's strategies are represented by all possible paths from initial states to a success states through atomic attacks in predefined attack graph [5,6].The defender's strategies for attacker's strategies get from known defense strategy set. In a mixed strategy, the attacker has a probability distribution over the set of paths and the mixed strategy may be represented by $p=(p_1,p_2,\cdots p_m)$ of probabilities such that $\sum_{i=1}^{m}p_i=1$. Similarly, a mixed strategy for defender is $q=(q_1,q_2,\cdots q_n)$ of probabilities such that $\sum_{j=1}^{n}q_j=1$.

2.3. Cost, Reward and Payoff Matrix

The ADG in strategic form is called a matrix game because the payoff function U can be represented by a matrix $U=\begin{pmatrix} s_{11} \cdots s_{1n} \\ \vdots \quad \vdots \\ s_{m1}\cdots s_{mn}\end{pmatrix}$ Where $s_{ij}=U(s_i,s_j)$.

The entries of the matrix are the reward of the row chooser and cost of the column chooser. If V is the value of the game, an optimal strategy, p, for attacker is characterized by the property that attacker's average payoff is at least V no matter what column j defender uses, i.e. $\sum_{i=1}^{m}p_i s_{ij}\geq V$ .Similarly, a strategy q is optimal for defender if and only if $\sum_{j=1}^{n}s_{ij}q_j\leq V$.

When both players use their optimal strategies the average payoff $p^TUq=\sum_{i=1}^{m}\sum_{j}^{n}p_i s_{ij}q_j$, is exactly V. This may be seen from the inequalities

$$V=\sum_{j=1}^{n}Vq_j\leq\sum_{j=1}^{n}(\sum_{i=1}^{m}p_i s_{ij})q_j=\sum_{i=1}^{m}\sum_{j=1}^{n}p_i s_{ij}q_j$$

$$=\sum_{i=1}^{m}p_i(\sum_{j=1}^{n}s_{ij}q_j)\leq\sum_{i=1}^{m}p_iV=V\ .$$

In order to quantify costs and rewards, we should first understand the relevant cost factors used to define them. Cost factors are often site-specific because each organization has its own security policies, information assets, and risk factors. Based on the investigation of Lee's research [6], we build our cost model which includes cost factors as follow: defense operation cost (*DOcost*), residual damage cost (*RDcost*) and defense negative cost (*DNcost*). *DOcost* is the amount of resources needed to defense an attack (type). We classify defense operation cost into three relative levels, based on their computational costs:

L1: defense operation cost is very small. For example, suspend process, IP blocking.

L2: use some system resources when defense operations were carried out. For example, kill the process.

L3: use much more system resources when defense operations were carried out. For example, create backup.

We can assign relative magnitudes to these features according to their computational costs. For example, Lee assigns a different cost weight level. A level 1 feature may cost 1 to 5, level 2 features may cost 10, and level 3 features may cost 100. In table 1, we list a number of known defense strategy and their levels.

Some defense strategy cannot defend the attack that may occur in the future result in some attack damage.

So we must consider the *RDcost* of a defense strategy, and we can quantify it as fellow: $RD\cos t(d) = \varepsilon D\cos t(a)$. Where $\varepsilon \in [0,1]$ is the degree damage cost of attack *a* when take defense strategy *d*. *Dcost* generally quantifies the maximum amount of resources or computing power that can be left unusable by the particular attack. *Criticality* measures the importance of the target of an attack. Similar to Northcutt's analysis [7], we assign 5 points for firewalls, routers, or DNS servers, 4 points for mail or Web servers, 2 points for UNIX workstations, 1 point for workstations. *Lethality* measures the degree of damage that could potentially be caused by some attack. Wenke Lee defines a relative lethality scale and uses it as the base damage cost [6]. The *Dcost* of an attack targeted at some resource is $criticality \times lethality$.

Table 1. Defense strategy descriptions

Defense strategy	Implementation requirements	*DOcost*
Generate Alarm	Kernel	L2
IP Blocking	Kernel	L1
Isolate Host	Kernel or User	L2
Suspend Process	Kernel	L1
Kill Process	Kernel or User	L2
Create Backup	User	L3
⋮	⋮	⋮
No defense	X	X

DNcost represents an effect of a defense action on a target system, which depends on defense strategies and target system. We can quantify the *DNcost* in the particular environment and defense action. For example, *DNcost* can be defined as follows: $DN\cos t(d,t) = availability \times \mu_a$ .Where $\mu_a \in [0,1]$ is the degree of *availability* of the target system *t*.

After the cost factors are defined, the cost values can be given when defense strategies cost analysis and assessment. The total defense cost (*TDcost*) of a defense strategy can be defined as follows:

$$TD\cos t = DO\cos t(d) + RD\cos t(a) + DN\cos t(d) \quad (1)$$

In the above *d* and *a* is separately a particular defense strategy and attack type.

2.4. Solve the ADG's Nash Equilibrium [8]

Definition 4: An outcome in a matrix ADG is called a saddle point or pure min-max equilibrium if the entry at that outcome is the minimum in its row, and the maximum of its column.

Definition 5: (**Saddle Point Principle**) If an ADG matrix has a saddle point, both players should play a strategy which the saddle point stipulates.

If there is no saddle point in the matrix ADG, we can solve it by linear program.

Let *U* be a ADG matrix, consider the game value $v = \max_p \min_q U(p,q) = \max_i \min_q U(i,q)$ .We need to find a probability vector *q* so that $v = \max_i U(i,q) = \max_i \sum_{j=1}^{n} s_{ij} q_j$ is minimum, i.e. *v* is smallest so that

(i) $q_j \geq 0 \, for 1 \leq j \leq n,$

(ii) $\sum_{j=1}^{n} q_j = 1$,

(iii) $v \geq \sum_{j=1}^{n} s_{ij} q_j, \quad i = 1, \cdots, m$.

By adding *c* to each entry (i.e. $s_{ij}+c$) and to *v*, there is nothing changed on *q*. Hence we can assume that all the entries are positive, so that $v > 0$. Let $y_j = q_j/v \geq 0$ for $1 \leq j \leq$ n, then $\sum_{j=1}^{n} q_j = 1/v$. The problem becomes

Maximize $y_1 + \cdot\cdot\cdot + y_n$,

Subject to $\sum_{j=1}^{n} s_{ij} q_j \leq 1, \quad 1 \leq i \leq m$.

This is indeed a linear program. So, we can solve the ADG matrix by linear programming method.

3. OADSD algorithm

The defense strategies that have the highest chance and with minimizing costs of blocking a possible attack are selected and deployed from the candidate set. The detail of this defense selection process is presented below.

Input: attack graph

Output: Optimal defense strategy

Algorithm:

(a) Get the set of attacker's strategies set $S_a = (s_1^a, s_2^a, \ldots, s_m^a)$ from the attack graph.

(b) Construct the defender's strategy set $S_d = (s_1^d, s_2^d, \ldots, s_n^d)$ the S_a from known defense strategy set. And compute the total cost of $s_j^d \in S_d$.

(c) Initialize the ADG=({*attacker*,*defender*},{S_a,S_d}, {U_a,U_d}), where U_a= -U_d is the payoff matrix. $s_{ij} = U(s_i^a, s_j^d)$ is payoff when the attacker use s_i^a and the defender use s_j^d .And it is computed as formula (1).

(d) Compute the Nash equilibria set E of ADG. Processes as follows:

(i) Test for a saddle point in the matrix ADG.

(ii) If there is no saddle point, solve it by linear program.

(e) Decide the optimal defense strategies.

For the length of manuscripts limit, the detail of analysis of algorithm is omitted.

4. Numerical analysis

Sheyner and Tao Zhang's example network[4,5] is shown in Figure 1. Some important host information is given in table 2.

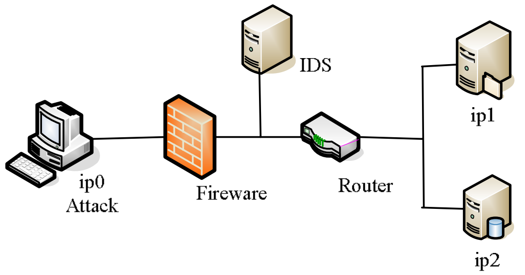

Figure 1.Example Network

Table 2. Host information descriptions

Host	OS	Services	Vulnerability
ip1	Linux	ftp, ssh	sshd buffer overflow, ftp .rhost overwrite
ip2	Linux	ftp, atabase	ftp .rhost overwrite, local buffer overflow

The attacker launches his attack starting from a single computer, ip0. His eventual goal is to disrupt the functioning of the database. So, the attacker needs root access on the database host ip2.There are three possible atomic attacks, identified as table 3.

Table 3. Atomic attack descriptions

Atomic Attack	Category	*Dcost*
0. Sshd Buffer Overflow	ROOT	100
1. Ftp.rhosts	R2L	50
2. Local Buffer Overflow	ROOT	100

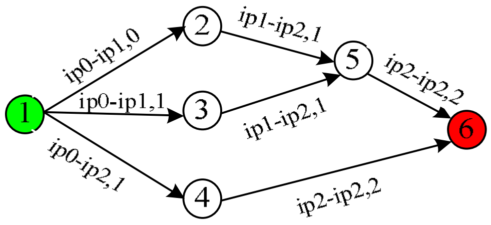

Figure2. Attack graph

Figure 2 depicts the attack graph that generated by Tao Zhang's method and we modify it. The node set S= {1, 2, 3, 4, 5, 6} represents the states of the network environment, where initial node '1' represents the first state and success node '6' represents the goal state of the attacker. The label 'ip0-ip1, 1' represents the attacker goes from host ip0 to host ip1 using the atomic attack 1. In Figure 2, an attack strategy refers to a sequence of labels that appear in the path from an initial node to a success node: s_1^a=(1→2→5→6) , s_2^a=(1→3→5→6) and $s_3^a=(1\rightarrow4\rightarrow6)$ .We can construct the strategy set S_d from table 1 for $S_a=(s_1^a,s_2^a,s_3^a)$, as table 4.

Table 4. Defense strategy descriptions

Defense strategy	*DOcost*	ε
s_1^d : Generate Alarm	10	$\varepsilon_0=\varepsilon_1=\varepsilon_2$ =0.8
s_2^d : IP Blocking	5	$\varepsilon_0=\varepsilon_1$ =0, ε_2 =1
s_3^d : Isolate Host	10	$\varepsilon_0=\varepsilon_1$ =0, ε_2 =1
s_4^d : Kill Process	5	$\varepsilon_0=\varepsilon_1$ =1, ε_2 =0.5
s_5^d : No defense	0	$\varepsilon_0=\varepsilon_1=\varepsilon_2$ =1

Now we compute *DTcost* of every defense strategy.

To simplify our analysis, we don't consider the *DNcost*. In our approach, each attack type is associated with a *Dcost* using the prior information, in particular costs developed by [6], as table 3 shown. *DOcost* and ε is shown table 4. ε_i, $i=0,1,2$ is the degree of attack damage cost when take strategy to defense atomic attack *i*. We compute the total cost of $s_i^d \in S_d$ and construct the payoff matrix

$$\begin{array}{c c}
 & \begin{array}{ccccc} s_1^d & s_2^d & s_3^d & s_4^d & s_5^d \end{array} \\
\begin{array}{c} s_1^a \\ s_2^a \\ s_3^a \end{array} & \begin{pmatrix} 210 & 105 & 110 & 155 & 250 \\ 170 & 105 & 110 & 185 & 200 \\ 130 & 105 & 110 & 105 & 150 \end{pmatrix}
\end{array}$$

In above payoff matrix, we direct find that s_2^d = IP Blocking- is optimal defense strategy with minimizing costs. The decision is coincident with real fact that IP Blocking can block the three attacks. The defender should use IP Blocking to harden the network and defend three attack strategies in advance.

5. Conclusion and future work

In this paper, we have presented a game-theoretic method for analyzing optimal active defense strategy decision in networks security. We regarded the interactions between an attacker and the defender as a two-player non-cooperative zero-sum game and formulated the ADG model for the game. Based on the ADG and cost-sensitive model, an optimal active defense strategy decision (OADSD) algorithm has been developed. Finally, we used a specific case study to show how attack strategies can be selected in real-world attack graph.

Nevertheless, our work in selecting optimal active defense strategy is still preliminary and several important research issues need to be further explored. In particular, in our future work (a) we would investigate attack taxonomy because it is essential in producing meaningful cost metrics; (b) we would investigate cost factors and quantified analysis of defense and attack.

Acknowledgements

This paper is supported by the National High-Tech Research and Development Plan of China under Grant Nos. 2007AA01Z406, 2007AA01Z442. The authors gratefully acknowledge helpful discussions with some members in our research center. We also thank anonymous reviewers for their constructive suggestions.

6. References

[1] K.-W. Lye and J. Wing, "Game strategies in network security," *Foundations of Computer Security Workshop in FLoC'02*, Copenhagen, Denmark, July 2002.

[2] P. Liu and W. Zang, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", *Proc. of the 10th ACM Computer and Communications Security Conference (CCS'03), Washington*, DC, October 2003, pp. 179-189.

[3] T. Alpcan and T. Bas¸ar, "A game theoretic approach to decision and analysis in network intrusion detection", *Proc. of the 42nd IEEE Conference on Decision and Control*, Maui, HI, December 2003, pp. 2595–2600.

[4] Oleg Sheyner, Joshua Haines, Somesh Jha, et al. "Automated generation and analysis of attack graphs", *Proceedings of 2002 IEEE Symposium on Security and Privacy*, Oakland, CA, 2002: pp.254-265.

[5] Zhang Tao, Hu mingzen, Yun Xiaochun, Li Dong, Sun Liang, "Study on the method to generate network attack graphs", *Journal of Chinese High Technology Letters*, volume 16(4), 2006, pp. 348–352.

[6] W. Lee, W. Fan, M. Millerand, S. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response", *Journal of Computer Security*, volume 10, 2000, pp. 5–22.

[7] S. Northcutt. *Intrusion Detection: An Analyst's Handbook*, New Riders, 1999.

[8] G. Owen, *Game Theory*, 3rded. New York, NY: Academic Press, 2001.