A Kind of network security behavior model Based on game theory

Xia ZhengYou [1] *Zhang* Shiyong [1]
[1]Department of Computer information & technologyFudan University Shanghai 200433
{ xiazhengyou@sina.com qos8@yahoo.com}

Abstract: In this paper, we study security interactive behavior between the hacker and the defender, under which an innovated new idea is emphasized. The process of attack and defend is supposed as the n different rational and non-cooperative players under incomplete information, which is accord with n person incomplete information game. When the hackers attack the defender, they attempt to get their satisfied payoff, however, the defenders always hope to get their satisfied payoff, which will form the Nash equilibrium of game theory. The defenders can use the Nash equilibrium point to analysis and asset their security. The defenders can also use The Nash equilibrium as the reference of security investment.

Keywords: game theory, hacker, defender, Nash equilibrium

I.Introduction

The Internet and web technologies have provided ease of access to information and an efficient communication channel for those who use it. However the ease of use and access to information has fostered problem of network security. The security is one of the hottest topics nowadays; awareness of its important continues to grow with new reports of hackers, organized crime, fringe groups, and even terrorists exploring technology for their own profit and motive. The need for secure network is greater than ever before. Whole sectors of society such as banking and telecommunications are dependent on the availability of reliable and secure network. Reflecting this fact is the ever-increasing size of the computer security marketplace and the importance governments are beginning to place on protecting information infrastructure. Unfortunately, this increased investment doesn't appear to be mitigating the number or cost of incidents from either internal or external sources.

In order to solve the security of network, many researchers have done many works. Security [1] is the protection against: illegal data disclosure; illegal data modification; illegal data destruction and denial of service. the types of attacks is described by EduardoB.Fernandez[2] and the detail of the methods of attack can be founded in [3]. Rogers [4] provided a review of the limited research that had previously been conducted and introduced new hacker taxonomy. .John Van Beverev[5] presented a conceptual model of hacker development and motivations, the model describing the development of hackers and motivations is constructed from existing psychological theories. Andrew P. moore[6]presents attack modeling for information security and survivability, it proposes a means to document information-security attacks in a structured and reusable form. Schneier[7] gives concept of attack tree to describes the process of attack. Diane lambert[8] apply probability theory to study measures of disclosure risk and harm. In the [9] [10], information security risk assessment and information technology common criteria security evaluation is presented. Though many researchers have done many works for network security and used different methods, They have studied hacker behavior, motivation or presents some model to analysis the hacker attack process or defense methods and tools, And so on. They have done little research for the interaction behavior between hacker and defender to study threat and risk assessments. In this paper we present a kind of method to analysis the interaction between behavior of hacker and the defender. The method is based on game theory [11][12]. The method can make us to study threat and risk assessments. We define interactive behavior of hacker and defender into two-person zero-sum game. We use the Nash equilibrium [13][14] theory to get the equilibrium point that the defender and hacker can hope to get, the point can analysis the cost of threat ,harm and defense between the defender and hacker.

The rest of this paper is organized as follows. In the next section, we shall present an overview of the game theory. Section 3 presents game between hacker and defender. In Section 4, we give a simple example to describe the game in the previous section. Finally, we conclude in Section 5 with directions for future work..

II.Network security behavior model

Games are characterized by a number of player or decision makers who interact, possibly threaten each other and form coalition, takes actions under uncertain conditions, and finally received some benefit or reward or possibly some punishment or monetary loss. Game theory was established as a field in its own right after the 1944 publication of the monumental volume theory of games and economic behavior by von Neumann and the economist Oskar Moirgenstern. In 1950,John Nash demonstrated that finite games have always have an equilibrium point, at which all players choose actions which are best for them given their opponents' choice. This central concept of non-cooperative games theory has been a focal point of analysis since then.

Definition1. The strategic form, or normal form, of a two-person zero-sum game is given by a triplet(X, Y, L), where

(1) X is a nonempty set ,the set of strategies of player I

0-7803-7840-7/03/$17.00 ©2003 IEEE.

(2) Y is a nonempty set, the set of strategies of player II

(3) L is a real-valued function defined on $X \times Y$. (thus ,L(x,y) is a real number for every $x \in X$,every $y \in Y$.

The interpretation is as follows, Simultaneously, Player I choose $x \in X$, II choose $y \in Y$, each unaware of the choice of the other. Then their choice are made known and I wins the amount L(x,y) from II..

Definition2. (X, Y, L) is sometimes called a matrix game because the payoff L can be represented by a matrix. If $X=(x_1,\ldots x_m)$ and $Y=(y_1,\ldots y_n)$, then by the game matrix or payoff we mean the matrix

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \quad \text{Where } u_{ij}=L(x_i,u_j). \qquad (2.1)$$

In this form ,player I choose a row ,player II choose a column. And II pays I the entry in the chosen row and column.

Theorem(Nash equilibria). Every finite n-person game in strategic form has at least one strategic equilibrium. (Proof refer to [13][14])

We Consider a game with $m \times n$ matrix A and value V. let $p=(p_1,\ldots ,p_m)$ be any optimal strategy for I and $q=(q_1,\ldots,q_n)$be any optimal strategy for II. Then

$$\sum_{j=1}^{n} a_{ij}q_j = \sum_{i=1}^{m} p_i a_{ij} \qquad (2.2)$$

for all i,j for which $p_i>0, q_j>0$

III.network security behavior model

The network security behavior model is matched as the game theory model as following figure3.1. We analyze the network security behavior model through this figure.

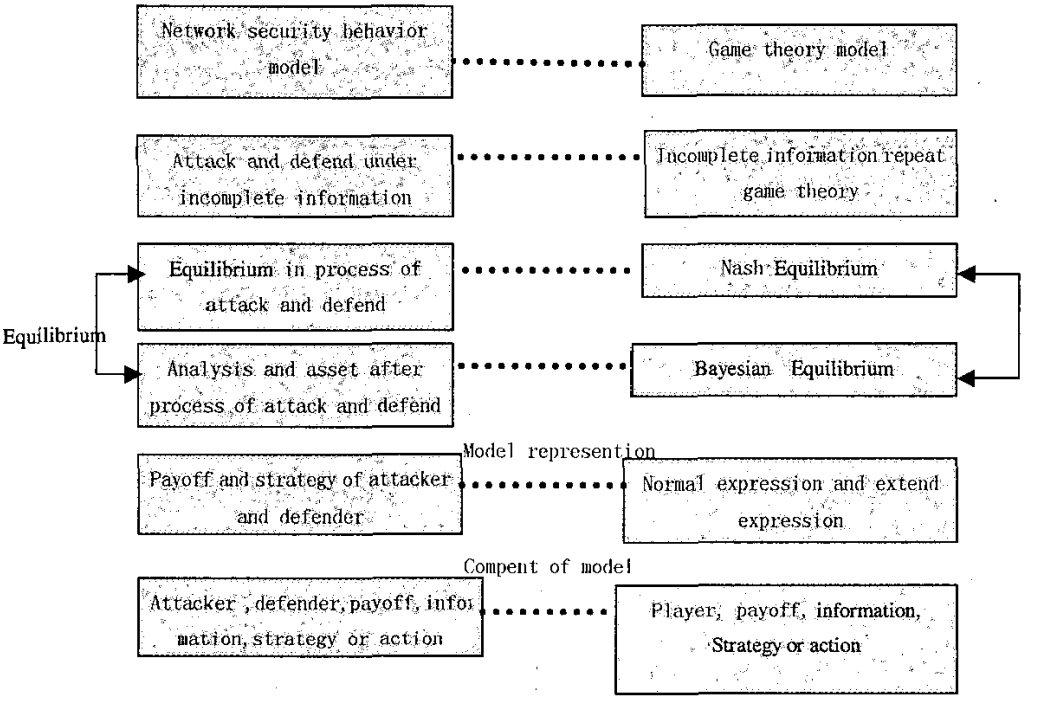

Figure3.1 security model and game theory

Network security behavior game model is based on a set of games known as infinitely repeated games of incomplete information. It uses the Bayesian Nash Equilibrium concept to determine the strategy, which a player should use repeatedly in Order to maximize his or her payoff. The **Nash and Bayesian equilibrium** concepts to predict behavior and analyze the decisions that made in conducting network defend. The goal of those playing the game is to maximize their utility. A player achieves this by discovering and repeatedly playing the one strategy or combination of strategies that maximizes his or her expected payoff. The utility of the game theory model is based on the ability to measure the player's level of equilibrium attainment. If the game model is unable to measure the player's or the majority of the players' attainment of equilibrium, then the game model is of little use for predicting human behavior. At this point, however, the concepts of infinitely repeated games and incomplete information must be related to the study of network security behavior.

Infinitely repeated refers to the fact that neither player knows when the game will end. Round after round is played with each player either winning or losing, and gaining his or her respective payoff. In this scenario, the player must make his or her decisions based on the strategy, which will provide the best average payoff over time. This is similar to information warfare where the defender cannot hope to successfully protect 100 percent of his information 100 percent of the time. The defender must choose a strategy, which best protects his or her information over time, dependent upon what kind of information is most important to the defender. Repeat play allows a player to change strategies on subsequent moves based on the information he or she learned from the outcome of the previous action. This is similar to any form of conflict and certainly of network attack event. As time goes by and actions are taken, a player will form perceptions about his opponent and his overall goals. As more information is gathered and processed, these perceptions could be refined and honed causing a change in strategy based on the new information.

Incomplete information refers to the fact that each player knows some or all of the information about himself but not his opponent. In the case of the network security behavior game model, a player knows his or her own payoff value but not that of his or her opponent. This shows the asymmetric nature of information warfare in that we often know the defenses as well as the value of the information we are protecting. However, we rarely know all the strategies available to our opponent or the value of the information to him, which could be different than the value to ourselves

Perfect information means that players know all the actions available to themselves and their opponents. Perfect information also involves the concept of game history, which is the knowledge of all moves made thus far in the game, also referred to as perfect recall. Complete information means that players know the payoffs available from all possible courses of game play.

The payoff function of the game captures all the possible payoffs in the game. Payoff functions can be one of three types: zero-sum, constant-sum or non-zero sum. Zero sum games involve players' whose goals directly conflict; thus a player can only win what the other player loses. Constant sum games require that only one player receive a non-zero payoff at any one time. Non-zero sum games have no restrictions on the game's payoff structure thus a player's payoff is related only to the course of play. The network security behavior game is a zero sum game,

IV.Analysis for security behavior model

In this section, we describe security behavior game model from three parts. In first part, the presumption and definition is presented; in the second part, the payoff of hacker and defender is described; in the last part, it is game between hacker and defender.

4.1 Presumption and definition

During the research for network security behavior, we consider the hackers and defenders as the research object. We analyze the interactive behavior of the hackers and defenders through the network security behavior model. When we research the game between hacker and defender, we must make some presumption and pre-definition, and get the simple model from the complex problem.

Hacker and defender make decision under uncertain condition, every player may

(1) Not know the parameters of environment.
(2) Not know the events that have happened during game.
(3) Not know action of other players

Rationality: a player is said to be rational if he seeks to play in a manner, which maximizes his own payoff. It is often assumed that rationality of all players is common knowledge. Hacker often chooses optimum methods to attack defender, as the defender always hopes to defense the hacker in a best way. Hacker and defender hope to maximize his own payoff during the game, so we can presume the hacker and defender is rational.

Non-cooperation game: the behavior between hacker and defender is considered as the non-cooperation and competition during game. In the non-cooperation theory, the hacker and defender are unable to communicate before decisions are made, or if such communication is allowed, the hacker and defender are forbidden or are otherwise unable to make blinding agreements on a joint choice of strategy. Of course, the main non-cooperative solution concept is the strategic equilibrium.

Form the above description, we can know the interaction behavior between hacker and defender is consonant with the idea of the game theory. The hackers and defenders are considered as the N different player of a game..

4.2 Payoff of the hacker and defend

Before we research the payoff of the hacker and the defender, we must define the following terms:

Exposure Factor (EF) – Represents the percentage of loss a realized threat event would have on a specific asset.

Average Rate of Occurrence (ARO) – Number that estimates the frequency in which a threat is expect to occur.

Single Loss Expectancy(SLE) – The dollar amount figure assigned to a single occurrence. Derived from the formula: Asset Value($) * EF = SLE

Annual Loss Expectancy (ALE) Derived from the formula: SLE * ARO = ALE

The payoff of the defender (pod)=safeguard asset –SLE – Cost of the defender

The cost of the defender includes the purchase, development, and/or licensing costs, the physical installation costs, and the normal operating costs.

The payoff of the hacker (pof)= the hacker's Expectancy for the attacking – cost of the hacker.

The cost of the hacker includes the time, money, device and so on.

4.3 Game model between the hacker and defender

The game between the hacker and the defender is a

two-person zero-sum game (X, Y, L). It is called be a finite game. The fundamental theory of game theory due to von Neumann states the situation encountered in the game of Odd-or-Even holds for all finite two-person zero-sum games. Specifically,

The Minimax Theorem [11][12]. For every finite two-person zero-sum game

(1) There is number V, called the value of the game
(2) There is a mixed strategy for the defender such that the defender's average gain is at least V no matter what the hacker does, and
(3) There is a mixed strategy for the hacker such that the hacker's average loss is at most V no matter what the defender does.

Consider an arbitrary finite two-person zero-sum game, (X, Y, L), with $m \times n$ matrix A (2.1). Lets us take the strategy space X to be the first m integers, X={1,2...m}, and similarly, Y={1,2...n}. A mixed strategy for the defender may be represented by a column vector, (p1, p2 ,...pm)T of probabilities that add to 1. Similarly, a mixed strategy for the hacker is an n-tuple q=(q1,...,qn)T. the sets of mixed strategies of the hacker and defender will be denoted respectively by X* and Y*.

$$X^* = \{p = (p_1,...p_m)^T : p_i \geq 0, \text{for} \quad i = 1,..,m \text{ and } \sum_1^m p_i = 1\}$$

$$Y^* = \{q = (q_1,...q_n)^T : q_j \geq 0, \text{for} \quad j = 1,..,n \text{ and } \sum_1^n p_j = 1\} \tag{4.2}$$

Suppose the hacker choose a column at random using $q \in Y^*$. If the defender choose row i, the average payoff to the defender is

$$\sum_{j=1}^{n} a_{ij} q_j = (Aq)_i \tag{4.3}$$

The ith component of the vector Aq. Similarly, if the defender uses $p \in X^*$ and the hacker choose column j ,then the defender's average payoff is

$$\sum_{i=1}^{n} p_i a_{ij} = (p^T A)_j \tag{4.4}$$

The jth component of the vector $p^T A$. More generally, if the defender uses $p \in X^*$ and the hacker uses $q \in Y^*$, the average payoff to the defender becomes

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij} q_j\right) p_i = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i a_{ij} q_j = p^T A q \tag{4.5}$$

Suppose it is known that the hacker is going to use a particular strategy $q \in Y^*$. Then the defender would choose that row i that maximizes (4.3); or, equivalently, he would choose that $p \in X^*$ that maximizes (4.5). His average payoff would be

$$\max_{1 \leq i \leq m} \sum_{j=1}^{n} a_{ij} q_j = \max_{p \in X^*} \quad p^T A q \tag{4.6}$$

Similarly, if it is known that the defender is going to use a particular strategy $p \in X^*$, then the defender would choose that column j that minimizes (4.4), equivalently, that $q \in Y^*$ that minimizes (4-5). Her average payoff would be

$$\min_{1 \leq j \leq n} \sum_{i=1}^{m} p_i a_{ij} = \min_{q \in Y^*} \quad p^T A q \tag{4.7}$$

Any $q \in Y^*$ that achieves the minimum in (4.7) is called a best response for the hacker against p.

Suppose now that the hacker is required to announce her choice a mixed strategy $q \in Y^*$ before the defender makes his choice. This changes the game to make it apparently more favorable to the defender. If the hacker announces q, then certainly the defender would use best response against q and the hacker would lose the quantity (4.6) on the average. Therefore, the hacker chooses to announce that q that minimizes (4.6). The minimum of (4.6) over all $q \in Y^*$ is denoted by $\overline{V}$ and called the upper value of the game(X, Y, L).

$$\overline{V} = \min_{q \in Y^*} \max_{1 \leq i \leq m} \sum_{j=1}^{n} a_{ij} q_j = \min_{q \in Y^*} \max_{p \in X^*} p^T A q \tag{4.8}$$

A similar analysis may be carried out assuming that I must announce his choice of a mixed strategy $p \in X^*$ before the hacker makes her choice, if the defender announces p, then the hacker would choose that column with the smallest average payoff, or equivalently that $q \in Y^*$ that minimizes the average payoff (4.7). Given that (4.7) is the average payoff to the defender if he announces p, he would therefore choose p to maximizes (4.7) and obtain on the average

$$\underline{V} = \max_{p \in X^*} \min_{1 \leq i \leq n} \sum_{j=1}^{m} p_i a_{ij} = \max_{p \in X^*} \min_{q \in Y^*} p^T A q \tag{4.9}$$

Definition If $\underline{V} = \overline{V}$, we say the value of the game exists and is equal to the common value of $\overline{V}$ and $\underline{V}$, denoted simply by V. if the value of the game exists, we refer to minimax strategies as optimal strategies.

Some simple algorithm can be used to solve finite game, for example, linear program [15]. In this paper, we don't discuss the algorithm for solving finite games and only give the new idea to study the network security behavior through research for interactive behavior between the hacker and the defender.

V. Conclusion

We study network security behavior model through the interactive of the hacker and the defender, under which a

new idea is emphasized. The network security behavior may be presented as n-person zero-sum game under incomplete information. In order to solve the game between the hacker and defender, we are attempting to do following research in the future: First, we will further construct one nicety coefficient function for game between the hacker and defender; second, we have to detailed classify the hacker and get their motivation and technology; last we need further research relation of security investment, security measure and target of the defender.

Biographies:

Xia Zhengyou (xiazhengyou@sina.com)received a B.S degree from Heifer university of Science & Technology, in 1996, an M.S degree from NanJing university of science &Technology in 1999. Now, He is attempting to receive PhD degree from Fudan University. His interests are in network security and management.

Zhang Shyong is professor and doctor director of FuDan University. His interests are network protocol and security.

Reference

[1] R.C. summers, Secure Computing: threats and safeguards, McGraw-Hill, 1997.

[2] E.B.Fernandez, An overview of Internet security, procs 1oth Intl. Workshop on database and system applications 1999, 837-841.

[3] A.Boulanger, Catapults and grappling hooks: The tools and techniques of Information warfare, IBM Sys, Journal, vol.37, No 1, 1998, 106-114.

[4] Rogers,M, Psychology of hackers: A new taxonomy, Available http://www.infowar.com,2001

[5] John Van Beveren, A conceptual model of hacker development and motivation, Journal of E-Business, Vol.1, Issue2. December 2000.

[6] Andrew P.Moore, Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Model , TECHNICAL REPORT CMU/SEI-2001-TR-029 ESC-TR-2001-029

[7] Schneier,B , Attack Trees: Modeling Security Threats, "Dr.Dobb's Journal, December 1999

[8] Diane Lambert Measures of Disclosures Risk and Harm , AT&T Bell Laboratories tech notes

[9] United states General Accounting Office Accounting Information Management Division, Information Security Risk Assessment, GAO/AIMD-00-33November 1999

[10] The Common Criteria Project Sponsoring Organizations, Common Criteria for Information Technology Security Evaluation, version 2.1 CCIMB-99-031 August 1999

[11] Guillermo Owen Game Theory ,second edition Academic press, 1982 New York London

[12] G.M.Adelson-velsky, Algorithms for Games, Springer-verlag New York,1988

[13] Nash, John F, Jr. , Equilibrium points in N-person games, Proceeding of the National Academy of Science of the United States of America 36,48-49.[53-151]

[14] Nash, John F, Jr. „ two-person cooperative games, Econometrical 21,128-140

[15] H. J. Greenberg, How to Analyse the Results of Linear Programs- Part 3: Infeasibility Diagnoses, Interfaces, Vol 23, No 6, pp. 120-139, 1993.

[16] G. M. Roodman, Post-Infeasibility Analysis in Linear Programming, Management Science, Vol. 25, No. 9, pp. 916-922, 1979.