Application of Stackelberg Security Games in Information Security

Ashot Abrahamyan
Russian-Armenian (Slavonic) University
Yerevan, Armenia
abrahamyanash@yahoo.com

Abstract—Information security has become a very important issue as organizations are increasingly becoming dependent on data and information technology for conducting their operation. There are several risks associated with information systems and well-developed models are needed to address those risks. Information systems are constantly under attack by several actors, including organized crime, political groups, and intelligence agencies. Organizations continue to invest resources to protect their assets. Banks make an especially attractive target for hackers and terrorists for financial gain from fraudulent transactions facilitated through hacking attacks. Both the attackers and defenders have clear motives and gains from their activities. Game theoretic concepts provide an ideal framework to model defender-attacker interactions, particularly Stackelberg Security Games. We posit that banks are leaders who create their security strategy and hackers follow by devising their hacking strategies to beat the banks security strategy. This paper is focused on application of Stackelberg model to information security in context of banks.

Keywords—Information Security; Risk Analysis

I. INTRODUCTION

Game theory is well suited to model security problems for different adversaries. In this paper we examine the possibility of achieving an optimum stable situation between targets (banks) and hackers is examined. The specific goal of the paper is to find the most effective investment strategies for financial institutions to keep the organization secure in the current environment. At any time based on the tools available to the hackers and financial institutions, a game that can quantitatively determine the optimum strategy can be devised.

Recent research activities were focused on Stackelberg Security Games that are applicable in many security resource allocation and scheduling problems [1]. Those games are not only suitable for physical security problems, but also in information security problems, there are also leaders and followers. Leader in case of information security is a security officer and the follower is a hacker. As information security technologies get better the cost of the attacker has risen and attackers invest significant resources in developing tools and technologies for their exploits. There are multiple types of attacks as well as multiple security measures to defend against the attacks; consequently, there are a lot of available strategies for both attackers and defenders. The problem is to find optimal strategy for the defender by accepting the rules of Stackelberg Security Games. This problem moves to find Strong Stackelberg Equilibrium, which is a solution to the problem.

In this paper the detailed description of Stackelberg Security Games and Bayesian Stackelberg Security Games is provided and its applicability in information security domain is discussed.

II. RELATED WORK

Different researchers explore the applicability of game-theoretic methods to model information security issues and there have been significant results in past years [14]. In work [6] the interaction between an attacker and IDS (Intrusion Detection System) was modeled as a stochastic (Markov) game and three different scenarios were discussed depend on available information for both attacker and defender. Illustrative examples and numerical analyses were presented for different cases.

Game theory has been used in modeling of information warfare, where static games with complete information were used [8], however there are some significant challenges in applying such methods when describing cyber-warfare, which are listed in [7]. The interactions between and attacker and systems administrator is modeled as a two-player stochastic game in [9]. For the given model Nash equilibria for both players (attacker and defender) were calculated. In the method described in [10] an attacker’s and administrator’s interaction is modeled as a two-player zero-sum stochastic game, where network is represented as a set of independent nodes with corresponding security assets and vulnerabilities. In [11] considered a game-theoretic model for intrusion detection in mobile ad-hoc networks. Proposed model is multi-stage dynamic non-cooperative game. In [12-13] is described a method of finding optimal investment strategy in information security with use of game theory. There was introduced a penalty parameter which is associated with the case of not making an investment in information security. Game theory is also used in risk assessment issues as shown in [14]. Particularly, there was modeled Markov game of threats and vulnerabilities.

III. STACKELBERG SECURITY GAMES

A Stackelberg game is a two-player game with a leader and a follower, where the leader acts first with the mixed strategy,
and the follower responds with a pure strategy after observing the leader’s strategy. With those strategies both players are trying to maximize their utilities. The leader is acting first by a mixed strategy and the follower is observing the leader’s strategy and then trying to maximize his or her payoff.

Let’s denote by \( L \) leader’s mixed strategy and by \( F \) set of follower’s pure strategies. In this case leader’s follower’s expected utilities will be \( \mu_i L + \mu_{f0} \) and \( \nu_i L + \nu_{f0} \) respectively. Let’s denote by \( U \) and \( V \) leader’s and follower’s utility matrices respectively:

\[
U = \left( \begin{array}{cc} \mu_{i0} & \mu_{f0} \\ \mu_i & \mu_f \end{array} \right), \quad V = \left( \begin{array}{cc} \nu_{i0} & \nu_{f0} \\ \nu_i & \nu_f \end{array} \right)
\]

Bayesian Stackelberg games allow taking into consideration multiple types of followers. This allows to model problems more widely with different types of attackers. In Bayesian Stackelberg Games type of adversary is drawn randomly from the set \( \{1, 2, \ldots, I\} \), where each type \( 1 \leq i \leq I \) has its prior probability \( p_i \) representing the likelihood of its occurrence. Leader acts by its mixed strategy knowing the distribution of all different types of followers, but leader doesn’t know the type of the follower at a certain time. For each follower’s type \( i \) there are utility matrices of leader and follower: \( U_i \) and \( V_i \).

Let’s denote by \( f = (f^1, f^2, \ldots, f^I) \) follower’s pure responses, where \( f^i \) is the pure strategy of follower type \( i \). In this case expected utilities can be defined for both leader and follower

\[
u(L,f) = \sum_{i=1}^{I} p_i u_i(L, f_i)
\]

where the leaders expected utility is

\[
u_i(L,f^i) = (\mu_i^j)^T L + \mu_{f0}
\]

\[
u_i(L,f^i) = (\mu_i^j)^T L + \nu_{f0}
\]

Stackelberg equilibrium [2]. To define Strong Stackelberg equilibrium we need to define a vector of functions

\[
g = (g^1, g^2, \ldots, g^I)
\]

where each \( g^i \) maps a leader’s mixed strategy to a pure strategy of follower with type \( i \), and \( g(L) \) is a vector of the follower’s responses to \( L \) according to \( g \). Now Strong Stackelberg Equilibrium can be formally defined:

For a given Bayesian Stackelberg Game with utility matrices \( U^1, V^1, \ldots, U^I, V^I \) and type distribution \( \mathbf{p} \), a pair of strategies \( (L, g) \) forms a Strong Stackelberg Equilibrium if and only if:

The leader plays a best response:

\[U(L,g(x)) \geq u(L', g(L')) \forall L'
\]

The follower plays a best response:

\[v(L, g(L)) \geq v(L, f), \forall 1 \leq i \leq I, \forall 1 \leq f \in F
\]

The follower breaks ties in favor of the leader:

\[u(L, g(L)) \geq u(L, f) \forall 1 \leq i \leq I, \forall f \text{ that is a best response to } L \text{ as above.}
\]

Stackelberg model is widely used in security domain, because it is one of the most suitable models to show the strategic interaction between defender and attacker. It is used in different scenarios. For instance, Stackelberg Games are used in the ARMOR system, which is deployed at the Los Angeles International Airport (LAX) [1], IRIS program is used by the US Federal Air Marshals (FAMS), and also have many other application for security modeling [2], [3].

IV. APPLICATION IN INFORMATION SECURITY DOMAIN

Stackelberg games are useful in modeling information security issues. In that case for instance the leader can be an information security officer (or organization) and the follower is a hacker (or an organized crime group). The leader acts first by deploying different information security tools to protect its resources. The follower can then respond by probing the network to determine its state and then respond to the leader using its pure strategy. Different types of followers can be construed as different types of attacks. It is statistically known the distribution of possible attacks. Attackers can scan the current state of the network, search for vulnerabilities and decide the best strategy to implement.

Security department can be referred as a leader because of the following points:

- Security policies/practices are open to public or easily identified through probes
- Potential security tools and measures are standard and well known. Hackers can infer security deployment by probing the network and often such information is publicly available from the security vendors or organizations themselves.
- Each security measure has its own vulnerabilities and weaknesses, which gives opportunity for attacker to choose best way to attack.

All these facts suggest that Stackelberg games are applicable in information security domain.

V. CASE OF BANKS

Above described model can be applied in case of information security modeling of banks. In this case, security department of bank is referred to as a leader and hackers as followers. The problem of information security management of banks is rising rapidly due to expansion of the use of mobile and Internet banking and a very strong dependence on the Internet of the banking system operations. Besides since banks deal with money, they are attractive targets for adversaries.

A bank has set of targets that should be protected. Security department uses different security tools to cover those targets regarding information security policy of the bank and different state regulations. All these documents are open to public in most cases. Moreover, the exact technology for security software and hardware is well known in most cases. These circumstances are making available observation of the security state of a certain bank for adversaries. By probing the bank system network hackers decide which attacking strategy to implement based on leader’s strategy.

By examining recent statistics of attacks in banking systems, security departments are familiar with different types of attacks and their likelihoods of occurrence. Based on that knowledge the problem of the bank is to find the optimal strategy for defense measures taking into consideration the fact...
that adversaries are able to observe it and respond in the best way that will give them the greatest result. The optimal strategy can be found by finding Strong Stackelberg Equilibrium in this type of security game.

VI. SOLUTIONS

There were significant advances in recent researches concerning solutions of Stackelberg Security Games, particularly finding Strong Stackelberg Equilibrium. For instance in [4] multiple linear programming method is suggested for finding Strong Stackelberg Equilibrium, but in this method number of LPs grows exponentially as the number of types of followers increases. In general, finding optimal strategy for the leader in Bayesian Stackelberg Games is NP-hard [4], but there are significant improvements in solutions. In [2] DOBBS method is introduced. The idea of that method is decomposing multiple LPs to single mixed-integer linear program (MILP). There is also Branch-and-Bound search method (HBGS) represented in [5] and other solutions that are all applicable to find optimal strategy for the leader. There are several different ways in which we can construct the game. We can consider strategies for the attacker at different levels i.e. at a level of DOS attack, Injection attack, and hybrid attack or we can consider different types of attackers such as DoS attackers and Injection attackers and strategize based on the specific attack type, e.g., SYN-flood.

We provide a simple example to illustrate the problem. For simplicity two types of followers (attackers) were discussed: Denial of Service attacks and Injection attacks with likelihoods 0.6 and 0.4 correspondingly. Each of these types has the following set of pure strategies:

- DoS: DDoS, ICMP-flood, SYN-flood, Smurf-ping
- Injection: SQL injection, Remote file inclusion, log injection, XML injection

Leader’s set of strategies is as follows:

- Passive Defense (DMZ, Firewall, Security Policies)
- Active Defense (DMZ, Firewall, Security Policies, Intrusion Detection Systems)
- Counter Attack (DMZ, Firewall, Security Policies, Intrusion Detection Systems, Network and System Log File Analysis, Launching DOS against hackers, identifying hackers through honey nets and darknets)

The strategies of the Leader (bank) and the follower (hacker) can be associated with specific payoffs for them. These values can be estimated by the cost of launching attacks, the rates of success, and the financial losses that banks incur based on the attacks. Very little data is available for counter attacks at this time but this technique is being investigated increasingly by intelligence agencies in order to protect national businesses.

VII. CONCLUSIONS AND FUTURE WORK

This paper is related to the application of Stackelberg Security games in information security. The detailed description of the model is given. Taking into consideration the form of the model it can be seen that it fits into information security domain where the role of the leader plays systems administrator or security officer and the follower is attacker (hacker). In future work particular examples will be discussed with certain types of attacks and defenses. Also experimental results will be given based on recent statistics.

REFERENCES
