Mathematical Problems of Computer Science 41, 74--80, 2014.

Stackelberg Security Games for Information Security Management of Financial Systems

Ashot A. Abrahamyan

Russian-Armenian (Slavonic) University
e-mail: abrahamyan_ash@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 being attacked by several actors, including, organized crime, political groups, and intelligence agencies. Organizations continue to invest resources to protect their assets. 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. This paper is focused on application of Stackelberg model to information security management of financial systems.

Keywords: Stackelberg security games, Information security, Financial systems.

1. Introduction

Game theory is well-suited to model security problems for different adversaries. Recent research activities were focused on Stackelberg Security games which are applicable to 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. Several facts are mentioned to state the goodness of information security management modeling of financial systems.

2. 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** the leader’s mixed strategy and by F – the set of follower’s pure strategies. In this case the leader’s-follower’s expected utilities will be $«_f^T \boldsymbol{L} + «_{f,0}$ and $\neg_f^T \boldsymbol{L} + \neg_{f,0}$, respectively. Let’s denote by U and V the leader’s and follower’s utility matrices, respectively:

$$U = \begin{pmatrix} «_{1,0} & «_{F,0} \\ «_1 & «_F \end{pmatrix}, \; V = \begin{pmatrix} \neg_{1,0} & \neg_{\mathrm{F},0} \\ \neg_1 & \neg_F \end{pmatrix}.$$

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 a type of adversary is drawn randomly from the set {1, 2, …, I}, where each type 1≤i≤I has its prior probability p^i representing the likelihood of its occurrence. The leader acts by its mixed strategy knowing the distribution of all different types of followers, but the 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.

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

$$u(\boldsymbol{L}, \boldsymbol{F}) = \sum_{i=1}^{I} p^i u^i(\boldsymbol{L}, f^i),$$

where

$$u^i(\boldsymbol{L}, f^i) = («^i_{f^i})^T \boldsymbol{L} + «_{f^{i,0}},$$

is the leaders expected utility against the follower with type I,

$$\neg^i(\boldsymbol{L}, f^i) = (\neg^i_{f^i})^T \boldsymbol{L} + \neg_{f^{i,0}}.$$

To find the best strategy for the leader it is needed to find Strong Stackelberg equilibrium [2]. To define the Strong Stackelberg equilibrium we need to define a vector of functions **g**=(g^1, g^2, …, 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 the Strong Stackelberg Equilibrium can be formally defined:

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

1) The leader plays a best response:

$$\mathrm{u}(\boldsymbol{L}, \boldsymbol{g}(\boldsymbol{L})) \geq u(\boldsymbol{L}', \boldsymbol{g}(\boldsymbol{L}')), \forall \boldsymbol{L}'.$$

2) The follower plays a best response:

$$\neg^{i}(\boldsymbol{L}, g^{i}(\boldsymbol{L})) \geq \neg^{i}(\boldsymbol{L}, f), \forall 1 \leq i \leq I, \forall 1 \leq f \leq F.$$

3) The follower breaks ties in favor of the leader:

$u^{i}(\boldsymbol{L}, g^{i}(\boldsymbol{L})) \geq u^{i}(\boldsymbol{L}, f), \forall 1 \leq i \leq I, \forall f$ that is a best response to **L** 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 the defender and the 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 applications for security modeling [2, 3].

3. 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. According to the recent research and statistics [6], [7] organizations are able to construct percentage distribution of attack techniques. 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:

1. Security policies are open to public in most cases.
2. 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.
3. Each security measure has its own vulnerabilities and weaknesses, which gives an opportunity for the attacker to choose the best way to attack.

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

4. Specifics of Information Security Problems in Financial Systems

Information security assurance of financial systems has its own specifics and has many differences with similar security strategies of other companies and organizations. First of all, the information that is stored in financial institutions in many cases represents real money, which is one of primary goals for different adversaries. Second, information security threats for financial organizations are sufficiently specific and countermeasures against those threats are often open to the public. Moreover, in other conventional organizations the stored information is threatened only by a little range of adversaries who are the competitors of the organization in most cases. In case of financial systems the range of threats is wider.

Let’s discuss some specific factors that affect the information security of financial systems:

1. The stored and processed information in financial systems represents real money. Using information systems different payments, transfers and other financial

operations are implemented; the illegal manipulation of such information may lead to serious losses. This feature expands the range of criminals.

2. The stored information in financial systems affects the interests of a large number of people and organizations – the clients. As a rule, this kind of information is confidential, and the organization is responsible for providing the required degree of privacy to their customers. Of course, customers are entitled to expect that the organization should take care of their interests, otherwise it may lead to the loss of reputation with all the consequences.
3. Information security of financial system (unlike most other companies) must provide high reliability of computer systems, even in case of emergency, because it is responsible not only for their money, but for the money of customers.
4. Sensitive information about clients are stored in financial systems, which leads to the widening of the range of potential attackers, who may be interested in theft or damaging of such information.

5. Case of Banks

For simplicity let’s take an example of financial system – a bank. The described model can be applied in case of information security modeling of banks. In this case, the 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 the expansion of the use of mobile and Internet banking and a very strong dependence on the Internet of the banking system operations. Besides, since the banks deal with money, they are attractive targets for adversaries.

A bank has a set of targets that should be protected. The security department uses different security tools to cover those targets regarding the 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 the hackers decide which attacking strategy to implement based on leader’s strategy.

By examining the 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 an 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.

Research in this field can be challenging as many offences may remain unknown to the public due to the fact, that the managers of such organizations are afraid to lose reputation. This fact makes difficulties due to the lack of sufficient information.

For the illustration of the proposed model lets consider case of banking web application. We will use the most critical security risks as strategies for the attacker (follower) and possible countermeasures for each risk as strategies for the defender (leader). Risks and countermeasures are illustrated in Table 1. Based on possible impacts of certain risk or countermeasures and taking into consideration corresponding costs implementation we can derive the payoff matrix (Table 2). In this example is taken into account the fact, that the follower can also decide to take no action at all (NA).

Table 1: Risks and Countermeasures

Security Risk	**Countermeasure**
SQL injection (SQLi)	Escaping routines (ER)
Cross-Site Scripting (XSS)	Escaping routines (ER)
Broken Authentication and Session Management (BASM)	Session Security (SS)
Insecure Direct Object Reference (IDOR)	Access Control (AC)
Cross-Site Request Forgery (CSFR)	CSFR Guard (CSFRG)
Security Misconfiguration (SM)	Environment Securing (ES)
Failure to Restrict URL Access (FRUA)	Access Control (AC)
Insufficient Transport Layer Protection (ITLP)	Secure Sockets Layer (SSL)

Table 2: Payoff Matrix

	SQLi	XSS	BASM	IDOR	CSRF	SM	FRUA	ITLP	NA
ER	7, -1	7, -1	-5, 2	-2, 0.5	-5, 2	-4, 2	-2, 0.5	-5, 1	-1, 0
SS	-6, 3	-6, 3	2, -2	-3, 0.5	-6, 2	-5, 2	-3, 0.5	-6, 1	-2, 0
AC	-6, 3	-6, 3	-6, 2	-2, -0.5	-6, 2	-5, 2	-2, -0.5	-6, 1	-2, 0
CSRFG	-6, 3	-6, 3	-6, 2	-3, 0.5	0, -2	-5, 2	-3, 0.5	-6, 1	-2, 0
ES	-6, 3	-6, 3	-6, 2	-3, 0.5	-6, 2	3, -1	-3, 0.5	-6, 1	-2, 0
SSL	-6, 3	-6, 3	-6, 2	-3, 0.5	-6, 2	-5, 2	-3, 0.5	0, -3	-2, 0

We will define two types of followers, A and B, with same payoff values but with different sets of possible pure strategies. Lets assume, that the follower type A can use any strategy, except NA, and the follower type B can't use CSRF and ITLP strategies. Calculations are done with the following primary conditions:

- likelihood of the appearance of the follower type A is 0.6;
- likelihood of the appearance of the follower type B is 0.4.

Here are the results of the calculations:

- maximum expected utility of the leader = -0.09499999999999931
- maximum expected utility of the follower type A = 1.3076923076923077
- maximum expected utility of the follower type B = 1.1
- pure strategy of the follower type A: XSS
- pure strategy of the follower type B: SQLi
- mixed strategy of the leader:
  - ✓ER: 0.4542307692307692
  - ✓SS: 0.20423076923076922
  - ✓AC: 0.0
  - ✓CSRFG: 0.06923076923076923
  - ✓ES: 0.2723076923076923
  - ✓SSL: 0.0

The presented results are consistent with overall statistics of attacks on web applications, where SQLi and XSS are considered as the most critical security risks. Therefore, based on the obtained results, information security resourse allocation should be implemented with use of probability distribution obtained in the mixed strategy of the leader to get the optimal defense strategy.

6. Solutions

There were significant advances in recent researches concerning the solutions of Stackelberg Security Games, particularly finding Strong Stackelberg Equilibrium. For instance, in [4] a multiple linear programming method is suggested for finding Strong Stackelberg Equilibrium, but in this method the number of LPs grows exponentially as the number of types of followers increases. In general, finding an 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 a Branch-and –Bound search method (HBGS) represented in [5] and other solutions which are all applicable to find an optimal strategy for the leader.

7. Conclusions and Future Work

This paper is related to the application of Stackelberg Security games in information security. A 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 the systems administrator or security officer and the follower is the 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

[1] M. Tambe, M. Jain, J. A. Pita and A. Jiang, “Game theory for security: key algorithmic principles, deployed systems, lessons learned”, in *50th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1822--1829, 2012.

[2] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez and S. Kraus, “Playing games with security: an efficient exact algorithm for Bayesian Stackelberg games”, in *Proc. of The 7th InternationalConference on Autonomous Agents and Multiagent Systems (AAMAS)*, pp. 895--902, 2008.

[3] D. Korzhyk, Z. Yin, C. Kiekintveld, V.Conitzer and M.Tambe, “Stackelberg vs nash in security games - an extended investigation of interchangeability, equivalence and uniqueness”, *Journal of Artificial Intelligence Research*, vol. 41, pp. 297--327, 2011.

[4] V. Conitzer and T. Sandholm, “Computing the optimal strategy to commit to”, in *Proc. of the 7th Association for Computing Machinery(ACM) Conference on Electronic Commerce (EC)*, pp. 82--90, 2006.

[5] M. Jain, E. Kardes, C. Kiekintveld, M. Tambe and F. Ordonez, “Security games with arbitrary schedules: A branch and price approach”, in *Proc. of Association for the Advancement of Artificial Intelligence (AAAI) Conference on Artificial Intelligence*, pp. 792--797, 2010.

[6] (2014) Kaspersky Lab website. [Online]. Available: http://www.kaspersky.com/

[7] (2014) Department for Business and Innovation Skills, UK website. [Online]. Available: https://www.gov.uk/government/organisations/department-for-business-innovation-skills/

Submitted 15.12.2013, accepted 28. 02. 2014.

Շտակելբերգի անվտանգության խաղերի կիրառությունը ֆինանսական համակարգերի անվտանգության կառավարման համար

Ա. Աբրահամյան

Ամփոփում

Տվյալ աշխատանքում նկարագրվում է խաղերի տեսության հիման վրա կառուցված ֆինանսական համակարգերի տեղեկատվական անվտանգության կառավարման մոդել՝ Շտակելբերգի խաղերի կիրառությամբ: Բերվում են որոշակի առանձնահատկություններ՝ կապված ֆինանսական համակարգերի տեղեկատվական անվտանգության հետ և Շտակելբերգի անվտանգության խաղերի նկարագրություն: Հետազոտության արդյունքում տրվում են փաստեր, որոնք հաստատում են Շտակելբերգի խաղերի կիրառության արդյունավետությունը ֆինանսական համակարգերի տեղեկատվական անվտանգության ռեսուրսների օպտիմալ բաշխման կառավարման մոդելավորման դեպքում:

Игры безопасности Штакельберга для управления информационной безопасностью финансовых систем

А. Абраамян

Аннотация

В данной работе описывается теоретико-игровая модель управления информационной безопасностью финансовых систем с применением игр Штакельберга. Описана специфика проблем информационной безопасности финансовых систем, и теория игр безопасности Штакельберга. Результаты исследований подтверждают эффективность использования игр безопасности Штакельберга в моделировании оптимального распределения ресурсов информационной безопасности в финансовых системах.