Target Information Trading - An Economic Perspective of Security

Jing Hou[1], Li Sun[1], Tao Shu[1(✉)], and Husheng Li[2]

[1] Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, USA
{jzh0141,lzs0070,tshu}@auburn.edu
[2] Department of Electrical Engineering and Computer Science, The University of Tennessee Knoxville, Knoxville, TN 37996, USA
hli31@utk.edu

Abstract. Ample evidence has confirmed the importance of information in security. While much research on security game has assumed the attackers' limited observation capabilities to obtain target information, few work considers the possibility that the information can be acquired from a data broker, not to mention exploring the profit-seeking behaviors of such an information service in the shrouded underground society. This paper studies the role of information in security problem when the target information is sold by a data broker to multiple competitive attackers. We formulate a novel multi-stage game model to characterize both the cooperative and competitive interactions of the data broker and attackers. Specifically, the attacker competition with correlated purchasing and attacking decisions is modeled as a two-stage stochastic model; and the bargaining process between the data broker and the attackers is analyzed in a Stackelberg game. Both the attackers' competitive equilibrium solutions and data broker's optimal pricing strategy are obtained. Our results show that with information trading, the target suffers from larger risks even when the information price is too high to benefit the attackers; and the information accuracy is more valuable when the target value is higher. Furthermore, the competition may weaken the information value to the attackers but benefit the data broker. The study contributes to the literature by characterizing the co-opetitive behaviors of the attackers with labor specialization, providing quantitative measures of information value from an economic perspective, and thus promoting a better understanding of the profit-seeking underground community.

Keywords: Security · Information market · Game theory · Economics

1 Introduction

Target information is undoubtedly a crucial factor of security problems in various applications for protecting critical infrastructure like transportation and computer networks. Attackers conduct surveillance to gain awareness of targets' vulnerabilities and security operations, based on which to make a selection of

S. Chen et al. (Eds.): SecureComm 2019, LNICST 305, pp. 126–145, 2019.
https://doi.org/10.1007/978-3-030-37231-6_7

where to attack and how much effort to take in attacking [1,2]. In reality, most often attackers have limited observation capabilities such that they may only have few or partial information about the target's vulnerability [3]. However, in some situations the attackers do not necessarily need to observe by themselves to gain the information. The widespread use of and thus an immerse demand for potential target information in hacker communities has spawned a *data brokers* industry [4]. The data brokers in crime society are specialized in collecting target information (e.g., software vulnerabilities, snippets of code, credit card numbers and compromised accounts) and sell them in black markets in exchange for financial gain [5]. For example, users of the underground forums regularly engage in the buying, selling and trading of illegally obtained information to support criminal activities [6]. As a report [7] published by TrendMicro states: "Underground hackers are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in-person fraud." The Shadow Brokers, which trades in compromised network data and exploits, is a representative of such a data broker as a hacker group. In June 2017, the computer virus NotPetya was able to spread by leveraging a vulnerability leaked by the Shadow Brokers [8]. More recently, Facebook, accused of privacy violations that could provide "material support" for terrorism potentially, was reported to face multibillion-dollar FTC fine [9]. Indeed, data brokers, as a boon to the cybercrime economy [10], have become an indispensable member of the illegally evolved supply chain called "cybercrime-as-a-service" [11].

While we do not have a clear picture of the information trading behaviors in the underground society, security researchers are taking more interest in exploring hacker communities. Initial studies of security experts have reached a consensus that one major motivation of hackers is profit-related (others include fame and skill improvement etc.) [12]. Our aim in this paper is to study the profit-driven attacking behaviors in a hacker community, with a particular emphasis on the role of target information provided by a data broker in security using economic analysis. More precisely, we would like to understand the value of traded target information—both for the sellers of this information and for the attackers that buy it. Through an economic analysis of the attacking behaviors with information trading, we would be able to provide a simple glimpse of complex society structure, and to better understand the phenomenon of hacking. These knowledge provide at least tentative insights for arriving at effective solutions to security problems with information leakage.

We consider one or multiple attackers that have limited observation capabilities of the potential target. They can approach a data broker that holds the vulnerability of the target. The target vulnerability determines how much effort the attackers need to take in order to launch a successful attack. Without the information, the attacker may choose not to act, fail or exert more effort than needed. The attackers could benefit from purchasing the information by launching a more targeted attack with less effort. Here we care about the value of the information for the attackers and how the data broker should price the information if they can obtain it, but how the data broker could obtain the information is beyond our focus. Besides, we talk about the scenario of multiple attackers when

the target value can be shared among them if they all deliver successful attacks. The assumption of competition among attackers through dividing up the value of a single asset is appropriate when they share the benefits of private goods as illegal resource access (like spectrum or other network resource utilization) and monopoly privileges (like stealing electronically stored information about consumers' personal data for market exploration). Similar assumptions can be found in [13], which adopts a rent-seeking model of security games where the asset value is divided among the attackers and the defender. We are interested in whether there is a positive or negative network externality in the information market due to the competition among the attackers, that is, would the existence of more potential buyers increases the value of the data broker's information or decreases it.

With the observation of the hierarchical and competitive structure in attacker behaviors, we present and study a multi-stage model of information market. In Stage I, the data broker determines the information price to the attackers. In Stage II, the attackers decide whether to buy or not. In Stage III, after obtaining the target information, the attackers decide whether to attack the target or not. The composed game provides an integrated view of security problem with competitive attackers and target information trading. The research questions we aim to answer include: (a) How would the attacker change its attacking decision once it has bought some detailed information of the target's vulnerability from the data broker? (b) How does the competition between the attackers affect their information purchasing decision and attacking decisions? (c) Is it beneficial for the data broker to set a low price such that all attackers would buy the information? Or should the data broker enhance the price when there is more potential buyers rather than one? (d) How are the decisions affected when the data has lower quality (only partial information is available for trading)?

The problems are challenging due to the following two reasons. First, there is lack of a systematic or quantitative framework to evaluate the information in a competitive crime community. Although it is intuitive that the more information, the better for the attackers, questions are still unexplored as what is the highest price that the attacker can accept? Does an attacker always benefit from buying the information if other attackers also buy it? Or is the information more valuable if other attackers do not buy? To the best of our knowledge, this is the first paper that tries to provide a unified framework of information market in security. We will provide insights regarding the impacts of target information trading on various parties: the increased attacking probability of the target, the expected utility increase for the attackers and the profit through selling the information for the data broker.

Second, the hierarchy attacker behaviors are interdependent across multiple stages. On one hand, the attacking decisions, including whether or not to attack, and with how much effort, are affected by the attackers' knowledge of the target. On the other hand, whether or not to buy the information is determined by how much utility gain can be expected from attacking. The competition among multiple attackers makes these decisions even more complex. This is different

from most competition analysis when the product can be sold to only one buyer and the game ends after the purchasing is done. Therefore, the structure of the game varies across the stages. We will model the game among the attackers as Bayesian games, to capture their limited observability, and model their purchasing-attacking decision process as a stochastic game. Besides, from the data broker's perspective, the purchasing probability of the buyers is not only determined by the competition game equilibrium among the attackers, but also affected by the target value and the price. We will use a Stackelberg game to model the pricing and purchasing decisions of the players.

Our main contributions can be summarized as follows.

- While most traditional security game model assume that target information is obtained through attackers' self-observation and learning, we consider an information market in hacker communities and propose a game-theoretic framework, which captures the multi-stage correlated behaviors of attackers. This information market model better fits the practice of a profit-seeking hacker communities with labor specialization. Our results show that in this information channel, information accuracy is more valuable for a more attractive target.
- Much previous work focus on interactions between a defender and single or multiple independent attackers, without consideration of the competitions among the attackers or the role of other players that assist in attacking. We incorporate the strategic interactions between multiple competitive attackers as in a Bayesian and stochastic game, and between the attackers and the data broker as in a Stackelberg game. Our analysis indicates that the value of information for the attackers could be weakened by their competition. Besides, with the assistance of a data broker, even if the information does not benefit the attackers under high price, the target may suffer from larger attacking risk. And the risk will be increased in a certain range confined by both the price and the target value.
- We provide the equilibrium solutions and characterize the conditions for the existence and uniqueness of the equilibrium under different target values. We show that if the target is not attractive enough, there may be multiple pure-strategy equilibria in the attackers' competition game. And whether there will be a strictly dominant pure-strategy is determined by the target value, the target vulnerability and the information price. Furthermore, in the Stackelberg game equilibria, it is not wise for the data broker to set a price low enough to attract all the buyers if the target is attractive enough to the attackers.

The remainder of this paper is organized as follows. Section 2 reviews the related literature. Section 3 introduces the model setups. In Sects. 4 and 5, we study the single attack model and the competition model, respectively. In Sect. 6, we provide an extension model with low information accuracy, and this paper is concluded in Sect. 7.

2 Related Work

Much of the research in security game has assumed that the attacker has perfect observation of the defense policy over potential targets and therefore been able to explore the value of commitment for the defender in a Stackelberg game framework [14]. Realizing that this assumption rarely hold in real-world domains, existing studies are turning their interests into the scenario of incomplete, inaccurate or uncertain information. Some work has proposed the version of the security game with bounded memory [15] or imperfect observations [16]. Others have assumed that the target information gained by the attackers can be learned more accurately by conducting a period of surveillance [17,18]. A more recent study which has pointed out the possibility that the defender is allowed to strategically disclose the number of resources to the attacker, further shows the importance of target information [19]. However, none of the above studies consider the possibility of intermediary information acquisition from a market. The value and the impacts of such a information service have hardly been addressed. Although there is already study evaluating the value of customer information for the retailers' pricing strategies in consumer market [4]. Their results cannot be applied to the security problem because the target in security problem may be not exclusive to the attackers as the merchandise is to consumers.

Our paper focuses on the information market in the context of hacker community. Hacker community is both devastating and prevalent because it facilities cooperation and allows for specialization among attackers, leading to more advanced and more economically efficient attacks. We can discern a growing interest among researchers in the enigmatic hacker community. Some studies have focused on the organization of the community, like identifying the key actors [5], discovering the types of collaborative attack patterns [20] or evaluating its sustainability [9]. Others provide a window into the society by microscopically analyzing the behaviors of the attackers, mostly addressing their cooperation in the form of coalition. Current studies assume that the attackers are heterogeneous in their non-task-specific efficiency, resource allocation or skill sets, and thus coalition is formed for more attacks or to gain higher total utility [21–23]. But the format of collusion with labor specialization, especially the information service, which is universal in hacker community, has not been fully explored. More specifically, the questions are not studied yet about how the attackers would benefit from information assistance, and what is the bargaining process that decides their reward allocations. The answers to these questions are crucial to investigate why and how information service is provided in hacker community, as well as when such cooperation is formed among profit-driven attackers. Besides, the competition among attackers for the limited resource pool is another factor that impacts the attacking decisions and rewards, while it is usually ignored in the existing research, except in [13]. In an attempt to fill the gap in the current literature on the incentives of complex behaviors in hacker society, this research take into consideration both the cooperation among attackers specialized in different tasks and competition among similar attackers. Specifically, we analyze the interactions between a data broker and two competing attackers

through a multi-stage game approach. The value of information is derived and the impacts of such information service are evaluated.

3 System Model and Problem Formulation

Consider two attackers trying to attack one potential target. The attackers have limited ability to obtain the vulnerabilities (or the protection level of the defender) about the target. But they can purchase the information from a data supplier, who has full or partial knowledge about the target's vulnerabilities. The data supplier needs to set a price for the information. And given the price, the attackers determine whether or not to make a purchase. Afterwards (when the information has been revealed to the attackers if purchase is made), they will decide whether to attack the target. All the players in our model are profit-motivated.

If a attacker successfully attacks the target, it receives utility $v > 0$, otherwise it receives zero utility. The value of v (also called the target value), reflecting the target attractiveness to the attackers, is a common knowledge to all the players. We restrict our model to the target resource that consumption by one agent would reduce consumption by others. That is, when multiple attackers successfully attack the target, they equally split the target value. In a two-attacker case, either would get a utility of $\frac{1}{2}v$. This assumption relies on the fact that the target pool in reality is finite and attackers compete for a common asset pool.

We define the success of a attacker as follows: if the attacker's effort e in attacking is not smaller than the target's protection level by its defender (or owner), we say the attacker succeeds in the attack. The problem is, the attacker itself is not aware of the exact value of the target protection level, which determines the minimum level of effort for attackers to successfully attack the target. In the following analysis, we will slight abuse the terms of target protection level or vulnerability and the minimum attacking effort needed, and use one symbol to denote it: θ. A smaller value of θ indicates a lower surveillance and thus less effort to launch a successful attack. Let us suppose the attackers only know the distribution of θ, which is normalized to be uniformly distributed on $[0, 1]$, with the largest value 1 implying the defender capacity. If an attacker tries to attack the target with an effort less than the actual value of θ, then it will fail.

Measured in both the success probability of an attack and the expected gain, the attacker's total utility function with an attacking effort e is written as

$$f = \mathbf{1}_{e \geq \theta}(e) * v - C(e). \tag{1}$$

Here $C(e)$ is the attacking cost which increases with the effort e. We will assume $C(e) = e$ for simplicity. Although this assumption represents a simple linear function between the effort and the cost, it is reasonable and would not affect the major insights obtained from our analysis.

The data supplier is a broker who collects and sells data about the target vulnerability or the target owner's protection level. This information tells how

much effort needed to launch a successful attack for the attackers, i.e. the actual value of θ. An attacker who buys the information could launch a targeted attack with exactly the minimum level of efforts needed. In Sect. 6, we all also study the situation when the data broker only has partial information about the target, which means that the information could only tell a more accurate range of θ than the attacker has. We are interested in how the data broker chooses to sell the data and what is the information value for all the players, and ignore the details of how the broker acquires the data.

We provide a framework for analyzing how the attacker's optimal information purchasing and attacking decisions could be made in the face of the competition and uncertainty about the target vulnerabilities. To better analyzing the impacts of competition, we assume the attackers are homogeneous. The attacker's objective is to maximize the expected benefit from an attack (taking into account the attacker's target valuation, the success probability of an attack and the cost involved in purchasing and attacking); the data broker sets the information price to maximize the expected profit (taking into account the purchasing probability of the attackers).

The model's timing proceeds as follows:

*Step*1. The data broker determines and broadcasts the information price p.

*Step*2. The attackers decide whether to buy the information or not. After the payments are made, the data broker delivers the target information to the buyer(s).

*Step*3. With the information available, the attackers decide how much effort will be taken in attacking (zero effort means not to attack).

*Step*4. After the attack, the corresponding utilities are gained by the attackers.

4 Single Attacker Model

As a benchmark, we consider the case where a monopolist attacker (*he*) will fully exploit this situation and extract all surplus from successfully attacking the target. He needs to make a decision of whether to buy the target information from a data broker (*she*), by comparing the two expected utilities as follows.

4.1 Not Buy Information

If the attacker does not buy information from the data broker, his expected utility function with effort level e is

$$f_0(e) = \int_0^e v d\theta - e = ve - e. \tag{2}$$

So the optimal solution is $e = 1$ with $f_0 = v - 1$ if $v > 1$ and $e = 0$ with $f_0 = 0$ if $v \leq 1$ (the 1st number in subscript of f denotes the number of attackers that buy the information).

4.2 Buy Information

If the attacker decides to buy the information θ from the data broker at price p and to attack the target, he would attack with exactly the effort θ.

Case 1: $v > 1$. The attacker would always attack since $\theta \leq v$, and his expected utility function is

$$f_{1,v\geq 1} = \int_0^1 (v-\theta)d\theta - p = v - \frac{1}{2} - p. \tag{3}$$

Compared with (2), if $v - \frac{1}{2} - p > v - 1$, or $p < \frac{1}{2}$, then the attacker would buy the information, else he prefers not to buy the information.

Case 2: $v \leq 1$. Only when $\theta < v$ would he attacks. Then his expected utility function is

$$f_{1,v<1} = \int_0^v (v-\theta)d\theta - p = \frac{1}{2}v^2 - p. \tag{4}$$

Similarly, compared with (2), if $\frac{1}{2}v^2 - p > 0$, or $p < \frac{1}{2}v^2$, then the attacker would buy the information, else he prefers not to buy the information.

Figure 1 plots the regions of the attacker's optimal decisions with different values of information price and target value. The attacker buys the target information only in regions I and III. On the other hand, in region II, the attacker would attack with the greatest effort $e = 1$; while in region IV, the attacker would neither buy nor attack. Specifically, the value of information for the attacker lies in region I where it helps to deduce the effort taken, or region III where attack is profitable when $\theta < v$. In other words, the value of the information for the attacker is an expected utility gain of $v - 0.5 - p - (v-1) = \frac{1}{2} - p$ if $v > 1$ and $p \leq \frac{1}{2}$ or $\frac{1}{2}v^2 - p$ if $v \leq 1$ and $p \leq \frac{1}{2}v^2$.

Besides, what the defender (or target owner) cares about is whether or not the attacker would choose to attack the target and with how much effort (i.e. successful or not). When no information is available to the attacker, he would not attack the target as long as $v \leq 1$. But when a data broker sells the information with a price low enough, the target would be successfully attacked even if $v \leq 1$. Therefore, the target is affected by the information trading only in region III.

4.3 Optimal Pricing Decisions of the Data Broker

We assume that when the attackers are indifferent between to buy and not to buy, they always choose to buy in favor of less uncertainty. If $v \leq 1$, the information price cannot be set to be larger than $p = \frac{1}{2}v^2$, otherwise no profit can be gained by the data broker. That is, the information should be sold at $p^* = \frac{1}{2}v^2$ if $v \leq 1$. Similarly, $p^* = \frac{1}{2}$ if $v > 1$. The corresponding expected profit for the data broker in single-attacker case is $\frac{1}{2}v^2$ when $v \leq 1$ and $\frac{1}{2}$ when $v > 1$. Therefore, we could say the information value for the data broker increases with the target value until the target becomes attractive enough to the attacker that he would attack anyway even without the information.

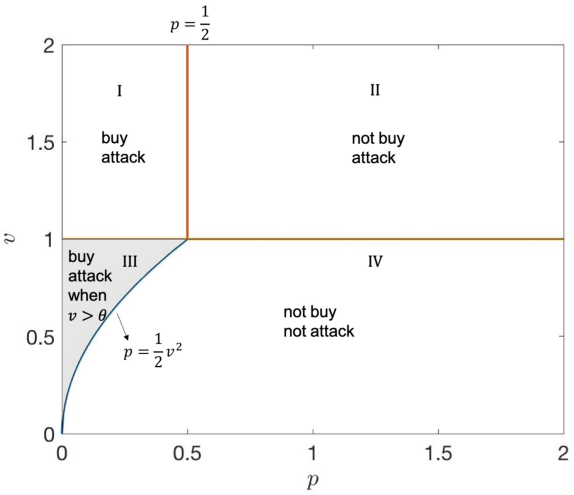

Fig. 1. The optimal decisions of single attacker

5 Competition Model

In this section we consider the scenario when there are two attackers (A and B) that could buy the same data for a target from the data broker (the sequence of the games is indicated in Fig. 2). The attackers make decisions independently. Following the work of [4], we restrict our attention to the case when the data set is sold only in one time block at Step 2 and this trade information is common knowledge (i.e., the data broker is willing to publicize its total sales quantity). Using backward induction in Stackelberg game, we first derive the attackers' optimal attacking decisions and their expected utilities assuming they have or have not bought the information, and then analyze their optimal purchasing decisions. Finally, we obtain the optimal pricing decisions for the data broker. Since the exact target information is not available to the attacker(s) before purchase, we can use a Bayesian game framework to model the scenario (with θ uniformly distributed on [0,1]). Besides, as the attacking game depends on the purchasing decisions made by both attackers in the previous game, the whole decision process of the attackers is modeled as a stochastic game.

5.1 Games of Attacking

In the game of attacking, the outcome depends on the informational structure—that is, on which attackers acquire information.

Both Do Not Buy Information. We first consider the situation when both attackers decide not to buy the information from the data broker. Whether or not the attackers would attack is determined by the value of the target. Therefore, we analyze the results of the attacking games with different values of v.

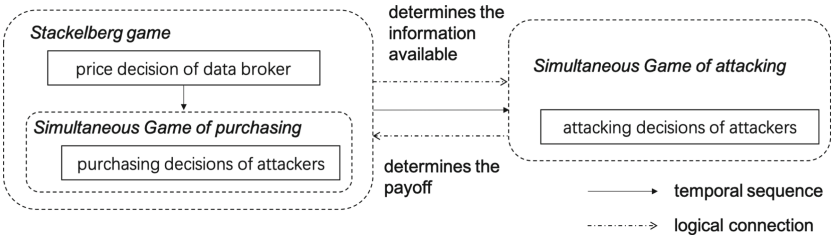

Fig. 2. Hierarchical game structure

Case 1: $v > 2$. If both attackers decide to attack, with effort e_A and e_B respectively, we suppose $e_A \leq e_B$ without loss of generality. Then attacker A's expected utility is $f_A(e_A) = \frac{1}{2}v\int_0^{e_A} d\theta - c_A = (\frac{1}{2}v - 1)e_A$, and attacker B's expected utility is $f_B(e_B) = \frac{1}{2}v\int_0^{e_A} d\theta + v\int_{e_A}^{e_B} d\theta - e_B$. To maximize $f_A(e_A)$, we have $e_A = e_B = 1$. If only one attacker attacks, his optimal decision is $e = 1$ with $f = v-1$; and the other attacker has zero utility. The attackers' payoffs for game of attacking when both of them have no information about the target are listed in Table 1 (with attacker A's strategies listed in rows and attacker B's strategies listed in columns). The only strictly dominant pure-strategy equilibrium can be analyzed as (attack, attack) with utility $f_{0,v>2} = \frac{1}{2}v - 1$ for both attackers.

Table 1. Payoff table for game of attacking when both attackers have no information

	Attack	Not attack
Attack	$\frac{1}{2}v-1,\ \frac{1}{2}v-1$	$v-1, 0$
Not attack	$0, v-1$	0, 0

Case 2: $1 < v \leq 2$. There are two pure-strategy Nash equilibria: (attack, not attack) and (not attack, attack). In such situations we will focus on the mixed-strategy Nash equilibrium solution. We suppose attacker A chooses to attack with probability q_A^{attack} and attacker B attacks with probability q_B^{attack}. Then $f_B(attack) = q_A^{attack}(\frac{1}{2}v - 1) + (1 - q_A^{attack})(v - 1) = f_B(not\ attack) = 0$, and similar equation holds for attacker A. Therefore, in mixed-strategy Nash equilibrium, $q_A^{attack} = q_B^{attack} = 2\frac{v-1}{v}$, and the expected utility for both attackers is $f_{0,1<v\leq 2} = (2\frac{v-1}{v})(2\frac{v-1}{v})(\frac{1}{2}v - 1) + 2\frac{v-1}{v}(1 - 2\frac{v-1}{v})(v - 1) = 0$.

Case 3: $v \leq 1$. Similar to the analysis above, the only strictly dominant pure strategy is (not attack, not attack) with utility $f_{0,v\leq 1} = 0$ for both attackers.

Both Buy Information. When both attackers buy information from the data broker, they will make the attacking decision after they obtain the information. Therefore, the attacking game is influenced by two factors: the target value and the minimum effort needs for a successful attack.

Table 2. Payoff table for game of attacking when both attackers buy the information

	Attack	Not attack
Attack	$\frac{1}{2}v-\theta-p$, $\frac{1}{2}v-\theta-p$	$v-\theta-p$, $-p$
Not attack	$-p$, $v-\theta-p$	$-p$, $-p$

Case 1: $v > 2$. The attackers would always benefit from attacking even if they split the value v since $\frac{1}{2}v > \theta$. Therefore, it is easy to derive that the only strictly dominant pure strategy is (attack, attack), and their expected utility is

$$f_{2,v>2} = \int_0^1 (\frac{1}{2}v - \theta)d\theta - p = \frac{1}{2}v - \frac{1}{2} - p. \tag{5}$$

Case 2: $1 < v \leq 2$. If both attackers decide to attack after they get the information θ, they both get a utility of $\frac{1}{2}v - \theta - p$. If only one attackers attack, then he would get a utility of $v - \theta - p$, while the other one gets $-p$. Their payoffs for this game are listed in Table 2. Therefore, when $\frac{1}{2}v - \theta > 0$, the only pure-strategy Nash equilibrium is (attack, attack). And when $\frac{1}{2}v - \theta \leq 0$, in mixed-strategy Nash equilibrium, each attacker would attack with probability $q_A^{attack} = q_B^{attack} = 2(1 - \frac{\theta}{v})$, and the expected utility for both attackers is $-p$. Therefore, the expected utility of each attacker is

$$f_{2,1<v\leq 2} = \int_0^{\frac{1}{2}v} (\frac{1}{2}v - \theta)d\theta + \int_{\frac{1}{2}v}^1 0d\theta - p = \frac{1}{8}v^2 - p. \tag{6}$$

Case 3: $v \leq 1$. If $\theta \geq v$, both attackers would not attack. And if $\theta < v$, the attacker gets a utility of $\frac{1}{2}v - \theta - p$ when both of them attack; when only one attacker chooses to attack, he would get a utility of $v - \theta - p$. Therefore, the only pure-strategy Nash equilibrium is (attack, attack) for the situation of $\frac{1}{2}v - \theta > 0$; and in mixed-strategy Nash equilibrium for $\frac{1}{2}v - \theta \leq 0$, each attacker would attack with probability $q_A^{attack} = q_B^{attack} = 2(1 - \frac{\theta}{v})$ and expected utility of $-p$. To sum up, the expected utility of each attacker is also $f_{2,v\leq 1} = \frac{1}{8}v^2 - p$.

Only One Attacker Buys Information. Without loss of generality, we consider the case when only attacker A buys the information. Then for attacker A, he would make the decision of attacking after he obtains the value of θ from the data broker, while attacker B has to make the attacking decision based on the distribution of θ. The payoffs for this game are listed in Table 3.

Table 3. Payoff table for game of attacking when only attacker A buys the information

	Attack	Not attack
Attack	$\frac{1}{2}v-\theta-p$, $\frac{1}{2}v-1$	$v-p-\theta$, 0
Not attack	$-p$, $v-1$	$-p$, 0

Case 1: $v > 2$. If both attackers decide to attack, then attacker B's utility function is $f_B(e_B) = \int_0^{e_B} \frac{1}{2}vd\theta - e_B = (\frac{1}{2}v - 1)e_B$, with $e_B = 1$ when $v > 2$. Attacker A's utility is therefore $\frac{1}{2}v - \theta - p$. If only attacker A attacks, then $f_A = v - p - \theta$, and $f_B = 0$. Else if only attacker B attacks, then $f_A = -p$, and $f_B = v - 1$. Therefore, the only pure-strategy Nash equilibrium is (attack, attack) with $f_{1,v>2,A} = \int_0^1 (\frac{1}{2}v - \theta)d\theta - p = \frac{1}{2}v - p - \frac{1}{2}$ and $f_{1,v>2,B} = \frac{1}{2}v - 1$.

Case 2: $1 < v \leq 2$. In this case, attacker B knows that if $\frac{1}{2}v - \theta \geq 0$, attacker A will certainly attack; that is, the probability of attacker A attacking is not smaller than the probability of $\frac{1}{2}v - \theta \geq 0$: $q_A^{attack} \geq \int_0^{\frac{1}{2}v} d\theta = \frac{1}{2}v$. If we assume attacker B should attack with probability q_B^{attack}, then its expected utility is $q_A^{attack} * q_B^{attack} * (\frac{1}{2}v - 1) + q_B^{attack} * (1 - q_A^{attack}) * (v - 1) = q_B^{attack} * (v - 1 - \frac{1}{2}vq_A^{attack})$. Since $q_A^{attack} \geq \frac{1}{2}v$, we have $v - 1 - \frac{1}{2}vq_A^{attack} \leq 0$. Therefore, to maximize attacker B's expected utility, $q_B^{attack} = 0$. And because attacker B would always choose not to attack, attacker A would attack when $1 < v \leq 2$. To sum up, the expected utilities are: $f_{1,1<v\leq 2,A} = \int_0^1 (v - p - \theta)d\theta = v - p - \frac{1}{2}$, and $f_{1,1<v\leq 2,B} = 0$.

Case 3: $v \leq 1$. Attacker B would not choose to attack even when attacker A does not attack. In this case, attacker A chooses to attack only when $\theta > v$. Therefore, $f_{1,v\leq 1,A} = \int_0^v (v - p - \theta)d\theta + \int_v^1 (-p)d\theta = \frac{1}{2}v^2 - p$, and $f_{1,v\leq 1,B} = 0$.

5.2 Games of Purchasing

Based on the equilibrium of the attacking games, the two attackers know their expected utilities when they choose to buy or not to buy the information. This situation forms a game of purchasing between two buyers. According to the results above under different values of v, we will analyze the game in three cases, with three payoff tables below.

Table 4. Payoff table for game of purchasing when $v \leq 1$

	Buy	Not buy
Buy	$\frac{1}{8}v^2 - p$, $\frac{1}{8}v^2 - p$	$\frac{1}{2}v^2 - p$, 0
Not buy	0, $\frac{1}{2}v^2 - p$	0, 0

Case 1: $v \leq 1$. According to the payoffs in Table 4, if $p < \frac{1}{8}v^2$, the only pure-strategy Nash equilibrium is (buy, buy). And if $\frac{1}{8}v^2 \leq p < \frac{1}{2}v^2$, there will be two pure-strategy Nash equilibria: (buy, not buy) or (not buy, buy). In the mixed strategy equilibrium, assume attacker A chooses to buy the information with probability q_A^{buy} and attacker B attacks with probability q_B^{buy}. We have $f_B(buy) = q_A^{buy}(\frac{1}{8}v^2 - 1) + (1 - q_A^{buy})(\frac{1}{2}v^2 - 1) = f_B(not\ buy) = 0$, and similar equation holds for attacker A. Therefore, in mixed-strategy Nash equilibrium, $q_A^{buy} = q_B^{buy} = \frac{\frac{1}{2}v^2 - p}{\frac{3}{8}v^2}$, and the expected utility for both attackers is 0. If $p \geq \frac{1}{2}v^2$, the only pure-strategy Nash equilibrium is (not buy, not buy).

Table 5. Payoff table for game of purchasing when $1 < v \leq 2$

	Buy	Not buy
Buy	$\frac{1}{8}v^2 - p$, $\frac{1}{8}v^2 - p$	$v - \frac{1}{2} - p$, 0
Not buy	0, $v - \frac{1}{2} - p$	0, 0

Case 2: $1 < v \leq 2$. According to the payoffs in Table 5, if $p < \frac{1}{8}v^2$, the only pure-strategy Nash equilibrium is (buy, buy). If $\frac{1}{8}v^2 \leq p < v - \frac{1}{2}$, there will be two pure-strategy Nash equilibria (buy, not buy) or (not buy, buy). In the mixed strategy equilibrium, either attacker would choose to buy with a probability of $q_A^{buy} = q_B^{buy} = \frac{v-\frac{1}{2}-p}{v-\frac{1}{2}-\frac{1}{8}v^2}$ and expected zero utility. And if $p \geq v - \frac{1}{2}$, the only pure-strategy Nash equilibrium is (not buy, not buy).

Table 6. Payoff table for game of purchasing when $v > 2$

	Buy	Not buy
Buy	$\frac{1}{2}v - \frac{1}{2} - p$, $\frac{1}{2}v - \frac{1}{2} - p$	$\frac{1}{2}v - \frac{1}{2} - p$, $\frac{1}{2}v - 1$
Not buy	$\frac{1}{2}v - 1$, $\frac{1}{2}v - \frac{1}{2} - p$	$\frac{1}{2}v - 1$, $\frac{1}{2}v - 1$

Case 3: $v > 2$. According to the payoffs in Table 6, if $p \geq \frac{1}{2}$, we have $\frac{1}{2}v - \frac{1}{2} - p < \frac{1}{2}v - 1$, and in this case, the only pure-strategy Nash equilibrium is (not buy, not buy). If $p < \frac{1}{2}$, we have $\frac{1}{2}v - \frac{1}{2} - p \geq \frac{1}{2}v - 1$, and the only pure-strategy Nash equilibrium is (buy, buy).

Figure 3 shows the equilibrium purchasing decisions under different values of price p and target value v.

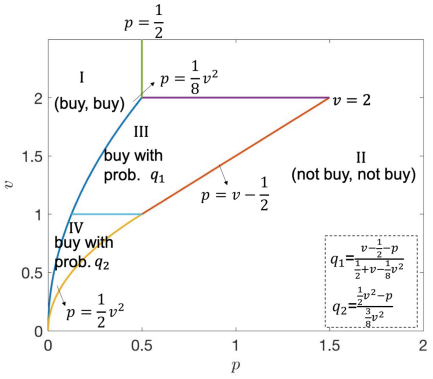

Fig. 3. The optimal purchasing decisions of two attackers

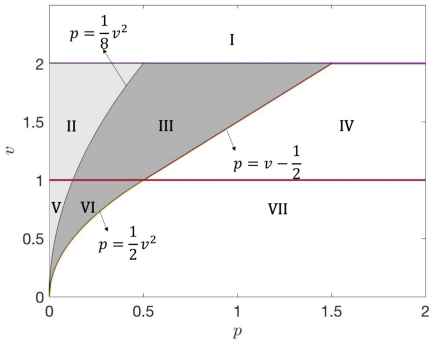

Fig. 4. Regions where attacking probability of the target is increased

By integrating the results in the game of purchasing with those in the game of attacking, We can now analyze the impacts of information trading for the

target. We already know that if no information is available, when $v > 2$, both attackers attack; when $1 < v \leq 2$, each attacker attacks with a probability $2\frac{v-1}{v}$; and when $v \leq 1$, no one attacks. While if information is leaked and can be bought by the attackers at price p from a data broker, Fig. 4 summarizes the seven regions in parameter space with the shaded areas are where more possible attacks are resulted from the information trading. The light grey region is where there is 100% possibility that the attacking probability will be increased. And the dark grey region is where the increase in attacking probability is determined by the attackers' purchasing behaviors.

The detailed impacts of the information leakage and trading on the attackers' attacking probability can be shown in Table 7. In regions I, IV and VII, the attackers make the same attacking decisions as in the situation of no information trading, because the price is so high that the attackers will not buy the information from the data broker. In regions II, III, V and VI however, the attacking probabilities are clearly increased.

Table 7. Attacking probability of the attackers w/o information trading

Region	No information	With information trading
I	1	1
II	$2(1-\frac{1}{v})$	1 if $\theta \leq \frac{1}{2}v$; $2(1-\frac{\theta}{v})$ if $\theta > \frac{1}{2}v$
III	$2(1-\frac{1}{v})$	$2(1-\frac{\theta}{v})$ if both buy info.; 1 if only one buys info.; $2(1-\frac{1}{v})$ if both do not buy info.
IV	$2(1-\frac{1}{v})$	$2(1-\frac{1}{v})$
V	0	1 if $\theta \leq \frac{1}{2}v$; $2(1-\frac{\theta}{v})$ if $\theta > \frac{1}{2}v$
VI	0	$2(1-\frac{\theta}{v})$ if both buy info.; 1 when $v > \theta$ if only one buys info.; 0 if both do not buy info.
VII	0	0

One can also obtain the value of information for the attackers. If no information is available, when $v > 2$, both attackers obtain an expected utility of $\frac{1}{2}v - 1$; otherwise, both attackers get zero expected utility. If the target information can be bought, we could represent the value of information for the attackers as the amount of increase in the attacker's expected utility. If $v > 2$ and $p \leq \frac{1}{2}$, there is a expected utility increase of $\frac{1}{2} - p$; if $v \leq 2$ and $p \leq \frac{1}{8}v^2$, the attackers are expected to have a utility gain of $\frac{1}{8}v^2 - p$. The results indicate that, in the mixed equilibrium of the competition game between the attackers, they are expected to benefit from the information only when the price is less than $\frac{1}{8}v^2$ for $v \leq 2$ or $\frac{1}{2}$ for $v > 2$. However, even if the information does not benefit the attackers as the price increases, the target is expected to be attacked more likely with information leakage (in regions III and VI of Fig. 4). Besides, if we compare the results above with those when no competitor exists for the attacker in Sect. 4, we could conclude that the value of information for the attackers is indeed weakened by their competition if the target value if not large enough ($v \leq 2$).

5.3 Optimal Pricing Decisions of the Data Broker

Now we further analyze the data broker's selling strategy to maximize her profit. She could set either a low price such that both attackers buy or a high price that attackers buy with certain probability.

Case 1: $v > 2$. The data broker would not set a price larger than $\frac{1}{2}$, otherwise both attackers would not be willing to make a purchase. In this case, the data broker's expected profit is $\pi^*_{v>2} = 2 * \frac{1}{2} = 1$ with optimal price $p^* = \frac{1}{2}$.

Case 2: $1 < v \leq 2$. If the data broker sets a price not larger than $\frac{1}{8}v^2$, both attackers would buy the information, which brings a profit of at most $\pi_{1<v\leq 2, p\leq \frac{1}{8}v^2} = \frac{1}{4}v^2$ for the data broker with $p_1 = \frac{1}{8}v^2$. If the data broker sets a price that satisfies $\frac{1}{8}v^2 < p \leq v - \frac{1}{2}$, the two attackers would make a purchase at the probability of $q_1 = \frac{v-\frac{1}{2}-p}{v-\frac{1}{2}-\frac{1}{8}v^2}$. In this case, an expected profit of $\pi_{1<v\leq 2, \frac{1}{8}v^2<p\leq v-\frac{1}{2}}(p) = q_1^2 * 2 * p + 2 * q_1 * (1 - q_1) * p = 2p\frac{v-\frac{1}{2}-p}{v-\frac{1}{2}-\frac{1}{8}v^2}$ will be gained. Because $\frac{\partial^2 \pi_{1<v\leq 2, \frac{1}{8}v^2<p\leq v-\frac{1}{2}}(p)}{\partial p^2} < 0$, the optimal price p_2 satisfies $\frac{\partial \pi_{1<v\leq 2, \frac{1}{8}v^2<p\leq v-\frac{1}{2}}(p)}{\partial p} = 0$, i.e., $p_2 = \frac{2v-1}{4}$. Now we can easily prove that $\pi_{1<v\leq 2, p\leq \frac{1}{8}v^2} = \frac{1}{4}v^2 < \pi_{1<v\leq 2, \frac{1}{8}v^2<p\leq v-\frac{1}{2}} = \frac{(v-\frac{1}{2})^2}{2v-1-\frac{1}{4}v^2}$ for $1 < v \leq 2$. Therefore, when $1 < v \leq 2$, the data broker's maximum expected profit is $\pi^*_{1<v\leq 2} = \frac{(v-\frac{1}{2})^2}{2v-1-\frac{1}{4}v^2}$ with optimal price $p^* = \frac{2v-1}{4}$.

Case 3: $v \leq 1$. Similarly, for both attackers buying the information, the data broker would set a price equal to $\frac{1}{8}v^2$, which brings a profit of $\pi_{v\leq 1, p\leq \frac{1}{8}v^2} = \frac{1}{4}v^2$. If the data broker sets a price that satisfies $\frac{1}{8}v^2 < p \leq \frac{1}{2}v^2$, the two attackers would make a purchase at the probability of $q_2 = \frac{\frac{1}{2}v^2-p}{\frac{3}{8}v^2}$. In this case, an expected profit of $\pi_{v\leq 1, \frac{1}{8}v^2<p\leq \frac{1}{2}v^2}(p) = q_2^2 * 2 * p + 2 * q_2 * (1 - q_2) * p = 2p\frac{\frac{1}{2}v^2-p}{\frac{3}{8}v^2}$ will be gained, which is maximized at $p = \frac{1}{4}v^2$, and we have $\pi_{v\leq 1, \frac{1}{8}v^2<p\leq \frac{1}{2}v^2} = \frac{1}{3}v^2$. In this case, since $\pi_{v\leq 1, \frac{1}{8}v^2<p\leq \frac{1}{2}v^2} > \pi_{v\leq 1, p\leq \frac{1}{8}v^2}$, it is optimal for the data broker to set a price of $p^* = \frac{1}{4}v^2$, and $\pi^*_{v\leq 1} = \frac{1}{3}v^2$.

Proposition 1 summarizes this section's main results. And Fig. 5 shows the optimal pricing strategy and corresponding expected profit of the data broker. It indicates that, the information value for the broker increases with the target value when the target value is not large enough ($v \leq 2$), but as the target is becoming attractive enough for the attackers ($v > 2$), the information value decreases to a certain value and remains unchanged.

Proposition 1. *The data broker's optimal price of the target information is determined by the target value for the attackers. When the target is not attractive enough, it is not wise to set a price low enough to attract two buyers. Specifically,*

(a) if $v \leq 1$, information is sold to the attackers at a price of $p^* = \frac{1}{4}v^2$, resulting each attacker making the purchase with a probability of 2/3;

(b) if $1 < v \leq 2$, *information is sold at* $p^* = \frac{2v-1}{4}$, *with a purchase probability of* $\frac{v-\frac{1}{2}}{2v-1-\frac{1}{4}v^2}$ *from each attacker;*

(c) else if $v > 2$, *information is sold to both attackers at* $p^* = \frac{1}{2}$.

Proof. See the text.

If we compare the data broker's expected profit in the single-attacker scenario with that in the multi-attacker scenario, we could find that, the impacts of competition among attackers on the information value for the data broker is determined by the target value: if the target value is small ($v \leq 1.24$), the data broker benefits from more potential buyers; while if the target value is large ($v > 1.24$), the information value is larger when there is only one attacker.

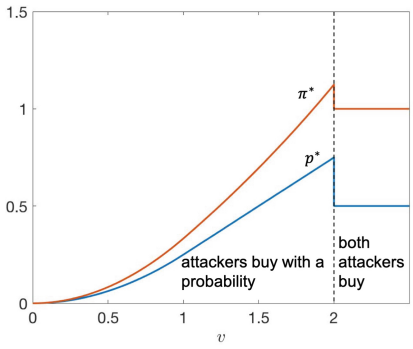

Fig. 5. The optimal pricing strategy and expected profit of the data broker

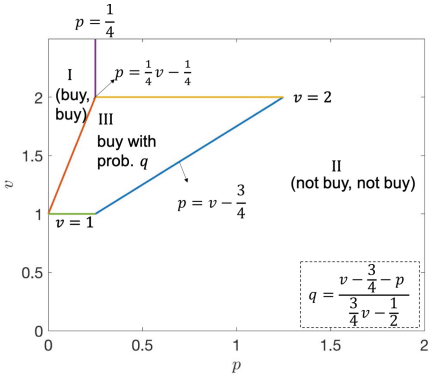

Fig. 6. The optimal purchasing decisions of two attackers under partial information

6 Extension-Partial Information Model

We consider now the possibility that the data supplier can only obtain partial information about the target, i.e., whether θ belongs to $[0, 0.5]$ or $[0.5, 1]$, but he cannot provide the exact value of θ. We analyze how this new informational structure affect attackers' purchasing and attacking decision games and model the price of information with low data quality.

6.1 Games of Attacking

We also start with the competition game of attacking given different purchasing decisions.

Both Do Not Buy Information. When nobody buys the information, the equilibrium results are the same as in Sect. 5.1.

Both Buy Information. When both attackers buy the information, two cases are considered:

Case 1: $\theta \in [0, 0.5]$. Both attackers know that θ is uniformly distributed within $[0, 0.5]$. If both of them attack, each obtains an expected utility of $f = \int_0^{0.5} \frac{1}{2} v * 2d\theta - 0.5 - p = \frac{1}{2}(v-1) - p$; else if only one attacks, then he obtains an expected utility of $f = \int_0^{0.5} v * 2d\theta - 0.5 - p = v - \frac{1}{2} - p$. Therefore, if $v > 1$, both of them would attack; if $\frac{1}{2} < v \leq 1$, each attacker would attack with probability $q_A^{attack} = q_B^{attack} = \frac{2v-1}{v}$, and the expected utility for both attackers is $-p$; otherwise, both would not attack.

Case 2: $\theta \in [0.5, 1]$. If both of them attack, each obtains an expected utility of $f = \int_{0.5}^1 \frac{1}{2} v * 2d\theta - 1 - p = \frac{1}{2}v - 1 - p$; else if only one attacks, then he obtains an expected utility of $f = \int_{0.5}^1 v * 2d\theta - 1 - p = v - 1 - p$. Therefore, if $v > 2$, both of them would attack; if $1 < v \leq 2$, each attacker would attack with probability $q_A^{attack} = q_B^{attack} = 2\frac{v-1}{v}$, and the expected utility for both attackers is $-p$; otherwise, both would not attack.

Considering the two cases $\theta \in [0, 0.5]$ and $\theta \in [0.5, 1]$ with equal probabilities for the attackers before they buy and obtain the information, the expected utility for the attacker when both of them buy information would be: $f_{2,v>2} = \frac{1}{2}(\frac{1}{2}(v-1) - p) + \frac{1}{2}(\frac{1}{2}v - 1 - p) = \frac{1}{2}v - \frac{3}{4} - p$, $f_{2,1<v\leq 2} = \frac{1}{4}(v-1) - p$, and $f_{2,v\leq 1} = -p$.

Only One Attacker Buys Information. For attacker B who does not buy the information, if both attackers attack, he is expecting a utility of $\frac{1}{2}v - 1$; if he attacks but attacker A does not attack, his expected utility is $v - 1$. Therefore: if $v > 2$, both attackers would attack, with $f_{1,v>2,A} = \frac{1}{2}(\frac{1}{2}v - \frac{1}{2} - p) + \frac{1}{2}(\frac{1}{2}v - 1 - p) = \frac{1}{2}v - \frac{3}{4} - p$ and $f_{1,v>2,B} = \frac{1}{2}v - 1$. If $1 < v \leq 2$, the optimal decision is (attack, not attack), with $f_{1,1.5<v\leq 2,A} = \frac{1}{2}(v - \frac{1}{2} - p) + \frac{1}{2}(v - 1 - p) = v - \frac{3}{4} - p$ and $f_{1,1.5<v\leq 2,B} = 0$. And if $v \leq 1$, attacker B would certainly not attack. In this case, if attacker A gets that $\theta \in [0, 0.5]$, he would only attack when $v > \frac{1}{2}$; and if A gets that $\theta \in [0.5, 1]$, he would not attack. Therefore, we have $f_{1,\frac{1}{2}<v\leq 1,A} = \frac{1}{4}v - \frac{1}{4} - p$, $f_{1,v\leq\frac{1}{2},A} = 0$ and $f_{1,v\leq 1,B} = 0$.

6.2 Games of Purchasing

From the equilibrium analysis above, we know that if $v < \frac{1}{2}$, both attackers would not attack, and therefore have no incentive to buy information. Figure 6 plots the attackers' optimal purchasing decisions of partial information in different ranges of v and p. Due to the page limitation, the analysis process is omitted.

The impact of partial information trading for the target is less than that of full information trading: the attacking probability increases only in the following two situations: (1) $1 < v \leq 2$, $p \leq \frac{1}{4}v - \frac{1}{4}$ and $\theta < 0.5$: both attackers would attack the target; and (2) $1 < v \leq 2$ and $\frac{1}{4}v - \frac{1}{4} < p \leq v - \frac{3}{4}$: both attackers would attack if they buy the information and find that $\theta < 0.5$, or the only one attacker who buys the information would certainly attack. But in these situations without the information, they would attack with probability $2\frac{v-1}{v}$.

As for the value of partial information to the attackers, we know that if no information is available, when $v > 2$, both attackers obtain an expected utility of $\frac{1}{2}v-1$; when $v \leq 2$, both attackers get zero expected utility. If partial information can be traded, when $v > 2$ and $p < \frac{1}{4}$, there is a expected utility increase of $\frac{1}{4} - p$; when $1 < v \leq 2$ and $p \leq \frac{1}{4}v - \frac{1}{4}$, the attackers are expected to have a utility gain of $\frac{1}{4}v - \frac{1}{4} - p$; and when $1 < v \leq 2$ and $\frac{1}{4}v - \frac{1}{4} < p \leq v - \frac{3}{4}$, the expected utility gain is $v - \frac{3}{4} - p$.

6.3 Optimal Pricing Decisions of the Data Broker

Due to lower data quality, we are expecting a lower price compared to the scenario when full information is traded. Specifically, the following proposition summarizes our main results:

Proposition 2. *Under partial information, if $v \leq 1$, the information is of no value to both the attackers and the data broker; if $1 < v \leq 2$, information is sold at $p^* = \frac{1}{2}v - \frac{3}{8}$, with a purchase probability of $\frac{2v-\frac{3}{2}}{3v-2}$ for each attacker; else if $v > 2$, information is sold to both attackers at $p^* = \frac{1}{4}$.*

Proof. The proof is similar to that of Proposition 1, and thus omitted here.

One can now compare the results under partial information with those under full information. The price for partial information is $\frac{1}{8}$ lower when $1 < v \leq 2$ and $\frac{1}{4}$ lower when $v > 2$. That is, information accuracy is more valuable for the data broker or the attackers for a more attractive target. Moreover, by comparing Figs. 3 and 6, we can derive that, for a target with lower value ($v < 1$), if the defender takes some effort to ensure that only partial information could be leaked, the attacking probability may decrease to zero.

7 Conclusion

We have studied a security problem with target information trading from an economic perspective. The interaction between a data broker and two attackers is formulated as a Stackelberg game where the data broker acts as the leader setting the price with the consideration of possible responses from the attackers. And the competition between two attackers is modeled as a type of stochastic game. We have evaluated the value of the information from the perspectives of different players respectively, which is related to: the acceptable price and the expected utility increase for the attackers, the changes in the attacking probabilities for the target, as well as the data broker's optimal selling strategy. We discover several interesting insights of the information market in the hacker community. For example, if the target is not so attractive, the information value for the attackers will be weakened by their competition, but the data broker would benefit from their competition; and the data broker prefers high profit margin over volume sales. Besides, information accuracy is more valuable of a more attractive target. Our results also provide some insights to the defense strategy:

to protect the information from leakage would avoid attacks if the target value is low enough, but when the target is highly attractive, more effort should be taken into the protection of the target itself than the protection of the information. Several directions for future research can stem from our paper. First, it will be worthwhile to investigate a specific type of attack. Second, the situation where the data broker does not reveal her total sales quantity is a problem that the attackers may encounter. Finally, the consideration of multiple attackers with different target evaluations would be an important future research direction.

Acknowledgments. The work of T. Shu is supported in part by NSF under grants CNS-1837034, CNS-1745254, CNS-1659965, and CNS-1460897. The work of H. Li is supported in part by NSF under grant CNS-1525226. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

References

1. An, B., Brown, M., Vorobeychik, Y., Tambe, M.: Security games with surveillance cost and optimal timing of attack execution. In: 12th International Conference on Autonomous Agent and Multi-agent System, St. Paul, MN, USA, pp. 223–230 (2013)
2. Southers, E.G., Tambe, M.: LAX-terror target: the history, the reason, the countermeasure. In: Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned, pp. 27–50. Cambridge University Press (2011)
3. Pita, J., Jain, M., Tambe, M., Ordóñez, F., Kraus, S.: Robust solutions to Stackelberg games: addressing bounded rationality and limited observations in human cognition. Artif. Intell. **174**(15), 1142–1171 (2010)
4. Montes, R., Sand-Zantman, W., Valletti, T.: The value of personal information in online markets with endogenous privacy. Manag. Sci. **65**(3), 1–21 (2018)
5. Benjamin, V., Chen, H.: Securing cyberspace: identifying key actors in hacker communities. In: IEEE International Conference on Intelligence and Security Informatics, pp. 24–29. IEEE, Arlington (2012)
6. Motoyama, M., McCoy, D., Levchenko, K., Savage, S., Voelker, G.M.: An analysis of underground forums. In: ACM SIGCOMM Conference on Internet Measurement Conference, pp. 71–80. ACM, Berlin (2011)
7. Hacking communities in the Deep Web. https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref. Accessed 5 Apr 2019
8. The hacks that left us exposed in 2017. https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html. Accessed 5 Apr 2019
9. Facebook could reportedly face multibillion-dollar FTC fine over privacy violations. https://www.theverge.com/2019/2/14/18225440/facebook-multibillion-dollar-ftc-fine-privacy-violations. Accessed 5 Apr 2019
10. USA Information Resources Management Association: Cyber Crime: Concepts, Methodologies, Tools and Applications. IGI Global, Hershey (2011)
11. Zhu, Q., Rass, S.: On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats. IEEE Access **6**, 13958–13971 (2018)
12. Leeson, P., Coyne, C.J.: The economics of computer hacking. J. Law. Econ. Policy **1**(2), 511–532 (2006)

13. Hausken, K., Bier, V.M.: Defending against multiple different attackers. Eur. J. Oper. Res. **211**(2), 370–384 (2011)
14. Yin, Z., Korzhyk, D., Kiekintveld, C., Conitzer, V., Tambe, M.: Stackelberg vs. Nash in security games: interchangeability, equivalence, and uniqueness. In: 9th International Conference on Autonomous Agents and Multi-agent Systems, Toronto, Canada, pp. 1139–1146 (2010)
15. Fang, F., Stone, P., Tambe, M.: When security games go green: designing defender strategies to prevent poaching and illegal fishing. In: 24th International Joint Conference on Artificial Intelligence, pp. 2589–2595. AAAI Press, Buenos Aires (2015)
16. Damme, E., Hurkens, S.: Games with imperfectly observable commitment. Games Econ. Behav. **21**(1–2), 282–308 (1997)
17. An, B., et al.: Security games with limited surveillance. In: 26th AAAI Conference on Artificial Intelligence, pp. 1241–1248. AAAI Press, Toronto (2012)
18. Zhuang, J., Bier, V.M., Alagoz, O.: Modeling secrecy and deception in a multiple-period attacker-defender signaling game. Eur. J. Oper. Res. **203**(2), 409–418 (2010)
19. Guo, Q., An, B., Bošanský, B., Kiekintveld, C.: Comparing strategic secrecy and Stackelberg commitment in security games. In: 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, pp. 3691–3699 (2017)
20. Du, H., Yang, S.J.: Discovering collaborative cyber attack patterns using social network analysis. In: Salerno, J., Yang, S.J., Nau, D., Chai, S.-K. (eds.) SBP 2011. LNCS, vol. 6589, pp. 129–136. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19656-0_20
21. Guo, Q., An, B., Vorobeychik, Y., Tran-Thanh, L., Gan, J., Miao, C.: Coalitional security games. In: International Conference on Autonomous Agents and Multi-agent Systems, Singapore, Singapore, pp. 159–167 (2016)
22. Gholami, S., Wilder, B., Brown, M., Thomas, D., Sintov, N., Tambe, M.: Divide to defend: collusive security games. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds.) GameSec 2016. LNCS, vol. 9996, pp. 272–293. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47413-7_16
23. Roy, A., Mohapatra, P., Kamhoua, C.: Game theoretic characterization of collusive behavior among attackers. In: IEEE International Conference on Computer Communications (INFOCOM), pp. 2078–2086. IEEE, Honolulu (2018)