The Value of Traded Target Information in Security Games

Jing Hou, Li Sun, Tao Shu, and Husheng Li

Abstract—**Ample evidence has confirmed the importance of information in security. While much research on security game has assumed the attackers' limited capabilities to obtain target information, few studies consider the possibility that the information can be acquired from a data broker, not to mention exploring the attackers' profit-seeking behaviors in the shrouded underground society. This paper studies the role of information in the security problem when the target information is sold by a data broker to multiple attackers. We formulate a novel multi-stage game model to characterize both the cooperative and competitive interactions of the data broker and attackers. The attackers' 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. The study contributes to the literature by exploring the behaviors of the attackers with labor specialization, and providing quantitative measures of information value from an economic perspective. The proposed frameworks characterize both the attackers' competitive equilibrium solutions and the data broker's pricing strategies under different market parameters. We also show how factors such as the quality of information, the heterogeneity in attackers' utilities, and their cooperative purchasing strategy would have an impact on the results.**

Index Terms—**Security, information market, game theory, economics.**

I. Introduction

TARGET information is undoubtedly a crucial factor of security problems in various attacks against critical infrastructures such as transportation and computer networks. Attackers conduct surveillance to gain awareness of targets' vulnerabilities and security operations, based on which to decide 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 have only little 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 immense demand for potential target information in hacker communities has spawned a *data brokers* industry [4]. The data brokers in crime society are specialists 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 social structure and to better understand the phenomenon of hacking. This knowledge would provide insights for arriving at effective solutions to information-leakage-induced security problems.

We consider one or multiple attackers that have limited observation capabilities on 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

Manuscript received June 18, 2020; revised December 30, 2020 and March 29, 2021; accepted April 4, 2021; approved by IEEE/ACM Transactions on Networking Editor R. La. Date of publication April 22, 2021; date of current version August 18, 2021. This work was supported in part by the National Science Foundation (NSF) under Grant CNS-2006998, Grant CNS-1837034, and Grant CNS-1745254. This article was presented in part at the EAI SecureComm 2019 Conference, Orlando, FL, USA. *(Corresponding author: Tao Shu.)*

Jing Hou, Li Sun, and Tao Shu are with the Department of Computer Science and Software Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: jzh0141@auburn.edu; lzs0070@auburn.edu; tshu@auburn.edu).

Husheng Li is with the Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville, TN 37996 USA (e-mail: hli31@utk.edu).

This article has supplementary downloadable material available at https://doi.org/10.1109/TNET.2021.3073273, provided by the authors.

Digital Object Identifier 10.1109/TNET.2021.3073273

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 (e.g., spectrum or other network resource utilization) and monopoly privileges (e.g., 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 increase the value of the data broker's information or decrease it. We also analyze an independent attacking scenario when the target is a type of "public good" and each successful attacker can obtain the whole target value regardless of other attackers' attacking behaviors. A comparison study is conducted between the competition and the independent scenario to better illustrate the impacts of the competition between attackers.

With the observation of the hierarchical and competitive structure in attacker behaviors, we present and study a multi-stage model of the information market. In Stage I, the data broker determines the information price. 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 a security problem with competing 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 about 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) For different attacker models (homogeneous/heterogeneous attackers), what are the conditions under which the attackers would benefit from the existence of the traded information? How does the value of information differ for different attackers? (d) 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 are more potential buyers rather than one? (e) How are the decisions affected when the data has lower quality (only partial information is available for trading)? Besides, we extend our model by taking the cooperative purchasing strategy into consideration, pertaining to two related questions: (f) when and how much do the attackers benefit from cooperative purchasing? (g) how does the cooperative purchasing strategy affect the risks of the target and the information price?

The problems are challenging due to the following two reasons. First, there is a 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 it? To the best of our knowledge, this is the first paper that tries to provide a unified quantitative framework of the security information market comprised of one data broker and multiple attackers. 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 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 analyses when a 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 buyer 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 models 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 profit-seeking hacker communities with labor specialization. Our results show how the traded information would benefit or hurt the attackers when they are competing and heterogeneous. We also show that in this information channel, information accuracy is more valuable for a more attractive target.
- Much previous work focuses on interactions between a defender and a single or multiple independent attackers, without consideration of the competition/cooperation among the attackers or the role of other players that assist in attacking. We incorporate the strategic interactions between multiple 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, and interestingly, the data broker might benefit from the competition between attackers. Besides, it is beneficial for the attackers to cooperate in purchasing only when the price is not high. We also show that, with the assistance of a data broker, the target suffers from higher risks even when the information price is too high to benefit the attackers. The risk is 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. Whether there is a strictly dominant pure-strategy is determined by the target value, the target vulnerability, and the information price. Furthermore, in the subgame-perfect Nash equilibrium where the strategies are mutual best responses [14], 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 II reviews the related literature. Section III introduces the model setups. In Section IV and V, we study the single attack model and the competition model, respectively. In Section VI, we provide an extension model with low information accuracy. Then cooperative purchasing is incorporated in Section VII. In Section VIII, we discuss the case of independent attackers. We extend our model to account for heterogeneous attackers in Section IX. The paper is concluded in Section X.

II. Related Work

Much of the research on security game has assumed that the attacker makes a 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 [15]. Realizing that this assumption rarely holds 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 [16] or imperfect observations [17]. Others have assumed that the target information gained by the attackers can be learned more accurately by conducting a period of surveillance [18], [19]. A more recent study which discusses the defender's strategic revelation of its commitment, further shows the importance of target information [20]. However, none of the above studies considers the possibility of purchasing information from a data broker in black markets. The value and the impacts of such an information service have hardly been addressed. Although there is already a study evaluating the value of customer information for the retailers in the consumer market [4], their results cannot be applied to the security problem because the target in the security problem may not be exclusive to the attackers as the set supply of merchandise is to the consumers.

Our paper focuses on the information market in the context of the hacker community. The 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, such as identifying the key actors [5], discovering the types of collaborative attack patterns [21] and 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 a coalition. Current studies assume that the attackers are heterogeneous with respect to non-task-specific efficiency, resource allocation, or skill sets, and a coalition is formed for more attacks or to gain higher total utility [22]–[24]. But the format of collusion with labor specialization, especially the information service, which is universal in the 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 determines their reward allocations. The answers to these questions are crucial to investigate why and how information service is provided in the hacker community, as well as when such a 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 the hacker society, this research takes 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 and/or cooperative attackers through a multi-stage game approach. The value of information is derived and the impacts of such information service are evaluated.

Part of the work has been presented at the EAI SecureComm 2019 conference, Orlando, FL. Compared to the conference version [25], this paper considers significantly extended models and provides more comprehensive numerical analysis with more insightful results, including the model of heterogeneous attackers, the incorporation of cooperative purchasing, the results with independent attackers, and more analyses on the value of traded information under different model setups.

III. System Model and Problem Formulation

We consider two attackers trying to attack one potential target. The attackers have limited ability to obtain the vulnerabilities (or the protection level set by 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 first sets a price for the information. Given the price, the attackers determine whether or not to make the purchase. Afterward (when the information has been revealed to the attackers), they need to decide whether to attack the target. All the players are profit-motivated. The notations used in the paper are given in Table I.

If an attacker successfully attacks the target, its expected reward is $v > 0$; otherwise, it receives a payoff of zero. The value of v (also called the target value), reflecting the target attractiveness to the attackers, is common knowledge to all the players. We restrict our model to the target resource whose 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, each gets a payoff 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 [26]. Note that it holds in two realistic scenarios: Firstly, one circumstance is a case where the 'first-winner-takes-all" [27]. That is,

TABLE I
LIST OF NOTATIONS

Notation	Explanation
v	Target value
e_i	Attacker i's attacking effort $(i, j \in \{A, B\})$
$C(\cdot)$	Attacking cost $(C(e) = e)$
θ	Target protection level (minimum attacking effort)
f_i	Attacker i's expected utility
p	Information price
q_i^{attack}	Attacker i's attacking probability
q_i^{buy}	Attacker i's information purchasing probability
π	Data broker's expected profit
u_i	Expected reward of a single successful attacker i
u_{ij}	Attacker i's expected reward with successful attackers i, j

the first attacker who mounts a successful attack receives the entire reward v, and the following attackers receive nothing. Considering the equal probability of being the first one to be successful, the expected reward of an attacker is $\frac{1}{2}v$ in a two-attacker case. Secondly, the target is assumed to be a quasi-public asset or display a negative network effect, whose value can diminish as more people use it. With the attackers being homogeneous, each attacker gets an equal share of the target value. This assumption of homogeneous attackers with equal share rule has been widely used in the security games literature ([26]–[28]). Apart from simplifying the analysis and exposition of our results, this model setup allows us to isolate the effect of the attacker heterogeneity and to highlight the effects of competition among attackers. We will relax these assumptions to analyze a more general case of heterogeneous attackers in Section IX.

We define the success of an attacker as follows: if the attacker's effort e in attacking is greater than or equal to 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 a successful attack. With a slight abuse of notation, let θ denotes the target protection level (from the other side: the target vulnerability) or the minimum attacking effort needed. A smaller value of θ indicates lower surveillance and thus less effort to launch a successful attack. Let us suppose the attackers only know the distribution of θ, which is uniformly distributed on $[0, 1]$ (normalized with respect to a sufficiently large upper bound that denotes the maximum possible defense capability of the defender). If an attacker's effort e is less than the actual value of θ, then it will fail. Note that our model focuses on the single-period attacking games where the attackers make one-shot decisions at the beginning with little information about the target vulnerability, and leaves out the multi-round attack problem where the information available to attackers could be updated from their observations in each round. As in [29], [30], and [31], for such a single-period attack game, the probability of a successful attack is assumed to be conditional on the attacker's strategic decision in terms of effort or investment allocation made before mounting the attack. This setup helps us to concentrate on the value of information acquired in black markets. The single-period framework can be justified by the fact that with the increasingly fierce confrontation in cyberspace, the process of cyber defense is typically characterized by rapid and frequent security patch upgrades, and as a result the effective lifespan of a fully disclosed vulnerability is short, shrinking the window of opportunity for the attacker [32], [33]. Therefore, in practice, there is often a small chance for multi-round attacks to take place, and the attack deployment decision can be made often only once. For example, a typical scenario that falls into this situation in practice is that after the first round of an attack, the vulnerability of the target being exploited by the attack is revealed to the defender, which will subsequently apply a security patch to fix that vulnerability, hence mitigating future rounds of the attack. The single-period setting also applies to the case where the duration of the target is short and hence it is impractical to mount multi-round attacks, such as eavesdropping on specific information that is transmitted once on a wireless network or jamming to disrupt a specific data transmission [33]. For those attacks that can be launched for multiple stages or rounds, our model applies to the first stage/round where little target information has been obtained, and the expected gain of a successful attack denotes the expected future gain for the next few rounds. While our model does not cover the cases of attackers' learning behaviors and advanced persistent threats, our model of profit-driven attackers purchasing information in black markets covers a significant fraction of realistic security concerns induced by information leakage.

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

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

Here $\mathbf{1}_{e \geq \theta}(e)$ is an indicator function, defined as: $\mathbf{1}_{e \geq \theta}(e) = 1$ if $e \geq \theta$, else $\mathbf{1}_{e \geq \theta}(e) = 0$. $C(e)$ is the attacking cost that 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 is 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 effort needed. In Section VI, 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 sells the data and what is the information value, 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. 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.

IV. Single Attacker Model

As a benchmark, we introduce the model where a monopolist attacker will extract all surplus from successfully attacking the target. Considering the sequential-move nature of the bargaining process between the attacker and the data broker, a two-stage Stackelberg game [14] is employed to analyze the decisions of the players. In practice, the data broker (the Stackelberg game leader) considers what the best response of the attacker (the follower) is (note that the follower's best response to an action of the leader is a piece of known information to the leader), i.e. whether it will buy the information once it has been informed of the price. The data broker then picks a price that maximizes its expected profit, anticipating the predicted response of the follower. The attacker actually observes this and in equilibrium makes an optimal purchasing decision as a response. The subgame-perfect Nash equilibrium, normally deduced by "backward induction" [14], is obtained in the following analysis. First, for a given information price, we derive the attacker's optimal purchasing and attacking decisions. Second, with the prediction of the attacker's response, the data broker's optimal price is analyzed.

A. Optimal Decisions of the Attacker

The attacker needs to make the decision of whether to buy the target information from a data broker, by comparing the two expected utilities as follows.

1) Not Buy Information: If the attacker does not buy the information from the data broker, its expected utility function with effort level e is

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

So the optimal solution is $e = 1$ with $f = v - 1$ if $v > 1$ and $e = 0$ with $f = 0$ if $v \leq 1$.

2) Buy Information: If the attacker decides to buy the information θ at price p and to attack the target, it would attack with exactly the effort θ.

Case 1: $v > 1$

The attacker would always attack since $\theta \leq v$ in this case, and its expected utility function is

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

Case 2: $v \leq 1$

Only when $\theta < v$ would it attack. Then we have

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

We can derive the attacker's optimal purchasing decision by comparing (3) and (4) with (2): When $v > 1$, if $v - \frac{1}{2} - p > v - 1$, or $p < \frac{1}{2}$, then the attacker would buy the information, otherwise it prefers not to buy the information. When $v \leq 1$, if $\frac{1}{2}v^2 - p > 0$ or $p < \frac{1}{2}v^2$, then the attacker would buy the information, otherwise it prefers not to buy the information. Fig. 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 an attack is profitable when $\theta < v$. In other words, the value of the information for the attacker is an expected utility increase of $v - \frac{1}{2} - p - (v - 1) = \frac{1}{2} - p$ if $v > 1$ and $p \leq \frac{1}{2}$ or $\frac{1}{2}v^2 - p$ if $v \leq 1$ and $p \leq \frac{1}{2}v^2$.

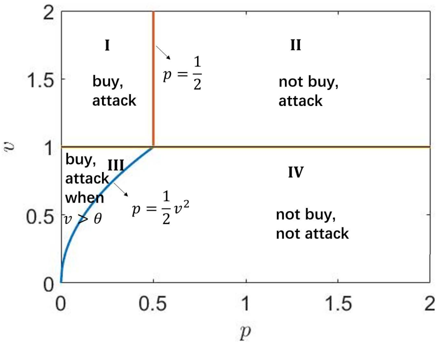


Fig. 1. The optimal decisions of single attacker.

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, it 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 in region III, which implies the importance of protecting the target information especially when the target value is not high for the attackers.

B. Optimal Pricing Decisions of the Data Broker

We assume that when the attackers are indifferent to whether to buy or 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. Therefore, the Stackelberg game equilibrium strategy of the data broker is given as follows:

$$p^* = \begin{cases} \dfrac{1}{2}v^2 & \text{if } v \leq 1, \\ \dfrac{1}{2} & \text{if } v > 1. \end{cases} \tag{5}$$

Under this price, the attacker's equilibrium strategy is to buy the information and mount the attack when $\theta < v$. The corresponding expected profit of the data broker, denoted as π, is $\frac{1}{2}v^2$ when $v \leq 1$ and $\frac{1}{2}$ when $v > 1$. We can see that the information value for the data broker increases with the target value until the target becomes attractive enough to the attacker that it would attack anyway even without the information.

V. Competition Model

In this section, we consider the scenario when there are two attackers (A and B) that could buy the same data of

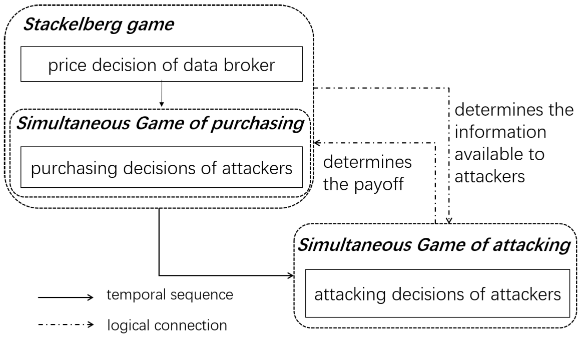

Stackelberg game
price decision of data broker
Simultaneous Game of purchasing
purchasing decisions of attackers
determines the payoff
determines the information available to attackers
Simultaneous Game of attacking
attacking decisions of attackers
temporal sequence
logical connection

Fig. 2. Hierarchical game structure.

TABLE II

PAYOFF TABLE FOR GAME OF ATTACKING WHEN NEITHER OF THE ATTACKERS HAS THE 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

TABLE III

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	$-p$, $v-\theta-p$	$-p$, $-p$

a target from the data broker. The attackers make decisions independently. Following the work of [4], we restrict our attention to the case where 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). The interactions between the data broker and two attackers are formulated in a three-stage hierarchical order of decision making, as shown in Fig. 2. Stage I: the data broker, as the leader in the Stackelberg game, sets the information price. Stage II: the attackers, as the followers, play a simultaneous game of purchasing. Stage III: the attackers make their attacking decisions with the information available when they play a simultaneous game of attacking. Similar to Section IV, We use backward induction to derive the equilibrium outcomes: 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.

A. Games of Attacking

For given purchasing decisions from two attackers, the attacking game is denoted by a tuple $\langle Q, S, U\rangle$. Set Q contains two players: {attacker A, attacker B}. Set S contains the strategies available to players: {attack, not attack} for each player. Set U contains the players' utility functions, which depend on the informational structure—that is, on which attackers purchase information. In the following analysis, we will characterize the solutions for the attacking game under different sets of purchasing decisions. We will use the solution concept of Nash equilibrium where no player can increase its own expected payoff by changing its strategy while the other player keeps its strategy unchanged.

1) Neither Buys Information: We first consider the situation when neither of the attackers decides 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.

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 $f_A(e_A) = \frac{1}{2}v\int_0^{e_A} d\theta - e_A = (\frac{1}{2}v-1)e_A$, 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, its optimal decision is $e = 1$ when $f = v-1$, and the other attacker has zero utility. The payoffs matrix of the game when neither of them has bought the information is illustrated in Table II (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 $f = \frac{1}{2}v-1$ for both attackers.

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 [34], in which the player assigns a positive probability to every pure strategy. We suppose attacker A chooses to attack w.p. q_A^{attack} and attacker B attacks w.p. q_B^{attack}. Then in mixed-strategy Nash equilibrium, $f_B(attack) = q_A^{attack}(\frac{1}{2}v-1)+(1-q_A^{attack})(v-1) = f_B(not\ attack) = 0$, and a similar equation holds for attacker A. Therefore, $q_A^{attack} = q_B^{attack} = 2\frac{v-1}{v}$, and the expected utility for both attackers is $f = (2\frac{v-1}{v})(2\frac{v-1}{v})(\frac{1}{2}v-1) + 2\frac{v-1}{v}(1-2\frac{v-1}{v})(v-1) = 0$.

Case 3: $v \leq 1$

By using a similar analysis as above, we can derive that the only strictly dominant pure strategy is (not attack, not attack) with utility $f = 0$ for both attackers.

2) 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 needed for a successful attack.

Case 1: $v > 2$

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

$$f = \int_0^1 (\frac{1}{2}v - \theta)d\theta - p = \frac{1}{2}v - \frac{1}{2} - p. \tag{6}$$

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 attacker attack, then it gets a utility of $v-\theta-p$, while the other one gets $-p$. Their payoffs for this game are listed in Table III. When $\frac{1}{2}v-\theta > 0$, the only pure-strategy Nash equilibrium is (attack, attack). When $\frac{1}{2}v-\theta \leq 0$, in mixed-strategy Nash equilibrium, we have $q_A^{attack} = q_B^{attack} = 2(1-\frac{\theta}{v})$, and the expected utility for both attackers is $-p$. Therefore, the expected utility of each

TABLE IV

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	$-p,\ v-1$	$-p,\ 0$

attacker is

$$f=\int_0^{\frac{1}{2}v}(\frac{1}{2}v-\theta)d\theta+\int_{\frac{1}{2}v}^1 0d\theta-p=\frac{1}{8}v^2-p. \qquad (7)$$

Case 3: $v\leq 1$

If $\theta\geq v$, neither of the attackers would attack. If $\theta<v$, the attacker gets a utility of $\frac{1}{2}v-\theta-p$ when both of them attack, and $v-\theta-p$ when only one attacker attacks. Therefore, the only pure-strategy Nash equilibrium is (attack, attack) when $\frac{1}{2}v-\theta>0$, and in mixed-strategy Nash equilibrium when $\frac{1}{2}v-\theta\leq 0$, the attacker would attack w.p. $q_A^{attack}=q_B^{attack}=2(1-\frac{\theta}{v})$ and have an expected utility of $-p$. To sum up, the expected utility of each attacker is $f=\frac{1}{8}v^2-p$.

3) Only One Attacker Buys Information: Without loss of generality, we consider the scenario where only attacker A buys the information. The payoffs for this game are listed in Table IV. It is important to note that attacker A's payoff function is its private information since the exact value of θ is not available to attacker B, and only its probability distribution is commonly known (with θ uniformly distributed on [0,1]). Therefore, the attacking game can be formulated as a Bayesian game with incomplete information [35]. We will analyze the Bayesian Nash equilibrium [35], where each attacker makes the decision to maximize its expected payoff. In this case, attacker A makes the decision after obtaining the value of θ from the data broker, while attacker B maximizes its expected payoff based on the distribution of θ.

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 $f_A=\frac{1}{2}v-p-\frac{1}{2}$ and $f_B=\frac{1}{2}v-1$.

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 greater than or equal to 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 would attack w.p. 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, $q_B^{attack}=0$. Because attacker B always chooses not to attack, attacker A would attack. To sum up, the expected utilities are: $f_A=v-p-\frac{1}{2}$, and $f_B=0$.

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, $f_A=\int_0^v(v-p-\theta)d\theta+\int_v^1(-p)d\theta=\frac{1}{2}v^2-p$, and $f_B=0$.

TABLE V

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	$0,\frac{1}{2}v^2-p$	$0,\ 0$

TABLE VI

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	$0,v-\frac{1}{2}-p$	$0,\ 0$

TABLE VII

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	$\frac{1}{2}v-1,\ \frac{1}{2}v-\frac{1}{2}-p$	$\frac{1}{2}v-1,\ \frac{1}{2}v-1$

B. Games of Purchasing

In the game of purchasing, the attackers decide whether to buy the information or not. Their joint strategies determine the specific payoff matrix of the attacking game to be played in the next stage. For example, if both attackers purchase the information, they will play the attacking game shown in Table III; if only one attacker makes the purchase, they will play the game in Table IV. Note that only the distribution of θ is known to both attackers before making their purchasing decisions. Therefore, the whole decision process of the attackers can be modeled as a stochastic game, in which there are multiple players and the next state of the game depends on the joint action of the players [36]. In this subsection, we will derive the Nash equilibrium of the purchasing game under different values of v, as shown in Tables V,VI, and VII, where the attackers' payoffs are their expected utilities based on the equilibrium of the corresponding attacking games determined by their purchasing strategies.

Case 1: $v\leq 1$

According to the payoffs in Table V, if $p<\frac{1}{8}v^2$, the only pure-strategy Nash equilibrium is (buy, buy). If $\frac{1}{8}v^2\leq p<\frac{1}{2}v^2$, there are two pure-strategy Nash equilibria: (buy, not buy) or (not buy, buy). In mixed strategy equilibrium, assume attacker A buys the information w.p. q_A^{buy} and attacker B buys w.p. 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 a similar equation holds for attacker A. Therefore, $q_A^{buy}=q_B^{buy}=\frac{\frac{1}{2}v^2-p}{\frac{3}{8}v^2}$, 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).

Case 2: $1<v\leq 2$

According to the payoffs in Table VI, 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 are two pure-strategy Nash equilibria (buy, not buy) or (not buy, buy). In mixed strategy equilibrium, we have $q_A^{buy}=q_B^{buy}=\frac{v-\frac{1}{2}-p}{v-\frac{1}{2}-\frac{1}{8}v^2}$. If $p\geq v-\frac{1}{2}$, the only pure-strategy Nash equilibrium is (not buy, not buy).

Case 3: $v>2$

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

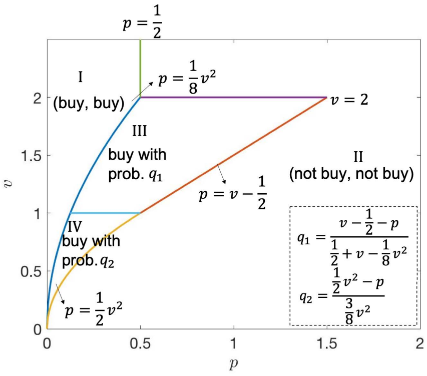


Fig. 3. Optimal purchasing decisions of two attackers.

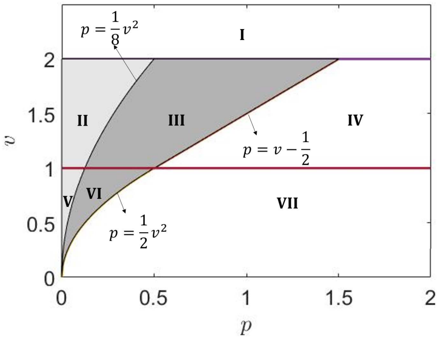


Fig. 4. Regions where attacking probability of the target is increased.

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).

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

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 w.p. $2\frac{v-1}{v}$, and when $v \leq 1$, no one attacks. While if the 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 result from the information trading. The light grey region is where the attacking probability is definitely increased since the price is low enough that both attackers buy the information. The dark grey region is where an increase in attacking probability is possible, which is determined by the attackers' purchasing behaviors. The increase in risks due to the information leakage and trading can be shown in Table VIII. The results imply that, when the value is highly attractive ($v \geq 2$), the attackers would launch the attack even without the information, and therefore the defender needs more defense effort; when $v < 2$, if the defender protects the information to the extent that the cost of acquiring and hence the price of information is high enough, the attack risk will not be increased, even if the information is leaked and traded.

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 an expected utility increase of $\frac{1}{2} - p$; if $v \leq 2$ and $p \leq \frac{1}{8}v^2$, there is an increase of $\frac{1}{8}v^2 - p$. Fig. 5(a) shows the value of traded information for the attacker, which increases with the target value and decreases with the price. 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 $p \leq \frac{1}{8}v^2$ for $v \leq 2$ or $p \leq \frac{1}{2}$ 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 & trading (in regions III and VI of Fig. 4).

TABLE VIII

ATTACKING PROBABILITY INCREASE WITH INFORMATION TRADING

Region	Attacking probability increase
I, IV, VII	0
II	$\min[\frac{2}{v} - 1, \frac{2}{v}(1 - \theta)]$
III	$\frac{2}{v}(1 - \theta)$ w.p. q_1^2, $\frac{2}{v} - 1$ w.p. $q_1(1 - q_1)$
V	$\min[1, 2(1 - \frac{\theta}{v})]$
VI	1 when $v > \theta$ w.p. $q_2(1 - q_2)$, $2(1 - \frac{\theta}{v})$ w.p. q_2^2

C. Optimal Pricing Decisions of the Data Broker

Now we further analyze the data broker's selling strategy in maximizing its profit. Intuitively, it could set either a low price such that both attackers buy or a high price that attackers buy with a certain probability. We show in Proposition 1 that its choice of pricing strategy depends on the attractiveness of the target.

Proposition 1: The Stackelberg game equilibrium strategies are determined by the target value for the attackers. When the target is not attractive enough, it is not wise for the data broker to set a price low enough to attract two buyers. Specifically, at the equilibrium:

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 w.p. 2/3;

b) else 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;

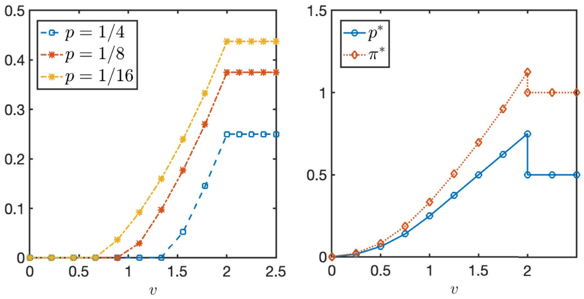
c) otherwise, both attackers buy the information at $p^* = \frac{1}{2}$.

Fig. 5(b) shows the data broker's optimal pricing strategy and corresponding expected profit π^*. It indicates that the information value for the broker, represented as its expected profit, increases with the target value when $v \leq 2$, but when the target is attractive enough for the attackers ($v > 2$), the information value decreases to a certain value and remains unchanged.

If we compare the data broker's expected profit in the single-attacker scenario with that in the multi-attacker scenario, we find that, counter-intuitively, the data broker does not always benefit from having more potential buyers due to the competition between the attackers. Specifically, if the target value is small ($v \leq 1.24$), the data broker is expected to earn more when there is only one potential buyer; while if the target value is large ($v > 1.24$), the information value is larger for the data broker when there are more attackers.

VI. EXTENSION: PARTIAL INFORMATION MODEL

We consider now the possibility that the data supplier can only obtain partial information about the target, i.e., whether



(a) For attacker (b) For data broker

Fig. 5. Value of traded information in competitive scenarios.

θ belongs to $[0, 0.5]$ or $[0.5, 1]$, but it cannot provide the exact value of θ. We analyze how this new informational structure affects the attackers' purchasing and attacking decisions and model the price of information with low data quality.

A. Games of Attacking

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

1) Neither Buys Information: When neither of the attackers buys the information, the equilibrium results are the same as those in Section V-A.

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

Case 1: $\theta \in [0, 0.5]$

If both of them attack, each obtains an expected utility of $f = \int_0^{0.5} \frac{1}{2}v * 2d\theta - \frac{1}{2} - p = \frac{1}{2}(v-1) - p$; else if only one attacks, then it obtains an expected utility of $f = \int_0^{0.5} v * 2d\theta - \frac{1}{2} - p = v - \frac{1}{2} - p$. Therefore, if $v > 1$, both of them would attack; if $\frac{1}{2} < v \leq 1$, the attacker would attack w.p. $q_A^{attack} = q_B^{attack} = \frac{2v-1}{v}$, and the expected utility for both attackers is $-p$; otherwise, neither would attack.

Case 2: $\theta \in [0.5, 1]$

If both of them attack, each obtains an expected utility of $f = \frac{1}{2}v - 1 - p$; else if only one attacks, then it obtains an expected utility of $f = v - 1 - p$. Therefore, if $v > 2$, both of them would attack; if $1 < v \leq 2$, $q_A^{attack} = q_B^{attack} = 2\frac{v-1}{v}$, and the expected utility for both attackers is $-p$; otherwise, neither would 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 buy the information is: $f = \frac{1}{2}(\frac{1}{2}(v-1)-p)+\frac{1}{2}(\frac{1}{2}v-1-p) = \frac{1}{2}v - \frac{3}{4} - p$ if $v > 2$, $f = \frac{1}{4}(v-1) - p$ if $1 < v \leq 2$, and $f = -p$ if $v \leq 1$.

3) Only One Attacker Buys Information: For attacker B who does not buy the information, if both attackers attack, it is expecting a utility of $\frac{1}{2}v - 1$; if it attacks but attacker A does not attack, its expected utility is $v - 1$.

Therefore, if $v > 2$, attacker B decides to attack. In this case, if attacker A gets that $\theta \in [0, 0.5]$, it would also attack, resulting an expected utility of $\frac{1}{2}v - \frac{1}{2} - p$, and if A gets that $\theta \in [0.5, 1]$, it would attack with an expected utility of $\frac{1}{2}v - 1 - p$. We thus have $f_A = \frac{1}{2}(\frac{1}{2}v - \frac{1}{2} - p) + \frac{1}{2}(\frac{1}{2}v - 1 - p) = \frac{1}{2}v - \frac{3}{4} - p$ and $f_B = \frac{1}{2}v - 1$. If $1 < v \leq 2$, attacker B knows that when $\theta \in [0, 0.5]$, attacker A would certainly attack, i.e., there is a higher probability that attacker A attacks. Therefore, attacker B would choose not to attack. Expecting this result, attacker A chooses to attack. We thus have $f_A = \frac{1}{2}(v - \frac{1}{2} - p) + \frac{1}{2}(v - 1 - p) = v - \frac{3}{4} - p$ and $f_B = 0$. If $v \leq 1$, attacker B decides not to attack. In this case, if attacker A gets that $\theta \in [0, 0.5]$, it would only attack when $v > \frac{1}{2}$, and if A gets that $\theta \in [0.5, 1]$, it would not attack. Therefore, we have $f_A = \frac{1}{4}v - \frac{1}{4} - p$ if $\frac{1}{2} < v \leq 1$, $f_A = 0$ if $v \leq \frac{1}{2}$ and $f_B = 0$.

TABLE IX

PAYOFF TABLE FOR GAME OF PURCHASING WHEN $\frac{1}{2} < v \leq 1$ UNDER PARTIAL INFORMATION

	buy	not buy
buy	$-p$, $-p$	$\frac{1}{4}v - \frac{1}{4} - p$, 0
not buy	0, $\frac{1}{4}v - \frac{1}{4} - p$	0, 0

TABLE X

PAYOFF TABLE FOR GAME OF PURCHASING WHEN $1 < v \leq 2$ UNDER PARTIAL INFORMATION

	buy	not buy
buy	$\frac{1}{4}v - \frac{1}{4} - p$, $\frac{1}{4}v - \frac{1}{4} - p$	$v - \frac{3}{4} - p$, 0
not buy	0, $v - \frac{3}{4} - p$	0, 0

TABLE XI

PAYOFF TABLE FOR GAME OF PURCHASING WHEN $v > 2$ UNDER PARTIAL INFORMATION

	buy	not buy
buy	$\frac{1}{2}v - \frac{3}{4} - p$, $\frac{1}{2}v - \frac{3}{4} - p$	$\frac{1}{2}v - \frac{3}{4} - p$, $\frac{1}{2}v - 1$
not buy	$\frac{1}{2}v - 1$, $\frac{1}{2}v - \frac{3}{4} - p$	$\frac{1}{2}v - 1$, $\frac{1}{2}v - 1$

B. Games of Purchasing

From the equilibrium analysis above, we know that if $v < \frac{1}{2}$, neither attacker would attack and therefore has no incentive to buy the information. Besides, the following three cases are considered according to different values of v. Tables IX, X and XI list the payoffs of two attackers in the game of purchasing.

Case 1: $\frac{1}{2} < v \leq 1$

The only equilibrium is (not buy, not buy).

Case 2: $1 < v \leq 2$

If $\frac{1}{4}v - \frac{1}{4} - p \geq 0$, both attackers would buy; if $\frac{1}{4}v - \frac{1}{4} - p < 0$ and $v - \frac{3}{4} - p > 0$, in mixed strategy equilibrium, $q_A^{buy} = q_B^{buy} = \frac{v - \frac{3}{4} - p}{\frac{3}{4}v - \frac{1}{2}}$; else if $\frac{1}{4}v - \frac{1}{4} - p < 0$ and $v - \frac{3}{4} - p < 0$, neither attacker decides to buy the information.

Case 3: $v > 2$

If $\frac{1}{2}v - \frac{3}{4} - p \geq \frac{1}{2}v - 1$, both attackers would buy; else, neither of the attackers buys the information.

Fig. 6 plots the attackers' optimal purchasing decisions of partial information in different ranges of v and p. The impact of partial information trading on 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 attack.

As for the value of partial information to the attackers, when $v > 2$ and $p < \frac{1}{4}$, there is an 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 increased by $\frac{1}{4}v - \frac{1}{4} - p$, as illustrated

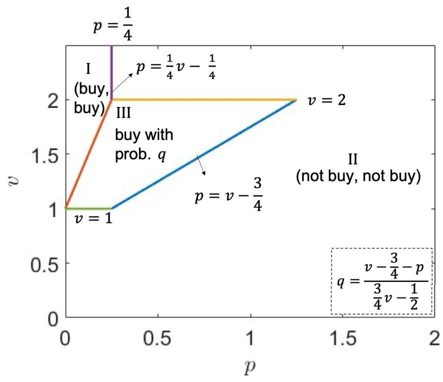
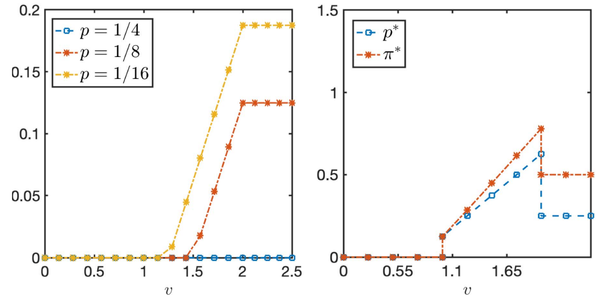


Fig. 6. Attackers' optimal purchasing decisions under partial information.



(a) For attacker (b) For data broker

Fig. 7. Value of traded information with partial information.

in Fig. 7(a). Moreover, by comparing Fig. 3 and Fig. 6, we see that, for a lower-value target ($v < 1$), if the defender takes some effort to ensure that only partial information could be leaked, the attacking probability may decrease to zero.

C. 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, we have:

Proposition 2: In Stackelberg game equilibrium under partial information, the strategies of the players are:

a) if $v \leq 1$, the attackers would not buy the information at any price;

b) else 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;

c) otherwise, both attackers buy the information at $p^* = \frac{1}{4}$.

One can now compare the results (shown in Fig. 7(b)) under partial information with those under full information. We could find that 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.

VII. Extension: Cooperative Purchasing

In this section, we are considering the cooperation between two attackers. Since the information can be reproduced with a negligible marginal cost, it is possible for two buyers to share the purchasing cost by sharing a copy of the data. We will call the process cooperative purchasing where two attackers only pay a total price p to the broker and share the information.

Naturally, there are several questions when cooperative purchasing behavior is of concern: (1) when would the attackers engage in cooperative purchasing? (2) how much will the attackers benefit from the cooperation? (3) will cooperative purchasing increase the risks of the target? and (4) if the data broker takes the possibility of cooperation between buyers into consideration, how would it set the price?

TABLE XII

Payoff Table for Game of Attacking Under Cooperative Purchasing

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

The new timeline of the process is: after the data broker announces the price, the attackers first decide whether to engage in cooperative purchasing. If not, each attacker will decide whether or not to buy the information by itself. Then with the information available, the attackers decide how much effort will be taken in attacking. The corresponding utilities are gained after the attack. We first analyze the attackers' attacking decisions after cooperative purchasing, and then compare the expected utilities with those in Section V to figure out when it is beneficial for them to cooperate; finally, the optimal price is derived for the data broker.

The payoffs for the game of attacking when they buy information cooperatively are listed in Table XII. It is straightforward to derive that when $v > 2$, the only strictly dominant pure strategy is (attack, attack) with an expected profit of $f = \frac{1}{2}(v-1-p)$ for each attacker; when $v \leq 2$, we have $q_A^{attack} = q_B^{attack} = \min[2(1-\frac{\theta}{v}), 1]$, with $f = \frac{1}{8}v^2 - \frac{1}{2}p$.

By comparing the expected profits with those obtained without cooperative purchasing, it is found that cooperative purchasing benefits the attackers only when the information price is lower than $\min[1, \frac{1}{4}v^2]$. We summarize the attackers optimal purchasing decisions in Fig. 8, which shows that the attackers engage in cooperative purchasing only in region I, and the attacker buys the information w.p. $q_A^{buy} = q_B^{buy} = \frac{v-\frac{1}{2}-p}{v-\frac{1}{2}-\frac{1}{8}v^2}$ in region II. The expected profit of an attacker is

$$f = \begin{cases} \dfrac{1}{2}(v-1-p) & \text{if } v > 2 \\ \dfrac{1}{8}v^2 - \dfrac{1}{2}p & \text{if } v \leq 2 \ \&\ p < \dfrac{1}{8}v^2 \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

The benefit, defined as the expected utility improvement through cooperative purchasing, can be derived as

$$\Delta f = \begin{cases} \dfrac{1}{2}p & \text{if } v > 2 \ \&\ p < \dfrac{1}{2} \text{ or } v \leq 2 \ \&\ p < \dfrac{1}{8}v^2 \\ \dfrac{1}{2} - \dfrac{1}{2}p & \text{if } v > 2 \ \&\ \dfrac{1}{2} < p < 1 \\ \dfrac{1}{8}v^2 - \dfrac{1}{2}p & \text{if } v \leq 2 \ \&\ p < \dfrac{1}{8}v^2. \end{cases} \tag{9}$$

The results indicate that, only when the price is not high ($p < \frac{1}{4}v^2$ for $v \leq 2$, and $p < 1$ for $v > 2$), it is beneficial for the attackers to cooperate. We can also see a potential increase in the attacking probability resulted from cooperative purchasing when $1 < v \leq 2$ and $\frac{1}{8}v^2 < p < \frac{1}{4}v^2$: an increase of $\min[1, 2(1-\frac{\theta}{v})] - 2(1-\frac{1}{v})$ w.p. $(1-q_A)^2$.

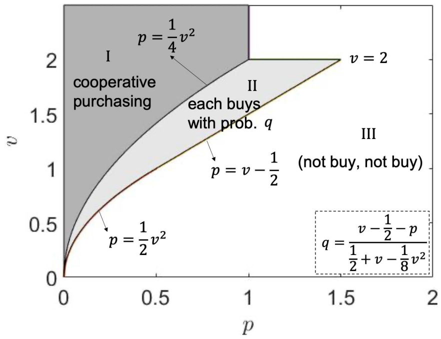


Fig. 8. Optimal decisions of competing attackers under cooperative purchasing.

Taking the changes in the attackers' purchasing behaviors into consideration, the data broker's optimal price is:

Proposition 3: In Stackelberg game equilibrium with the consideration of cooperative purchasing, the data broker's optimal price of the target information is given as:

$$p^* = \begin{cases} \frac{1}{4}v^2 & \text{if } v \leq 2, \\ 1 & \text{if } v > 2. \end{cases} \tag{10}$$

At this price, the attackers always engage in cooperative purchasing.

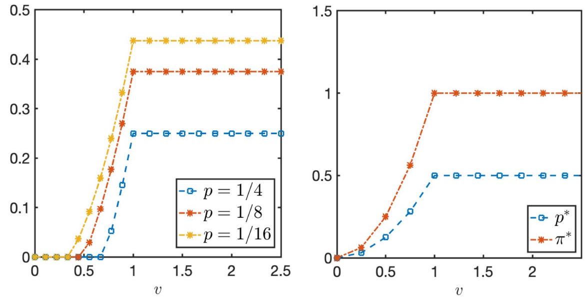
Proposition 3 indicates that the data broker enhances its price when the target value is large ($v > 1$) if cooperative purchasing is considered. However, the data broker's expected profit gets decreased a little bit when the target value $v \leq 2$ due to the cooperative purchasing.

VIII. Alternative Setup: Independent Model

In this section, we consider the case where the attackers do not compete for the target value, i.e., each successful attacker receives a utility v in the case of multiple attackers instead of splitting the target value. This is referred to as the independent attack scenario in the following analysis. This assumption is suitable for the situation when the target is a type of "public good" that is non-rival (i.e., the consumption by one agent does not reduce consumption by others) [13]. We first analyze the optimal decisions of the attackers and the data broker; then a comparison between the results with those in Section V is made in order to investigate the impacts of competition.

Since there is no competition between the attackers, the model reduces to a standard Stackelberg game between the data broker and the attackers, with no simultaneous game between the attackers. In Section IV, we have derived that a single attacker would buy the information if the target value is high that $v > 1$ and the price satisfies $p \leq \frac{1}{2}$, or if $v < 1$ and $p \leq \frac{1}{2}v^2$. When there are two attackers, their purchasing and attacking decisions are the same as shown in Fig. 1. The value of information for the attacker is illustrated in Fig. 9(a). If we compare the results above with those of the competition model in Section V, we conclude that, under the same target value and information price, it is less likely for the attackers to make the purchase in the competitive scenario. This result is consistent with our intuition and implies that the value of information for the attackers is weakened by their competition.

Similarly, the data broker's optimal price is $p^* = \frac{1}{2}v^2$ if $v \leq 1$, and $p^* = \frac{1}{2}$ if $v > 1$, as shown in Fig. 9(b).



(a) For attacker

(b) For data broker

Fig. 9. Value of information in independent scenarios.

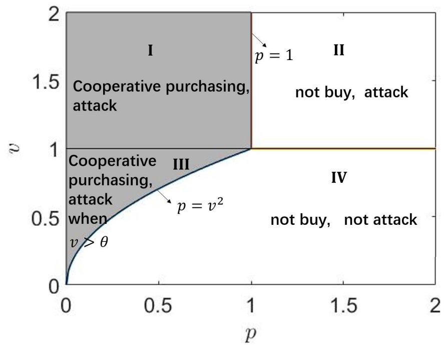


Fig. 10. Optimal decisions of independent attackers under cooperative purchasing.

A comparison of the results with those in Fig. 5(b) shows us some interesting observations: first, when $v \leq 1.5$, the price is lower in a competitive scenario than in a independent scenario since the data broker needs to improve sales; while when $1.5 < v \leq 2$, the price is higher in competitive scenario for larger marginal profit; and when $v > 2$, the price is the same for both competitive and independent scenario since both attackers would buy the information as long as $p \leq \frac{1}{2}$. The data broker's corresponding expected profit for a two-attacker case without competition is v^2 if $v \leq 1$ and 1 if $v > 1$. Interestingly, the data broker benefits from the competition between attackers if $1.86 < v \leq 2$, when the optimal price in the independent scenario is much higher than that in the competitive scenario.

If we take cooperative purchasing into consideration, Fig. 10 shows the attackers' optimal decisions under different values of p and v. Compared with the results shown in Fig. 8 of the competitive scenario, cooperative purchasing benefits the attackers in more cases related to different values of p and v in the independent scenario. The phenomenon can be explained as follows: intuitively, it is always beneficial to reduce purchasing cost when there is no competition in attacking; however, in the competitive scenario, the attackers face a risk of having to split the target value under cooperative purchasing. Therefore the final purchasing decision needs to be made by considering the trade-off between less purchasing cost and the increased competitive risk.

IX. Extension: Heterogeneous Attackers

In this section, we discuss the robustness of our insights to an alternative modeling assumption, where the heterogeneous attackers do not split the target value but their utilities could be compromised by their competition. Specifically, attackers

TABLE XIII

PAYOFF TABLE FOR GAME OF ATTACKING WITH HETEROGENEOUS ATTACKERS WHEN ONLY ATTACKER A BUYS INFORMATION

	attack	not attack
attack	$u_{AB} - \theta - p,\ u_{BA} - 1$	$u_A - \theta - p,\ 0$
not attack	$-p,\ u_B - 1$	$-p,\ 0$

A and B are heterogeneous in that the benefits they derive from the same target could be different.

We denote the expected reward of attacker i as $u_i(v)$ if only i successfully attacks the target with a value of v, and $u_{ij}(v)$ if both attackers succeed ($i, j \in \{A, B\}$), where $u_{ij}(v) \leq u_i(v)$, $u_A(v) \neq u_B(v)$ and $u_{AB}(v) \neq u_{BA}(v)$. The equilibrium solutions of the game are determined by all the values of u_i and u_{ij} ($i, j \in \{A, B\}$). The game analysis process is similar to that for homogeneous attackers but the analytical solutions include a larger number of cases. Due to the page limit, we present one representative case to illustrate each game and briefly discuss the impacts of the attacker heterogeneity on the equilibrium results. In our numerical example, we investigate a situation involving a high-profit attacker and a low-profit attacker and examine how each player would benefit from the information trading.

A. Games of Attacking

In the games of attacking, considering whether each value of u_i and u_{ij} is larger than 1 (the largest value of θ), we will have 9 cases. Next we take a nontrivial case as an example where $u_A(v) > 1$, $u_B(v) > 1$, $u_{AB}(v) < 1$, $u_{BA}(v) < 1$ and present the following equilibrium results.

1) Neither Buys Information: When nobody buys the information, attacker i would attack w.p. $q_i^{attack} = \frac{u_i - 1}{u_i - u_{ij}}$ ($i, j \in A, B$), and the expected utility is 0 for both attackers.

2) Both Buy Information: Attacker i will launch the attack when $u_{ij} > \theta$. If both u_{AB} and u_{BA} are smaller than θ, then attacker i would attack w.p. $q_i^{attack} = \frac{u_i - \theta}{u_i - u_{ij}}$.

3) Only One Attacker Buys Information: This is a game with asymmetric information. When only attacker A buys the information, the payoffs are listed in Table XIII. We can derive that, if $\Delta_1 = u_{AB}(u_{BA} - u_B) + (u_B - 1) > 0$, then $q_B^{attack} = 1$, and $f_A = \frac{1}{2}u_{AB}^2 - p$, $f_B = \Delta_1$. Else if $\Delta_1 \leq 0$, then $q_B^{attack} = 0$ and $q_A^{attack} = Prob(u_A > \theta) = 1$, $f_A = u_A - \frac{1}{2} - p$, $f_B = 0$. The detailed analysis is provided in the supplementary materials. Similarly, when only attacker B buys the information, if $\Delta_2 = u_{BA}(u_{AB} - u_A) + (u_A - 1) > 0$, then $q_A^{attack} = 1$, and $f_B = \frac{1}{2}u_{BA}^2 - p$, $f_A = \Delta_2$. Else if $\Delta_2 \leq 0$, then $q_A^{attack} = 0$ and $q_B^{attack} = 1$, $f_B = u_B - \frac{1}{2} - p$, $f_A = 0$.

B. Games of Purchasing

Based on the equilibrium results above, we have four cases in games of purchasing depending on the values of Δ_1, Δ_2: ($\Delta_1 \leq 0$, $\Delta_2 > 0$), ($\Delta_1 > 0$, $\Delta_2 \leq 0$), ($\Delta_1 \leq 0$, $\Delta_2 \leq 0$), and ($\Delta_1 > 0$, $\Delta_2 > 0$). Suppose $u_{AB} \leq u_{BA}$ without loss of generality, Table XIV lists the payoffs for the case of ($\Delta_1 \leq 0$, $\Delta_2 \leq 0$) as an example.

According to Table XIV, if $(\frac{1}{2}u_{AB}^2 - p)(u_A - \frac{1}{2} - p) < 0$ and $(T - p)(u_B - \frac{1}{2} - p) < 0$, attacker A chooses to buy w.p. $q_A^{buy} = \frac{u_A - \frac{1}{2} - p}{u_A - \frac{1}{2} - \frac{1}{2}u_{AB}^2}$, and attacker B buys w.p. $q_B^{buy} = \frac{u_B - \frac{1}{2} - p}{u_B - \frac{1}{2} - T}$. Otherwise, there is only one pure-strategy Nash equilibrium.

TABLE XIV

PAYOFF TABLE FOR GAME OF ATTACKING WITH HETEROGENEOUS ATTACKERS WHEN $\Delta_1 \leq 0$, $\Delta_2 \leq 0$ AND $u_{AB} \leq u_{BA}$ ($T = u_{BA}u_{AB} + u_B(u_{BA} - u_{AB}) - \frac{1}{2}u_{BA}^2$)

	buy	not buy
buy	$\frac{1}{2}u_{AB}^2 - p,\ T - p$	$u_A - \frac{1}{2} - p,\ 0$
not buy	$0,\ u_B - \frac{1}{2} - p$	$0,\ 0$

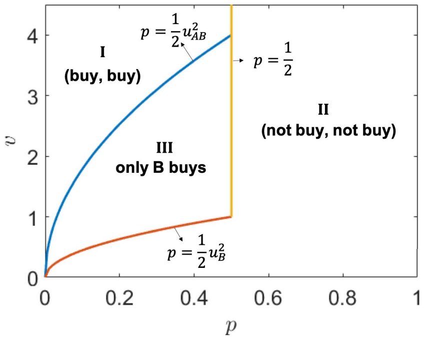


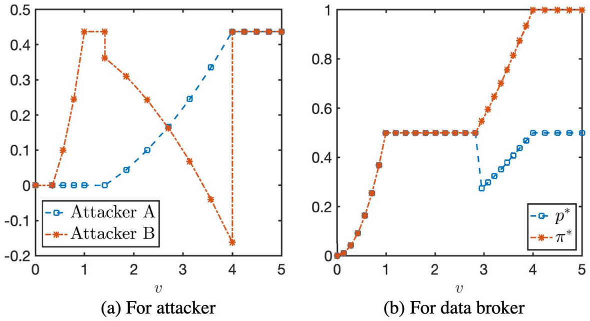
Fig. 11. Optimal purchasing decisions of heterogeneous attackers.

As an illustration purpose, we consider attacker B to be able to benefit more from attacking the target than attacker A. Fig. 11 shows the equilibrium purchasing decisions when $u_A = 0.7v$, $u_B = v$, $u_{AB} = 0.25v$, and $u_{BA} = 0.85v$. Our results show that if the price is low enough (in region I, $p < \frac{1}{2}u_{AB}^2$), both attackers purchase the information. The risk of the target, in terms of the attacking volume, is increased by the information trading in both regions I and III under some conditions ($u_B > \theta$ if $v < 1$, $u_{AB} > \theta$ otherwise). These observations are consistent with those in our base model.

We compare the results with those shown in Fig. 3 and find that attacker B, the high-profit attacker, has more tendency to buy the information than attacker A. In region III, only attacker B buys the information. An intuitive explanation is: the target is less attractive and therefore the information is of less value to attacker A who lacks the incentive to engage in information trading. Besides, Fig. 12(a) plots the value of traded information for the attackers under different target value when $p = \frac{1}{16}$. It is interesting to find that: If the target value is small ($v < 1.414$), only attacker B benefits from the traded information since the marginal gain for attacker A is too low to make the purchase. As the target value increases, attacker A benefits more from the information, while attacker B benefits less in the range of $1.414 \leq v < 4$. If $2.697 \leq v < 4$, the existence of the traded information even hurts attacker B. This is because attacker A is more likely to mount the attack with the traded information, resulting in the competition between the attackers and therefore a decrease in attacker B's expected utility. If the target value is large enough ($v \geq 4$), both attackers benefit from the traded information since they would launch attacks even without the information.

C. Optimal Pricing Decisions of the Data Broker

The changes in the attackers' purchasing behaviors lead to a different pricing policy of the data broker, as illustrated in Fig. 12(b). In the example, if $v \leq 1$, information is sold at



(a) For attacker

(b) For data broker

Fig. 12. Value of traded information with heterogeneous attackers.

$p^* = \frac{1}{2}v^2$; if $1 < v \leq 2.828$ (when $u_{AB}^2 < 0.5$), $p^* = 0.5$; else, $p^* = \frac{1}{2}u_{AB}^2$. It is seen that, when v is large enough that $u_{AB}^2 > 0.5$, the data broker lowers the price in order to attract both attackers; otherwise, the data broker tends to win only the higher-profit attacker. Similar to the case of homogeneous attackers, the data broker benefits from having more potential buyers if the target value is large ($v > 2.828$).

As for the impact of competition on the optimal price, one can notice that, if the target value is not small ($2.828 < v < 4$), the attackers benefit from their competition in terms of having a lower information price set by the data broker to attract both attackers; while if $v < 1.428$, attacker A would face a higher price due to the competition because attacker B could accept a higher price than attacker A. This result is different from our base model, where the competition decreases the price for the low-value target ($v < 1.5$) and increases it for the high-value target ($1.5 < v < 2$). That being said, the impact of attackers' competition on the information price is complicated by several factors including both the attackers' heterogeneity and the target value.

X. 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. 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 into 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 might benefit from their competition under some conditions. However, the data broker does not always benefit from having more potential buyers considering the competition between the attackers, especially when cooperative purchasing is expected under a low target value. In the case of heterogeneous attackers, the data broker prefers to set a high price to attract only the high-profit attacker when the target value is not high. Besides, information accuracy is more valuable of a more attractive target for the attackers and the data broker. 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 future research directions are worth exploring. First, as an application of the model proposed in this paper, it will be worthwhile to investigate a specific type of attack (e.g. eavesdropping, spoofing, or denial of service) and evaluate the value of a specific type of security information (e.g. users' activity data) to be traded in a black market. Second, the situation where the data broker does not reveal its total sales quantity is a problem that the attackers may encounter. Therefore, another direction is to extend the game model between the attackers to account for incomplete information. Third, one implicit assumption in our model is that the data broker charges attackers the same price for the information. For heterogeneous attackers, it is instructive to consider the selling strategy of price discrimination and characterize the conditions under which price discrimination is profitable. Another important future research direction is to take collaborative attack or combined efforts of attackers into consideration. In this situation, one can incorporate cooperative game theory to study how the attackers coordinate their efforts and share their joint payoff and investigate how their collaborative behaviors could have an impact on the information value.

Acknowledgment

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] B. An, M. Brown, Y. Vorobeychik, and M. Tambe, "Security games with surveillance cost and optimal timing of attack execution," in *Proc. AAMAS*, 2013, pp. 223–230.

[2] E. Southers and M. Tambe, "Lax-terror target: The history, the reason, the countermeasure," in *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. New York, NY, USA: Cambridge Univ. Press, 2011, pp. 27–50.

[3] J. Pita, M. Jain, M. Tambe, F. Ordóñez, and S. Kraus, "Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition," *Artif. Intell.*, vol. 174, no. 15, pp. 1142–1171, Oct. 2010.

[4] R. Montes, W. Sand-Zantman, and T. Valletti, "The value of personal information in online markets with endogenous privacy," *Manage. Sci.*, vol. 65, no. 3, pp. 1342–1362, Mar. 2019.

[5] V. Benjamin and H. Chen, "Securing cyberspace: Identifying key actors in hacker communities," in *Proc. IEEE Int. Conf. Intell. Secur. Informat.*, Jun. 2012, pp. 24–29.

[6] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, "An analysis of underground forums," in *Proc. ACM SIGCOMM Conf. Internet Meas. Conf. (IMC)*, 2011, pp. 71–80.

[7] P. Pierluigi. *Hacking Communities in the Deep Web*. Accessed: Apr. 5, 2019. [Online]. Available: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-%web/#gref

[8] L. Selena. *The Hacks That Left us Exposed in 2017*. Accessed: Apr. 5, 2019. [Online]. Available: https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the%-year/index.html

[9] K. Makena. *Facebook Could Reportedly Face Multibillion-Dollar FTC Fine Over Privacy Violations*. Accessed: Apr. 5, 2019. [Online]. Available: https://www.theverge.com/2019/2/14/18225440/facebook-multibillion-dolla%r-ftc-fine-privacy-violations

[10] *Cyber Crime: Concepts, Methodologies, Tools and Applications*. Hershey, PA, USA: IGI Global, 2011.

[11] Q. Zhu and S. Rass, "On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats," *IEEE Access*, vol. 6, pp. 13958–13971, 2018.

[12] P. T. Leeson and C. J. Coyne, "The economics of computer hacking," *JL Econ. Pol'y*, vol. 1, pp. 511–532, Dec. 2005.

[13] K. Hausken and V. M. Bier, "Defending against multiple different attackers," *Eur. J. Oper. Res.*, vol. 211, no. 2, pp. 370–384, Jun. 2011.

[14] R. S. Gibbons, *Game Theory for Applied Economists*. Princeton, NJ, USA: Princeton Univ. Press, 1992.

[15] 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," *J. Artif. Intell. Res.*, vol. 41, pp. 297–327, Jun. 2011.

[16] F. Fang, P. Stone, and M. Tambe, "When security games go green: Designing defender strategies to prevent poaching and illegal fishing," in *Proc. 24th Int. Joint Conf. Artif. Intell.*, 2015, pp. 1–9.

[17] E. van Damme and S. Hurkens, "Games with imperfectly observable commitment," *Games Econ. Behav.*, vol. 21, nos. 1–2, pp. 282–308, Oct. 1997.

[18] B. An *et al.*, "Security games with limited surveillance," in *Proc. 26th AAAI Conf. Artif. Intell.*, 2012, pp. 1–8.

[19] J. Zhuang, V. M. Bier, and O. Alagoz, "Modeling secrecy and deception in a multiple-period attacker–defender signaling game," *Eur. J. Oper. Res.*, vol. 203, no. 2, pp. 409–418, Jun. 2010.

[20] Q. Guo, B. An, B. Bošanský, and C. Kiekintveld, "Comparing strategic secrecy and Stackelberg commitment in security games," in *Proc. 26th Int. Joint Conf. Artif. Intell.*, Aug. 2017, pp. 3691–3699.

[21] H. Du and S. J. Yang, "Discovering collaborative cyber attack patterns using social network analysis," in *Proc. Int. Conf. Social Comput., Behav.-Cultural Modeling, Predict.* Berlin, Germany: Springer, 2011, pp. 129–136.

[22] Q. Guo, B. An, Y. Vorobeychik, L. Tran-Thanh, J. Gan, and C. Miao, "Coalitional security games," in *Proc. AAMAS*, 2016, pp. 159–167.

[23] S. Gholami, B. Wilder, M. Brown, D. Thomas, N. Sintov, and M. Tambe, "Divide to defend: Collusive security games," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2016, pp. 272–293.

[24] A. Roy, C. A. Kamhoua, and P. Mohapatra, "Game theoretic characterization of collusive behavior among attackers," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2018, pp. 2078–2086.

[25] J. Hou, L. Sun, T. Shu, and H. Li, "Target information trading-an economic perspective of security," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Cham, Switzerland: Springer, 2019, pp. 126–145.

[26] D. Florêncio and C. Herley, "Where do all the attacks go," in *Economics of Information Security and Privacy III*. New York, NY, USA: Springer, 2013, pp. 13–33.

[27] D. Pym, J. Swierzbinski, and J. Williams, "The need for public policy interventions in information security," Univ. Aberdeen, Aberdeen, U.K., Working Paper, 2013. Accessed: Apr. 16, 2021. [Online]. Available: http://aura.abdn.ac.uk/bitstream/2164/2966/1/10007783_Swierzbinski_15786328_20131010.pdf

[28] C. Ioannidis, D. Pym, and J. Williams, "Sustainability in information stewardship: Time preferences, externalities, and social co-ordination," *RN*, vol. 14, p. 15, Dec. 2014.

[29] M. Cremonini and D. Nizovtsev, "Risks and benefits of signaling information system characteristics to strategic attackers," *J. Manage. Inf. Syst.*, vol. 26, no. 3, pp. 241–274, Dec. 2009.

[30] A. Yolmeh and M. Baykal-Gürsoy, "Two-stage invest–defend game: Balancing strategic and operational decisions," *Decis. Anal.*, vol. 16, no. 1, pp. 46–66, Mar. 2019.

[31] G. Kuper, F. Massacci, W. Shim, and J. Williams, "Who should pay for interdependent risk? Policy implications for security interdependence among airports," *Risk Anal.*, vol. 40, no. 5, pp. 1001–1019, May 2020.

[32] T. Li, J.-D. Wang, Y. Chen, and N. Wang, "A multi-stage game approach applied to network security risk controlling," in *Proc. IEEE 2nd Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Mar. 2017, pp. 2518–2522.

[33] S. Mitra and S. Ransbotham, "Information disclosure and the diffusion of information security attacks," *Inf. Syst. Res.*, vol. 26, no. 3, pp. 565–584, Sep. 2015.

[34] M. Dresher, "Games of strategy: Theory and applications," Rand Corp Santa Monica, Santa Monica, CA, USA, Tech. Rep. RAND/CB-149-1, 1961. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA473407.pdf

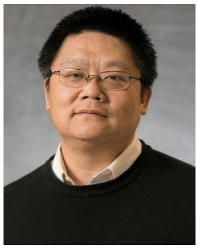
[35] J. Levin. (2020). *Games of Incomplete Information*. [Online]. Available: http://web.stanford.edu/jdlevin/Econ

[36] M. Bowling and M. Veloso, "An analysis of stochastic game theory for multiagent reinforcement learning," Pittsburgh Pa School Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-CS-00-165, 2000. [Online]. Available: https://tardir/tiffs/a385122.tiff(dtic.mil)

Jing Hou received the B.S. degree in computing science from Nanjing Tech University, Nanjing, China, in 2004, and the Ph.D. degree in systems engineering from Southeast University, Nanjing, in 2011. She is currently pursuing the Ph.D. degree with the Department of Computer Science and Software Engineering, Auburn University. Her research interests include wireless communications and network economics.

Li Sun received the M.S. and Ph.D. degrees in systems engineering from Southeast University, China, in 2008 and 2013, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Software Engineering, Auburn University. He was a Visiting Scholar with RWTH Aachen University, Germany, from 2009 to 2011. His research interests include machine learning, optimization, and their applications in wireless networking systems.

Tao Shu received the B.S. and M.S. degrees in electronic engineering from the South China University of Technology, Guangzhou, China, in 1996 and 1999, respectively, the Ph.D. degree in communication and information systems from Tsinghua University, Beijing, China, in 2003, and the Ph.D. degree in electrical and computer engineering from The University of Arizona in 2010. He is currently an Associate Professor with the Department of Computer Science and Software Engineering, Auburn University. Prior to his academic position, he was a Senior Engineer with Qualcomm Atheros Inc., from December 2010 to August 2011. His research aims at addressing security and performance issues in wireless networking systems, with strong emphasis on system architecture, protocol design, and performance modeling and optimization.



Husheng Li received the B.S. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1998 and 2000, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2005. From 2005 to 2007, he worked as a Senior Engineer at Qualcomm Inc., San Diego, CA, USA. In 2007, he joined the Department of EECS, The University of Tennessee, Knoxville, TN, USA, as an Assistant Professor, where he was promoted to Associate Professor in 2013 and a Full Professor in 2018. His research is mainly focused on statistical signal processing, wireless communications, networking, smart grid, and game theory. He was a recipient of the Best Paper Awards of *EURASIP Journal on Wireless Communications and Networking* in 2005, *EURASIP Journal of Advances in Signal Processing* in 2015, IEEE GLOBECOM 2017, IEEE ICC 2011, and IEEE SmartGridComm 2012, and the Best Demo Award of IEEE GLOBECOM in 2010.