3-way Game Model for Privacy-Preserving Cybersecurity Information Exchange Framework

Iman Vakilinia
Dept. of Computer Science and Eng.
University of Nevada, Reno, NV, USA
ivakilinia@unr.edu

Deepak K. Tosh
Dept. of Computer Science
Norfolk State University, VA, USA
dktosh@nsu.edu

Shamik Sengupta
Dept. of Computer Science and Eng.
University of Nevada, Reno, NV, USA
ssengupta@unr.edu

Abstract*—With the growing number of cyberattack incidents, organizations are required to have proactive knowledge on the cybersecurity landscape for efficiently defending their resources. To achieve this, organizations must develop the culture of sharing their threat information with others for effectively assessing the associated risks. However, sharing cybersecurity information is costly for the organizations due to the fact that the information conveys sensitive and private data. Hence, making the decision for sharing information is a challenging task and requires to resolve the trade-off between sharing advantages and privacy exposure. On the other hand, cybersecurity information exchange (CYBEX) management is crucial in stabilizing the system through setting the correct values for participation fees and sharing incentives. In this work, we model the interaction of organizations, CYBEX, and attackers involved in a sharing system using dynamic game. With devising appropriate payoff models for each player, we analyze the best strategies of the entities by incorporating the organizations' privacy component in the sharing model. Using the best response analysis, the simulation results demonstrate the efficiency of our proposed framework.

***Index Terms*—Cybersecurity information-sharing, privacy-preservation, information sanitization, game theory**

I. Introduction

As the number and complexity of cyberattack incidents are increasing, organizations are required to have proactive knowledge on the cybersecurity landscape for efficiently defending their resources. To this end, organizations need to develop the culture of sharing their threat information with others in addition to production and internal consumption of these critical information only. The exchange of cyber-threat information can be advantageous in multiple ways which aims to achieve (1) cyber situational awareness, (2) operational control such as dynamic update of enterprise security components by continuous monitoring and knowledge from latest shared information, (3) strategic advantage that can help in planning for future upgrade to the organization's security infrastructure. This sort of collaboration can potentially help in reducing the cyber risks and increasing the security posture of organizations.

Despite the benefits of cybersecurity information sharing, several challenges still exist which are briefed in the following. (1) Potential lack of trust among the sharing parties to avoid the barriers of cybersecurity information sharing, (2) Risk of privacy violation, reputation/financial loss, etc. due to sensitive information exposure while sharing the information, (3) Absence of standardized platform and infrastructure for information sharing and consumption. Thus, the organizations need to adopt appropriate sanitization techniques to filter out the sensitive information from the threat data before sharing. However, doing so can also reduce the relevancy of the shared information to some extent for the receiving party.

Considering the presence of a cyber-threat information management entity in the sharing system, namely cybersecurity information exchange (CYBEX) [1], organizations participate in CYBEX to share each others' threat related knowledge. Since organizations will be looking for security enhancements by participating in CYBEX's sharing framework, it is worthy to impose a participation cost on the organizations. On the other side CYBEX will be interested to incentivize the organizations on their truthful information sharing in the system which has positive externality effect on other organizations' participation behavior. Therefore, optimal participation cost and incentive are necessary to evaluate from the CYBEX point of view so as to succeed in the sharing process. At the same time, open exchange of critical cyber-threat information attracts attackers to exploit the participating organizations based on the gathered information on specific vulnerabilities. So, attackers allocate their efforts and resources depending on the located vulnerabilities to succeed in exploiting the organizations. Therefore, the organizations' strategy would be to enforce appropriate sanitization on the threat related information before sharing. The conflict among the three entities (organizations, attackers, CYBEX) mandates to bring the concepts from game theory to resolve the challenge of effective sharing, which constitutes our contributions in the paper.

In this work, we particularly model the entities involved in cybersecurity information exchange (CYBEX) in form of a dynamic game. From the attackers' point of view, the goal is to maximize the benefit of attacking a set of organizations by optimally investing its resources for each vulnerability and organization. From the organizations' perspective, it is crucial to understand how much information to share into the system, based on which the incentives from CYBEX is decided. Whereas from the CYBEX's perspective, it is essential to decide on the amount of incentive rate for sharing of information and the amount of admission charge. Here, if CYBEX does

This research is supported by the National Science Foundation (NSF), USA, Award #1528167.

not set the incentives correctly, then organizations may not share information effectively and as a result, the organizations might leave CYBEX due to the fact that cost of joining to the system is higher than their gain from the sharing system.

This paper is organized as follows. Prior research works in the domain of cybersecurity information sharing are briefed in the Section II. In Section III, we present the system model and payoff model of involved players. The detailed analysis of the game is conducted in Section IV. The experimental results and discussions are presented in Section V. Finally, Section VI provides concluding remarks of the paper.

II. Related Work

Using micro-economics models, various cybersecurity information sharing frameworks [2]–[4] are studied in the past which emphasize on enhancing production efficiency. Authors in [3] [5] provide necessary and sufficient conditions to verify this fact that optimal information security can be attained at a lesser cost provided security information is shared. Since organizations share their threat data, some might take the opportunity to free-ride without exchanging anything back. Thus appropriate incentivization mechanism is required to prohibit the free-riding on other firms' security information so that no firm can gain more by making under-investment. Authors in [6] has presented a Bayesian game for sharing vulnerabilities in a competitive environment and developed a monetary-free sharing mechanism by considering competitive loss, direct loss and market shrinkage into account, which encourages the organizations to invest and share at the same time. The research presented in [7] has proposed an evolutionary game-theoretic framework for cyber-threat information sharing where CYBEX dynamically controls the participation cost so as to enhance participation in the sharing framework. Garrido-Pelaz et al. [8] presented a cybersecurity information sharing model for a set of correlated organizations, where functional dependency network analysis is opted for propagating attack information and a game model is used to decide whether to share information or not.

The prior research works have focused mostly on how organizations can be motivated to share their information and how their security investment will be affected by doing so. However, the inescapable fact in the threat sharing is that the information content may involve several personal identifiable information (PII) which could lead to user privacy issues. Although such knowledge in the shared information may have importance in resolving behavioral aspects of cyber attacks, but it will upset the organization whose information is shared with the community. Hence, there exists a trade-off of how much filtration should be done on the information content prior to sharing and cost of privacy that needs to be resolved. Therefore, we propose a 3-way game model by considering CYBEX, organizations, and attacker as players of the game, where CYBEX decides appropriate incentives to motivate organizations for sharing, organizations look for an optimal sanitization rate to keep their privacy cost low, and the attacker aims to maximize its attack impact.

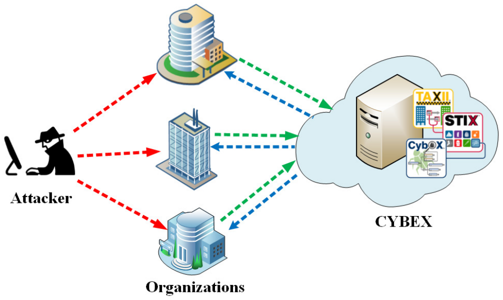


Fig. 1: Players in the CYBEX system

III. System Model

The proposed system considers a set of profit-seeking organizations $\mathcal{O} = \{o_1, ..., o_n\}$ to establish the cybersecurity information sharing platform. Since sharing threat-related information is costly, we assume an entity (CYBEX) to facilitate the sharing process. As a responsibility, CYBEX also decides the appropriate incentives for sharing information and also the necessary admission charge for each organization. We refer CYBEX as $\mathcal{C}$ in rest of the paper. For each cycle of information sharing, $\mathcal{C}$ charges o_i with the admission fee δ_i. $\mathcal{C}$ sets this fee based upon the gain of each organization from the system. For the simplicity of the analysis and without loss of generality, we consider that the participant organizations $\mathcal{O}$ have deployed the systems with a common set of vulnerabilities $V = \{v_1, ..., v_m\}$. These vulnerabilities can be potentially exploited by attackers $\mathcal{A}$. Each organization has the option to share their vulnerabilities information inside the CYBEX. Since there are sensitive information existing in the sharing data, organizations are applying filtering to the data before sharing them with the CYBEX. In the next subsection we investigate the cost of sharing in this setting. Fig. 1 depicts the system players.

A. Modeling the vulnerability information sharing

In the beginning, we need to mathematically model and present a metric for vulnerability sharing information such that the changes of privacy preserving techniques can be displayed. To model sharing the information of a vulnerability, we consider that each v_j has a set of features. To successfully detect a vulnerability, all of its features should be discovered. Let q_j represent the number of v_j's features. The vector $\mathcal{V}_{i,j} = [\hat{v}_1, \cdots, \hat{v}_{q_j}]$ is the information available to o_i regarding v_j. Here $\hat{v}_k \in \{0, 1\}$ is a flag to indicate if the feature information is available in data or not. Let $\eta(\mathcal{V}_{i,j}) \in [0, 1]$ quantify the vulnerability information vector and be calculated as the following.

$$\eta(\mathcal{V}_{i,j}) = || \mathcal{V}_{i,j} ||_1 / q_j \quad (1)$$

Here, $|| \mathcal{V}_{i,j} ||_1$ is the L_1 norm of $\mathcal{V}_{i,j}$. As $\eta(\mathcal{V}_{i,j})$ increases, it is expected that the probability of successfully detecting the attack over v_j increases, since more information about the vulnerability is available. Due to the privacy concerns, organizations may filter their data before sharing the vulnerability information with CYBEX. Fig.2 shows an example

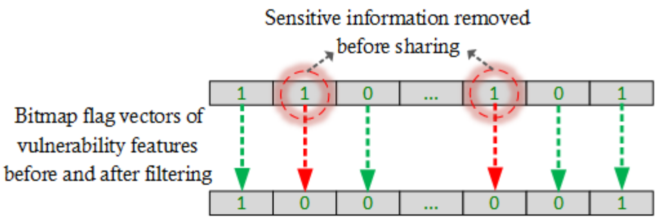


Fig. 2: Organizations filter sensitive information before sharing

of the filtration process of vulnerability information before and after sharing information. Hence, the following inequality must satisfy for the shared information ($\hat{\mathcal{V}}_{i,j}$) due to filtration process.

$$\eta(\hat{\mathcal{V}}_{i,j}) \leq \eta(\mathcal{V}_{i,j}) \tag{2}$$

Let $\bar{\mathcal{V}}_j$ represent the aggregated information of vulnerability v_j. The total shared information regarding v_j in the CYBEX can be represented as the following.

$$\bar{\mathcal{V}}_j = \vee_{i=1}^{n} \hat{\mathcal{V}}_{i,j} \tag{3}$$

B. *Utilities of the Players*

Here, we model the utility functions for the players involved in the CYBEX sharing system including the attacker.

1) Attacker's Utility: The probability of the successful vulnerability exploitation is dependent on the following set of variables: (1) amount of vulnerability sharing information, which has a direct impact for causing cyber attack, (2) attacker's investment, which by increasing the attacker can increase the chance of successful attack exploitation, (3) organization's security investment, which help to decrease the chances of being exploited due to the attack. Since each vulnerability has a specific exploitability in the different organizations, we also consider a vulnerability exploitability parameter for the organizations. Now, we propose the following candidate function to model the probability of successful vulnerability exploitation. $\mathcal{A}$ successfully exploits v_j over o_i with the probability $p_{i,j}$:

$$p_{i,j} = (1 - \eta(\hat{\mathcal{V}}_j)) \log(1 + \mu_{i,j}) \xi_{i,j} / e^{I_i} \tag{4}$$

With increasing the organization's security investment I_i, the probability of success attack decreases, $\frac{\partial p_{i,j}}{\partial I_i} < 0$; but at a decreasing rate $\frac{\partial^2 p_{i,j}}{\partial I_i^2} > 0$. The parameter $\xi_{i,j}$ is the exploitability of v_j for the o_i. $\mu_{i,j}$ represents the $\mathcal{A}$'s investment. By increasing the $\mathcal{A}$'s investment, the probability of successfully exploit the vulnerability increase $\frac{\partial p_{i,j}}{\partial \mu_{i,j}} > 0$, but at a decreasing rate $\frac{\partial^2 p_{i,j}}{\partial \mu_{i,j}^2} > 0$. By sharing information about the vulnerability, organizations can decrease the probability of the successful attack. If all features of a vulnerability are shared in the system $\eta(\hat{\mathcal{V}}_j) = 1$ then we assume that the organizations are able to perfectly detect and defend against the attack (e.g. patch the vulnerability). Thus, in this case, the probability of the successful attack is $p_{i,j} = 0$. The attacker $\mathcal{A}$'s expected gain $G_{i,j}$ can be:

$$G_{i,j} = p_{i,j} g_{i,j} - \mu_{i,j} \tag{5}$$

Here $g_{i,j}$ declares the profit of the successful attack on v_j over o_i.

The $\mathcal{A}$'s expected gain from exploiting all of the vulnerabilities over the organizations involved in CYBEX is:

$$\hat{G} = \sum_{i=1}^{n} \sum_{j=1}^{m} (p_{i,j} g_{i,j} - \mu_{i,j}) \tag{6}$$

Here n is the number of organizations and m is the number of vulnerabilities. Attacker's goal is to maximize the total gain $\hat{G}$ by minimizing the investment $\mu_{i,j}$ and increasing the probability of exploitation $p_{i,j}$.

2) Organization's Utility: To model the organization's utility, first we need to define the risks related to privacy in cybersecurity information sharing. Shared information might convey sensitive data about organizations which can be exploited by the attackers. Cybersecurity information might carry private set information which can help attackers in target reconnaissance. For example, network logs have following information: IP-addresses, network architecture, security safeguards and their configuration, available services and their corresponding ports, personnel names/identifiers and etc. Although organization can reduce these sensitive information breach by applying privacy preserving techniques such as generalization and sanitization, there is an indirect relation between the quality of the shared data and the level of privacy preserving. In other words, by increasing the level of privacy preservation, the utility of shared data decreases correspondingly.

Let $a_{i,j} \in [0, 1]$ represent the sanitization rate, which is the amount of sanitization/generalization of the data before publishing to the CYBEX. Here $a_{i,j} = 0$ declares the published information is the same as original information and $a_{i,j} = 1$ means no information will be shared. Each organization sets this value based on the sensitivity of the information.

Let $\gamma_{i,j}(\mathcal{V}_{i,j})$ be the incentive obtained from sharing information regarding v_j. The incentive value is the prize that organization receives from $\mathcal{C}$. Hence we have:

$$\gamma_{i,j}(\mathcal{V}_{i,j}) = \eta(\mathcal{V}_j).f(\sum_{k \in n \setminus i} g_{k,j}) \tag{7}$$

Here $f(.)$ is the scaling function. The incentive value is calculated based on the amount of shared information and the impacts of exploiting the vulnerability over the organizations participating in CYBEX. In other words, it is proportional to the loss that could be saved by other organizations through utilizing the shared information and hence applying the patches to the vulnerability[1]. We consider that the organization's loss and the attacker's gain are equal. Now by applying the sanitiation rate, we can calculate the effective incentive rate $\gamma_{i,j}(\hat{\mathcal{V}}_{i,j})$ after sanitization:

$$\gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) = (1 - a_{i,j}).\gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) \tag{8}$$

[1] In our model, CYBEX is able to estimate the loss that exploiting vulnerabilities causes. This can be done through applying risk assessment techniques.

Here the incentive value decreases with the increasing of sanitization rate. Let $\rho_{i,j}$ represent the expected privacy cost, and $\hat{\rho}_{i,j}(a_{i,j})$ calculate the effective privacy cost that o_i incurs for sharing the information about v_j after sanitization. This value is a function of sanitization rate $a_{i,j}$ which has been applied over the information before publishing them. By applying privacy preserving techniques, first organization removes the highest sensitive values from their data and gradually sanitizes less sensitive values. Hence by increasing the sanitization rate, privacy cost decreases $\frac{\partial \hat{\rho}_{i,j}}{\partial a_{i,j}} < 0$, but at a decreasing rate $\frac{\partial^2 \hat{\rho}_{i,j}}{\partial \hat{\rho}^2_{i,j}} > 0$. We model the effective privacy cost as[2]:

$$\hat{\rho}_{i,j}(a_{i,j}) = (2^{(1-a_{i,j})} - 1).\rho_{i,j} \tag{9}$$

The expected utility of o_i in the CYBEX is:

$$u_i(a_{i,j}) = \sum_{j=1}^{m}((1-p_{i,j}).g_{i,j} + \gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) - \hat{\rho}_{i,j}(a_{i,j})) - \delta_i \tag{10}$$

o_i has the option to decrease the cost of privacy by performing privacy-preserving techniques such as generalization/sanitization. But on the other hand the level of privacy preserving affects the utility of the data and correspondingly decrease the incentive value. Organization's goal is to maximize $u_i(a_{i,j})$ by applying the appropriate sanitization rate $a_{i,j}$.

3) CYBEX's Utility: CYBEX's Utility is the sum of utilities of $\mathcal{O}$ participating in cybersecurity information sharing with the constraint of stability.

Definition 1. CYBEX stability is the state that organizations are motivating to participate in cyberseurity information sharing. The admission charge and incentive rates should preserve the stability of the system. CYBEX's stability has the four following requirements:

(1)- For each v_j and o_i, the incentive rate should be higher than the privacy cost of the shared information, otherwise organization does not share information.

$$\gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) - \hat{\rho}_{i,j}(a_{i,j}) > 0, \qquad \forall i \in n, j \in m \tag{11}$$

(2)- The total expected gain from applying shared information should be more than the amount of incentive rate.

$$\sum_{k=1}^{n-1}(1-p_{k,j}).g_{k,j} - \gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) > 0, \quad \forall k \in n\backslash\{i\} \tag{12}$$

(3)- The total given incentive values should be lesser than the whole budget of CYBEX which is achieved through admission charges.

$$\sum_{i=1}^{n}\delta_i - \sum_{i=1}^{n}\sum_{j=1}^{m}\gamma_{i,j}(\hat{\mathcal{V}}_{i,j}) \geq 0 \tag{13}$$

(4)- To meet the fairness requirement, the admission charge for each organization should be equal to the fractional of the total expected gain of the organization through accessing the shared information. It means organizations should be charged based on their gain of the system.

$$\delta_i = \epsilon.\sum_{j=1}^{m}(1-p_{i,j}).g_{i,j} \tag{14}$$
$$s.t. \qquad 0 < \epsilon < 1$$

Here ϵ is the coefficient for admission charge, which is enforced by $\mathcal{C}$. If this value is large, organizations will not be interested to join the CYBEX. Table I depicts the notations used in the paper.

TABLE I: Notations used in this paper

Notation	Description
$\rho_{i,j}$	o_i's expected privacy cost for sharing information regarding v_j
$\mathcal{V}_{i,j}$	Available features of v_j
$\hat{\mathcal{V}}_{i,j}$	$\mathcal{V}_{i,j}$ after applying filtering
$\bar{\mathcal{V}}_j$	Total shared information regarding v_j
q_j	Number of v_j features
$\eta(\mathcal{V}_{i,j}) \in [0,1]$	Quantification of $\mathcal{V}_{i,j}$
$a_{i,j} \in [0,1]$	The sanitization rate before publishing to the CYBEX
$p_{i,j}$	The probability of successfully exploiting v_j over o_i
$g_{i,j}$	The profit/loss of the successful attack/exploit on v_j over o_i
$\mu_{i,j}$	Attacker's investment to exploit v_j over o_i
$\xi_{i,j}$	The exploitability of v_j for o_i
I_i	The security investment of o_i
δ_i	The CYBEX admission fee
$G_{i,j}$	Attacker's expected gain from exploiting v_j over o_i
$\hat{G}$	Attacker's total expected gain in the CYBEX
$\gamma_{i,j}(.)$	The incentive rate for sharing information about v_j
$u_i(.)$	The utility of o_i in the CYBEX
ϵ	The determinative coefficient for the admission charge
$\hat{\epsilon}_j$	The determinative coefficient of incentive rate for v_j

IV. Game Specification and Analysis

For each v_j detected by $\mathcal{A}$, we consider the strategies of $\mathcal{A}$ as a tuple of $\{[\Psi, (\mu_{i,j})_{\substack{i=1,..,n \\ j\in\Psi}}]\}$ such that $\Psi \subseteq O$. In other words, $\mathcal{A}$'s strategy is to choose the sequence of organizations to attack and dedicate an investment value for the attack correspondingly. The strategy of o_i is $\Pi_i = (a_{i,j})_{j=1,...m}$, which indicates how much of the information the organization is going to share into the system. The strategy of the $\mathcal{C}$ is $\Lambda = (\gamma_{i,j}(.), \delta_i)_{\substack{i=1,..,n \\ j=1,...,m}}$ which is a decision over the proper value for admission charge and incentive rates for each sharing into the system. An instance of the CYBEX game is then:

$$\Gamma = \{(A, O, \mathcal{C}), (\Psi, \Pi, \Lambda), (\hat{G}, (u_i)_{i=1,..,n}, \hat{u}_c)\} \tag{15}$$

This game is not simultaneous and players are not aware of payoffs and strategies of each other. In addition, players can not observe the other player's move. Therefore the game is classified as dynamic, incomplete, and imperfect information. Organizations have the option to share the information about the attack within CYBEX. If the organizations share this information with other organizations, the probability of the

[2] We could also use any other function as long as it satisfies the required property.

success attack is decreased according to the equation (4). Let $w = [p_{i,j}, g_{i,j}, \rho_{i,j}, \gamma_{i,j}(.), \delta_i]_{\substack{i=1,..,n \\ j=1,...,m}}$ be a realization of the world state. Here, we analyze the best strategy of each player which leads to the Nash Equilibrium point.

A. Attacker Perspective

From $\mathcal{A}$'s perspective, the optimization problem is finding the best sequence of the organizations to attack and also dedicate the proper investment for each attack. Formally for each v_j, $\mathcal{A}$'s best response strategy is:

$$\begin{aligned} &(\mu^*_{i,j})_{i\in\Psi} \in \text{arg max } G(\Psi, (\mu_{i,j})_{i\in\Psi}|w) \\ &s.t. \qquad \sum_{i\in\Psi} \mu_{i,j} \leq \tau \end{aligned} \tag{16}$$

From the above equation, if $\mathcal{A}$ estimates the gain of each attack, then this problem is the reduction of knapsack problem, where organizations corresponding to the weighted items and attacker's total investment corresponding to the knapsack size. If we assume that $\mathcal{A}$ can estimates the variables existed in equation (4) then the optimal value of $(\mu_{i,j})_{\substack{j=1,..,m \\ i\in\Psi}}$ is:

$$\begin{aligned} &\frac{\partial G_{i,j}}{\partial \mu_{i,j}} = p'_{i,j}.g_{i,j} - 1 = 0 \\ &\mu^*_{i,j} = \frac{(1-\eta(\hat{\mathcal{V}}_j)).\xi_{i,j}.g_{i,j}}{e^{I_i}} - 1 \end{aligned} \tag{17}$$

In the above equation, if the value of $\mu^*_{i,j} \leq 0$, it means the total gain of the attack is less than the investment requirement and hence the best strategy for the attacker is to not-attack o_i for v_j. The best strategy for $\mathcal{A}$ is to first attack the set of organization's who are not sharing any information about the attack to CYBEX. Then $\mathcal{A}$ decides on the sequence of organizations to attack based on $g_{i,j}$.

B. Organization Perspective

From the $\mathcal{O}$'s point of view, the optimization problem is supposed to be finding the optimal value of sanitization rate to maximize the expected utility function for a given state of the world w. Formally we have:

$$\begin{aligned} &(a^*_{i,j})_{j=1,...,m} \in \text{arg max } u_i((a_{i,j})_{j=1,...,m} \mid w) \\ &s.t. \qquad 0 \leq (a_{i,j})_{j=1,...,m} \leq 1 \end{aligned} \tag{18}$$

For v_j, the optimal value of $a_{i,j}$ equals to:

$$\begin{aligned} &\frac{\partial u_i(.)}{\partial a_{i,j}} = \gamma'_{i,j}(\hat{\mathcal{V}}_{i,j}) - \hat{\rho}'_{i,j}(a_{i,j}) = \\ &(1-a_{i,j})'.\gamma_{i,j}(.) - (2^{(1-a_{i,j})} - 1)'.\rho_{i,j} = 0 \\ &a^*_{i,j} = 1 - [log\frac{\gamma_{i,j}}{ln(2)\rho_{i,j}}] \end{aligned} \tag{19}$$

C. CYBEX Perspective

From the CYBEX perspective, the best response strategy is supposed to be the finding of the best value for incentive rates and admission charges to maximize the expected utilities of all the organization in such a way that organizations utilities increase fairly. Formally we have:

$$(\gamma_{i,j}(.), \delta_i)_{\substack{i=1,..,n \\ j=1,...,m}} \in \text{arg max } \sum_{i=1}^{n} u_i(w|(\gamma_{i,j}(.), \delta_i)) \tag{20}$$

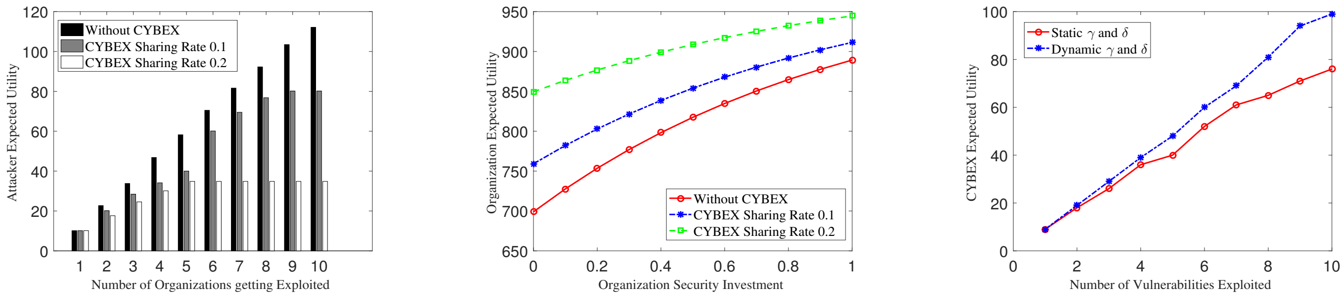
CYBEX should charge each organization, based on the amount of saving they could have through accessing the shared information. On the other hand, CYBEX should set the incentive rate such that it is less than the total gain of the other organizations' benefits of the shared information. We are proposing a heuristic approach (Algorithm 1) to calculate the efficient values of the incentive rates and the admission charges. This algorithm recursively increases the determinative coefficients $\epsilon, \hat{\epsilon}_j$. From equations (10) and (20), it can be seen that CYBEX best strategy is to keep $\epsilon, \hat{\epsilon}_j$ values as less as possible. $\epsilon, \hat{\epsilon}_j$ are proportional to the inverse number of the organizations joined into the system, as the number of organizations increase, this value is decreasing. The algorithm stops when the constraints are met.

Algorithm 1 Finding the optimal values of $\gamma_{i,j}$ and δ_i

```
//Calculation of Incentive Rate for each vulnerability
procedure IncentiveRate(w)
    for each $j \in m$ do
        Initialize $\hat{\epsilon}_j \leftarrow 0$
        for number of steps do
            $\gamma_{i,j}(.) \leftarrow (\hat{\epsilon}_j \times \sum_{k\in n\setminus\{i\}}(1-p_{k,j}) \times g_{k,j})$
            if $\gamma_{i,j}(.) > \rho_{i,j}(.)$ then
                return $\gamma_{i,j}(.)$
            else $\hat{\epsilon}_j + = s$
            end if
        end for
    end for
end procedure
//Calculation of Admission Charge
procedure AdmissionCharge(w)
    Initialize $\epsilon \leftarrow 0$
    for number of steps do
        if $\sum_{i=1}^{n}\sum_{j=1}^{m}\gamma_{i,j}(.) > \epsilon \times \sum_{j=1}^{m}(1-p_{i,j}).g_{i,j}$ then
            $\epsilon + = s$
        else return $\epsilon \times \sum_{j=1}^{m}(1-p_{i,j}).g_{i,j}$
        end if
    end for
end procedure
```

V. Simulation Result

In this section, we evaluate the result of simulations. We investigate the utility of the game players. First we investigate the expected utility of the attacker with the presence



(a) Attacker's Expected Utility

(b) Organization's Expected Utility

(c) CYBEX's Expected Utility

Fig. 3: Expected utility of the players in CYBEX game

of cybersecurity information sharing framework. We assume $n = 10, m = 5, I_i = i$. Organizations are sharing information with the rates of 0.1 and 0.2 when CYBEX is deployed. In other words, the value of the $\eta(\hat{\mathcal{V}}_j)$ after each attack will increase by 0.1 and 0.2 respectively. Here, attacker randomly chooses organizations to attack. The result is averaged of 100 simulations. The exploitability and attack gain is assumed to be $g_{i,j} = \xi_{i,j} = 2 \times i$. Attacker's investment is calculated based on equation (17). Fig. 3a depicts the attacker's expected utility. As it can be seen in the picture, sharing cybersecurity information dramatically decreases the attackers gain which directly causes the reduction of organizations' loss.

In the next simulation, we investigate the organizations' expected utility when joining to the cybersecurity information sharing system. Here, for comparison purpose, we set the parameters as follows: $\mu_{i,j} = \xi_{i,j} = 1, g_{i,j} = 1000$. Fig. 3b depicts the benefit of joining cybersecurity information sharing when the security investment varies. Although increasing the security investment decrease the probability of successful attack, this growth has a decreasing rate. Sharing cybersecurity information decrease the chance of successful attack considerably while the joining to this system is not costly.

In the final simulation, we investigate CYBEX utility. In this experiment we consider two models for setting incentive rate and admission charge. The first model consider the static values for these parameters and the second model applies the dynamic algorithm 1. The other parameters are set as follows: $\rho_{i,j} \sim \mathcal{N}(8,5), g_{k,j} \sim \mathcal{N}(10,5), m = 10, k \in n \backslash \{i\}$. In the case of constant setting we have $\gamma_{i,j}(.) = 10, \delta_i = 10$. If the privacy cost is larger than incentive rate, then organization is not sharing information into the system. For the dynamic incentive rate and admission charge setting we consider step value as $s = 0.1$. The expected utility is the average of expected utility among organizations. Fig. 3c depicts the utility of the CYBEX with different strategies for setting incentive rate and admission charge. As it can be seen in the picture, the dynamic approach is gaining better utility specifically when the number of vulnerabilities increase. By applying dynamic approach CYBEX can manage the incentive rate based on the total gain obtained from sharing information.

VI. Conclusion

Considering the impact of cyber attacks at organizational level, it is crucial to adopt the sharing of cyber-threat information as a common practice. However, privacy of participating organization remains a bottleneck in self-motivating toward exchange of such critical information. In this paper, we have studied the problem of sharing cybersecurity information with consideration of privacy cost in account. Considering the involvement of three category of players such as organizations, attackers, and CYBEX, we formulated a dynamic game among them to derive the optimal strategy of how much sanitation an organization must choose to keep its net benefit maximum. At the same time, CYBEX figures out the optimal incentive amount to motivate organizations to share and participation cost to impose using best response analysis. The simulation results show the efficiency of our proposed framework.

References

[1] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, and S. Adegbite, "Cybex: The cybersecurity information exchange framework (x.1500)," *SIGCOMM Comput. Commun. Rev.*, vol. 40, pp. 59–64, Oct. 2010.

[2] E. Gal-Or and A. Ghose, "The economic consequences of sharing security information.," *Economics of information security*, vol. 12, pp. 95–105, 2004.

[3] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[4] K. Hausken, "Information sharing among firms and cyber attacks," *Journal of Accounting and Public Policy*, vol. 26, pp. 639–688, 2007.

[5] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating it security investments," *Communications of the ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[6] M. Khouzani, V. Pham, and C. Cid, "Strategic discovery and sharing of vulnerabilities in competitive environments," in *International Conference on Decision and Game Theory for Security*, pp. 59–78, Springer, 2014.

[7] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7341–7346, IEEE, 2015.

[8] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana, "Shall we collaborate?: A model to analyse the benefits of information sharing," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 15–24, ACM, 2016.