Cyber-threats Information Sharing in Cloud Computing: A game Theoretic Approach

Charles Kamhoua[1], Andrew Martin[2], Deepak K. Tosh[3], Kevin A. Kwiat[1], Chad Heitzenrater[2], Shamik Sengupta[3‡]
[1]Air Force Research Laboratory, Information Directorate, Cyber Assurance Branch, Rome, NY
[2]University of Oxford, Department of Computer Science, Oxford, UK
[3]University of Nevada, Reno, Department of Computer Science and Engineering, Reno, NV
{Charles.Kamhoua.1; Kevin.Kwiat}@us.af.mil Andrew.Martin@cs.ox.ac.uk; {dtosh;ssengupta}@unr.edu

***Abstract*—Cybersecurity is among the highest priorities in industries, academia and governments. Cyber-threats information sharing among different organizations has the potential to maximize vulnerabilities discovery at a minimum cost. Cyber-threats information sharing has several advantages. First, it diminishes the chance that an attacker exploits the same vulnerability to launch multiple attacks in different organizations. Second, it reduces the likelihood an attacker can compromise an organization and collect data that will help him launch an attack on other organizations. Cyberspace has numerous interconnections and critical infrastructure owners are dependent on each other's service. This well-known problem of cyber interdependency is aggravated in a public cloud computing platform. The collaborative effort of organizations in developing a countermeasure for a cyber-breach reduces each firm's cost of investment in cyber defense.**

Despite its multiple advantages, there are costs and risks associated with cyber-threats information sharing. When a firm shares its vulnerabilities with others there is a risk that these vulnerabilities are leaked to the public (or to attackers) resulting in loss of reputation, market share and revenue. Therefore, in this strategic environment the firms committed to share cyber-threats information might not truthfully share information due to their own self-interests. Moreover, some firms acting selfishly may rationally limit their cybersecurity investment and rely on information shared by others to protect themselves. This can result in under investment in cybersecurity if all participants adopt the same strategy.

This paper will use game theory to investigate when multiple self-interested firms can invest in vulnerability discovery and share their cyber-threat information. We will apply our algorithm to a public cloud computing platform as one of the fastest growing segments of the cyberspace.

I. Introduction

Our national security, economic prosperity and daily life rely on a secure and resilient cyberspace. We depend on a worldwide communication network to command and control our weapon system, to ensure our financial transactions, and to guarantee our food and water supply. However, the frequency and cost of successful cyber-attacks around the world continues to increase exponentially despite the growth of cybersecurity investment in technical solutions such as cryptography, formal verification, agility, intrusion detection, survivability and resiliency. This shows that cybersecurity needs not only technical solutions but also mathematical innovation and cybersecurity laws and regulation.

In the United States for instance, there have been several regulations and executive orders that are focused on sharing cybersecurity information among public and private organizations. In October 13, 2011, the United States Securities and Exchange Commission (SEC) issued a guidance [1] requiring that companies disclose cyber incidents including a description of the costs. Furthermore, more than 44 states in the US have already passed similar laws. Those laws are consistent with previous work [2] showing that firms spend less on information security when they are mandated to share security information. However, many companies fear that the information disclosed may be used in legal lawsuit against them.

President Obama signed the Executive Order 13636 - Improving Critical Infrastructure Cybersecurity on Feb 12, 2013, [3] proposing that critical infrastructure owners and operators voluntarily adopt the White House Cybersecurity Framework (i.e., the Framework). Cyber-threats information sharing among different organizations (including the US government) is a key point of the Framework. Under this Framework, the US Government will share unclassified and classified cyber-threat information with the private sector. It also establishes cyber-threat information sharing among private companies and between private companies and the government. The National Institute of Standards and Technology (NIST) has proposed the preliminary version of the Framework and subsequently the final Framework came out on February 13, 2014 [4]. The government would like to facilitate warnings of cyber threats before those threats turn into successful attacks on critical infrastructures. Cutting edge research and development are crucial to understand the impact of cyber-threat information sharing among self-interested rational players as most critical infrastructures are privately owned and operated.

Models of quantitative analysis of cybersecurity, such as game theory, are increasingly popular in this decade. This is because by definition, game theory is the mathematical study of conflict among rational agents [5] and cybersecurity is a frightful conflict that involves rational agents. A rational behavior as formulated in a standard game theoretic framework

• Approved for Public Release; Distribution Unlimited: 88ABW-2015-3159, 23 Jun 2015.

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

can capture the essential feature of an agent in cyberspace [6]; that is each agent takes a course of action that he believes will maximize his expected utility given multiple uncertainties. Evidently, cyber agents have different utilities or payoffs. Cyber attackers want to maximize the system damage while cyber defenders (e.g., users, network administrators) want to minimize such damage. Game theory can also guide legislative action or help analyze its consequences on cybersecurity.

Cyber defenders can form a strategic coalition to fight against cyber-attacks at a minimum cost by sharing their cyber-threat information, as advocated in the new White House Cybersecurity Framework. Cyber-threat information sharing has the potential to deny an attacker the possibility to exploit the same vulnerability again to compromise multiple users. Ideally, each user who is a victim of an attack shares the attack with others so that they can quickly update their intrusion detection systems before another cybersecurity event occurs. Correctly implemented, information sharing helps to prevent or avoid successful cyber-attacks.

Cloud computing is one of the fastest growing segments of the cyberspace. That is because cloud computing is cost efficient, e.g., cloud users can reduce spending on technology infrastructure and have easy access to their information without up-front or long-term commitment of resources. However, security in cloud computing is more challenging than the security of traditional networks. That is because Virtual Machines (VMs) can start, stop, and move from hypervisor to hypervisor at the click of a button. Cloud security techniques have to be able to easily deal with these movements. Therefore, a game theoretic model for traditional network may not be suitable in a cloud computing environment. Moreover, different public cloud users share a common platform such as the hypervisor. A common platform intensifies the well-known problem of cybersecurity interdependency [7], [8], [9], [10] as an attacker who gains access to the hypervisor can start, stop, and modify all of the VMs that are housed on that hypervisor. The result is a more challenging execution environment due to the risk aggregation from many users sharing the same platform. A single attack on a cloud provider can compromise thousands of users at a huge cost.

This work considers a set of users in a public cloud who share the same hypervisor. The goal of our game model is to provide incentive to all cloud participants to invest in vulnerability discovery and share their cyber-threat information despite the potential cost involved. In particular, our game model will find out what are the necessary conditions under which a rational user in a public cloud will share his discovered vulnerabilities.

II. Background on Cloud Computing Security and Information Sharing

This section presents a background of cloud security to set the context of our game model. Zissis et al. [11] differentiate between public and private cloud structures by stating that private cloud technology is for inter-organizational operations and no third party is required while public and community cloud computing utilize a third party for a variety of service platforms. Such service platforms that cloud computing provides, include Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

An IaaS cloud provides a user access to virtualized hardware, presented by a hypervisor (e.g., VMware, Xen, KVM) and encapsulated in a VM, where the user is able to deploy and run arbitrary software including operating systems and applications on the underlying shared hardware. A PaaS cloud provides a user a language-specific platform (e.g., JVM, .Net) to deploy and run an arbitrary applications developed using the given language on the underlying shared platform. A SaaS cloud provides a user access to a particular application (e.g., web-based email, document editor) where the user can use the functionality provided by the underlying shared application. Although these different levels of cloud services can be built separately, it is increasingly common to build a high-level cloud service using resources provided by a lower-level one (e.g., build a SaaS on resources from PaaS and a PaaS on resources from IaaS), so that the former can benefit from the elasticity and economics provided by the latter. Therefore, although this work focuses on VM-based hosting of mission-critical applications in an IaaS setting, its outcomes can also generate an impact to other models of cloud computing. Although private clouds share some of the benefits and drawbacks of public clouds, the issues of privacy, security, trust, and cyber-threat information sharing arise mainly in a public cloud platforms, as many of the users' computing capabilities are outsourced to a third party owner who leases the technology in a variety of ways. Therefore we focus on the public cloud; so in this work private cloud entities will not be discussed further. In fact, private clouds allow users from the same organization to run their internal applications on shared resources. Therefore, in a game theoretic sense, there should be less conflict of interest among private cloud users since they belong to the same organization and can freely share cyber-threat information.

The support for security isolations from existing cloud systems is limited. The different VMs sharing the same resources may belong to competing organizations as well as unknown attackers. From the perspective of a cloud user, there is no guarantee whether the underlying hypervisor or the co-resident VMs are trustworthy. The shared resources make privacy and perfect isolation implausible. There is a risk that attacks such as a covert side channel be used to extract another user's secret information or launch a Denial of Service (DoS) attack. Cross-side channel attacks between VMs are possible in a public cloud when the VMs share the same hypervisor, CPU, memory, and storage and network devices. In addition, some of the resources can be partitioned (e.g., CPU cycles, memory capacity, and I/O bandwidth), some of which are VMs shared resources that cannot be well partitioned such as last-level cache (LLC), memory bandwidth, and IO buffers. The shared resources can be exploited by attackers to launch cross-side channel attacks.

Many researchers have investigated cache-based side chan-

nel. Ristenpart et al. [7] show that a malicious user can analyze the cache to detect a co-resident VM's keystroke activities and map the internal cloud infrastructure and then launch a side-channel attack on a co-resident VM. Bates et al. [8] demonstrate the ability to initiate a covert channel of 4 bits per second, and confirm co-residency with a target VM instance in less than 10 seconds.

We can see that cloud security gives rise to interdependency among the users with potential externalities. We will use this interdependency in our model to design incentives for cyber-threat information sharing showing that each rational user will find that his self-protection depends on the protection of others which ultimately builds upon the cyber-threat information shared. Therefore, the possibility of side-channel attack in a public cloud can be turned into an incentive for all users to share all cyber-threats with others, in order to prevent future damage that may result from a similar attack on another VM.

The researches in [12][13][14][15][2][16] analyze information sharing in the context of cybersecurity. Those papers show that multiple factors impact cyber threat information sharing including competition [14], free riding [2], interconnection [17], and the possibility to exploit vulnerabilities for cyber war [16]. However, none of those work look into sharing cybersecurity information in cloud computing.

In our past work [18], we present an evolutionary game theoretic model to self-enforce firms toward participating in sharing framework by utilizing the participation cost in a tactical way. The work in [14] uses a two stage Bayesian game to analyze the information sharing decision of two strategic and competing firms. They established that the sharing strategies are unique and dominant, and are in the simple forms of full-sharing or no sharing completely determined by the competitive nature of the security findings.

Gordon et al. [2] show that information sharing can increase the level of information security while each firm reduces the amount spent on cybersecurity. Further, the optimum level of information security for a firm without information sharing can be attained by the firm at a lower cost when cyber-threat information is shared. However, without additional incentives to encourage full reporting, each firm can free-ride on the information security of others. Free-riding will result in an under-investment in information security so that all benefits to information sharing disappear.

Wu et al. [17] use game theory to model the cybersecurity investment of interconnected firms. When a firm's information systems are difficult to breach, the hackers chose to attack the less secure firm's information systems that are connected and easier to breach. They showed that in the absence of economic incentives, an interconnected firm is unwilling to increase its security investment when its trusted interdependence relationship with partners becomes tighter.

Moore et al. [16] explore the trade-offs between attack and defense of Information systems in cyber war. The paper uses game theory to model vulnerability discovery and exploitation, where nations must choose between protecting themselves by sharing vulnerability information with vendors or pursuing an offensive advantage while remaining at risk. They showed that at least one nation will have an incentive to not share cyber threat information.

III. System Model

Figure 1 illustrates our system model: A public cloud with m users that we denote User 1, User $2 \cdots$ User m. Each user runs several applications illustrated by Application $1 \cdots$ Application k in Figure 1. Technically, the users may run a different number of applications without any impact on this model. The Monitor has three purposes. First, it monitors the activities of the underlying VM to collect cyber-threat information. Second, it actively shares the collected threats with the Information Sharing and Analysis Center (ISAC). Finally, it consumes the information from the ISAC to protect the user, OS and VM.

The different applications require an operating system to function and that operating system in turn manages a VM in the cloud. In practice, a single user may use several operating systems or numerous VMs. However, we consider the architecture in Figure 1 to simplify the exposition. As it is a common practice in a public cloud, we consider that the different VMs from the different users share the same hypervisor and hardware, as depicted in Figure 1. The hypervisor can be of various types, such as the Kernel-based Virtual Machine (KVM), Xen, and VMware. The common factor is that the VMs share the same platform and in doing so expose each user to potential collateral damage.

We consider the possibility of a random hardware failure to be a rare event and neglect that possibility in our analysis in order to focus on intelligent cyber-attacks. It is well known that the users' security heavily depends on the cloud provider. As we are analyzing cybersecurity information sharing based on interdependency among the user, our model considers that the provider always monitors and shares all cyber-threats. This is to separate cloud client-to-client vulnerability sharing and cloud host-to-client vulnerability sharing. However, any model that analyzes cloud host-to-client vulnerability sharing can be superposed to our model. Thus, the attacker compromises the hypervisor in two steps. The first step is to compromise a user's VM. The second step is to use the compromised VM to attack the hypervisor.

We distinguish two types of attacks depending on the extent of the consequence: a restricted attack and an unrestricted attack. A restricted attack on User i only compromises the applications, operating system and VM that belong to User i; the hypervisor is not affected after a restricted attack. An unrestricted attack has consequences that can cross a VM to reach the hypervisor, i.e. the hypervisor is compromised. We consider that all the users suffer the consequences (damage) if the hypervisor is compromised. This is because an attacker who compromises the hypervisor can then compromise all the VMs on that public cloud imposing collateral damage. Thus, a rational user has a strong incentive to share his cyber-threats to prevent collateral damage. This will be one of the incentives in our model.

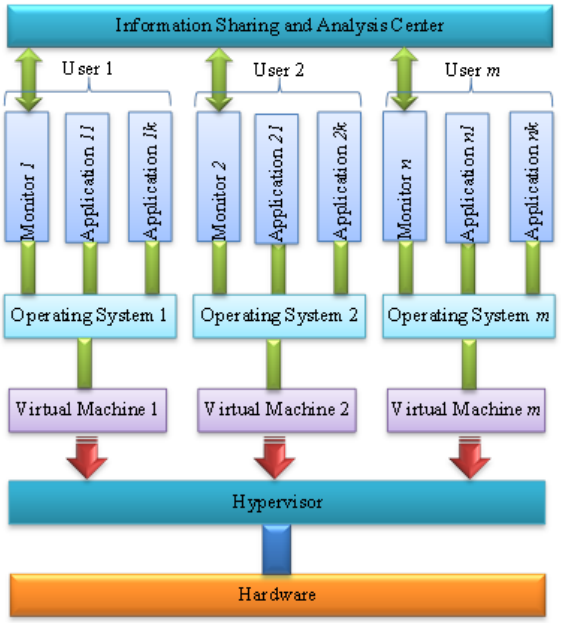

Fig. 1: System Model

IV. Game Model

Cyber-threat information sharing in a public cloud is a scenario suitable for game theoretic analysis. That is because common resources shared by users such as the hypervisor make the security of each user directly dependent on the security of others and these externalities are often overlooked.

We consider a two player game with two users that can share their vulnerabilities through the Information Sharing and Analysis Center, as in Figure 1. The players are User i and User j that share the same hypervisor on a public cloud as also illustrated in Figure 1. The exact number of vulnerabilities N in the public cloud is unknown but has an expected value n known to the two players. Figure 2 shows the Venn Diagram illustration of discovered vulnerabilities when both users invest to discover those vulnerabilities. A user that does not invest to discover vulnerabilities will not discover any vulnerability and thus has nothing to share. A user that invests in the discovery of vulnerabilities will not discover all the vulnerabilities, so it is realistic to assume that some of the vulnerabilities may go undetected despite the users' investment. Users' investment in our model is not to gather and examine the information about past cyber-attacks (e.g., forensic), but to discover the vulnerabilities and patch the system (VMs) before an attacker can exploit those vulnerabilities to launch an attack. Users invest as a proactive measure. However, any model that deals with vulnerabilities post-attack could also be superposed to this model. In the Venn diagram of Figure 2, the set of vulnerabilities discovered by User i, User j, and the attacker are represented by V_i, V_j and V_a respectively. Recall that a user who does not invest to discover vulnerabilities will not discover any vulnerability. Therefore, V_i (respectively V_j) is an empty set if User i, (respectively User j) choose not to invest. However, the set V_a is never empty since by its nature, the attacker is always looking for new vulnerabilities.

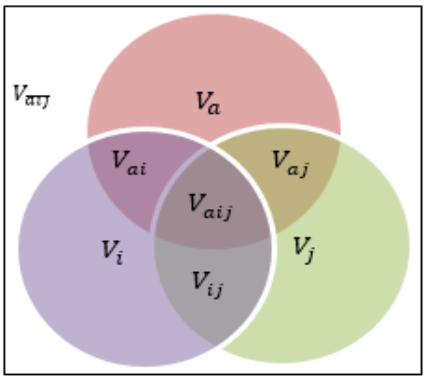

Fig. 2: Venn Diagram Illustration of Discovered Vulnerability

Parameters	Definition
c	Cost of investment in vulnerability discovery
d	Damage caused by an exploited vulnerability
s	Expected cost of sharing a vulnerability
N	Number of vulnerabilities
n	Expected number of vulnerabilities
$P_i, P_j = p$	Probability that User i/User j discovers a vulnerability given that he has invested
$P_a = p$	Probability that the attacker discovers a vulnerability
π	Probability that the attacker compromises the hypervisor given that a VM is compromised

TABLE I: Notations

$V_{\overline{aij}}$ represents the set of undiscovered vulnerabilities. The probability that a vulnerability belong to the set V_i, V_j or V_a is given by P_i, P_j and P_a respectively. Those probabilities can be estimated using a red team experiment in a cloud to find the average number of vulnerabilities a player discover. Remember that $P_i = 0$ (respectively $P_j = 0$) if User i, (respectively User j) choose not to invest. Similarly, the definition of $P_{ij}, P_{ai}, P_{aj}, P_{aij}$, and $P_{\overline{aij}}$ follow from the Venn diagram of Figure 2.

We assume that the attacker and the two users have similar capabilities to discover vulnerabilities and they independently discover those vulnerabilities. Thus,

$$P_i = P_j = P_a = p \tag{1}$$

$$P_{ij} = P_{ai} = P_{aj} = p^2 \tag{2}$$

$$P_{aij} = p^3 \tag{3}$$

However, it is straightforward to extend our model to the case that the attacker and the two users have different capabilities to discover vulnerabilities and their discovery of a vulnerability is not independent.

We denote by c a user's cost associated with the investment in vulnerability discovery. We assume that both users have similar costs and that the vulnerabilities are homogeneous. Moreover, we consider that the attacker is always successful when exploiting a vulnerability that is not discovered or shared between users. When a vulnerability is not discovered by User i and User j also does not discover it or decides not to share that vulnerability with User i, then an attacker can exploit that vulnerability and this will result in a damage to User i that we denote d, and vice versa.

USER i \ User j	$\bar{I}\bar{S}$	$I\bar{S}$	IS
$\bar{I}\bar{S}$	$\{-pnd - \pi pnd;$ $-pnd - \pi pnd\}$	$\{-pnd - \pi(p-p^2)nd;$ $-c-(p-p^2)nd - \pi pnd\}$	$\{-(p-p^2)nd - \pi(p-p^2)nd;$ $-c - spn - (p-p^2)nd - \pi(p-p^2)nd\}$
$I\bar{S}$	$\{-c-(p-p^2)nd - \pi pnd;$ $-pnd - \pi(p-p^2)nd\}$	$\{-c-(p-p^2)nd - \pi(p-p^2)nd;$ $-c-(p-p^2)nd - \pi(p-p^2)nd\}$	$\{-c-(p-2p^2+p^3)nd - \pi(p-p^2)nd;$ $-c - spn - (p-p^2)nd - \pi(p-2p^2+p^3)nd\}$
IS	$\{-c - spn - (p-p^2)nd$ $-\pi(p-p^2)nd;$ $-(p-p^2)nd - \pi(p-p^2)nd\}$	$\{-c - spn - (p-p^2)nd$ $-\pi(p-2p^2+p^3)nd;$ $-c-(p-2p^2+p^3)nd$ $-\pi(p-p^2)nd\}$	$\{-c - spn - (p-2p^2+p^3)nd$ $-\pi(p-2p^2+p^3)nd;$ $-c - spn - (p-2p^2+p^3)nd$ $-\pi(p-2p^2+p^3)nd\}$

TABLE II: Game in Normal Form

When User i discovers a vulnerability and decides not to share it with User j, then the same vulnerability can be exploited by the attacker to launch an attack on User j (in case User j has not discovered that vulnerability), compromise the hypervisor with probability π and then compromise User i through a side channel attack. Thus, the possibility of side channel attack can constrain User i to share its discovered vulnerability. There is a cost s involved when a user shares a vulnerability. This represents the potential reputation lost, liability, and risk of lawsuit. Our stage game in normal form is represented in Table II, which is a symmetric game. Each user decides to invest in vulnerability discovery and to share those vulnerabilities simultaneously in a one-shot game. Thus, the three strategies available to a user are: not invest and not share ($\bar{I}\bar{S}$); invest and not share ($I\bar{S}$); and invest and share (IS). The strategy not invest and share ($\bar{I}S$) is not a possibility because a user that does not invest will not discover any vulnerability and cannot have any vulnerability to share.

The payoffs in Table II are calculated according to Equation (1), (2), (3), the Venn diagram in Figure 2, and the parameters in Table I. For instance, in the strategy profile ($\bar{I}\bar{S}$,$\bar{I}\bar{S}$), the payoff for User i has two components. A loss from direct attack is the product pnd because the attacker discovers a vulnerability with probability p, the expected number of vulnerabilities is n, and each vulnerability causes damage d. A loss from side channel attack is the product πpnd because a side channel attack goes through User j (thus the product pnd as explained above) and the hypervisor gets compromised with probability π. Furthermore, we add the cost c when a user invests and the cost spn when a user shares. The different probabilities are adjusted depending on the action chosen by a user and its opponent.

As another example, in the strategy profile $(I\bar{S}; I\bar{S}$, the payoff for User i has three components, $-c-(p-p^2)nd - \pi(p-p^2)nd$. The first component is c, the cost of investment. The second component is $-(p-p^2)nd$, the loss from direct attack with probability $p(1-p)$ or $(p-p^2)$. Recall that an attack is successful when an attacker discover a vulnerability (with probability p) while the attacker do not discover it (with probability $(1-p)$). Taking the product, this yields $p(1-p)$. The third component is $-\pi(p-p^2)nd$, the loss from side channel attack.

V. Game Analysis

The game in Table II is a symmetric game. We analyze the game and present the possible Nash Equilibrium (NE) profile.

Proposition 1 (a): The game has pure strategy Nash equilibrium $(\bar{I}\bar{S}; \bar{I}\bar{S})$, if the following two conditions are satisfied: (i) $c > p^2nd$, and (ii) $c + spn > (1+\pi)p^2nd$.

Proof: The symmetric game presented in Table II has pure NE strategy $(\bar{I}\bar{S}; \bar{I}\bar{S})$, if strategy $\bar{I}\bar{S}$ is the best response strategy of user i as well as user j. Therefore, user i and j's best strategy must be $\bar{I}\bar{S}$. Hence there is no profitable deviation from strategy $(\bar{I}\bar{S}; \bar{I}\bar{S})$. As the game is symmetric in nature, it is sufficient to check the best response conditions of one player, which will also be same for the other player too. This assumption has been considered for proving the other propositions presented later in the paper. Now we can derive the following conditions through best-response analysis.

$$-pnd - \pi pnd > -c - (p-p^2)nd - \pi pnd$$
$$\implies c > p^2nd \quad (4)$$
$$-pnd - \pi pnd > -c - spn - (p-p^2)nd - \pi(p-p^2)nd$$
$$\implies c + spn > (1+\pi)p^2nd \quad (5)$$

Proposition 1 (b): The game has pure strategy Nash equilibrium $(I\bar{S}; I\bar{S})$, if the following two conditions are satisfied: (i) $c < p^2nd$, and (ii) $s > \pi pd$.

Proof: Both users prefer to invest in vulnerability discovery but do not share their discoveries, if there is no profitable deviation from the strategy $(I\bar{S}; I\bar{S})$. We now obtain the necessary conditions.

$$-pnd - \pi(p-p^2)nd < -c - (p-p^2)nd - \pi(p-p^2)nd$$
$$\implies c < p^2nd \quad (6)$$
$$\text{And, } -c - spn - (p-p^2)nd - \pi(p-2p^2+p^3)nd < -c - (p-p^2)nd - \pi(p-p^2)nd$$
$$\implies s > \pi dp(1-p) \quad (7)$$

Proposition 1 (c): The game has pure strategy Nash equilibrium $(IS; IS)$, if the following two conditions are satisfied: (i) $c + spn < (1+\pi)ndp^2(1-p)$, and (ii) $s < \pi dp(1-p)$.

Proof: Both users invest in vulnerability discovery, and prefer to share the discovered vulnerability if there is no profitable deviation from the strategy profile $(IS; IS)$. Thus, $(IS; IS)$ will be NE strategy profile, provided the following conditions are satisfied.

$$-(p-p^2)nd - \pi(p-p^2)nd < [-c - spn - (p-2p^2+p^3)nd - \pi(p-2p^2+p^3)nd]$$
$$\implies c + spn < (1+\pi)ndp^2(1-p) \quad (8)$$

$$\text{And, } -c-(p-2p^2+p^3)nd-\pi(p-p^2)nd < -c-spn-(p-2p^2+p^3)nd-\pi(p-2p^2+p^3)nd$$
$$\implies s < \pi dp(1-p) \quad (9)$$

As we derived the necessary conditions for the three interesting NE strategy profiles, these relational constraints are not sufficient to show that there cannot exist any other equilibrium strategies in addition to these three. Existence of any equilibrium strategy other than the above three might create an imbalance situation in the framework, where one user can free-ride on the other user's shared information. Hence the other probable NEs must be strictly avoided, resulting in the following proposition:

Proposition 2:

1) If Equation (4) and (5) hold, then $(\bar{IS};\bar{IS})$ is the only Nash equilibrium of the game.
2) If Equation (6) and (7) hold, then $(I\bar{S};I\bar{S})$, is the only Nash equilibrium of the game provided one of the following conditions hold true. (i) $c > \pi pd$, or (ii) $c + spn > (1+\pi)p^2nd$
3) If Equation (8) and (9) hold, then $(IS;IS)$ is the only Nash equilibrium of the game.

Proof 2 (a): As shown in Equation (4) and (5), strategy $\bar{IS}$ is best response strategy of user i and user j due to the symmetric nature of the game. Thus $(\bar{IS};\bar{IS})$ is a NE strategy profile. It can be observed that the strategy profile $(I\bar{S};I\bar{S})$ cannot be a NE as the condition (4) and (6) act opposite to each other. Similarly, $(IS;IS)$ is also not NE because of the conflicting nature of condition (5) and (8). Now the NE profile $(IS;I\bar{S})$ is possible along with $(IS;IS)$, if (i) $s < \pi dp(1-p)$ and (ii) $c+spn < (1+\pi p)^2nd - \pi p^3nd$. However, the condition (ii) cannot be true because of Equation (5) states the opposite. Hence IS cannot be a best response strategy of user i, when user j plays strategy $I\bar{S}$ and vice-versa. Therefore, $(\bar{IS};\bar{IS})$ is the only NE of the game when equation (4) and (5) hold true.

Proof 2 (b): From Equation (6) and (7), we can state that $I\bar{S}$ is best response strategy of user i as well as user j. Thus, it is a NE strategy profile. Due to symmetric nature of the game, it is true that no other row/column strategy that intersects cell $(I\bar{S};I\bar{S})$ can be NE too. The strategy profile $(\bar{IS};\bar{IS})$ and $(IS;IS)$ also cannot be NE because relational constraints (6) and (7) cannot be valid for the corresponding NE conditions give in Equation (4) and (9) respectively. However, the strategy profiles $(IS;\bar{IS})$ and $(\bar{IS};IS)$ can be NE, provided the following conditions are satisfied:

$$-pnd-\pi pnd < -c-spn-(p-p^2)nd-\pi(p-p^2)nd$$
$$\implies c+spn < (1+\pi)p^2nd \quad (10)$$
$$\text{And, } -c-(p-p^2)nd-\pi pnd < -c-spn-(p-p^2)nd-\pi(p-p^2)nd$$
$$\implies s < \pi pd \quad (11)$$

However, this equilibrium strategy should be avoided due to the possibility of exploitation of a user's investment for bug discovery and sharing by another user, which is also termed as free-riding on another firm's efforts. Therefore, the strategy profile $(I\bar{S};I\bar{S})$ can be the only NE in this scenario, only when either condition (10) or (11) does not hold true.

Proof 2 (c): This proposition can be proved in the similar manner as the proposition 1(a) proved earlier. It can be observed that the condition (8) and (9) ensures that IS is the best response strategy of both players. This voids the chances of other possible NE strategies such as $(\bar{IS};\bar{IS})$ and $(I\bar{S};\bar{IS})$ because the relational constraints (8) and (9) do not hold true for their NE conditions (5) and (7). Thus, it is mandatory to show that the strategy profiles $(\bar{IS};I\bar{S})$ and $(I\bar{S};\bar{IS})$ are not NE strategies. These two strategies can be NE only when the conditions (i) $s > \pi pd$ and (ii) $c < p^2nd$ are satisfied. However, the condition (ii) cannot be true as the condition $s < \pi pd(1-p)$ should be true as per Equation (9) to let the strategy profile $(IS;IS)$ be the Nash equilibrium strategy. Hence, the strategy profile $(IS;IS)$ is the only NE profile in this situation provided the condition (8) and (9) are satisfied.

VI. Numerical Results and Discussion

In this section, we report the results obtained from numerical analysis, showing the regional Nash equilibrium plots under different values of the critical parameters like vulnerability discovery probability (p), damage caused due to exploiting the discovered vulnerability (d), probability that attacker compromises the hypervisor (π), cost of investment (c), and cost of sharing a vulnerability (s).

Figure (3) depicts the possible Nash equilibrium strategy profiles when the damage caused by a vulnerability and probability of attacker compromising hypervisor vary, assuming $c = 1, n = 10, s = 0.3$, and $\pi = 0.1$. We observe that users prefer to both invest for vulnerability discovery and share them when the damage caused due to the vulnerability and probability that an attacker compromises the hypervisor is high. So the investment towards vulnerability discovery and sharing with peers user helps the user to prevent the attacker's effort to find the same vulnerability and exploit it. However, when the damage cost is low and probability of compromising the hypervisor is also low, then the users better off not sharing their discoveries because they do not lose substantially than when sharing their vulnerabilities. The crucial point to notice here is that the users must invest to discover vulnerabilities regardless of the damage caused by exploiting the vulnerability and the probability of an attacker compromising the hypervisor, which will benefit the users to remain secured from the attacker's exploitation using the undiscovered vulnerabilities. However, sharing is a choice for the users dependent on the cost involved in it.

To understand the NE strategy profile when vulnerability discovery probability (p) and hypervisor compromising probability (π) vary, we have conducted experiment to find the Nash equilibrium strategies for different π and p values by fixing the value of damage (d) as 20 and keeping the value of other variables intact. As shown in Figure (4), the users prefer to invest in vulnerability discovery and share, if the

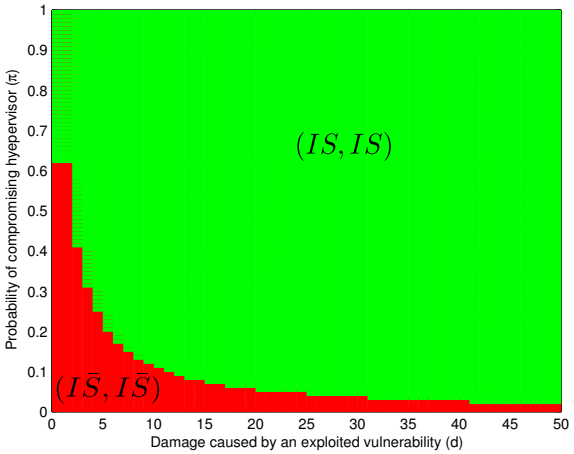

Fig. 3: Hypervisor Compromise probability Vs. damage cost

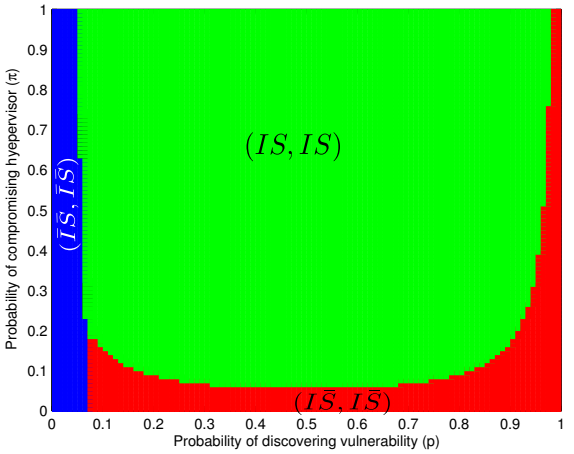

Fig. 4: Hypervisor Compromise probability Vs. vulnerability discovery probability

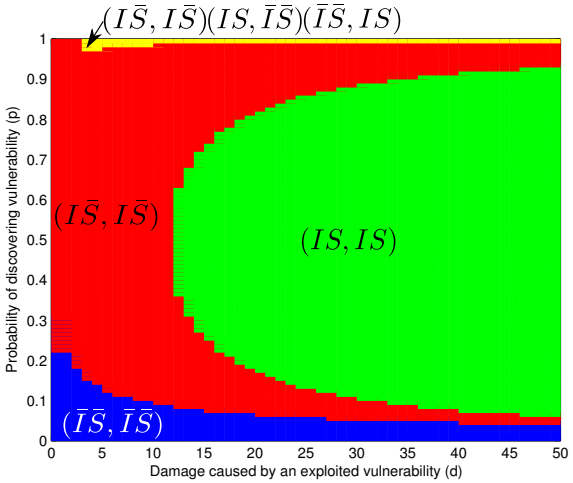

Fig. 5: Probability that attacker compromises hypervisor Vs. Damage caused

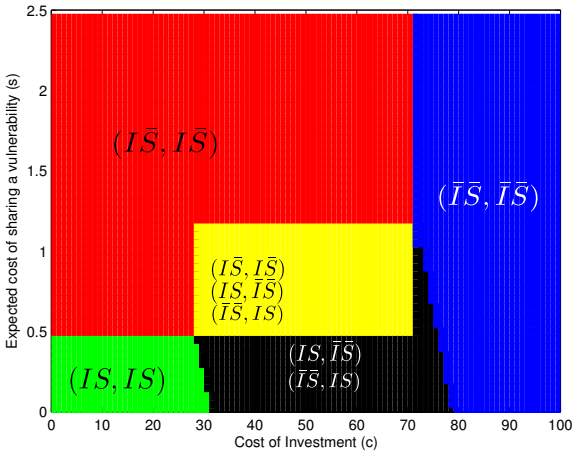

Fig. 6: Cost of sharing Vs. Cost of Investment

discovering probability is not very low or very high and hypervisor compromising probability is not very low. This case occurs due to benefits of investment and sharing, which cannot be derived from strategies $(\bar{I}\bar{S}; \bar{I}\bar{S})$ or $(I\bar{S}; I\bar{S})$. However, at very low probability of vulnerability discovery (p), all players are demotivated to invest. When p increases and π is low, the users prefer to invest without sharing their discoveries because the attacker is less likely to compromise the hypervisor. At very high probability of vulnerability discovery (p), sharing vulnerability is not profitable because each player has a high chance to discover all vulnerability itself without relying on the help of others.

In Figure (5), we analyze the NE strategy profiles at different regions of p and d combinations. Interestingly, we find that users are more inclined to invest in vulnerability discovery after a certain threshold of discovering probability (p) beyond which users are satisfied with their vulnerability discovery. However, they do not share these discoveries until damage cost exceeds a limit, after which the users better off taking the NE strategy $(IS; IS)$. It can be understood that users do not invest or share if the discovery probability is very low, as the difficulty in discovering any vulnerabilities prohibit investment. Hence, very high investment might not help in improving the vulnerability discovery process. There remains a small chance that a user might free-ride on another user's vulnerability discovery if they can easily discover the vulnerabilities, i.e. the probability of vulnerability discovery is close to 1. Therefore, this kind of scenario must be avoided to ensure that every player truthfully behaves and reciprocates the exchange of vulnerability discoveries.

Figure (6) gives a summary of NE profiles at different cost of investment (c) and sharing vulnerability (s) assuming $d = 20, p = 0.6$, while keeping other parameter intact. The users are inclined to invest for vulnerability discovery and share them only when the cost of investment and sharing is low. If the cost of investment is very high then the users avoid investment, thus do not share as well. It is observed that if the cost of investment is less than certain threshold value and expected cost of vulnerability sharing is more than certain limit, the users prefer not to share any vulnerabilities even though they invest to discover more vulnerabilities. The center region and black region in the plot are the special cases

where, one user might take strategy IS and other takes exactly opposite, resulting in a free-ride situation on the former user's shared information. Free-riding behavior can be prevented by choosing the cost of investment and cost of sharing carefully, which ensures that the players do not fall into the center or black region.

Finally, we plot the expected payoff variation with respect to increasing vulnerability discovery probability (p) and damage cost (d) in Figure (7). The dark bars in the figure point that the user changes his strategy after the occurrence of the bar. The net payoff function follows a downward concave characteristics w.r.t. probability of discovering vulnerability. We observe that when the damage cost is low ($d = 5$), then the user mostly sticks to the NE strategy $(I\bar{S}; I\bar{S})$ after the vulnerability discovery probability (p) exceeds 0.15, which is the center region of curve representing $d = 5$. However, when p is very low the users neither invest nor share. As shown in the plot, interesting scenarios occur when the damage cost (d) increases. The users choose $(\bar{I}\bar{S}; \bar{I}\bar{S})$ when p is close to 0, but they change their strategy to $(I\bar{S}; I\bar{S})$ quickly depending on how large is the damage (d). In the plot, the payoff jumps to a relatively higher value, when the users update their strategy $(I\bar{S}; I\bar{S})$ to $(IS; IS)$ and degrades to a lower value when they do the vice-versa. This strategy reversal happens when the probability of discovering vulnerability (p) is very high, where the users feel confident about discovering breaches on their own and do not want to share any of their discoveries with other user. As the damage (d) increases to very high value, the users mostly prefer to invest and share, whereas the payoff received is minimal.

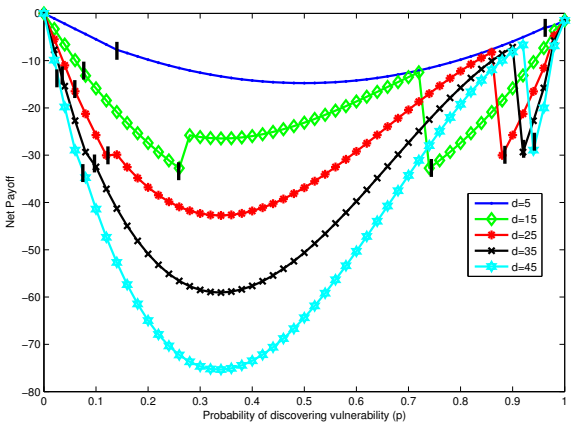

Fig. 7: Payoff Vs. Vulnerability discovery probability

VII. Conclusions

We have built an analytical framework that uses game theory to model cyber-threat information in public cloud computing. The game theoretic model captures the tradeoffs between the desirable security of public cloud users and the risk of sharing cyber-threats. Our game theoretic framework captures the conditions under which public cloud users are motivated to monitor and to share cyber-threats. At very low probability of vulnerability discovery, all players are demotivated to invest and then will not share any vulnerability. Also, user will not share vulnerability if they are easy to discover.

Future model extension includes the extension of the current model to more than two users and the consideration of heterogeneous vulnerabilities, heterogeneous players and incomplete information. We will also investigate the possibility of repeated interaction as a mean to enforce information sharing. Finally, we will compare the theoretical prediction of our game model with real data on cyber-threat information sharing.

References

[1] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] 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.

[3] E. Order, "13636–improving critical infrastructure cybersecurity," *Federal Register*, vol. 78, no. 33, p. 11739, 2013.

[4] N. I. of Standards, T. (NIST), and U. S. of America, "Framework for improving critical infrastructure cybersecurity," 2014.

[5] R. B. Myerson, "Game theory: analysis of conflict," *Harvard University*, 1991.

[6] D. K. Tosh, M. Molloy, S. Sengupta, C. A. Kamhoua, and K. A. Kwiat, "Cyber-investment and cyber-information exchange decision modeling," in *Proceedings of the 7th International Conference on Cyberspace Safety and Security (CSS)*. IEEE, 2015, pp. 1219–1224.

[7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 199–212.

[8] A. Bates, B. Mood, J. Pletcher, H. Pruse, M. Valafar, and K. Butler, "Detecting co-residency with active traffic analysis techniques," in *Proceedings of the 2012 ACM Workshop on Cloud computing security workshop*. ACM, 2012, pp. 1–12.

[9] C. Kamhoua, L. Kwiat, K. Kwiat, J. S. Park, M. Zhao, M. Rodriguez *et al.*, "Game theoretic modeling of security and interdependency in a public cloud," in *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*. IEEE, 2014, pp. 514–521.

[10] L. Kwiat, C. A. Kamhoua, K. A. Kwiat, J. Tang, and A. Martin, "Security-aware virtual machine allocation in the cloud: A game theoretic approach," in *Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on*. IEEE, 2015, pp. 556–563.

[11] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

[12] Q. Xiong and X. Chen, "Incentive mechanism design based on repeated game theory in security information sharing," in *2nd International Conference on Science and Social Research (ICSSR 2013)*. Atlantis Press, 2013.

[13] C. Z. Liu, H. Zafar, and Y. A. Au, "Rethinking fs-isac: An it security information sharing network model for the financial services sector," *Communications of the Association for Information Systems*, vol. 34, no. 1, p. 2, 2014.

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

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

[16] T. Moore, A. Friedman, and A. D. Procaccia, "Would a'cyber warrior'protect us: exploring trade-offs between attack and defense of information systems," in *Proceedings of the 2010 workshop on New security paradigms*. ACM, 2010, pp. 85–94.

[17] Y. Wu, G. Feng, N. Wang, and H. Liang, "Game of information security investment: Impact of attack types and network vulnerability," *Expert Systems with Applications*, vol. 42, no. 15, pp. 6132–6146, 2015.

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