Game Theoretic Modeling of Security and Interdependency in a Public Cloud

Charles A. Kamhoua[1], Luke Kwiat[2], Kevin A. Kwiat[1], Joon S. Park[3], Ming Zhao[4], Manuel Rodriguez[1]
{charles.kamhoua.1; luke.kwiat.ctr; kevin.kwiat; manuel.rodriguez-moreno.1.ctr}@us.af.mil; jspark@syr.edu; ming@cs.fiu.edu
[1]Air Force Research Laboratory, Information Directorate, Cyber Assurance Branch, Rome, NY
[2]University of Florida, Department of Industrial and Systems Engineering, Gainesville, FL
[3]Syracuse University, School of Information Studies (*i*School), Syracuse, NY
[4]Florida International University, School of Computing and Information Sciences, Miami, FL

***Abstract*— As cloud computing thrives, many small organizations are joining a public cloud to take advantage of its multiple benefits. Cloud computing is cost efficient, *i.e.*, cloud user can reduce spending on technology infrastructure and have easy access to their information without up-front or long-term commitment of resources. Moreover, a cloud user can dynamically grow and shrink the resources provisioned to an application on demand. Despite those benefits, cyber security concern is the main reason many large organizations with sensitive information such as the Department of Defense have been reluctant to join a public cloud. This is because different public cloud users share a common platform such as the hypervisor. A common platform intensifies the well-known problem of cyber security interdependency. In fact, an attacker can compromise a virtual machine (VM) to launch an attack on the hypervisor which if compromised can instantly yield the compromising of all the VMs running on top of that hypervisor. Therefore, a user that does not invest in cyber security imposes a negative externality on others. This research uses the mathematical framework of game theory to analyze the cause and effect of interdependency in a public cloud platform. This work shows that there are multiple possible Nash equilibria of the public cloud security game. However, the players use a specific Nash equilibrium profile depending on the probability that the hypervisor is compromised given a successful attack on a user and the total expense required to invest in security. Finally, there is no Nash equilibrium in which all the users in a public cloud will fully invest in security.**

Keywords- Cloud computing; cyber security; externalities; game theory; interdependency

I. INTRODUCTION

The cloud now figures largely in the information infrastructure. It is critical because of its rapidly expanding size and scope. What is more notable than the regular security issues any network would have is that public clouds exhibit a unique type of interdependency because of the ability of an attacker to propagate his attack through the hypervisor to all VMs using the hypervisor. This eliminates a very important aspect of regular network security in which an attacker would have to go through a multi-hop process in order to launch an indirect attack. Thus, a public cloud at its current stage leaves its users more susceptible to a 'bad neighbor' effect where an unsecure user might allow another to be indirectly attacked. In a dense network of VMs, an attacker may launch an indirect attack on a User *j* by first compromising the VMs of User *i* and then attacking User *j* as a prime target. This creates a risk connection between the users of a cloud where a 'large' player (one who has a high potential loss) will not use cloud services due to the risk imposed by a 'small' player (low potential loss from a successful compromise). This threat is worsened when a small player will not invest in security measures since it could (correctly) rationalize that an attacker will attack the larger user anyway, so investing would be pointless. Definitely, a single user of a public cloud cannot protect itself if other users are not doing the same. This means that a user will be protected if it defends itself while other users are also securing their asset. When there are two or more rational entities that face interdependent choices, we can use game theory to model their behaviors, as it is indeed "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers" [1].

There are several main contributions this paper makes. Primarily, it aims to model these behaviors that govern the actions of different users on the cloud using game theoretical concepts. Along with modeling the choices of cloud users, it will be shown that the small user imposes a negative externality, or a cost imposed unwittingly upon an otherwise uninvolved party—most notably the larger user. This will, in turn, spur the large player to invest more often than the small player since the large player is usually the prime target. The outcome: there is no Nash equilibrium in which all the players will fully invest in security. Lastly, we will prove that the probability that the hypervisor of a cloud is compromised given a successful attack on a VM will determine if we have a pure or mixed strategy Nash equilibrium.

After the related work in Section II, Section III will explain the cloud architecture common to the public cloud model that is incorporated into our game model. Section IV will explain and set up the problem in the context of game theory and diagram the problem in a normal form game. Section V describes and shows the equilibria changes in accordance with changes to the game parameters. Section VI show the numerical results that graphically demonstrates how the equilibrium changes following a change in the parameters. Section VII concludes the paper.

II. BACKGROUND AND RELATED WORK

Through globalization, firms are becoming increasingly dependent upon each other. Thus, it would be logical to assume that their choices would reflect the actions of their

Approved for Public Release; Distribution Unlimited: 88ABW-2013-5145
Dated 9 DEC 2013.

978-1-4799-5063-8 2014
U.S. Government Work Not Protected by U.S. Copyright
DOI 10.1109/CLOUD.2014.75

competitors and benefactors with a given set of information. A paper from the National Bureau for Economic Research (NBER) carefully looked at multiple scenarios involving game theory and the subsequent interdependency of the players in airline security [2]. It was shown that with airline security, one's own investment in baggage security was heavily dependent on the choices of the other airline. This was since one's own security is compromised by the lack of security on another airline or complemented by the reinforcement of the rival's airline security. However, unlike the airline interdependent security problem where a bomb can only destroy one airline, a virus in a public cloud or computer network can compromise many VMs including the VM in which the attack originated.

A multi-tenant public cloud environment is analogous to our airline example: different users (the airline's passengers) share common resources (the airline's baggage handlers) presenting a new security risk that does not exist when each user has dedicated servers (each passenger having a private airplane). Unlike an organization having exclusive use of computational resources, the resource sharing that occurs in the cloud enables unforeseen exploitation of weaknesses by attackers. In our airline example, merely securing the baggage handlers may be insufficient; instead, passengers may have to pass a personal, individual screening. Similarly, the commonality of computational resources without an equal commonality of user-instantiated security creates an avenue for launching an attack on other tenants i.e., a negative externality due to interdependency and resource sharing.

In Tamer Basar's and Tansu Alpcan's book [3], they explain the devastating costs of failure to properly protect a network. They show how an attacker can infiltrate a network at one node, but spread to other nodes (or infrastructures) due to contagion. Kamhoua *et al*. analyzed cyber security problem that cannot be solved by a single agent [4]. Their evolutionary game model shows that security depends on the initial trust among the agent.

Service platforms that cloud computing provide 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 paper 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 (further information can be seen in [5]). Although private clouds do share some of the benefits and drawbacks of public clouds, the issues of privacy, security, and trust arise from mainly 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 paper 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.

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 resource makes privacy and perfect isolation implausible. There is a risk that 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. Some of the resources can be partitioned (*e.g*., CPU cycles, memory capacity, and I/O bandwidth). VMs also share 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 attack. Although a multi-tenant public cloud-computing environment provides various advantages, it also introduces new challenges and concerns, especially on security issues. For instance, the security problems on a shared cloud resource (e.g., cloud storage devices, network services, software components, etc.), which are originally rooted from one of the tenants via internal vulnerabilities or external cyber-attacks, may eventually affect the service quality and security of all the tenants in the same cloud-computing environment. Unfortunately, we cannot simply assume that there would be a single authority who could comprehensively maintain all the possible issues, not only technical but also non-technical, across the tenants.

Moreover, existing cloud service providers do not provide sufficient security guarantees to their tenants. In fact, the service-level agreements (SLAs) of representative cloud providers (e.g., Amazon EC2/S3, Windows Azure, Google Compute Engine) specify only the provisions related to service up time, and there is no mentioning of security in these SLAs at all.

Many researchers have investigated cache based side channel. Ristenpart *et al*. [6] 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*. [7] 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.

Given the danger of a cross-side channel attacks, some user may require physically isolated resource to the cloud provider. Zhan *et al.* [8] introduce HomeAlone - a defensive tool that help a user to determine if his VMs have an exclusive use of a physical machine. HomeAlone can detect the activity of an intruder's co-resident VM by analyzing a portion of the L2 memory cache set aside by his VMs. The same technique can be used to detect adversarial VMs which try to extract information through the side channel due to their usual cache activity pattern. This solution, however, requires that all the user VMs to be co-resident which is often difficult to achieve and make them more vulnerable to hardware and hypervisor failures. We consider in this paper only scheme in which the VMs from different users share the same resources.

III. System Model

Fig. 1 illustrates our system model: A public cloud with n users that we denote User 1, User 2 … User n. Each user runs several applications illustrated by Application 1 … Application k in Fig. 1. Technically, the users may run different number of applications without any impact on this model. 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 Fig. 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 in Fig. 1. The hypervisor can be of different types such as the Kernel-based Virtual Machine (KVM), Xen, and VMware. The common factor is that the VMs share the same platforms.

We consider the possibility of a random hardware failure to be a rare event and neglect that possibility in our analysis. It is well known that the users security heavily depend on the cloud provider. We are analyzing security interdependency among the users. Therefore our model considers that 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. This means that the public cloud provider takes all the necessary measures to prevent an attacker from directly compromising the hypervisor without using a compromised VM. This is to separate cloud client-to-client interdependency and cloud host-to-client interdependency. However, any model that analyzes cloud host-to-client interdependency can be superposed to our model.

We distinguish two types of attack 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. We consider that all the users suffer the consequences (damage) if the hypervisor is compromised. This is because an attacker that compromises the hypervisor can then compromise all the VMs on that public cloud.

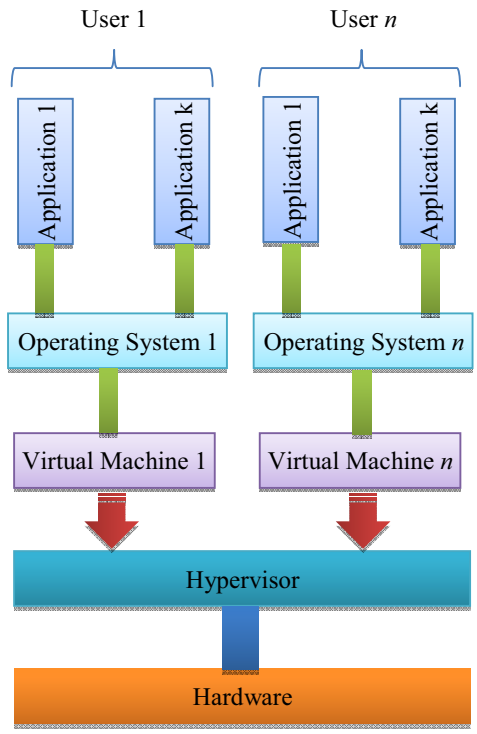

Figure 1: System Model Illustration

We can see that an unrestricted attack cause collateral damage. A direct attack on User i can go through his VMs to compromise the hypervisor and ultimately affect the VM of another User j. We also call that an indirect attack on User j.

IV. Game Model

This section considers a game with three players: An attacker and two users (User i and User j). The three players are assumed to be rational, which means that each player has an understanding of the system and has the ability to perform the necessary calculation to only take the actions that maximize his expected payoff. The attacker has two strategies: launch an attack on User i (A_i) and launch an attack on User j (A_j). The attacker can only use one of the two strategies at a time. The attacker strategy to launch an attack on User i may consist of a multi-stage process involving steps such as scanning, collecting information, credential compromising, executing attack payload, establishing backdoor, cleaning footholds and avoiding firewalls. Choosing to invest is a binary decision for each user in which the two users can either *Invest* (I) in security to maintain a minimum security standard and increase their protection or *Not invest* (N), *i.e.,* there is no partial investment in security. The strategy Invest may consist of multiple actions such as system monitoring, reconfiguration, patching, updating software, and buying a new antivirus. Investment in security requires a total expense e. A strategy profile is a 3-tuple that indicates the action of each player, e.g., the strategy (N, I, A_j) shows that User i does not invest (N), User j invests (I), and the attacker attacks User j (A_j).

The probability of a successful attack on a user, given that he has invested in security, is q_I and the probability of a successful attack on a user, given that he has not invested, in security is q_N. We assume that $0 \leq q_I < q_N \leq 1$. (1)

We have $q_I < q_N$ because any rational user will only invest in security measures that diminish his chance to get compromised.

The probability that the hypervisor is compromised given a successful attack on a user is denoted π . Our model considers that at least some successful attack on a VM will reach the hypervisor or that $\pi > 0$. In fact $\pi = 0$ means that a successful attack on a VM would never reach the hypervisor which would be a strong assumption. Also, not all the successful attacks on a VM can compromise the hypervisor ($\pi < 1$). Thus we have $0 < \pi < 1$. (2)

We consider that there is a high profile User *j* and a low profile User *i*. In case of a security breach, the high profile user incurs more loss than the low profile user. The high profile User *j's* expected loss from a security breach is L_j and the expected loss from User *i* is L_i. Then we consider that

$$0 < L_i < L_j. \quad (3)$$

We will show that this imbalance affects the investment decision of each player and may yield positive and negative externalities. A positive (negative) externality is an action of a player that transfers a positive (negative) effect onto a third party. In fact, when a (high profile) user in a public cloud invests in security to protect his applications, operating system and VM, he also protects the hypervisor which in turn protects other users from an indirect attack or cross-side channel attack. This yields a positive externality to other users in a public cloud. On the contrary, if a (low profile) user chooses not to invest in security, he provides an easy attack path to the hypervisor and thus exposes all other user of a public cloud to a cross-side channel attack. This yields a negative externality to other users in a public cloud.

The accuracy of our model depends on the correct estimation of the probabilities q_I, q_N, π and the loss $L_i$and L_j. We propose two different approaches to estimation. The first approach is the QuERIES approach [9]. The QuERIES approach estimate the probabilities and costs of successful attacks by first building an attack graph represented as a Partially Observable Markov Decision Process (POMDP). Then QuERIES uses a controlled red-team experiment and information market mechanisms to estimate the POMDP parameters. The outcome of an information market is a collective estimate of a quantity. The red-teams have real financial incentives for making correct predictions of the POMDP probabilities. Finally, the POMDP's optimum policy is calculated to derive the different probabilities and cost.

The second approach to estimate the relevant probabilities and cost associated with our model is based on historical data. In fact, In October 2011, the United States Securities and Exchange Commission (SEC) issued a new guidance [10] requiring that companies disclose cyber incidents including a description of the costs, other consequences and the relevant insurance coverage. Those data can now be aggregated to estimate the relevant probabilities and cost associated with our model.

In addition, each user has a reward R from using the cloud computing services. The reward R can be calculated as a function of a user's multiple benefit of using the cloud such as: reduced spending on technology infrastructure, easy access to their information without up-front or long-term commitment of resources, and dynamically grow and shrink the resources provisioned to an application on demand.

Finally, we consider that a User *i* can detect and identify a co-resident VM from User *j* in the cloud via side-channel analysis as in HomeAlone [8]. Further, a skillful attacker will first scan a public cloud to learn about the different users, their weakness and vulnerabilities before to launch an attack. Also, each player's expected loss from a security breach and the related probability, his total expense required to invest in security and the reward from using the cloud are known or can be estimated by others [9-10]. Therefore, our model assumes that the player's identity, strategy and payoff are common knowledge among the players.

Table I shows the game model in normal form. We can see that Table I is a combination of two tables (left and right). The left table shows the game model when the attacker target User *i*. Therefore, User *j* can only be subject to collateral damage after a successful attack on User *i* and compromising of the hypervisor (which can happen with probability $q_I\pi$ if User *i* invest or probability $q_N\pi$ if User *i* do not invest). Similarly, the right table shows the game model when the attacker targets User *j* and User *i* can only be subject to collateral damage. The fourth line in each table shows when User *i* chooses to invest while the fifth line shows when User *i* chooses not to invest. In each table, the decision of User *j* is represented in the third (Invest) and fourth (Not invest) column. The payoffs in each block are represented in three lines. The first line is User *i's* payoff. The second line is User *j's* payoff. The attacker payoff is represented in the third line.

TABLE I: GAME MODEL IN NORMAL FORM

		Attack *i*	
		User *j*	
		I	*N*
User *i*	*I*	$\{R - e - q_I L_i;$ $R - e - q_I \pi L_j;$ $q_I L_i + q_I \pi L_j\}$	$\{R - e - q_I L_i;$ $R - q_I \pi L_j;$ $q_I L_i + q_I \pi L_j\}$
	N	$\{R - q_N L_i;$ $R - e - q_N \pi L_j;$ $q_N L_i + q_N \pi L_j\}$	$\{R - q_N L_i;$ $R - q_N \pi L_j;$ $q_N L_i + q_N \pi L_j\}$

		Attack *j*	
		User *j*	
		I	*N*
User *i*	*I*	$\{R - e - q_I \pi L_i;$ $R - e - q_I L_j;$ $q_I \pi L_i + q_I L_j\}$	$\{R - e - q_N \pi L_i;$ $R - q_N L_j;$ $q_N \pi L_i + q_N L_j\}$
	N	$\{R - q_I \pi L_i;$ $R - e - q_I L_j;$ $q_I \pi L_i + q_I L_j\}$	$\{R - q_N \pi L_i;$ $R - q_N L_j;$ $q_N \pi L_i + q_N L_j\}$

The payoffs are calculated as follows: If the player chooses the strategy profile (I, I, A_i), both users invest (play I) while the attacker's target User i (A_i) (left table, fourth line, third column). Then both users get the reward R. Both users incur expense e because both of them have invested in security. Since the attacker targets User i that will be compromised with probability q_I (because User i has invested), it will incur a loss L_i if compromised. This will result in an expected loss of $q_I L_i$. User j is not targeted but can incur a loss L_j if the attack on User i is successful (which happen with probability q_I) and the hypervisor is compromised (which happen with probability π). This is an expected loss of $q_I \pi L_j$ and can also be called collateral damage or loss from an indirect attack. The attacker payoff is the sum of the expected loss of all the users $U_a(I, I, A_i) = q_I L_i + q_I \pi L_j$. The attacker's partial payoff $q_I L_i$ comes from a direct attack on User i while the second part of his payoff $q_I \pi L_j$ is the result of an indirect attack on User j through the hypervisor. The players' payoffs in the other seven strategies profiles are calculated in a similar way.

V. GAME ANALYSIS

The main goal of this analysis is to derive the different Nash equilibria of the game in Table I and understand its consequence for both users. At a Nash equilibrium profile, no player can increase his payoff by a unilateral deviation. Also, each player is playing his best response to other players' best strategies. Therefore the Nash equilibrium can help predict the behavior of any rational player *i.e.*, that want to maximize his payoff in a game.

We observe that a user that is the prime target must be hurt before the other user suffers a collateral damage. Recall that the prime target's VM must be cracked before the hypervisor is compromised. Thus, we consider in the remaining of this analysis that each user prefers to invest to not investing when he believe that he is the attacker's prime target. For User i this translates to

$$R - e - q_I L_i \geq R - q_N L_i \Rightarrow e \leq (q_N - q_I) L_i \qquad (4)$$

Similarly, for User j this translates to

$$R - e - q_I L_j \geq R - q_N L_j \Rightarrow e \leq (q_N - q_I) L_j \qquad (5)$$

Also observe that investing in security is the best option to either User i or User j if and only if he believes that he will be the attacker's prime target. Also, the attacker targets only the player that gets him the higher total payoff (consisting of a direct and indirect payoff).

Theorem 1:

If $\pi \leq \pi_0 = \frac{q_I L_j - q_N L_i}{q_N L_j - q_I L_i}$, then the game in Table I admits a pure strategy Nash equilibrium profile (N, I, A_j).

If $\pi > \pi_0$, there are three possible mixed strategy Nash equilibria depending on the required expense for security e.

Proof:

A simple analysis of the eight different pure strategies in Table I shows that the only possible pure Nash equilibrium is when User j invests while User i does not and the attacker plays A_j. This is because in other cases, there is at least one player who can increase his payoff by a unilateral deviation.

When User j invests while User i does not.

$$\begin{aligned} U_a(N, I, A_j) - U_a(N, I, A_i) \\ &= (q_I \pi L_i + q_I L_j) - (q_N L_i + q_N \pi L_j) \\ &= (q_I L_i - q_N L_j)\pi + (q_I L_j - q_N L_i) = f(\pi) \end{aligned}$$

We can see that $f(\pi)$ is a linear function with slope $(q_I L_i - q_N L_j)$ and initial value $(q_I L_j - q_N L_i)$. From (1) and (3) we have the slope $q_I L_i - q_N L_j < 0$. Thus, $f(\pi)$ is decreasing. Moreover, there is a unique value of π such that

$$f(\pi) = 0 \Rightarrow \pi = \pi_0 = \frac{q_I L_j - q_N L_i}{q_N L_j - q_I L_i}, \qquad (6)$$

Furthermore, we have $f(\pi) > 0$ for $\pi < \pi_0$ and $f(\pi) < 0$ for $\pi > \pi_0$.

Also, $f(1) = (q_I L_i - q_N L_j) + (q_I L_j - q_N L_i)$

$$= (q_I - q_N)(L_i + L_j) < 0. \qquad (7)$$

The last inequality holds because of (1).

In addition, the initial value is

$$f(0) = q_I L_j - q_N L_i, \qquad (8)$$

which can be either negative or positive. Observe that because of (2) the condition $\pi \leq \pi_0$ can holds if $0 < \pi_0 < 1$, and by the Intermediate Value Theorem and based on (7) and (8) is only possible when $f(0) > 0 \Rightarrow q_N L_i < q_I L_j \Rightarrow$

$$L_i < \frac{q_I}{q_N} L_j. \qquad (9)$$

Then we can distinguish two cases (a) and (b).

Case (a): If $\pi \leq \pi_0$, then we have $U_a(N, I, A_j) - U_a(N, I, A_i) \geq 0$. Thus the attacker prefers to attack User j than to attack User i. User j prefers to invest than not to invest (see (5)). User i not being the attacker's prime target prefer not to invest. Then the strategy profile (N, I, A_j) is the pure strategy Nash equilibrium of the game because no player can increase his payoff by a unilateral deviation.

Case (b): If $\pi_0 < \pi$ (regardless of the sign of $f(0)$) we have $f(\pi) < 0$ and then $U_a(N, I, A_j) - U_a(N, I, A_i) < 0$. The attacker prefers to attack User i than to attack User j. Thus the strategy profiles (N, I, A_j) cannot be Nash equilibrium because the attacker can increase his payoff by changing his strategy to A_i. This get us to the strategy profile (N, I, A_i) that also cannot be a Nash equilibrium because User i being the attacker's prime target can increase his payoff by changing his strategy from N to I (see (4)). Then the attacker will prefer to play A_j than A_i. After that, User i will prefer changing his strategy from I to N. This brings us back to the strategy (N, I, A_j) . Therefore, this circular reasoning tells us that there is no pure strategy Nash equilibrium. However, there will be a mixed strategy Nash equilibrium that is the object of our next analysis.

Mixed Strategy Nash Equilibrium:

To find the mixed strategy Nash equilibrium, we set three variables α, β, λ with $0 \leq \alpha, \beta, \lambda \leq 1$. (10)

α represents the probability by which the User i plays I. Similarly, User j plays I with probability β and the attacker attack j with probability λ.

By definition, User i plays a mixed strategy if and only if his payoff $U_i(I)$ when playing I is equal to his payoff $U_i(N)$ when Playing N. This translates to:

$$U_i(I) = U_i(N) \Rightarrow (1 - \lambda)\beta(R - e - q_I L_i)$$

$$+(1-\lambda)(1-\beta)(R-e-q_I L_i)+\lambda\beta(R-e-q_I\pi L_i)$$
$$+\lambda(1-\beta)(R-e-q_N\pi L_i)=(1-\lambda)\beta(R-q_N L_i)$$
$$+(1-\lambda)(1-\beta)(R-q_N L_i)+\lambda\beta(R-q_I\pi L_i)$$
$$+\lambda(1-\beta)(R-q_N\pi L_i)$$
$$\Rightarrow \lambda=\lambda_i=\frac{(q_N-q_I)L_i-e}{(q_N-q_I)L_i}. \quad (11)$$

Equation (4) shows that $0 \le \lambda_i \le 1$. Also,

$$U_i(I) < U_i(N) \Rightarrow 0 \le \lambda_i < \lambda \le 1, \quad (12)$$

and

$$U_i(I) > U_i(N) \Rightarrow 0 \le \lambda < \lambda_i \le 1. \quad (13)$$

This means that, if the attacks on User *j* are more frequent than λ_i(and then User *i* is attacked less often), then User *i* prefers to play *N*. User *i* plays *I* otherwise.

Similarly, User *j* plays a mixed strategy if and only if his payoff $U_j(I)$ when playing *I* is equal to his payoff $U_j(N)$ when playing *N*. This translates to:

$$U_j(I)=U_j(N) \Rightarrow \lambda=\lambda_j=\frac{e}{(q_N-q_I)L_j}. \quad (14)$$

Equation (5) shows that $0 \le \lambda_j \le 1$. Also,

$$U_j(I) < U_j(N) \Rightarrow 0 \le \lambda < \lambda_j \le 1, \quad (15)$$

and

$$U_j(I) > U_j(N) \Rightarrow 0 \le \lambda_j < \lambda \le 1. \quad (16)$$

Further, the attacker plays a mixed strategy if and only if his payoff $U_a(A_i)$ when attacking User *i* is equal to his payoff $U_a(A_j)$ when attacking User *j*. This translates to:

$$U_a(A_i)=U_a(A_j) \Rightarrow \beta(L_j+\pi L_i)-\alpha(L_i+\pi L_j)$$
$$=\left(\frac{q_N}{q_N-q_I}\right)\left[(L_j+\pi L_i)-(L_i+\pi L_j)\right]. \quad (17)$$

Given the condition in (11), (14) and (17), we can distinguish three cases that we denote Case 1, 2 and 3 depending on if $\lambda_j=\lambda_i$, $\lambda_j<\lambda_i$, or $\lambda_j>\lambda_i$. Furthermore, we will see that the total expense required to invest in security *e* determine which of the mixed strategy is used.

Case 1: If $\lambda_j=\lambda_i \Rightarrow e=e_0=\frac{(q_N-q_I)L_iL_j}{L_i+L_j}$, (18)

then any strategy profile $\{\alpha I+(1-\alpha)N;\beta I+(1-\beta)N;\lambda_j A_j+(1-\lambda_j)A_i\}$, with α and β set according to (17) is a mixed strategy Nash equilibrium. Recall that (10) must hold.

We can see that when $\lambda_i \neq \lambda_j$, the conditions in (12)-(13) and (15)-(16) dictate that only one user plays a mixed strategy at a time while the other plays a pure strategy. Moreover the attacker chooses the value of λ that corresponds to the user playing the mixed strategy. This consideration is critical to understand the next two cases.

Case 2: If $\lambda_j<\lambda_i \Rightarrow e<e_0=\frac{(q_N-q_I)L_iL_j}{L_i+L_j}$, (19)

and $\lambda=\lambda_i$, then according to (16), User *j* plays the pure strategy *I*. Thus $\beta=1$. Setting $\beta=1$ in (17) yields

$$\alpha=\alpha_0=\frac{q_N(L_i+\pi L_j)-q_I(L_j+\pi L_i)}{(q_N-q_I)(L_i+\pi L_j)}. \quad (20)$$

We can verify that $0<\alpha_0<1$ when $\pi>\pi_0$ and (1), (2) and (3) hold. Therefore, the strategy profile $\{\alpha_0 I+(1-\alpha_0)N;I;\lambda_i A_j+(1-\lambda_i)A_i\}$ is a mixed strategy Nash equilibrium. However, If $\lambda_j<\lambda_i$ and $\lambda=\lambda_j$, then we can verify that there is no possible mixed strategy.

Case 3: If $\lambda_j>\lambda_i \Rightarrow \frac{(q_N-q_I)L_iL_j}{L_i+L_j}<e<(q_N-q_I)L_i$. (21)

Note that the last inequality must hold because of (4). Thus according to (12), when $\lambda=\lambda_j$, User *i* plays the pure strategy *N*. Thus $\alpha=0$. Setting $\alpha=0$ in (17) yields:

$$\beta=\beta_0=\frac{q_N[(L_j+\pi L_i)-(L_i+\pi L_j)]}{(q_N-q_I)(L_j+\pi L_i)}. \quad (22)$$

We can verify that $0<\beta_0<1$ when $\pi>\pi_0$ and (1), (2) and (3) holds. Therefore, the strategy profile $\{N;\beta_0 I+(1-\beta_0)N;\lambda_j A_j+(1-\lambda_j)A_i\}$ is a mixed strategy Nash equilibrium. However, If $\lambda_j>\lambda_i$ and $\lambda=\lambda_i$, then we can verify that there is no possible mixed strategy. ■

In short, it is important for a high profile user to be collocated with other high profile user in a public cloud. The notion of externality has always being perceived in the housing market. In fact, the value of other home in the same neighborhood influences the price of any particular home. As a consequence, a rational home buyer will try to find out who are his neighbors before buying a home. A similar concept should apply to cloud computing. It can be important that a cloud user knows who his neighbors are. A cloud user's neighborhood is the set of user with whom he shares the same resource (hypervisor, CPU cycle, DRAM of the physical machine, physical memory, and network buffers).

VI. Numerical Results

Our game analysis has provided a detailed exposition of our game model and its equilibrium properties. The numerical results in this section are derived from our game analysis. The main variables used in calculating pure and mixed strategy equilibrium were $R, q_I, q_N, L_i, L_j, \pi$, and e. We will use specific numbers to provide concrete examples and examine the three cases in which we will increase e, L_j, and π individually while *ceteris paribus*.

A. Changes in User j's Payoff with Probability π

In this first scenario, we will take the value of π to be variable while setting values for all the other parameters. We will take $q_N=0.5, q_I=0.1, R=1.2, L_i=1, L_j=10$. Those values are chosen to illustrate some of the non-intuitive implication of our game model. Using (6), we can see that $\pi_0=0.102$. Furthermore, with (18) we can see that $e_0=0.3636$. Moreover, (21) gives us $0.3636<e<0.4$. Recall that in case of a mixed strategy Nash equilibrium ($\pi>\pi_0=0.102$), the value of *e* determines which of the mixed strategy Nash equilibrium (Case 1, 2 or 3) is selected by the players. In Fig. 2, we set $e=0.3$ ($e<e_0$) so that once the critical value of π is reached, the mixed strategy Nash equilibrium will be as Case 2.

We immediately see that the payoff for User *j* in pure Nash equilibrium is negative. When the payoff of a rational user is negative, he prefers not to use the cloud. So, for all values of $\pi \le 0.102$ the User *j*, will not use the cloud because the risk of security breach and negative externalities of using the cloud are greater than the multiple benefits that cloud computing provides. Recall that in the pure strategy

Nash equilibrium, User j is at a disadvantage because he is the attacker's only target.

However, at $\pi = 0.102$ there is a strategy change from pure to mixed due to (6) as at this point the strategies shift. There is a concurring change in the function used as it is a new set of equations governing the strategies. This allows for a positive payoff for $0.102 < \pi \leq 0.47837$ and implies that User j will participate in the cloud for the aforementioned values of π. These results are seemingly counterintuitive since the hypervisor has a higher probability of being compromised when User j participates in cloud activities than when he does not. This is explained by the equilibrium shift to a mixed strategy where the attacker is not only attacking User j but also User i. This lowers User j's potential loss and thus shifts his payoff upwards.

Examining Fig. 2 again, the payoff becomes negative again as π crosses 0.47837, which shows that User j will again not participate in the cloud for all values of $0.47837 < \pi \leq 1$ since the probability of being compromised from an indirect attack is now too high to justify cloud usage.

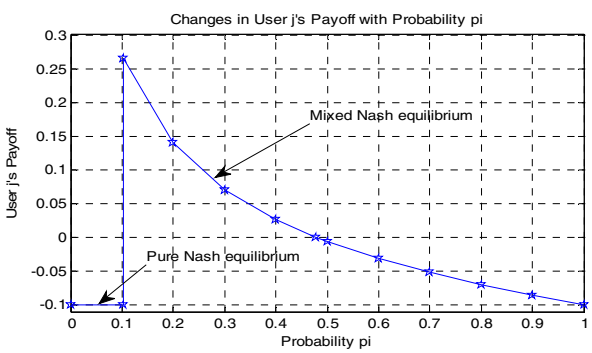

Figure 2: Changes in User j's payoff with probability π with $e < e_0$.

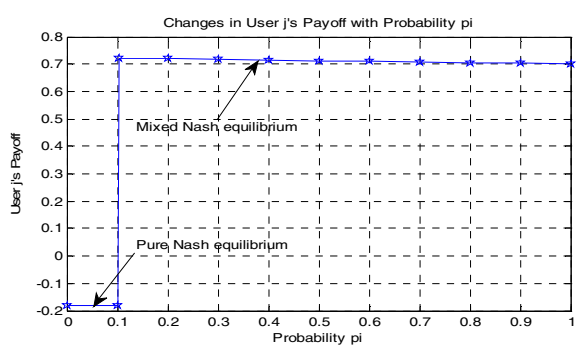

Figure 3: Changes in User j's payoff with probability π with $e > e_0$.

By setting $e = 0.38$ and upholding (21), Fig. 3 shows the strategy shift from pure Nash equilibrium to the mixed Nash equilibrium in Case 3. Once π crosses 0.102, a change in payoff from negative to positive, as in Fig. 2, makes the cloud a viable option. Interestingly, the payoff does not cross over again to become negative after this original movement of equilibriums. This means that for all values of $0.102 < \pi \leq 1$, User j will participate in the cloud if $0.3636 < e < .4$. Another surprising result is that User j's payoff is higher in Fig. 3 compared to Fig. 2 although the required expense in security e in Fig. 3 is higher. User j's invests with probability β_0 in Case 3 as opposed to the pure strategy I in Case 2 which results in greater savings when the expense e is big.

B. *Changes of User j's Payoff with the Security Expense e*

In the case of $\pi \leq 0.102 = \pi_0$, User j has only one (pure) strategy, whose payoff of $R - e - q_I L_j$ yields a simple linear function of e that we do not represent here.

In Fig. 4, we have set $\pi = 0.11 > \pi_0$ and thus we can see the three different case of mixed strategy: Case 2 ($e < 0.3636$), Case 1 ($e = 0.3636$) and Case 3 ($3636 < e < .4$). The major shift from Case 2 to Case 3 occurs at the threshold of $e = 0.3636$ (Case 1) due to (18) stated in the previous analysis. For $0 \leq e < 0.3636$, the change from using to not using the cloud occurs at $e = 0.08606$ when the payoff becomes negative.

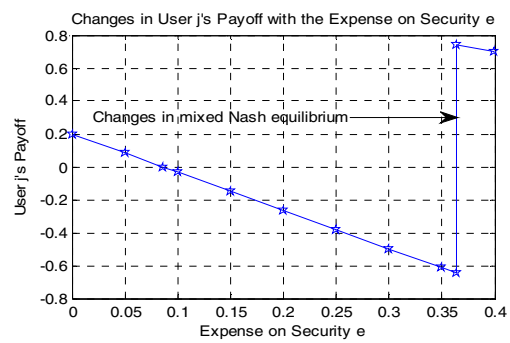

Figure 4: Changes of User j's payoff with the expense e with $\pi > \pi_0$.

When the expense e increases and $0.3636 < e < 0.4$, the shift in mixed Nash equilibrium from Case 2 to Case 3 causes the payoff to change and become positive. Thus it becomes possible for User j to profitably use cloud services. This is a counter intuitive result from this analysis. One may expect an increase of the expense e to never benefit User j. However, in this game theoretic setting, User j's payoff depends not only of his own action but also on the action of User i and the attacker. The increase of the expense e changes User i's and the attacker's strategy in such a way that it has an overall positive effect on User j's payoff. In Case 3, User j invests with probability β_0 as opposed to 1 in Case 2. This yields some savings that increase User j's overall payoff.

C. *Changes in User j's payoff with his loss from security breach L_j*

We will now look in Fig. 5 at the phenomena in equilibrium changes associated with varying values of L_j. For the rest of the analysis of L_j, we will set $\pi = 0.1$ and $e = 0.3$. Recall that we have set $L_i = 1$. Therefore, L_j is a direct indication of how much time L_j is bigger than L_i.

As can be seen in Fig. 5, any value of $L_j \geq 9.8$ will result in a pure Nash equilibrium due to (6). Further, (18) shows that when $3 < L_j < 9.8$ the mixed strategy Nash equilibrium profile of Case 2 will hold, Case 1 holds for $L_j = 3$, and if $1 < L_j < 3$, then Case 3 will be used.

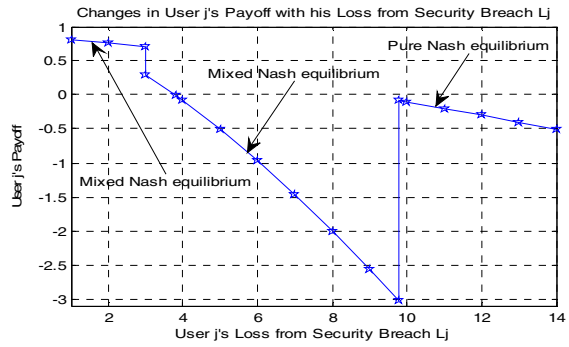

Figure 5: Changes in User j's payoff with his loss from security breach L_j.

These results show that Case 3 is the "best" of all the equilibriums because User j's potential loss L_j is so close to User i's loss L_i. An obvious result is that User j's payoff is maximized in Case 3 when L_j is close to $L_i = 1$. That is because there is no imbalance between L_i and L_j and thus the negative externalities are minimized. The negative externality in a public cloud security can be mitigated by putting VMs that have similar potential loss from a security breach in the same physical machine. However, a surprising result is that User j' s payoff jump up when switching from the mixed Nash equilibrium (Case 2) to the pure Nash equilibrium despite the fact that L_j become substantially greater than L_i. This prediction is not possible without a thorough game theoretic analysis.

A change in the value of R will cause the graph to translate upward or downward depending on the new value of R selected. For instance, if the reward for using the cloud is increased from 1.2 to 4.4, the entire payoff scheme from $1 \leq L_j \leq 14$ becomes positive since the increased level of reward increases the payoff.

Remark: The model we have presented in this paper has considered two users and one attacker. However, our model can be extended to more than two users and multiple attackers. Regarding the threshold value of π below which we have a pure strategy Nash equilibrium, (6) translate to

$$\pi_0^* = \frac{q_I L_n - q_N L_{n-1}}{q_N L_n - q_I L_{n-1}}. \qquad (23)$$

L_n is the loss of the biggest user whiles L_{n-1}represents the second biggest user. As before, the game admits a multitude of mixed strategies if $\pi > \pi_0^*$. The expense e will determine the specific mixed strategy the players choose. An extended analysis is not shown because of space limitation.

VII. Conclusion

The lack of an accurate evaluation of the negative externalities that a high profile organization using the cloud may be at the mercy of has prevented many such organizations to join a public cloud and take advantage of its multiple benefits. The negative externalities of using a public cloud come from the fact that the users are not perfectly isolated from one another. They share common resources such as the hypervisor, the last-level cache (LLC), memory bandwidth, and IO buffers that cause interdependency.

The game model analyzes the potential collateral damage from an indirect attack and cross side channel attack. The game has multiple possible Nash equilibria. The Nash equilibrium of the game depends on the probability that the hypervisor is compromised given a successful attack on a VM and the required expense for security.

Definitely, the negative externality in a public cloud security can be mitigated by putting VMs that have similar potential loss from a security breach in the same physical machine. By utilizing game theory, we can more accurately describe the nature of the attacker and his motives. However, sometimes our best friend can be our worst enemy. Other player behaviors can be seemingly erratic and even counterintuitive, which can be very dangerous when your decisions are based on the decisions of others. With game theory, we can quell some of this contradictory behavior that is characteristic of network security and bring clarity to this complex topic.

Acknowledgment

This research was performed while Dr. Joon Park and Dr. Manuel Rodriguez held a National Research Council (NRC) Research Associateship Award at the Air Force Research Laboratory (AFRL). This research was supported by the Air Force Office of Scientific Research (AFOSR).

References

[1] R. Myerson (1991). "*Game Theory: Analysis of Conflict,"* Harvard University Press, p. 1.

[2] G. Heal, H. Kunreuther. *"You only die once: Managing discrete interdependent risks,"* No. w9885. National Bureau of Economic Research, 2003.

[3] T. Alpcan, T. Başar. "Network security: A decision and game-theoretic approach," Cambridge University Press, 2010.

[4] C. Kamhoua, N. Pissinou, K. Makki. *"Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy,"* IEEE International Conference on Communications (ICC), 2011.

[5] Zissis, Dimitrios, and Dimitrios Lekkas. *"Addressing cloud computing security issues,"* Future Generation Computer Systems 28.3 (2012): 583-592.

[6] T. Ristenpart, E. Tromer, H. Shacham, S. Savage. *"Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,"* In the proceedings of the 16th ACM Conference on Computer and Communications Security, CCS'09, Chicago, IL, USA, October 2009.

[7] A. Bates, B. Mood, J. Pletcher, H. Pruse, M. Valafar, K. Butler *"Detecting Co-Residency with Active Traffic Analysis Techniques,"* in the proceedings of the 2012 ACM Cloud Computing Security Workshop (CCSW) in conjunction with the 19th ACM Conference on Computer and Communications Security, October 2012, Raleigh, North Carolina, USA.

[8] Y. Zhang, A. Juels, A. Oprea, M. Reiter *"HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis,"* in the proceedings of IEEE Symposium on Security and Privacy, May 2011, Oakland, California, USA.

[9] L. Carin, G. Cybenko, J. Hughes, *"Cybersecurity Strategies: The QuERIES Methodology,"* Computer, vol.41, no.8, pp.20-26, Aug. 2008.

[10] United States Securities and Exchange Commission http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm