2015 IEEE 8th International Conference on Cloud Computing

Security-aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach

Luke Kwiat[1], Charles A. Kamhoua[2], Kevin A. Kwiat[2], Jian Tang[3], Andrew Martin[4]

kwiatluke@gmail.com; {charles.kamhoua.1; kevin.kwiat}@us.af.mil; jtang02@syr.edu; Andrew.Martin@cs.ox.ac.uk

[1]University of Florida, Department of Industrial and Systems Engineering, Gainesville, FL

[2]Air Force Research Laboratory, Information Directorate, Cyber Assurance Branch, Rome, NY

[3]Syracuse University, Department of Electrical Engineering and Computer Science, Syracuse, NY

[4]University of Oxford, Department of Computer Science, Oxford, UK

***Abstract*—With the growth of cloud computing, many businesses, both small and large, are opting to use cloud services compelled by a great cost savings potential. This is especially true of public cloud computing which allows for quick, dynamic scalability without many overhead or long-term commitments. However, one of the largest dissuasions from using cloud services comes from the inherent and unknown danger of a shared platform such as the hypervisor. An attacker can attack a virtual machine (VM) and then go on to compromise the hypervisor. If successful, then all virtual machines on that hypervisor can become compromised. This is the problem of negative externalities, where the security of one player affects the security of another. This work shows that there are multiple Nash equilibria for the public cloud security game. It also demonstrates that we can allow the players' Nash equilibrium profile to not be dependent on the probability that the hypervisor is compromised, reducing the factor externality plays in calculating the equilibrium. Finally, by using our allocation method, the negative externality imposed onto other players can be brought to a minimum compared to other common VM allocation methods.**

Keywords—Cloud Computing; game theory; virtual machine allocation; cyber security; externality

I. INTRODUCTION

Cloud computing is quickly becoming a standard resource in the IT toolbox and shows no signs of slowing down. It is predicted that "By 2017, nearly two-thirds of all workloads will be processed in the cloud" as well as a growth of cloud traffic of 370% from 2012-2017 [10]. Given this astounding growth, it becomes exceedingly challenging for security to keep pace. This is especially true since demand for security can often be overlooked by clients in favor of performance and reliability since security is difficult to quantify and holds less tangible benefits than the former. However, the current issues surrounding cloud security are still very apparent. Security-aware companies are still fearful over the theft of confidential or sensitive data, which poses as a "significant barrier to the adoption of cloud services" [15].

The argument of lacking security measures in the cloud holds a lot of ground. Many providers do not even know the extent of the security vulnerabilities and this issue is compounded by the unique structure of the cloud. Many different users run virtual machines on the same physical hardware which can allow an attacker to proliferate his attack throughout the hypervisor and onto all VMs running on that hypervisor. In this way, one user's VM may be susceptible to an indirect attack when a direct attack is launched on a different user's VM on the same hypervisor. This is possible based on unknown security vulnerabilities of the hypervisor, which, once compromised, can allow an attacker to target every VM on the targeted hypervisor [11]. This phenomenon is not prevalent in traditional networks, where an attacker must use a multi-hop method to indirectly attack a victim. Thus, this interdependency between users on the same hypervisor is a unique challenge to cloud computing providers: how to allocate virtual machines for optimum security.

In a cloud setting, an attacker can launch an indirect attack on User j by first compromising the VM's of User i, going through the hypervisor, and then compromising the VM's of User j. This creates a risk-connection where the security of User j is dependent on User i and vice versa. This especially true if there is a large difference in the potential total loss that can be suffered by User i and j, since the larger of the users could be discouraged from using the cloud since its potential loss is much greater. With only 56% of cloud users saying they trust cloud providers with sensitive information and an even smaller 30% knowing what measures cloud providers actually use for security, this problem is still very evident [12]. Due to the interdependent nature of the cloud users, we may use game theory to model their choices. This is possible since game theory is the "mathematical models of conflict and cooperation between intelligent rational decision-makers." [13]

There are several contributions this paper makes. First, its focus is on modeling the choices of several rational players in the cloud within a game theoretical framework. We also propose that the solution to the externality problem in [1] is through effective VM allocation management of the cloud provider to ensure delivery of maximum security for all cloud users. Along with solving the externality problem generated inherently by the cloud, our paper also provides the proof that Nash equilibrium will be the optimal solution for our model. We wish to use the knowledge gained from this model to influence cloud providers to make optimal security-based virtual machine allocation decisions.

Approved for Public Release; Distribution Unlimited: 88ABW-2015-0108, Dated 13 Jan 2015.

2159-6190/15 $31.00 © 2015 IEEE
DOI 10.1109/CLOUD.2015.80

IEEE computer society

Section II will focus on related works and how this paper differentiates from them. Section III will elaborate on the cloud architecture common to many cloud structures that will be used in our game model. Section IV will be the set-up of the game model and diagram the game in normal (matrix) form. After analyzing the game result in Section V in the simplest case, we will extend our model in Section VI. Section VII will present numerical results and compare our model's negative externality to other common allocation methods. Section VIII concludes the paper.

II. Background & Related Work

A major issue in cloud computing is how the cloud provider will allocate the virtual machine instances created by a constant stream of clients. There are many ways to go about this problem that has been looked at in previous papers. Many of the solutions offered are virtual machine allocation based on load-balancing techniques, energy consumption, or both. [2][5][8][9]. Wei et al. [5] use game theory in order to maximize the efficiency of resources within a cloud computing environment. Beloglazov et al. [9] offered several algorithmic solutions rooted in heuristics for energy and performance. Jing Xu and Jose A. B. Fortes [2] introduced several algorithms to achieve allocative efficiency such as Beloglazov et al. did. Jalaparti et al. [8] attempted to solve the issue of cloud resource allocation with game theory similar to Wei et al. They sought to model the intricate client to client and client to provider interactions using game theory.

Game theory has also been applied to cloud computing in certain aspects, including infrastructure resilience [3], cloud usage pricing [4], and virtual machine allocation [5], [6] [8].

Han et al. [6] demonstrated a new method of infiltration that can be exploited through the cloud and not traditional computing: through side channels. This gives rise to new risks as hardware to create VM's is shared between users, which attackers can exploit. By starting a VM in the same server as a target user, an attacker can siphon sensitive information from them, including web traffic and even encryption keys. This paper uses game theory to find the best method for mitigating such attacks that have been shown to have a 40% success rate of VM's achieving co-location with the target users VM [7].

Rao et al. [3] studied the ability of a cloud computing entity within the framework of game theory to provide a given capacity C at a certain probability P given a physical or cyber attack on their infrastructure. A simple game was set up in which a cloud provider with a certain amount of servers S was to defend against an attacker attacking these servers. Among the possible ways to mitigate attack was for the provider to use reinforcement strategies, which decreased attacker utility. It was concluded through several tests that the survivability of an attack (the ability to operate at capacity C under probability P) was heavily influenced by the cost of defense and the cost of an attack. If the cost of a defense is high, then the provider chooses to defend the sites and thus the survivability was 0 in this case due to an attack.

Kunsemoller and Karl [4] examined the economics of cloud computing and its viability for a given business to use. Game theory was specifically used to model a few circumstances in which it would be economically beneficial to use cloud services. Payoff for the provider is clearly maximized if they charge the highest price in which there is a cost benefit for the client to use cloud services, or the breakeven point.

Outside of game theory or VM allocation, another important work includes Ristenpart et al. [7] and their work on discovering new vulnerabilities in the cloud structure. They looked at the idea of co-resident attacks on virtual machines within the cloud network. Unlike any predecessor, however, this paper used empirical evidence and actual data from running experiments on the Amazon EC2 cloud. They began by running all 5 instance types that EC2 offers across 3 available placement zones within the cloud. From this it was determined that IP assignment is very uniform in that IP addresses are partitioned by availability zones (most likely to make it each to manage separate network connectivity for these zones). Using this information, there was a test to determine co-residence on network-based technology (it was also shown that this type of technology need not be used). Eventually it was shown that an efficient attacker can achieve co-residence up to 40% of the time an attack is launched. Once co-residence was achieved, several methods could be used to extract information from or damage the victim. This included measuring cache usage, launching DOS attacks, keystroke timing attacks, stealing cryptographic keys and estimating traffic rates. It was concluded that currently for unconditional security against cross-VM attacks, one must avoid co-residence.

Kamhoua et al. [1] viewed attacks on the hypervisor and compromising virtual machines from a game theoretical perspective. One of the larger issues presented in [1] is also present in this paper: interdependency. Interdependency in [1] dealt mainly with the issue of one user's lack of investment compromising the security integrity of another user on the same hypervisor since an attack on the hypervisor may propagate to other users. This is also present in the current paper but emphasized to a much lesser extent and is not the main focus. Interdependency in general still plays a crucial role in both papers, however, and the choices of the players reflect the relevant payoffs of the other players as well. In the current paper we resolve the negative externality in [1] that one player imposes on another. Our solution is through effective VM allocation management of the cloud provider to ensure delivery of maximum security for all cloud users. The negative externalities are minimized because users with similar potential loss choose to be located on the same hypervisor. This is one of the main contributions of our paper.

III. System Model

A public cloud infrastructure that is running on Hypervisor H_1 has n users that are denoted as User U_{11}, U_{12} ... U_{1n} whom each run virtual machines VM_{11}, VM_{12} ... VM_{1n}. Note that the first subscript states which hypervisor each user is located on and the second subscript denotes the user number. For example, the first user operating on hypervisor 3 is written as

U_{31} and a second user as U_{32}. Additionally, we do not make the distinction between the cloud tenant and user. For practical purposes, the tenant is the true entity that manages the VM's as a liaison while the 'user' in cloud terminology is the end user who hires the tenant and benefits from the cloud (and also the one to realize any ill effects of asset loss). We will assume that the cloud tenant will act in good faith (and do what is the most secure or best) for the end user and thus the remainder of the paper will refer to the end user only. Each user may run multiple virtual machine instances (and multiple operating systems) but it will be assumed that each user runs one VM for simplification purposes as it will be shown later that multiple VM's run by one user may be mathematically combined into one VM. The number of applications run by a user will also not impact the model. Although the physical infrastructure a cloud use will vary (such as different hypervisors like Xen, VMware, KVM), the underlying principle of a shared platform in which users are exposed to collateral damage holds true.

It is evident that several issues arise within the cloud infrastructure once this model is examined. Users that run on the same hypervisor are susceptible to a 'bad neighbor' effect in which an attacker, who has compromised one user's VMs, may transverse across the hypervisor to launch an attack on another user's VMs on the same hypervisor. This is the problem of interdependency. We hold that if the hypervisor is compromised, then that all users located on that hypervisor will be compromised (and suffer the consequences) as well. This is because once an attacker compromises the hypervisor, all VM's hosted on that hypervisor can be freely compromised by the attacker. However, if a user does not have VMs on the same hypervisor than the one being targeted, then they will not suffer the consequences. This remark will play an important role later in the paper. Section IV will now explain and setup the problem in the context of game theory.

IV. Game Model

This section considers four players, an attacker and three users, acting across two hypervisors. The four players are assumed to be rational, and that they all have an understanding of the system in which the game is played. Furthermore, it is expected that each player can calculate and maximize their payoff (i.e., utility). In Section VI we extend the problem to *n* players and *m* hypervisors.

Along with the commonly applied game-theoretic assumptions of rationality and common knowledge of the game's space, we further assume that the attacker has 3 strategies: to launch an attack on User 1 (this strategy will be denoted as A_1), on User 2 (A_2) or on User 3 (A_3). The attacker may only attack one user directly at a time. The strategy to launch an attack may include steps such as: collecting information, credential compromising, executing attack payload, establishing backdoor, and scanning. The strategy for the User 2 is binary since that user's only choices are to *invest* (*I*) in security or to *not invest* (*N*) in security. In the instance of choosing to invest in security, the user will be allocated to hypervisor 2 (H_2) while no investment in security will result in User 2 being allocated to hypervisor 1 (H_1). The user that chooses to invest may take multiple courses of action, including updating software, buying new antivirus software, and applying stricter system monitoring. In this way, H_2 is the more secure platform for security- conscious cloud users. It is important to note that throughout the remainder of the paper, we shall refer to users that *invest (do not invest)* in cloud security and users that are allocated to H_2 (H_1) interchangeably.

Furthermore, User 1 will automatically be allocated onto H_1 *(no investment in security)* and User 3 will be allocated to H_2 *(investment in security)*. This means that the only user making a choice as to invest in security or not will be User 2. Since User 2 will have two strategies (*I* or *N*) and the attacker has three strategies (A_1, A_2, or A_3), there are a total of six possible permutations in the normal form game, as diagramed in Table 1.

The reason for the automatic allocation of User 1 and User 3 is as follows: It is assumed that the relative 'importance' of each user is determined by the total maximum loss that can be suffered by the user if compromised. This is denoted by L_1, L_2, and L_3 with the subscripts corresponding to each respective user. This means that if User 1's virtual machines were compromised, then User 1 would suffer a loss totaling L_1. Additionally, we assume that

$$L_1 < L_2 < L_3 \qquad (1)$$

Which implies that User 3 will suffer the most costly damage (for example, through loss of information, trade secrets, client information, etc.) if its virtual machines are compromised, and User 1 the least amount of damage. Since User 3 faces the biggest potential for loss and User 1 the least, it is logical that User 3 would invest into security (and be allocated to H_2) and that User 1 would not invest in security (and be allocated to H_1). Thus, the only cloud user making an investment choice in this game will be User 2. The sufficient conditions under which User 1 and 3 will always be allocated to H_1 and H_2, respectively, will be shown in the model extension. Additionally, the strategy profile for the game is stated in Table 1 as *(attacker strategy, User 2 strategy)*. For example, the profile of an attacker that attacks User 1 while User 2 invests in security is given as (A_1, *I*).

The probability of an attack that is successful on an individual user that has invested in security is given as q_I, who pays cost e for his investment. If they have not invested in security, then the probability of compromise is q_N. It is assumed that

$$0 < q_I < q_N < 1 \qquad (2)$$

Because if $q_I > q_N$ then no logical user would choose to invest in security since it does not lower their chance of being compromised.

The probability for a successful attack on the hypervisor after one of its VM is compromised is given as π, where we assume

$$0 < \pi < 1 \qquad (3)$$

It is strong to assume that there will be no chance of a successful attack on the hypervisor ($\pi = 0$), especially since the current hypervisor security situation is very unclear [11].

We also consider that not all attacks on the hypervisor will definitively allow for compromise ($\pi = 1$) and thus Equation (3) results. Lastly, it is assumed that the reward from using cloud services (either invested, *I*, or not invested *N*) is given as R. This could include monetary savings from outsourcing IT or on-demand resources that can dynamically change depending on the relative need.

Looking again to the normal form game on Table 1, the attacker's strategies are represented in the row (and the top equation of the six game possibilities gives the attacker's payoff) and User 2's strategies are shown on the column (and the bottom six equations give the user's payoff). Thus, a game profile of (A_1, *I*) would give the attacker a payoff of $q_N L_1$ and User 2 a payoff of $R - e$.

The payoffs are calculated as follow, taking strategy profile (A_1, *I*) as a first example: User 2 will receive reward *R* from using the cloud services (this is true for all 6 game possibilities) and will pay expense *e* for the cost of paying for extra security. Since User 2 is *not* being attacked directly and is located on the *different* hypervisor from what is being targeted, the user's expected loss from a successful attack is 0. Thus, the payoff for User 2 is $R - e$. For the attacker targeting User 1, since User 1 has not invested its chance of being compromised is q_N. To find the probabilistic loss of User 1, we must multiply the chance of compromise by its total possible loss (L_1), which gives an expected loss of $q_N L_1$. Since User 1 is the only user located on the first hypervisor, the total gain for the attacker targeting User 1 is $q_N L_1$.

Taking the strategy profile (A_1, *N*) as another example, we can see that the payoff for User 2 is the reward *R* minus $q_N \pi L_2$. The quantity $q_N L_2$ is the expected loss from a successful compromise of User 2. However, we must multiply this quantity by π since User 2 is not a *direct target* and in order to be compromised the attacker must first compromise the hypervisor. If User 2 was the main target of the attacker, as seen in strategy profile (A_2, *N*), we can see that User 2's payoff is the reward *R* minus the expected loss $q_N L_2$ – without the value π since the attacker need not go through the hypervisor in order to compromise the virtual machines of User 2 if User 2 is a direct target.

Table 1: Game Model in Normal Form

		User 2	
		N	*I*
Attacker	A_1	$q_N L_1 + q_N \pi L_2$ $R - q_N \pi L_2$	$q_N L_1$ $R - e$
	A_2	$q_N L_2 + q_N \pi L_1$ $R - q_N L_2$	$q_I L_2 + q_I \pi L_3$ $R - e - q_I L_2$
	A_3	$q_I L_3$ R	$q_I L_3 + q_I \pi L_2$ $R - e - q_I \pi L_2$

When viewing the strategy profile (A_2, *I*) from the attacker's perspective we can see that his reward is twofold. His payoff from attacking User 2 is $q_I L_2$ (User 2's expected loss). In addition, the quantity of $q_I \pi L_3$ is added to the attacker's payoff since User 3 lies on the same hypervisor (H_2) as User 2 even though User 3 is not directly being targeted by the attacker. Since User 3 is not a direct target, and the attacker must propagate his attack through the hypervisor first before compromising User 3. As a result, π is multiplied to User 3's expected loss (giving $q_I \pi L_3$), and thus the total payoff for the attacker is $q_I L_2 + q_I \pi L_3$. Similar methods are used to derive the other payoffs for all of the other profiles.

V. Game Analysis

In this analysis we seek the different Nash equilibrium from the game model. In game theory, when the Nash equilibrium profile is reached, no player can improve his utility by unilaterally deviating from the result. At this point, no player wants to change their strategy since it is the best response based on the other player's actions, which means all players' choices are in a Nash equilibrium profile. In this way, Nash equilibrium can predict the behavior of rational agents.

We make the following three observations. First, (A_1, *N*) cannot be a Nash equilibrium since the attacker can improve his utility by playing A_2. Second, (A_2, *I*) cannot be a Nash equilibrium since the attacker can improve his utility by playing A_3. Third, (A_3, *I*) cannot be a Nash equilibrium since User 2 can improve his utility by playing *N*. However, we can have the pure strategy Nash equilibrium profile (A_3, *N*), (A_2, *N*) and (A_1, *I*) under the specific conditions below.

Theorem 1:

If $L_3 > \frac{q_N}{q_I}(L_2 + \pi L_1)$. $\quad$ (4)

Is true, then the strategy profile (A_3, *N*) is Nash equilibrium of the game in Table 1.

Theorem 2:

If $L_3 < \frac{q_N}{q_I}(L_2 + \pi L_1)$, $\quad$ (5)

and

$e > (q_N - q_I)L_2$, $\quad$ (6)

then the strategy profile (A_2, *N*) is a Nash equilibrium.

Theorem 3:

If $L_1 > \frac{q_I}{q_N}(L_3 + \pi L_2)$ $\quad$ (7)

and

$e < q_N \pi L_2$ $\quad$ (8)

Then the strategy profile (A_1, *I*) is a Nash equilibrium

The proof of those Theorems is straightforward. We omit them because of space limitation. If none of the conditions of Theorems 1, 2 or 3 for pure Nash equilibrium are fully met, then the problem admits a mixed Nash equilibrium.

Mixed Nash Equilibrium

A mixed Nash equilibrium is different from pure Nash in the sense that the players do not play a single strategy with an absolute certainty but rather with a probabilistic strategy for each choice. For example, User 2 might play *N* with probability $\frac{3}{4}$ and *I* with probability $\frac{1}{4}$. The conditions and formulas for the equations of mixed Nash will be shown.

Theorem 4:

If the following 3 conditions hold:

$L_3 < \frac{q_N}{q_I}(L_2 + \pi L_1)$, $\quad$ (9)

$e < (q_N - q_I)L_2$, $\quad$ (10)

$$L_1 < \frac{q_I}{q_N}(L_3 + \pi L_2), \qquad (11)$$

Then the game admits a mixed strategy Nash equilibrium.

Proof:

We can see that if (11) holds, the strategy A_1 is never an optimum and is not needed for calculations for the equations of Nash equilibrium. Thus, we will only use strategy profiles A_2 and A_3 for the attacker. The reasoning given is as follows: If the defender (User 2) chooses to not invest, the attacker prefers to play A_2 because Equation (9) holds. When the attacker plays A_2, the defender prefers to switch from not investing to investing to avoid the attacker, since Equation (10) holds. Thus, if User 2 invests and moves from H_1 to H_2 the attacker prefers to switch his strategy from A_2 to A_3 because (1) and (3). Lastly, since the attacker is now playing A_3 the defender will want to switch from investing to not investing in order to avoid an indirect compromising of virtual machines. As a result, these four strategy profiles circulate among each other indefinitely with no final stoppage point. This shows that there is no pure Nash equilibrium (because there is no strategy in which both players will remain for certain) but rather a strategy profile of each player that plays a given strategy probabilistically.

Remark: Note that this circulation of strategies does not include A_1 as a strategy for the attacker, showing that this strategy will *never* be an optimum for the attacker and thus never played. The remaining 4 choices ((A_2, N), (A_2, I) (A_3, N), A_3, I)) that result will be the payoffs that are used to calculate mixed Nash equilibrium.

At the mixed Nash equilibrium, User 2 must randomize in such a way that the *attacker* is indifferent to choosing either strategy, or $U_a(A_2) = U_a(A_3)$. Let α be the probability by which User 2 choose N. This gives:

$$U_a(A_2) = \alpha(q_N L_2 + q_N \pi L_1) + (1-\alpha)(q_I L_2 + q_I \pi L_3) \qquad (12)$$

$$U_a(A_3) = \alpha(q_I L_3) + (1-\alpha)(q_I L_3 + q_I \pi L_2) \qquad (13)$$

As stated, in order to find α we must equalize these two functions and solve. This gives:

$$\alpha = \frac{q_I[(L_3 + \pi L_2) - (L_2 + \pi L_3)]}{q_N(L_2 + \pi L_1) - q_I(L_2 + \pi L_3) + q_I \pi L_2} \qquad (14)$$

which means that User 2 will play strategy N with probability α and I with probability $(1-\alpha)$.

We will now examine the attacker's mixed Nash equilibrium by letting $\beta(A_2) + (1-\beta)(A_3)$ being the strategy of the attacker. Given this, we can see that

$$U_d(N) = \beta(R - q_N L_2) + (1-\beta)(R) \qquad (15)$$

$$U_d(I) = \beta(R - e - q_I L_2) + (1-\beta)(R - e - q_I \pi L_2) \qquad (16)$$

At the mixed Nash equilibrium, the attacker must randomize in such a way that the *defender* (User 2) is indifferent to choosing either strategy. Equalizing these two equations and solving out for β leaves us with:

$$\beta = \frac{(e + q_I \pi L_2)}{q_N L_2 - q_I L_2(1-\pi)} \qquad (17)$$

Next, It is straightforward to verify that $0 < \alpha < 1$ and $0 < \beta < 1$ in all instances so there is no case in which any values produce an inappropriate value for α or β. We will extend this model's scope beyond three users and its implications.

VI. Model Extention & Discussion

For our model extension, all our previously stated assumptions remain in place except the number of users is now increased to n. The number of hypervisors remains at two. In practice, there is a one-to-one mapping of hypervisors to physical servers, so with m hypervisors cloud clients can pay for increasingly structured levels of security, with H_1 being the least secure and H_m being the most secure. The reasoning we applied for two hypervisors is the same for m hypervisors.

One of the main results that we can draw from n users is that among all the n users there will only be one discrete user in which they alone will make a decision as to which hypervisor they allocate, i.e., all other users will remain static in their allocation choice regardless of the number of players. This is why User 1 and User 3 were statically placed in H_1 and H_2, respectively. The observation behind this is as follows: there exists only one user who will sit on the threshold of choosing between investing in security and not investing in security because all other users' expected loss magnitudes balance out. This makes this user unique; unlike the other users, this one is unable to choose between invest or not invest in a binary sense, since whatever hypervisor the user chooses to allocate will be attacked because the user will 'tip' the payoff for the attacker in that direction. This gives rise to this unique player having a mixed Nash equilibrium whereas all other players have pure, and static, Nash equilibrium.

Since the attacker will always attack the 'largest' player in the targeted hypervisor, if the unique user were to allocate to H_1, the unique user will be the direct victim of the attack since by default it will be the largest player on H_1. This is because all players will be grouped by loss potential on the hypervisors since a small loss gap between players will minimize the externality imposed on each other and thus maximize security. This is a well-studied problem in game theory and is known as Hotelling's Law [14]. In this context, players are self-grouping by potential maximum loss. Thus, having the largest and smallest potential loss players grouped on one hypervisor and all of the in-between potential loss players on another hypervisor is not observed; rather, players will be will be allocated with other users with similar total loss potentials.

Formally, for a game having n players and with critical User l ($1 < l < n$), Users $1, 2 \ldots l\text{-}1$ will be located on H$_1$ and Users $l\text{+}1,\ l\text{+}2 \ldots\ n\text{-}1,\ n$ will be located on H_2. If User l chooses to allocate to H$_1$, then he will be the direct target of the attack. If he chooses to allocate to H_2, then User n will be the direct target and User l merely becomes an indirect target by factor π. Thus, in order for a user to be the pivotal user, the following two equations must be satisfied:

$$q_N \pi L_1 + \cdots + q_N \pi L_{l-1} + q_N L_l > q_I \pi L_{l+1} + \cdots + q_I L_n \qquad (18)$$

$$q_N \pi L_1 + \cdots + q_N L_{m-1} < q_I \pi L_m + q_I \pi L_{m+1} + \cdots + q_I \pi L_{n-1} + q_I L_n \qquad (19)$$

As can be seen, the pivotal user shifts the inequality and thus the where the attacker will focus his attack. Furthermore, we can verify that User 1 and n will always choose to not invest (H_1) and invest (H_2), respectively if the range of e is as

$$L_1(q_N - q_I \pi) < e < L_n(q_N - q_I) \qquad (20)$$

VII. Numerical Results and Analysis

The game analysis provides an in-depth explanation of the pure and mixed Nash equilibria. Our key variables in the analysis were R, q_N, q_I, L_1, L_2, L_3, π and e. We show how User 2's payoff changes with respect to a change in some selected variables, and how sometimes after a certain threshold is passed that the equilibrium may shift.

A. Changes in User 2's payoff with respect to L_2

In this first section we provide to set specific values for all of the aforementioned constants save for L_2 and graph the results. For our first example we will take $R = 1.5$, $q_I = .1$, $q_N = .4$, $\pi = .1$, $L_1 = 1$, $L_3 = 100$, and $e = .4$. Using Equation 20, we see that $.39 < e < 30$, so this verifies that e is an appropriate value. Looking at Figure 1, we can see the payoff of User 2 change as L_2 increases.

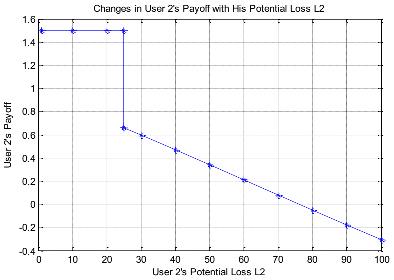

Figure 1: Changes in User 2's Payoff with his Potential Loss L_2.

The first thing we can immediately see is that there is a strategy change from (A_3, N) to mixed Nash equilibrium at L_2 = 24.9. This is because from $1 < L_2 < 24.9$, the condition for pure Nash equilibrium is satisfied (4) up until 24.9. After that, Equation (4) is falsified, all 3 conditions of mixed Nash equilibrium are fulfilled, and thus a strategy change occurs at this point. Notice that as L_2 approaches the value of L_3, there is diminishing payoff from using the cloud and even turns negative at $L_2 \approx 77$ for the given value of R. In fact, as L_2 increases, α and β decrease and User 2 *Invests* less often. However, the frequency of direct attack on User 2 increases to cause the decrease on User 2's payoff. The implications of a negative payoff is that after reaching a negative payoff, User 2 will completely opt out of using cloud services.

B. Changes in User 2's payoff with respect to e

Moving onto Figure 2, we hold all of the same values as before except we set L_2 = 10, L_3 = 20 and graph the applicable value of e with respect to changing payoff.

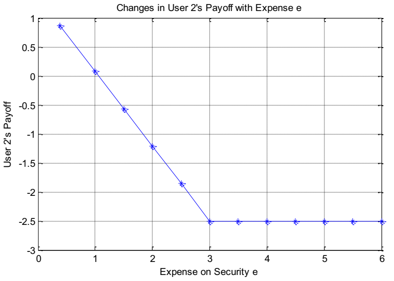

Figure 2: Changes in User 2's Payoff with Expense *e*.

Too high of a value for L_3 will always result in profile (A_3, N), so therefore the potential loss values will be more closely clustered in this example. As shown before, the range for e is given in Equation (20) which results in $.39 < e < 6$. This will be our range for the x-axis. We can see a strategy change from mixed Nash equilibrium to pure Nash at $e = 3$. This is intuitive since after that threshold, the choice of investing for User 2 becomes too expensive and unfeasible and thus the pure Nash equilibrium (A_2, N) results. Note that User 2 will not invest in cloud security at this Nash equilibrium even though they know they are a direct target of the attacker. Furthermore, for the selected value of R User 2 will not use of cloud services at all unless there is a low value of e (specifically $e = 1.213$).

C. Changes in User 2's payoff with respect to π

Figure 3 shows the changing payoff of User 2 as we change the probability of compromising the hypervisor, π. We use the same values as set in analysis B, change π from a constant to a variable, and set $e = .4$.

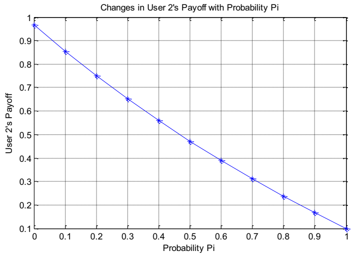

Figure 3: Changes in User 2's Payoff with Probability π.

It is apparent that there is no shift in Nash equilibrium across all values of $0 < \pi < 1$. These results are not surprising, as an increasing π only slightly increases the externality imposed onto User 2 by other users. The increasing externality problem imposed by an increasing π does not pose a significant difference to change any strategies of the player. This is a very significant discovery since in [1] there was a Nash equilibrium shift if π reached a certain threshold but in this analysis it is not the case, thus validating one of the main aims of this research to reduce the externality imposed onto one user by another. However, it is possible that π may shift the Nash equilibrium this only in exceptional cases in which the conditions for two different Nash equilibria are very close to being met. One instance is that if $L_3 \approx \frac{q_n}{q_i}(L_2 + \pi L_1)$, then π may shift the inequality either way and thus change the Nash equilibrium. In most cases, the Nash equilibrium will not change from the initial conditions and is a very positive sign that this security based allocation will have an effect of mitigating the externality problem.

It is apparent that a direct attack is much more of an importance when deciding where to allocate. As we will see in the next variable analysis, the $\frac{q_I}{q_N}$ ratio is also very important in determining the prevalent Nash equilibrium.

D. Changes in User 2's payoff with respect to q_I

For this section we will take $R = 1.5$, $q_N = .5$, $\pi = .1$, $L_1 = 1$, $L_2 = 10$, $L_3 = 20$, and $e = .4$.

(same values in part B and C except for q_N), using q_I as a variable. We take $0 < q_I < .5$ (since $q_I < q_N$) and the results can be seen on Figure 4. For small values of q_I, the pure Nash profile (A_1, I) exists. This makes sense since if the probability for compromising a VM on the secure hypervisor was too low as to discourage any type of attack, then it would be a higher payoff for the attacker to target those users who chose to not invest.

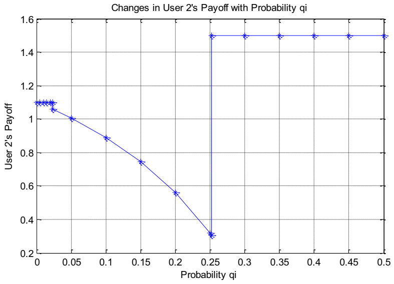

Figure 4: Changes in User 2's Payoff with probability q_I.

At $q_I \approx .0238$, the Nash equilibrium changes to a mixed strategy and then changes again to the pure Nash equilibrium (A_3, N) at $q_I \approx .2525$. This second switch of Nash equilibria also is feasible since as the $\frac{q_I}{q_N}$ ratio becomes closer to 1, the $\frac{L_3}{L_2}$ ratio becomes more a dominant factor in the calculations and at the second threshold the disparity becomes so large such that $L_3 \gg L_2$ and the switch to strategy profile (A_3, N) occurs.

E. Model Extension to $n = 10$ users

In this section we will continue our model extension and not limit our discussion to simply three players. We will take $R = 1.5$, $q_N = .4$, $q_N = .1$, $\pi = .1$, $e = .4$ as before and, per section VI, set the number of users as $n = 10$. For all of our potential loss values, we will use $L_1 = 1$, $L_2 = 2$, $L_3 = 3$, $L_4 = 4$, $L_5 = 5$, $L_6 = 6$, $L_7 = 7, L_8 = 8, L_9 = 9, L_{10} = 10$.

Our next step is to find which of the ten users the pivotal user is while the remaining nine stay static. Thus, we must find the user such that Equations (18) and (19) are true.

By calculating individual potential losses, we find that User 4 is the pivotal user.

Using Equation (20), we find that $.39 < e < 3$ which shows our selected value of e is within the restricted range. It is important to note that the value of e will have a strong influence on the prevailing Nash equilibrium. If $.39 > e$ then the price for security would be so inexpensive that it would be logical for all users (1-10) to allocate to H_2. If $e > 3$ then the security would be so expensive such that no user would want to invest in security (and all will as a result allocate to H_1). Within the allowable range given by (26) there is some interesting results. From $.39 < e < 1.56$ there will be a mixed strategy in which User 4 will have a mixed Nash equilibrium while all other users will remain in their respective hypervisors. (U_1, U_2, and U_3 allocate to H_1 while U_5, U_6, U_7, U_8, U_9, and U_{10} allocate to H_2). The threshold of 1.56 is determined by the maximum value in which User 4 will potentially still pay for security. Past this point, investing in security will become too expensive and thus $1.56 < e < 3$ will result in a pure Nash equilibrium in which U_1, U_2, U_3, and U_4 allocating to H_1 while all other users allocate to H_2.

To further show the critical role of User 4, we have diagrammed the changing payoff structure for the attacker on Figure 5 as the number of users of each hypervisor changes.

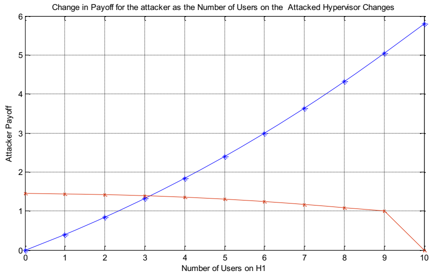

Figure 5: Change in attacker's Payoff with the Number of Users on the attacked hypervisor.

As can be seen, one line (blue) represents the attacker payoff for attacking H_1, and another (red) shows the attacker payoff for attacking H_2. For example, the payoff for the attacker targeting H_2 if all users are located on H_1 is 0. If there is 1 user on H_2 (by default User 10), then the attackers payoff is $q_I L_{10}$, which is 1.0. As the number of users on the hypervisor increases, the attacker payoff increases. The opposite will be true if the number of players decreases.

We can see that the payoffs for each strategy (attacking H_1 versus attacking H_2) intersect between when there are three and four players on H_1 and the remaining players on H_2, which corresponds to User 4 as pivoting user. This means that at this point the attacker becomes aware of which hypervisor User 4 has allocated, since User 4's hypervisor allocation stems from pursuit of a higher payoff. As stated before, the strategy that U_4 chooses will depend on the prevailing value of e. Since $e = .4$, we will have a mixed Nash equilibrium.

In Figure 6 we show the reduced externality from the mixed strategy placement of User 4 and the optimum placement of the other users.

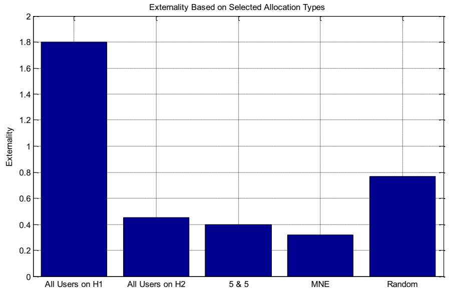

Figure 6: Externality Based on Selected Allocation Types

The first and second bars represent the total externality if all users were placed on H_1 and H_2, respectively. This was calculated by adding all the payoffs of the attacker that contained a factor of π. So the externality of all users on H_2 was calculated as the sum of $q_I \pi L_9 + \cdots + q_I \pi L_1$ and H_1 similarly. This would be an externality for a fairly common allocation method such as for power consumption where all users are clustered on as few hypervisors as possible. The third bar represents the externality from five VM's located on

H_1 and H_2 each, which is supposed to represent another common allocation method: load balancing. Given our initial conditions, the attacker would attack H_1 with probability 1 and thus the externality is calculated as $q_N\pi L_1 + q_N\pi L_2 + q_N\pi L_3 + q_N\pi L_4$. With five users on H_1, the largest user (U_5) will be the direct target while all other players will be calculated in the externality Figure since they are all indirect targets.

The fourth bar shows the externality imposed onto other users in the instance of the mixed Nash equilibrium. As can be seen, the negative externality is significantly reduced compared to both power consumption and load balancing allocation methods, to the magnitude of 20% externality reduction from the second closest value (bar three).

The fifth bar shows the externality imposed onto other users when using random placement, which is a common VM allocation method. This value was determined by randomly allocating the VM's among H_1 and H_2 10 times and averaging the result. This allocation is the worst except for placing all users in the less secure hypervisor H_1. Our proposed allocation method based on mixed strategy Nash equilibrium has 125% externality reduction as compared to the random allocation method.

VIII. Concluding Remarks

The unique properties of a cloud computing structure can allow for new avenues of attack. One of the issues presented was the one of externality, where one user's lack of security may affect another who has significantly more to lose. The paper in [1] presented the externality problem within the context of game theory, and this paper aimed to solve it. By allowing users to allocate to hypervisors based on whether they have invested in security or not, we can reduce a negative externality that users may impose on each other. In allowing this type of allocation over traditional means, such as load balancing or energy optimization, we observe that users will cluster to the same hypervisor as other users based on the most similar loss potentials in order to minimize the negative interdependent effects. Additionally, we have shown that with this type of VM allocation mechanism, there is no significant strategy change with respect to the value of π, which is further proof that the negative externalities in this model are mitigated. This remains true even at extreme values such as $\pi \approx 0$ or $\pi \approx 1$. These findings are supported in Figure 6 by showing that our allocation method resulted in the lowest amount of externality by a fair margin.

Thus, the Nash equilibrium strategy is more susceptible to the initial conditions such as the potential loss the users face or the cost of investment. It is apparent that the value of e plays a crucial role in determining the Nash equilibrium as shown in section E of the Numerical Results. For cloud providers, this information is very useful in that they may set the value of e and pre-determine the Nash equilibrium best suited for the maximum level of security and minimized externality. For the end users, knowledge of these values can be crucial in examining whether the cloud is a useful tool to use for reducing cost or a concept that has yet to prove its worth due to its subtle yet inherent dangers. Our future work will consider incomplete information games where the users do not know the magnitude of other players' expected loss.

RefrenceS

[1] Charles Kamhoua, Luke Kwiat, Kevin Kwiat, Joon Park, Ming Zhao, Manuel Rodriguez, "Game Theoretic Modeling of Security and Interdependency in a Public Cloud" in the proceedings of IEEE International Conference on Cloud Computing, (IEEE CLOUD 2014) Anchorage, Alaska, June 2014.

[2] Xu, Jing, and Jose AB Fortes. "Multi-objective virtual machine placement in virtualized data center environments." *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*. IEEE, 2010.

[3] Zhuang, Jun, et al. "Cloud Computing Infrastructure Robustness: A Game Theory Approach." (2012).

[4] Künsemöller, Jörn, and Holger Karl. "A game-theoretical approach to the benefits of cloud computing." *Economics of Grids, Clouds, Systems, and Services*. Springer Berlin Heidelberg, 2012. 148-160.

[5] Wei, Guiyi, et al. "A game-theoretic method of fair resource allocation for cloud computing services." *The Journal of Supercomputing* 54.2 (2010): 252-269.

[6] Han, Yi, et al. "Security Games for Virtual Machine Allocation in Cloud Computing." *Decision and Game Theory for Security*. Springer International Publishing, 2013. 99-118.

[7] Ristenpart, Thomas, et al. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009.

[8] Jalaparti, Virajith, and Giang D. Nguyen. "Cloud resource allocation games." (2010).

[9] Beloglazov, Anton, and Rajkumar Buyya. "Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers." *Concurrency and Computation: Practice and Experience* 24.13 (2012): 1397-1420.

[10] Cisco Global Cloud Index: Forecast and Methodology, 2012–2017

[11] Vaughan-Nichols, Stephen. "Hypervisors: The Cloud's Potential Security Achilles Heel." *www.zdnet.com*. CBS Interactive, 29 Mar. 2014. Web. 14 July 2014.

[12] "Thales Finds Organizations More Confident Transferring Sensitive Data to the Cloud despite Data Protection Concerns." *Https://www.thales-esecurity.com/company/press/news*. Thales E-Security, 25 June 2013. Web. 22 July 2014.

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

[14] Hotelling, Harold (1929), "Stability in Competition", *Economic Journal* **39** (153): 41–57, doi:10.2307/2224214

[15] J. Horrigan "*Use of cloud computing applications and services,"* Pew Internet & American Life project memo, September 2008.