A Study of Security Requirements Negotiation

Xinfeng Ye
Department of Computer Science
The University of Auckland
Auckland, New Zealand
xinfeng@cs.auckland.ac.nz

Abstract—**In service computing, a system is integrated by using the services of many service providers. The security of the services that constitutes the system affects the security of the integrated system. This paper studied the issues relating to security requirements of an integrated system using a game theoretical approach. It modeled a class of service computing applications as a security game. Using the game, the service providers and the system owners can analyse the security level and the security investment of the system. Using the results of the analysis, the system owners and the service providers can be more objective in their service level agreement negotiation.**

Keywords- security, service level agreement, game theory

I. INTRODUCTION

In service-oriented architecture, a system can be built from the services of many service providers. These services are connected over the Internet. Unfortunately, the Internet has attracted malicious users that intend to advance their own interest by exploiting security weaknesses of the services [5, 15]. As most attackers are motivated by financial gains [2, 4], many researchers have studied the use of game theory in countering the security threats [6, 7, 9]. These studies intend to discovery the relationship between the security investment and the security threats facing the systems.

For a system integrated from services of several service providers, the security of the system depends on the security provided by each of the service providers. Varian [13] modelled the security of a network as three security games (i.e. best effort, weakest-link and total effort games), and, studied how the behaviour of each network participant might affect the overall security of the network. Many applications in service computing have different usage patterns from the applications studied in [13]. To cope with these shortcomings of the games proposed in [13], Ye [17] proposed two security games for studying the security of two classes of service computing applications. However, the games in [17] do not cover one of the most widely used classes of service computing applications in which the service providers share the workload.

Survey showed that system owners are willing to invest in measures that prevent attacks and mitigate the damages from security breaches [11]. Security is regarded as one of the quality of service attributes. Customers and service providers should reach an agreement on the level of security that the service providers should provide when they negotiate a service level agreement (SLA). It is important to develop a method that allows the customers and the service providers to examine the relationship between the threats to systems and the efforts for countering the threats. The analysis result produced by such a method would help the customers and the service providers to reach a SLA more easily.

This paper proposed a game that complements the work in [17]. The game is used to model a class of service computing applications in which the service providers can share the workload of the system. The game was studied to determine how the system owner should negotiate with the service providers to encourage them to exert high security efforts. The proposed game allows the service providers and the system owners to analyse the security level of their systems. By analysing the threats to their services and their own defence capability, the service providers can be more objective in specifying the level of security that they can offer to the system owner. By studying how the service providers react to the threats to their services, the system owners can decide what incentives can be used to make the service providers deploy high defence efforts to protect their services.

This paper is structured as follows. §II presents some backgrounds on game theory. §III introduces the concepts and some assumptions about the system. §IV describes a security game for modeling a class of service computing applications. §V concludes the paper.

II. GAME THEORY BACKGROUND

In game theory [12], a *game* consists of a set of n players, $\{1, 2, \ldots, n\}$. Each player i has its own set of possible strategies, Ω_i. To play the game, each player selects a strategy $\omega_i \in \Omega_i$. $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ denotes a *strategy profile* selected by the players. For a strategy profile $\omega = (\omega_i, \omega_{-i})$, ω_i denotes the strategy chosen by player i while $\omega_{-i} = (\omega_1, \omega_2, \ldots, \omega_{i-1}, \omega_{i+1}, \ldots, \omega_n)$ represents the strategies picked by other players. $\Omega = \Omega_1 \times \Omega_2 \times \ldots \times \Omega_n$ denotes the set of all possible strategy profiles. Each player i has a utility function $u_i: \Omega \rightarrow \mathbf{R}$ that calculates the payoff of player i for a given strategy profile.

A strategy profile $\omega \in \Omega$ where $\omega = (\omega_i, \omega_{-i})$ is a *Nash equilibrium* if and only if, for each player i and every

$\omega_i' \in \Omega_i$, $u_i(\omega_i, \omega_{-i}) \geq u_i(\omega_i', \omega_{-i})$. That is, in a Nash equilibrium, no player can increase its payoff by unilaterally deviating from its strategy. A Nash equilibrium corresponds to a stable state of the game.

A function $f(x)$ is an *increasing function* if $f(b) \geq f(a)$ for all $b > a$. Conversely, function $f(x)$ is a *decreasing function* if $f(b) \leq f(a)$ for all $b > a$. According to calculus [16], if the derivative $f'(x)$ of $f(x)$ satisfies $f'(x) > 0$ on an interval (a, b), then $f(x)$ is increasing on (a, b). If $f'(x) < 0$, $f(x)$ is decreasing on (a, b).

III. Assumptions and Terminologies

It is assumed that a system consists of the services of several service providers. *Service* and *service provider* are used interchangeably in this paper. The services are independent of each other. That is, the system owner needs to negotiate a SLA with each of the services. The services in a system form a *service group*, denoted as *S*. Each service is interested in maximising its payoff, and the system owner is interested in maximising the security of her system. An adversary wants to compromise the system by breaching the security of the services that make up the system.

Defence efforts refer to the various security techniques employed by the services, e.g. firewall filtering, deploying intrusion detection and prevention systems, etc. The level of defence efforts represents the techniques and the recourses available to a service. For each service *i* ($1 \leq i \leq n$), (a) the level of the defence efforts chosen by *i* is e_i ($0 \leq e_i \leq 1$), (b) the effort's unit cost to *i* is c_i ($c_i > 0$), and (c) the payment to *i* for carrying out its tasks successfully (i.e. *i* does not suffer from any security breach) is v_i. Hence, the cost for carrying out defence is $c_i e_i$. It is assumed that e_i has been normalised across all the services in a service group such that 1 means the maximum amount of protection efforts that can be possessed by a service. As service providers have different capability, generally speaking, for many service providers, their maximum possible e_i, denoted as e_i^{max}, is less than 1. e_i^{max} is called the *defence capability* of the service *i*.

Similarly, the adversary's *attack effort level* measures the amount of efforts that the adversary puts into attacking a system. The attack effort level is represented as e_a ($0 \leq e_a \leq 1$). The unit cost for carrying out attack is c_a ($c_a > 0$). Hence, the cost of attack is $c_a e_a$. The payment to the adversary for successfully compromising a service *i* is $v_{a,i}$. In practice, it is impossible for a customer to know the precise value of c_a and $v_{a,i}$. However, a customer can hire a security consultant to analyse the types of security threats to the system and the types of adversaries. Thus, it is possible to have an estimate on the c_a and $v_{a,i}$ of different types of adversaries.

It is assumed that the probability of a system being compromised depends on the attack and the defence efforts exerted by the adversary and the services respectively. Thus, the probability that service *i* is compromised is "$e_a(1 - e_i)$". The likelihood that service *i* defeats an attack is "$1 - e_a(1 - e_i)$". As a consequence, "$v_i\big(1 - e_a(1 - e_i)\big)$" is the expected payment that service *i* receives for carrying out its task successfully.

A *security game* is a game-theoretic model that captures the reasoning used by the services and the adversary when they decide how much effort they put into defending or attacking the system. It also allows the system owner to analyse the incentives that need to be given to the services for inducing high level of defence efforts.

The utility functions of the services and the adversary have e_a and e_i ($1 \leq i \leq n$) as variables. This is because, (a) e_a and e_i are the strategies determined by the adversary and the services while playing the game, and (b) all other parameters are either intrinsic to the player, e.g. c_i, or are determined by the system owner and the service providers during SLA negotiation, e.g. v_i.

It is assumed that, once a service is compromised, it becomes unavailable. As the level of defence effort of each service is directly linked to the security of the system, the game is regarded as being played between the adversary and all the service providers of the system. Thus, a strategy profile consists of *2n* items. The first *n* items are the strategies taken by the service providers. The last *n* items are the strategies used by the adversary against each of the services. That is, in strategy profile $(\omega_1, \omega_2, \dots, \omega_{2n})$, ω_{2i} is the adversary's strategy against service *i*'s strategy ω_i where $1 \leq i \leq n$.

A list of the notations used in the paper is given below:

S	the IDs of the services, $S = \{1, 2, \dots, n\}$
$v_{a,i}$	the adversary's payment for compromising service *i*
e_a	the attack effort of the adversary, $0 \leq e_a \leq 1$
e_a^{max}	the maximum attack effort of the adversary
e_i	the defence effort of service *i*, $0 \leq e_i \leq 1$
e_i^{max}	the maximum defence effort of service *i*
c_a	the unit cost of attack effort
c_i	the unit cost of defence effort
b_i	bonus for having defence effort
r_i	defence effort related payment
$\gamma_{j,i}$	the increment (in percentage) to service *i*'s payment due to service *j*'s unavailability

IV. Mutually Supporting Partnership Game

In this game, the services in a system carry out their tasks independently. The services belong to different security domains. That is, compromising a service does not increase the odds that the adversary could successfully compromise any other services in the system. The services are mutually supporting. If a service becomes unavailable, the workloads of the service are shared by the other service providers in the system.

An example of a mutually supporting partnership system is a content distribution network. The network consists of many service providers at different geographical locations. The customers of the network access the information from

their closest service provider. If a service provider becomes unavailable, customers' requests sent to the unavailable service are redirected to the other service providers in the network.

The payoff of the adversary is analysed first. As the probability of compromising service i is $e_a(1-e_i)$, $v_{a,i}e_a(1-e_i)$ is the expected payment to the adversary. The utility function of the adversary against service *i* is:

$$u_{a,i} = v_{a,i}e_a(1-e_i) - c_a e_a \quad \text{where } v_{a,i} > c_a \qquad (1)$$

The adversary needs to have positive payoff if it attacks a service. If $v_{a,i} \le c_a$, the service can set e_i to 0 (i.e. the service does not use any defensive measures) to make the payoff of the adversary a non-positive value. Clearly, this does not make sense. Thus, "$v_{a,i} > c_a$" holds in (1).

From (1), it can be seen that, if the value of e_i is fixed, $u_{a,i}$ can be regarded as a function of variable e_a. The partial derivative of $u_{a,i}$ with respect to e_a is:

$$\frac{\partial u_{a,i}}{\partial e_a} = v_{a,i}(1-e_i) - c_a$$

According to §II, the sign of the value of $\frac{\partial u_{a,i}}{\partial e_a}$ determines how to maximise $u_{a,i}$. Thus, they are discussed separately.

Analysis 1 ($\frac{\partial u_{a,i}}{\partial e_a} < 0$):

Let $\frac{\partial u_{a,i}}{\partial e_a} < 0$ and solve the inequality below:

$$v_{a,i}(1-e_i) - c_a < 0$$

It can be seen that, if $e_i > \frac{v_{a,i}-c_a}{v_{a,i}}$, then $\frac{\partial u_{a,i}}{\partial e_a} < 0$.

According to §II, if $\frac{\partial u_{a,i}}{\partial e_a} < 0$, $u_{a,i}$ is a decreasing function. This means that $u_{a,i}$ decreases as the value of e_a increases. Thus, the adversary would set e_a to its smallest value, i.e. 0, to maximise $u_{a,i}$. This means that the adversary gives up attacking the system if the defence effort satisfies "$e_i > \frac{v_{a,i}-c_a}{v_{a,i}}$".

Analysis 2 ($\frac{\partial u_{a,i}}{\partial e_a} > 0$):

Let $\frac{\partial u_{a,i}}{\partial e_a} > 0$ and solve the inequality below:

$$v_{a,i}(1-e_i) - c_a > 0$$

It can be seen that, if $e_i < \frac{v_{a,i}-c_a}{v_{a,i}}$, then $\frac{\partial u_{a,i}}{\partial e_a} > 0$.

According to §II, if $\frac{\partial u_{a,i}}{\partial e_a} > 0$, $u_{a,i}$ is an increasing function. This means $u_{a,i}$ increases as the value of e_a gets bigger. Thus, to maximise its payoff, the adversary would set e_a to its maximum value, i.e. e_a^{max}. That is, the adversary would push to its limit in attacking the service.

Analysis 3 ($\frac{\partial u_{a,i}}{\partial e_a} = 0$):

Let $\frac{\partial u_{a,i}}{\partial e_a} = 0$ and solve the equation below:

$$v_{a,i}(1-e_i) - c_a = 0$$

It can be seen that, if $e_i = \frac{v_{a,i}-c_a}{v_{a,i}}$, then $\frac{\partial u_{a,i}}{\partial e_a} = 0$. Substitute e_i in $u_{a,i}$ with $\frac{v_{a,i}-c_a}{v_{a,i}}$. It can be seen $u_{a,i} = 0$. That is, the payoff of the adversary is 0. As the adversary attacks a system for financial gains, it can be said that the adversary would not attack the system when "$e_i = \frac{v_{a,i}-c_a}{v_{a,i}}$" due to the lack of any financial incentive.

Observation 1: When $e_i \ge \frac{v_{a,i}-c_a}{v_{a,i}}$, the adversary would not attack the service. If $e_i < \frac{v_{a,i}-c_a}{v_{a,i}}$, the adversary would exert maximum attack effort. □

The payoffs of the services are discussed now. As explained in §III, the probability that service *i* is secure is "$1-e_a(1-e_i)$". Thus, the expected payment of service *i* is "$v_i\big(1-e_a(1-e_i)\big)$".

If a service *j* becomes unavailable, part of *j*'s load will be taken over by service *i*. Let $\gamma_{j,i}$ ($\gamma_{j,i} \ge 0$) be the percentage of increased payments to service *i* due to the unavailability of service *j*. $\gamma_{j,i}$ is determined by the system owner when the system is configured. That is, the owner specifies the amount of traffic to *j* that should be redirected to service *i* when service *j* is unavailable. Based on the amount of traffic being redirected to *i*, $\gamma_{j,i}$ can be determined.

Since "$e_a\big(1-e_j\big)$" is the probability that service *j* is compromised and "$1-e_a(1-e_i)$" is the odds that service *i* can successfully fend off attacks, "$e_a\big(1-e_j\big)(1-e_a(1-e_i))$" is the likelihood that *i* is functioning while *j* is unavailable. Hence, "$\gamma_{j,i}v_i e_a\big(1-e_j\big)(1-e_a(1-e_i))$" is the expected payment that service *i* will receive due to service *j* being compromised.

The utility function of service i is defined below. In the function, b_i is a bonus given to service *i* for providing at least $\frac{v_{a,i}-c_a}{v_{a,i}}$ level of defence. r_i is a defence effort-related payment for inducing the service to use high defence effort. v_i, b_i and r_i are determined by the system owner and the service provider during their SLA negotiation.

$$\begin{cases} \text{If } e_i^{max} \ge \frac{v_{a,i}-c_a}{v_{a,i}} \text{ and } e_i \ge \frac{v_{a,i}-c_a}{v_{a,i}} \\ \quad u_i = v_i\big(1-e_a(1-e_i)\big) \\ \qquad + \sum_{j\in S-\{i\}} \gamma_{j,i}v_i e_a\big(1-e_j\big)(1-e_a(1-e_i)) - c_i e_i + b_i \\ \text{If } e_i^{max} \ge \frac{v_{a,i}-c_a}{v_{a,i}} \text{ and } e_i < \frac{v_{a,i}-c_a}{v_{a,i}} \\ \quad u_i' = v_i\big(1-e_a(1-e_i)\big) \\ \qquad + \sum_{j\in S-\{i\}} \gamma_{j,i}v_i e_a\big(1-e_j\big)(1-e_a(1-e_i)) - c_i e_i \\ \text{If } e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}} \\ \quad u_i'' = v_i\big(1-e_a(1-e_i)\big) \\ \qquad + \sum_{j\in S-\{i\}} \gamma_{j,i}v_i e_a\big(1-e_j\big)(1-e_a(1-e_i)) - c_i e_i + r_i e_i \end{cases}$$

The services in the service group can be divided into two sets based on whether their defence capability is greater than $\frac{v_{a,i}-c_a}{v_{a,i}}$. Let $G = \{i \in S | e_i^{max} \ge \frac{v_{a,i}-c_a}{v_{a,i}}\}$ and $L = \{i \in$

$S|e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}\}$. The payoffs of the services in G and L are discussed separately. First the utilities of the services in G are analysed.

Analysis 4 ($e_i^{max} \geq \frac{v_{a,i}-c_a}{v_{a,i}}$):

It can be seen that, if e_a and e_j are fixed, u_i is a function of variable e_i. The partial derivatives of u_i and u_i' with respect to e_i are:

$$\frac{\partial u_i}{\partial e_i} = \frac{\partial u_i'}{\partial e_i} = v_i e_a + \sum_{j \in S-\{i\}} \gamma_{j,i} v_i {e_a}^2 (1 - e_j) - c_i$$

As we are studying how the attacker's behaviour would affect the payoff of the service provider, $\frac{\partial u_i}{\partial e_i}$ is regarded as a function of e_a. According to §III, for most service providers, "$e_j < 1$" holds. Without loss of generality, it can be assumed that, for some services, "$0 \leq e_j < 1$" holds. If "$e_j < 1$", "$1 - e_j > 0$". Also, v_i and $\gamma_{j,i}$ are both positive values according to their definitions. Hence, "$\sum_{j \in S-\{i\}} \gamma_{j,i} v_i (1 - e_j) > 0$" holds. As a result, $\frac{\partial u_i}{\partial e_i}$ and $\frac{\partial u_i'}{\partial e_i}$ are upward parabolas of variable e_a that are similar to the one shown in Figure 1.

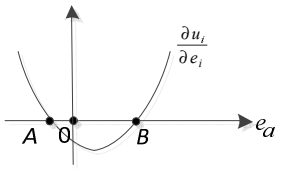

Figure 1 The Shape of $\frac{\partial u_i}{\partial e_i}$ and $\frac{\partial u_i'}{\partial e_i}$

To determine whether the parabola intersects with the e_a-axis, the solution for the quadratic equation below is considered:

$$\sum_{j \in S-\{i\}} \gamma_{j,i} v_i (1 - e_j) {e_a}^2 + v_i e_a - c_i = 0 \quad (2)$$

According to [16], quadratic equation (2) has a solution if the following holds:

$${v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j) \geq 0 \quad (3)$$

As discussed earlier, "$(1 - e_j) \geq 0$" holds. According to the definitions of c_i, v_i and $\gamma_{j,i}$, they are all greater than 0. Thus, inequality (3) holds. This means that the parabola must intersect with e_a-axis. According to [16], the two intersection points are:

$$A = \frac{-v_i - \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}}{2 v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}$$

$$B = \frac{-v_i + \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}}{2 v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}$$

$\because 1 - e_j > 0, c_i > 0, v_i > 0, \gamma_{j,i} > 0$

$$\therefore -v_i - \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)} < 0$$

$$\therefore A = \frac{-v_i - \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}}{2 v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)} < 0$$

$$\because {v_i}^2 < {v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)$$

$$\therefore v_i < \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}$$

$$\therefore -v_i + \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)} > 0$$

$$\therefore B = \frac{-v_i + \sqrt{{v_i}^2 + 4 c_i v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)}}{2 v_i \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)} > 0$$

Therefore, the two intersection points are on either side of the origin as shown in Figure 1.

According to **Observation 1**, the adversary will not attack the service (i.e. $e_a = 0$) if $e_i \geq \frac{v_{a,i}-c_a}{v_{a,i}}$. From Figure 1, it can be seen that $\frac{\partial u_i}{\partial e_i} \leq 0$ when $e_a = 0$. Hence, u_i is a decreasing function. As a result, the service provider would set $e_i = 0$ to maximise its payoff. Since the adversary would start attacking the system once e_i drops below $\frac{v_{a,i}-c_a}{v_{a,i}}$, the system owner wants the service providers set e_i to at least $\frac{v_{a,i}-c_a}{v_{a,i}}$ to deter attacks. The system owner offers incentive b_i to service provider i if i provides at least $\frac{v_{a,i}-c_a}{v_{a,i}}$ defence effort. The payoff of the service provider when $e_i = \frac{v_{a,i}-c_a}{v_{a,i}}$ can be obtained by setting $e_a = 0$ (since the adversary does not attack when $e_i \geq \frac{v_{a,i}-c_a}{v_{a,i}}$) in u_i. Hence,

$$u_i = v_i - c_i \frac{v_{a,i} - c_a}{v_{a,i}} + b_i \quad (4)$$

According to **Observation 1**, the adversary will attack the system with maximum effort if $e_i < \frac{v_{a,i}-c_a}{v_{a,i}}$. If the service provider sets $e_i = 0$, the payoff of the service provider can be obtained by substituting $e_a = e_a^{max}$ in u_i'. Hence,

$$u_i' = v_i (1 - e_a^{max}) + \sum_{j \in S-\{i\}} \gamma_{j,i} v_i e_a^{max} (1 - e_j)(1 - e_a^{max}) \quad (5)$$

The service provider would only provide defence effort $e_i \geq \frac{v_{a,i}-c_a}{v_{a,i}}$ if "(4) > (5)" holds. That is, the payoff for providing defence effort is higher than the payoff for having no defence effort. Solve the inequality "(4) > (5)", the following can be obtained:

$$b_i > c_i \frac{v_{a,i} - c_a}{v_{a,i}} - v_i e_a^{max} (1 + \sum_{j \in S-\{i\}} \gamma_{j,i} (1 - e_j)(1 - e_a^{max}))$$

This means that, if the incentive b_i is high enough, the service provider will provide defence efforts.

Observation 2: If the following inequality holds,

$$b_i > c_i \frac{v_{a,i} - c_a}{v_{a,i}} - v_i e_a^{max}(1 - \sum_{j \in S-\{i\}} \gamma_{j,i}(1 - e_j)(1 - e_a^{max})$$

the service provider would set defence effort to $\frac{v_{a,i}-c_a}{v_{a,i}}$. □

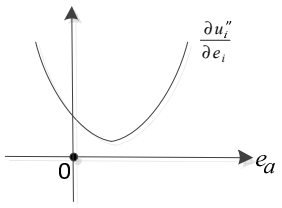

Figure 2 The Shape of $\frac{\partial u_i''}{\partial e_i}$

Next, the utilities of the services in *L* are analysed.

Analysis 5 ($e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}$):

$$\frac{\partial u_i''}{\partial e_i} = v_i e_a + \sum_{j \in S-\{i\}} \gamma_{j,i} v_i {e_a}^2 (1 - e_j) - c_i + r_i$$

Using the same analysis as the one in **Analysis 4**, it can be seen that $\frac{\partial u_i''}{\partial e_i}$ is an upward parabola of variable e_a that is similar to the one in Figure 2. As the service provider's maximum defence capability is less than $\frac{v_{a,i}-c_a}{v_{a,i}}$, according to **Observation 1**, the adversary will attack the service with maximum effort e_a^{max}. The system owner would want the service provider to use maximum defence effort. Thus, it is necessary to make u_i'' an increasing function. This means that $\frac{\partial u_i''}{\partial e_i} > 0$ should hold for all possible values of e_a. Therefore, the parabola in Figure 2 should not intersect with the e_a-axis. That is, the quadratic equation (i.e. $\frac{\partial u_i''}{\partial e_i} = 0$) below does not have any solution.

$$\sum_{j \in S-\{i\}} \gamma_{j,i} v_i (1 - e_j) {e_a}^2 + v_i e_a - c_i + r_i = 0$$

According to [16], the quadratic equation does not have a solution when the following holds:

$${v_i}^2 - 4(r_i - c_i) v_i \sum_{j \in S-\{i\}} \gamma_{j,i}(1 - e_j) < 0$$

$$\therefore r_i > \frac{v_i}{4 \sum_{j \in S-\{i\}} \gamma_{j,i}(1 - e_j)} + c_i$$

This means that, if the system owner gives sufficient incentive r_i to induce the service provider to put in defence effort, the service provider will put in maximum defence effort.

Observation 3: If the following inequality holds,

$$r_i > \frac{v_i}{4 \sum_{j \in S-\{i\}} \gamma_{j,i}(1 - e_j)} + c_i$$

the service providers in *L* will put in maximum efforts in defending its service. □

As it is in the system owner's interest to make the system secure, it is reasonable to assume that the system owner will satisfy the requirements regarding b_i and r_i identified in **Observations** 2 and 3. As a result, all the service providers in *G* would have $e_i = \frac{v_{a,i}-c_a}{v_{a,i}}$ while every service provider in *L* would have $e_i = e_i^{max}$. Hence, **Observations** 2 and 3 can be rewritten as below:

Observation 2': If the following inequality holds:

$$b_i > c_i \frac{v_{a,i} - c_a}{v_{a,i}} - v_i e_a^{max}(1 - (1 - e_a^{max}) \left(\sum_{j \in L-\{i\}} \gamma_{j,i}(1 - e_j^{max}) + \sum_{j \in S-\{i\}} \frac{\gamma_{j,i} c_a}{v_{a,j}} \right))$$

the service providers in *G* would set defence effort to $\frac{v_{a,i}-c_a}{v_{a,i}}$.

Observation 3': If the following inequality holds:

$$r_i > \frac{v_i}{4(\sum_{j \in G-\{i\}} \frac{\gamma_{j,i} c_a}{v_{a,j}} + \sum_{j \in L-\{i\}} \gamma_{j,i}(1 - e_j^{max}))} + c_i$$

the service providers in *L* will put in maximum efforts in defending their services. □

From observations 1, 2' and 3', the following can be obtained:

Result: In the mutually supporting partnership game,

- If $e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}$, the system owner must ensure that "$r_i > \frac{v_i}{4(\sum_{j \in G-\{i\}} \frac{\gamma_{j,i} c_a}{v_{a,j}} + \sum_{j \in L-\{i\}} \gamma_{j,i}(1 - e_j^{max}))} + c_i$" to induce maximum defence effort by service *i*; service *i* should deploy maximum defence effort; and, the adversary would exert maximum attack effort.
- If $e_i^{max} \geq \frac{v_{a,i}-c_a}{v_{a,i}}$, the system owner must ensure that "$b_i > c_i \frac{v_{a,i}-c_a}{v_{a,i}} - v_i e_a^{max}(1 - (1 - e_a^{max}) \left(\sum_{j \in L-\{i\}} \gamma_{j,i}(1 - e_j^{max}) + \sum_{j \in S-\{i\}} \frac{\gamma_{j,i} c_a}{v_{a,j}} \right))$" to inspire service *i* to use defence measures; service *i* should set e_i to $\frac{v_{a,i}-c_a}{v_{a,i}}$; and, the adversary would set e_a to 0.
- Strategy profile $(\omega_1, \omega_2, \ldots, \omega_{2n})$ is a Nash equilibrium where $\forall i: \{j \in \mathbb{Z} | 1 \leq j \leq n\}$

$$\omega_i = \begin{cases} e_i^{max} & if\ e_i^{max} < \frac{v_{a,i} - c_a}{v_{a,i}} \\ \frac{v_{a,i} - c_a}{v_{a,i}} & if\ e_i^{max} \geq \frac{v_{a,i} - c_a}{v_{a,i}} \end{cases}$$

$$\omega_{2i} = \begin{cases} e_a^{max} & if\ e_i^{max} < \frac{v_{a,i} - c_a}{v_{a,i}} \\ 0 & if\ e_i^{max} \geq \frac{v_{a,i} - c_a}{v_{a,i}} \end{cases}$$

V. Related Work

Ye [17] proposed two security games for studying service computing applications. The two games aimed at two classes of service computing applications. The two classes of applications are: (a) the services in a system rely on each other to function correctly, and (b) the services in a system are independent of each other and they do not share any workload of each other. The game proposed in this paper studies the applications in which the services work independently and share the workload of the system. This type of applications is commonly seen in service computing, e.g. contents delivery network. Thus, the work in this paper complements the work in [17].

Rass [14] treated the security provisioning problem as a 2-player zero-sum game. The players are the service provider and the attacker. As a system normally consists of many service providers, different from Rass' approach, the model in this paper allows an arbitrary number of players in a game. Also, the scheme in this paper not only considers the interest of the service providers, it takes into account the interests of the customer as well. Thus, the terms in a SLA would be more acceptable to both the customer and the service providers.

Varian [13] classified the security of a networked system into three categories, and, analysed the security investment using a public goods game-theoretical framework. Varian focused on two-player games with heterogeneous effort costs and benefits from reliability. Grossklags et al. [6,2] generalises the work in [13]. Instead of being two-player games, the games in [6,2] are n-player games. Khouzani et al. [8] studied the impact of a regulator on improving the security of the Internet. Mavronicolas et al. [10] investigated the defence of a distributed system by a group of interdependent defenders. Apart from the weakest-link game studied in [13], the games mentioned above do not match the scenarios in service computing applications. For the weakest-link game, unlike this paper, Varian did not address how to inspire the services to apply high security efforts.

Amin et al. [1] studied the security of a system that consists of a set of entities. Fan et al. [3] used a stochastic game model to evaluate attack-defence process in cloud computing. Amin's and Fan's schemes both focused on discovering the best defence strategy for the system. Different to their schemes, the scheme in this paper helps the customer to identify the incentives that induce the service providers to maximise their defence efforts.

VI. Conclusions

This paper models the security of a class of service computing applications as the mutually supporting partnership game. The modelling enables the studying of the relationships between the security of a system and the level of defence/attack efforts deployed by the services and the adversary. The Nash equilibrium of the game were analysed from the perspectives of the service providers and the adversary. This paper identified the incentives that need to be used to motivate the services exerting high defence efforts. As the analyses consider the interests of both the service providers (i.e. high payoff) and the customers (i.e. high system security), the results of the analyses should make the customers and the service providers be more objective in their SLA negotiations. Hence, it would be easier for them to reach an agreement that satisfies all parties.

References

[1] Amin S., Schwartz G. A., and Sastry S. S. 2013. Security of interdependent and identical networked control systems. Automatica 49, 1 (January 2013), 186-192.

[2] Christin N., Egelman S., Vidas T., and Grossklags J. 2011. It's all about the benjamins: an empirical study on incentivizing users to ignore security advice. In Proc. of the 15th intl. conference on Financial Cryptography and Data Security (FC'11), Springer, 16-30

[3] Fan G., Yu H., Chen L., Liu D. A Game Theoretic Method to Model and Evaluate Attack-Defense Strategy in Cloud Computing. IEEE SCC 2013: 659-666

[4] Florêncio D., Herley C. Where Do All the Attacks Go? 2013, in Economics of Information Security and Privacy III, 13-33, Springer

[5] Gross G. "FCC chairman calls on ISPs to adopt new security measures," http://www.computerworld.com/s/article/9224485/FCC chairman calls on ISPs to adopt new security measures, February 2012, accessed on 15/02/2014

[6] Grossklags J., Christin N. and Chuang J. 2008. Secure or insure?: A game-theoretic analysis of information security games. In Proceedings of the 17th ACM International Conference on World Wide Web (WWW). 209–218.

[7] Grossklags, J. and Johnson, B. 2009. Uncertainty in the weakest-link security game. In Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets). 673–682

[8] Khouzani M. H. R., Sen S., Shroff N. B. An economic analysis of regulating security investments in the Internet. INFOCOM 2013: 818-826

[9] Manshaei M. H., Zhu Q., Alpcan T., Bacşar T., and Hubaux J. 2013. Game theory meets network security and privacy. ACM Comput. Surv. 45, 3, Article 25

[10] Mavronicolas M., Monien B., and Lesta V. P. 2013. How many attackers can selfish defenders catch?. Discrete Appl. Math. 161, 16-17 (November 2013), 2563-2586.

[11] Narasimhan B. and Nichols R. 2011. State of Cloud Applications and Platforms: The Cloud Adopters' View, IEEE Computer, Vol. No. 3, 24-28

[12] Nisan N., Roughgarden T., Tardos E., Vazirani V. V. 2007, Algorithmic Game Theory, Cambridge University Press

[13] Varian H. 2004. System reliability and free riding. In L. Camp and S. Lewis (ed.), Economics of Information Security (Advances in Information Security, Volume 12), pages 1–15. Kluwer Academic Publishers.

[14] Rass S. 2013. On Game-Theoretic Network Security Provisioning. J. Netw. Syst. Manage. 21, 1 (March 2013), 47-64.

[15] Reuters. Target breach could cost hundreds of millions, http://www.reuters.com/article/2013/12/20/target-breach-expenses-idUSL2N0JZ03I20131220, accessed on 15/02/2014

[16] Strang G. 1991. Calculus, Wellesley

[17] Ye X., 2014. A Game-Theoretic Analysis of Security Investment for Service Computing Applications, Proceedings of the 2014 IEEE World Congress on Services