A Game-Theoretic Analysis of Security Investment for Service Computing Applications

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

Abstract—**In service computing, a system can be built by integrating the services from different service providers. The security of such system is closely linked to the security of the services that make up the system. This paper studied the security investment of some service computing applications using a game theoretical approach. It proposed two security games for modeling two classes of service computing applications. Using the games, the service providers and their customers can analyse the security level and the security investment of a system. The results of the analysis should allow the customers and the service providers be more objective in their service level agreement negotiation, and make it easier for them to reach an agreement.**

Keywords- system security, service level agreement

I. INTRODUCTION

In service-oriented architecture, a system can be integrated by using the services provided by different 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. Security breaches and intrusions into governmental and financial computer systems are causing billions of dollars of lost [5, 17]. 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, 11]. These studies intend to discovery the relationship between the security investment and the security threats facing the systems.

For a system consisting of services from several service providers, the security of the system links to the level of security offered by each of the service providers. For example, if one service in the system is compromised, part of the system or the whole system might become non-operational. Hence, there is a strong connection between the security of the individual services and the security of the whole system. Varian [15] 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. In the total effort game, the security of the system depends on the sum of the efforts exerted by each participant of the system. In the weakest link game, the security of the system is determined by the security of the participant that puts minimum effort in defending the system. In the best effort game, the security of the system depends on the maximum effort that a participant places in system defence. Many applications in service computing have different usage patterns from the applications studied in [15]. For example, as each service can be accessed over the Internet, if an attacker manages to compromise a single service in a service computing application, the operation of the whole system is likely to be affected. Therefore, the best effort and the total effort games cannot be used to examine the security of many systems in service computing. Although the weakest-link game can be used to analyse the security of a class of service computing applications, [15] did not discuss how to provide incentives to make the participants exert maximum efforts in defending the system.

Survey showed that system owners are willing to invest in measures that prevent attacks and mitigate the damages from security breaches [13]. 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 two security games for modelling two classes of service computing applications. Each of the games was investigated to find out how the customers should negotiate the terms in the SLA to encourage the service providers to exert high security efforts. The proposed games allow the service providers and the customers 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 their customers. By studying how the service providers react to the threats to their services, the customers would be able to decide how to provide incentives to induce the service providers to deploy high defence efforts to protect their

services. The proposed scheme takes into account of the interests of both the customers and the service providers. Thus, the solutions are acceptable to both the customers and the service providers.

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 two security games, and uses the two games to study the security of two classes of service computing applications. §V concludes the paper.

II. GAME THEORY BACKGROUND

In game theory [14, 19], a *game* consists of a set of n players, $\{1, 2, \dots, n\}$. Each player i has its own set of possible strategies, Ω_i. To play the game, each player selects a strategy $\omega_i \in \Omega_i$. $\omega = (\omega_1, \omega_2, \dots, \omega_n)$ 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 $\omega_{-i} = (\omega_1, \omega_2, \dots, \omega_{i-1}, \omega_{i+1}, \dots, \omega_n)$ represents the strategies picked by other players. $\Omega = \Omega_1 \times \Omega_2 \times \dots \times \Omega_n$ 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 [18], 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 owner of the system is called the *customer*. The services are independent of each other. That is, the customer 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 customer 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, disallowing certain types of traffic, 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 system is v_a. In practice, it is impossible for a customer to know the precise value of c_a and v_a. 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 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 customer to analyse the incentives that need to be given to the services for inducing high level of defence efforts. In the security game, each service decides on its level of defence efforts individually, and all decisions are made simultaneously.

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 customer and the service providers during SLA negotiation, e.g. v_i.

It is assumed that, once a service is compromised, the attacker would make the service un-useable. That is, a compromised service 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 $1 \le i \le n$.

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	the adversary's payment for compromising a system
$v_{a,i}$	the adversary's payment for compromising service *i*
e_a	the attack effort of the adversary, $0 \le e_a \le 1$
e_a^{max}	the maximum attack effort of the adversary
e_i	the defence effort of service *i*, $0 \le e_i \le 1$
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
p	penalty for being compromised
b, b_i	bonus for having defence effort
r_i	defence effort related payment
$\alpha_{j,i}$	the proportion of service *i*'s payment affected by service *j*'s unavailability

IV. Security Games for Service Computing

A. Tightly Integrated Partners Game

In this game, the services that constitute a system rely on the information provided by each other to function correctly. That is, the normal operation of the system requires all the services to be available. If one of the services is compromised, the system is rendered to useless. Also, as the service providers are tightly integrated, an adversary might be able to use the credentials that it obtained from a compromised service to gain un-authorized access to the information on other services in the system.

An example of a tightly integrated system is an enterprise system in which the accounting system is operated by a service provider, say s_1, while the enterprise's data are hosted by another service provider, say s_2. In order to carry out its task, s_1 needs to access the data residing on s_2. If s_2 is compromised and becomes unavailable, s_1 will not be able to access the data required for carrying out its task. On the other hand, if the security of s_1 is breached, the adversary can use the credentials obtained from s_1 to access the information on s_2.

In this game, as the adversary can compromise the whole system by breaching the security of any of the services, the security of the system depends on the service that puts the least effort in system defence. Let id_min denote the ID of the service whose defence effort is the lowest among all the services. e_{id_min} denotes the defence effort put in by service id_min. As explained in §III, the probability that the security of service id_min is breached is "$e_a(1 - e_{id\_min})$". Thus, the probability that the system is compromised is "$e_a(1 - e_{id\_min})$".

The payoff of the adversary is analysed first. As the adversary can only obtain its rewards if it successfully breaks into the system, the expected payoff of the adversary is "$v_a e_a(1 - e_{id\_min})$". Assume that the adversary attacks each service in the system with the same amount of effort. Thus, the total cost for the adversary is $nc_a e_a$ where *n* is the number of services in the system. Thus, the utility function of the attacker is:

$$u_a = v_a e_a(1 - e_{id\_min}) - nc_a e_a \quad (1)$$

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

$$\frac{\partial u_a}{\partial e_a} = v_a(1 - e_{id\_min}) - nc_a$$

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

Analysis 1 ($\frac{\partial u_a}{\partial e_a} < 0$):

Let $\frac{\partial u_a}{\partial e_a} < 0$ and solve the inequality below:

$$v_a(1 - e_{id\_min}) - nc_a < 0$$

It can be seen that, if $e_{id\_min} > 1 - \frac{nc_a}{v_a}$, then $\frac{\partial U_a}{\partial e_a} < 0$.

According to §II, if $\frac{\partial u_a}{\partial e_a} < 0$, u_a is a decreasing function. This means that u_a 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. This means that the adversary gives up attacking the system if the lowest level of defence effort satisfies "$e_{id\_min} > 1 - \frac{nc_a}{v_a}$".

Analysis 2 ($\frac{\partial u_a}{\partial e_a} > 0$):

Let $\frac{\partial u_a}{\partial e_a} > 0$ and solve the inequality below:

$$v_a(1 - e_{id\_min}) - nc_a > 0 \quad (2)$$

It can be seen that, if $e_{id\_min} < 1 - \frac{nc_a}{v_a}$, then $\frac{\partial u_a}{\partial e_a} > 0$.

According to §II, if $\frac{\partial u_a}{\partial e_a} > 0$, u_a is an increasing function. This means u_a 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 system.

Analysis 3 ($\frac{\partial u_a}{\partial e_a} = 0$):

Let $\frac{\partial u_a}{\partial e_a} = 0$ and solve the equation below:

$$v_a(1 - e_{id\_min}) - nc_a = 0$$

It can be seen that, if $e_{id\_min} = 1 - \frac{nc_a}{v_a}$, then $\frac{\partial u_a}{\partial e_a} = 0$. Substitute e_{id_min} in u_a with $1 - \frac{nc_a}{v_a}$. It can be seen $u_a = 0$. That is, the payoff is 0. As the adversary attacks a system for financial gains, it can be said that the adversary would not attack the system when "$e_{id\_min} = 1 - \frac{nc_a}{v_a}$" due to the lack of any financial incentive.

Observation 1: When $e_{id\_min} \ge 1 - \frac{nc_a}{v_a}$, the adversary would not attack the system. If $e_{id\_min} < 1 - \frac{nc_a}{v_a}$, the adversary would exert maximum attack effort. □

Next, the utility function of the service that provides the lowest defence effort is discussed. As explained in §III, the

probability that service id_min is secure is "$1 - e_a(1 - e_{id\_min})$". Thus, the expected payment of service id_min is "$v_{id\_min}\left(1 - e_a(1 - e_{id\_min})\right)$". The customer imposes a penalty p on service id_min as a punishment for allowing the system to be compromised. Thus, "$pe_a(1 - e_{id\_min})$" is the expected penalty received by service id_min. In (3), b is a bonus given to the service provider for deploying defence effort to a level no less than "$1 - \frac{nc_a}{v_a}$". The expected penalty "$pe_a(1 - e_{id\_min})$" should always be greater than the bonus to make the service providers put in sufficient level of defence effort to ensure the system is not compromised. Thus, "$pe_a(1 - e_{id\_min}) > b$" should be satisfied. v_{id_min}, b and p are decided by the customer and the service in the SLA negotiation. The utility function of service id_min is defined below:

$$\begin{cases} \text{If } e_{id\_min}^{max} \geq 1 - \frac{nc_a}{v_a} \text{ and } e_{id\_min} \geq 1 - \frac{nc_a}{v_a}\text{:} \\ \quad u_{id\_min} = v_{id\_min}\left(1 - e_a(1 - e_{id\_min})\right) \\ \qquad -pe_a(1 - e_{id\_min}) - c_{id\_min}e_{id\_min} + b \\ \qquad \text{where } pe_a(1 - e_{id\_min}) > b \quad (3) \\ \text{Otherwise:} \\ \quad u'_{id\_min} = v_{id\_min}\left(1 - e_a(1 - e_{id\_min})\right) \\ \qquad -pe_a(1 - e_{id\_min}) - c_{id\_min}e_{id\_min} \quad (4) \end{cases}$$

The rationales behind functions u_{id_min} and u'_{id_min} are explained next. It can be seen that, for a given e_a, u_{id_min} and u'_{id_min} are functions of variable e_{id_min}. The partial derivatives of the two functions with respect to e_{id_min} are:

$$\frac{\partial u_{id\_min}}{\partial e_{id\_min}} = \frac{\partial u'_{id\_min}}{\partial e_{id\_min}} = v_{id\_min}e_a + pe_a - c_{id\_min} \quad (5)$$

Analysis 4 ($e_{id\_min}^{max} \geq 1 - \frac{nc_a}{v_a}$):

(3) is the utility function of the service when "$e_{id\_min} \geq 1 - \frac{nc_a}{v_a}$". According to Observation 1, when "$e_{id\_min} \geq 1 - \frac{nc_a}{v_a}$", the adversary would set $e_a = 0$ to maximise its utility. Substituting e_a with 0 in $\frac{\partial u_{id\_min}}{\partial e_{id\_min}}$, it can be seen that:

$$\frac{\partial u_{id\_min}}{\partial e_{id\_min}} = -c_{id\_min}$$
$$\because\ c_{id\_min} > 0$$
$$\therefore\ \frac{\partial u_{id\_min}}{\partial e_{id\_min}} < 0$$

This means u_{id_min} is a decreasing function of variable e_{id_min} when "$e_a = 0$". Since "$0 \leq e_{id\_min} \leq 1$", service id_min would want to set "$e_{id\_min} = 0$" to maximise its payoff. However, according to inequality (2), when the defence effort of service id_min drops below "$1 - \frac{nc_a}{v_a}$", $\frac{\partial U_a}{\partial e_a}$ becomes a positive value. As a result, the adversary would want to use its maximum effort to maximise its payoff.

The customer needs service id_min to put in at least "$1 - \frac{nc_a}{v_a}$" amount of defence effort to deter attacks. Thus, the customer needs to ensure that the payoff of the service provider when "$e_{id\_min} = 1 - \frac{nc_a}{v_a}$" is not lower than the payoff when "$e_{id\_min} = 0$". Let $e_a = 0$. The payoffs of the service when "$e_{id\_min} = 1 - \frac{nc_a}{v_a}$" and "$e_{id\_min} = 0$" can be computed using formulas (3) and (4) respectively. Thus,

$$u_{id\_min} = v_{id\_min} - c_{id\_min}\left(1 - \frac{nc_a}{v_a}\right) + b$$
$$u'_{id\_min} = v_{id\_min}$$

Let $u_{id\_min} > u'_{id\_min}$ (i.e. make provider id_min have the incentive to put at least "$1 - \frac{nc_a}{v_a}$" amount of effort in defence). Solve the inequality to obtain the following:

$$b > c_{id\_min}(1 - \frac{nc_a}{v_a})$$

Observation 2: If "$e_{id\_min}^{max} \geq 1 - \frac{nc_a}{v_a}$" and "$b > c_{id\_min}(1 - \frac{nc_a}{v_a})$", service id_min should set defence effort to $1 - \frac{nc_a}{v_a}$. □

Analysis 5 ($e_{id\_min}^{max} < 1 - \frac{nc_a}{v_a}$):

Let $\frac{\partial u'_{id\_min}}{\partial e_{id\_min}} < 0$, and substitute $\frac{\partial u'_{id\_min}}{\partial e_{id\_min}}$ with the expression in (5). Solve the inequality to obtain $e_a < \frac{c_{id\_min}}{v_{id\_min}+p}$. Since $\frac{\partial u'_{id\_min}}{\partial e_{id\_min}} < 0$, u'_{id_min} is a decreasing function. Thus, the service provider would not want to put any effort into defence. This is because, compared with the probability of an attack being successful, the cost of defending is too high. Hence, it is not worth the effort.

Conversely, when $e_a > \frac{c_{id\_min}}{v_{id\_min}+p}$, $\frac{\partial u'_{id\_min}}{\partial e_{id\_min}} > 0$ holds. That is, u'_{id_min} is an increasing function. Thus, the service provider would want to put maximum effort in defending the system to maximise its own payoff.

It can be seen that, if v_{id_min} (i.e. the payment to service id_min) and p (i.e. the penalty) are sufficiently high, $\frac{c_{id\_min}}{v_{id\_min}+p}$ would be close to 0. That is, service id_min is willing to use maximum defence effort even if the adversary only put in little attack effort. In other words, a high v_{id_min} or p would encourage the service to use the utmost of its defence capability.

Observation 3: When $e_{id-min}^{max} < 1 - \frac{nc_a}{v_a}$, the customer should choose v_{id_min} and p to make $\frac{c_{id-min}}{v_{id\_min}+p}$ close to 0. This would make service id_min set $e_{id\_min} = e_{id\_min}^{max}$. □

It can be seen that, when "$e_{id\_min}^{max} \geq 1 - \frac{nc_a}{v_a}$", the service provider has the capability to successfully defend against attacks. However, in order to deter attacks, the customer needs to provide incentives for the service provider to maintain certain level of defence. When "$e_{id-min}^{max} < 1 - \frac{nc_a}{v_a}$", both the service provider and the adversary have a chance to win. Therefore, they would both put in maximum efforts in defence and attack.

Next, the utility function of the service providers whose defence effort is not the lowest is discussed. As the probability that the system is not compromised is "$1 - e_a(1 - e_{id\_min})$", the expected payment to the service is "$v_i\left(1 - e_a(1 - e_{id\_min})\right)$". The utility function is:

$$u_i = v_i\left(1 - e_a(1 - e_{id\_min})\right) - c_i e_i \quad (6)$$

Since $\frac{\partial u_i}{\partial e_i} = -c_i$ where $(1 \le i \le n \wedge i \ne id\_min)$ and $c_i > 0$, $\frac{\partial U_i}{\partial e_i} < 0$ holds. Thus, u_i is a decreasing function of variable e_i. Hence, service provider *i* would want to set e_i to its smallest value to maximise u_i. As service *i* is not the one that provides the lowest defence effort, the smallest value for e_i is e_{id_min}. Hence, every service has "$e_i = e_{id\_min}$".

Observation 4: All the services set their defence efforts to e_{id_min}. □

The following theorem shows that a service always has a higher payoff if it avoids being the one that puts in the lowest defence effort.

Theorem: In the tightly integrated partners game, the strategy of putting the lowest defence effort gives lower payoff than the strategy of avoiding being the lowest security effort contributor.

Proof: As u_i in (6) is a decreasing function, it can be seen that u_i reaches its maximum value when $e_i = e_{id\_min}$. Thus, according to (6), the payoff of service *i* is:

$$u_i = v_i\left(1 - e_a(1 - e_{id\_min})\right) - c_i e_{id\_min} \quad (7)$$

If service *i* is the lowest defence effort contributor (i.e. $i = id\_min$), its utility is calculated using formula (3) or (4). Thus, in (3) and (4), $v_{id\_min} = v_i$. Also,

$\because\ p > 0, e_a \ge 0, 0 \le e_{id\_min} \le 1$

$\therefore\ pe_a(1 - e_{id\_min}) \ge 0$

Hence, comparing u_i in expression (7) with formula (4), it can be seen:

$$u'_{id\_min} < u_i \quad (8)$$

According to formula (3), $pe_a(1 - e_{id\_min}) > b$. Thus, $b - pe_a(1 - e_{id\_min}) < 0$ holds. Comparing u_i in expression (7) with formula (3), it can be seen:

$$u_{id\_min} < u_i \quad (9)$$

According to (8) and (9), service *i* always has a higher payoff if it is not the lowest defence effort contributor. Hence, the theorem holds. □

According to the theorem, each service provider would increase their defence effort to avoid being the one that provides the lowest defence effort.

Observation 5: The lowest defence effort must be offered by the service that has the lowest defence capability. □

As it is in the customer's interest to make the system secure, it is reasonable to assume that the customer will satisfy the conditions regarding b, v_{id_min} and p identified in Observations 2 and 3. Hence, according to Observations 1 to 5, the following result can be obtained.

Result 1: In the tightly integrated partners game,

- Service id_min is the one that has the lowest defence capability. That is, $\forall i: S.\ e_{id\_min}^{max} \le e_i^{max}$.
- If $e_{id\_min}^{max} < 1 - \frac{nc_a}{v_a}$, the customer must choose v_{id_min} and p to make $\frac{c_{id\_min}}{v_{id\_min}+p}$ close to 0; all the services should set their defence efforts to $e_{id\_min}^{max}$; and, the adversary would set e_a to e_a^{max}. Strategy profile $(\omega_1, \omega_2, \dots, \omega_{2n})$ where $\forall i: \{j \in \mathbb{Z} | 1 \le j \le n\}.(\omega_i = e_{id\_min}^{max} \wedge \omega_{2i} = e_a^{max})$ is a Nash equilibrium.
- If $e_{id\_min}^{max} \ge 1 - \frac{nc_a}{v_a}$, the customer must ensure that $b > c_{id\_min}(1 - \frac{nc_a}{v_a})$; the services should all set their defence level to $1 - \frac{nc_a}{v_a}$; and, the adversary would set e_a to 0. Strategy profile $(\omega_1, \omega_2, \dots, \omega_{2n})$ where $\forall i: \{j \in \mathbb{Z} | 1 \le j \le n\}.(\omega_i = 1 - \frac{nc_a}{v_a} \wedge \omega_{2i} = 0)$ is a Nash equilibrium.

B. Independent Partnership Game

In this game, the services in a system carry out their tasks independently. That is, the successful execution of a task by a service does not depend on whether any of the other services are available. 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.

Although the services work independently, their availability might influence the system's users' decisions on whether using other services in the system. An example of the class of applications covered by this game is a travel agent system. Assume (a) the system includes a flight booking service, a hotel reservation service and a rental car booking service, and (b) the services are provided by different service providers. The reservation of flight ticket, hotel room and rental car can all be carried out alone. That is, each service can function independently without requiring any information from other services. However, a user might prefer to carry out all the bookings together. Thus, if one of the services in the system is unavailable (i.e. the user cannot carry out all the bookings using the system), the user might choose to use another system instead. Thus, although the services do not rely on each other to function, the availability of a service might affect the number of visits that other services receive.

It is assumed that the adversary applies the same amount of effort in attacking each of the service providers. $v_{a,i}$ is the payoff of the adversary if it successfully compromises service *i*. 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:

$$u_{a,i} = v_{a,i}e_a(1 - e_i) - c_a e_a \quad \text{where } v_{a,i} > c_a \quad (10)$$

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 (10).

The partial derivative of $u_{a,i}$ with respect to e_a is:

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

Using the same analysis method as the one used for analysing the attacker in the tightly integrated partners game (i.e. Analysis 1 to 3), the following observation can be made.

Observation 6: When $e_i \geq \frac{v_{a,i}-c_a}{v_{a,i}}$, the adversary should not attack the system. If $e_i < \frac{v_{a,i}-c_a}{v_{a,i}}$, the adversary should use maximum attack effort. □

The payoffs of the services are discussed now. Let $\alpha_{j,i}$ $(0 \leq \alpha_{j,i} < 1)$ be the proportion of service *i*'s payments (i.e. the percentage of visits) that are affected by the unavailability of service *j*. $\alpha_{j,i}$ can be estimated by surveying the potential users of the system. Since "$e_a(1 - e_j)$" 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, "$e_a(1 - e_j)(1 - e_a(1 - e_i))$" is the likelihood that *i* is functioning while *j* is unavailable. Hence, "$\alpha_{j,i} v_i e_a(1 - e_j)(1 - e_a(1 - e_i))$" is the expected affected payment of service *i* due to service *j* being compromised. It is assumed that $\alpha_{j,i}$ has been tuned[1] to satisfy the inequality in (11). The inequality means that the total proportion of service *i*'s lost payment should not exceed 1. This is a reasonable assumption. As all the services can function independently in this game, a user can still use service *i* even if all the other services of the system are unavailable.

$$\sum_{j \in S-\{i\}} \alpha_{j,i} < 1 \quad (11)$$

The utility function of the service providers are 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 customer and the service provider during the SLA negotiation.

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

[1] $\alpha_{j,i}$ has factored in the possibility that the failures of multiple services prevent the same set of users from accessing service *i*.

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

Analysis 6 ($e_i^{max} \geq \frac{v_{a,i}-c_a}{v_{a,i}}$):

Using the same method for analysing the utility of service id_min in the tightly integrated partners game under condition $e_i^{max} \geq 1 - \frac{nc_a}{v_a}$ (i.e. Analysis 4 in §IV.A), the following observation can be made:

Observation 7: When $e_i^{max} \geq \frac{v_{a,i}-c_a}{v_{a,i}}$, the bonus value for service *i* should satisfy $b_i > c_i(\frac{v_{a,i}-c_a}{v_{a,i}})$. If $b_i > c_i(\frac{v_{a,i}-c_a}{v_{a,i}})$, service *i* should set defence effort to $\frac{v_{a,i}-c_a}{v_{a,i}}$. □

As it is in the customer's interest to make service *i* to have at least $\frac{v_{a,i}-c_a}{v_{a,i}}$ level of defence, it is reasonable to assume that the customer would ensure that $\forall i: G. b_i > c_i(\frac{v_{a,i}-c_a}{v_{a,i}})$ holds.

Analysis 7 ($e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}$):

The partial derivative of u_i'' with respect to e_i is:

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

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 $e_j < 1$, $1 - e_j > 0$. Hence, "$-v_i \sum_{j \in S-\{i\}} \alpha_{j,i}(1 - e_j) < 0$" holds. As a result, $\frac{\partial U_i''}{\partial e_i}$ is a downward parabola of variable e_a as shown in Figure 1.

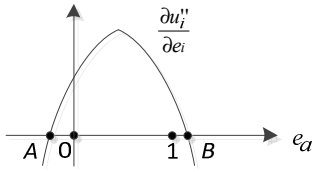

Figure 1 The Shape of the Partial Derivative of u_i''

If e_a and e_j $(j \in S - \{i\})$ are treated as constants in u_i'', it can be seen that u_i'' is a function of variable e_i. Thus, when $\frac{\partial u_i''}{\partial e_i} > 0$, u_i'' is an increasing function, and service *i* would deploy maximum defensive effort to maximise its payoff. Hence, the customer needs to make sure that $\frac{\partial u_i''}{\partial e_i}$ always evaluates to a positive value within the range of e_a. Since $0 \leq e_a \leq 1$, the customer needs to set the value of v_i and r_i such that the two intersection points *A* and *B* in Figure 1 must satisfy $A \leq 0$ and $B \geq 1$.

According to Observation 7, all the services in *G* would set their defence efforts to $\frac{v_{a,i}-c_a}{v_{a,i}}$. That is, $\forall i: G. e_i = \frac{v_{a,i}-c_a}{v_{a,i}}$.

For the services in L, if $\forall i: L. \frac{\partial u_i''}{\partial e_i} > 0$ holds, the services would use maximum defence effort. Hence, the value of e_j in $\frac{\partial u_i''}{\partial e_i}$ is either $\frac{v_{a,i}-c_a}{v_{a,i}}$ or e_j^{max}. Thus, $\frac{\partial u_i''}{\partial e_i}$ can be written as:

$$\frac{\partial u_i''}{\partial e_i} = v_i e_a - v_i {e_a}^2 \left(\sum_{j\in L-\{i\}} \alpha_{j,i}\left(1-e_j^{max}\right) + \sum_{j\in G-\{i\}} \alpha_{j,i}\left(1-\frac{v_{a,i}-c_a}{v_{a,i}}\right)\right) - c_i + r_i$$

$$= v_i e_a - v_i {e_a}^2 \left(\sum_{j\in L-\{i\}} \alpha_{j,i}\left(1-e_j^{max}\right) + \sum_{j\in G-\{i\}} \alpha_{j,i}\frac{c_a}{v_{a,i}}\right) - c_i + r_i$$

Let $\mathcal{H} = \sum_{j\in L-\{i\}} \alpha_{j,i}\left(1-e_j^{max}\right) + \sum_{j\in G-\{i\}} \alpha_{j,i}\frac{c_a}{v_{a,i}}$

$$\therefore \frac{\partial u_i''}{\partial e_i} = -v_i \mathcal{H} {e_a}^2 + v_i e_a - c_i + r_i$$

Let $\frac{\partial u_i''}{\partial e_i} = 0$ to find the intersection points A and B in Figure 1. Solve the quadratic equation below:

$$-v_i \mathcal{H} {e_a}^2 + v_i e_a - c_i + r_i = 0$$

$$\therefore\ e_a = \frac{v_i \pm \sqrt{{v_i}^2 + 4v_i(r_i - c_i)\mathcal{H}}}{2v_i\mathcal{H}}$$

To ensure that there are solutions for e_a, the following inequality must hold:

$${v_i}^2 + 4v_i(r_i - c_i)\mathcal{H} \geq 0 \quad (12)$$

Since $v_i > 0$, (12) means the following must hold:

$$v_i \geq 4(c_i - r_i)\mathcal{H} \quad (13)$$

In order to make $\frac{\partial u_i''}{\partial e_i} > 0$ for all possible values of e_a within the range [0..1], the following inequalities must hold:

$$\frac{v_i + \sqrt{{v_i}^2 + 4v_i(r_i - c_i)\mathcal{H}}}{2v_i\mathcal{H}} \geq 1 \quad (14)$$

$$\frac{v_i - \sqrt{{v_i}^2 + 4v_i(r_i - c_i)\mathcal{H}}}{2v_i\mathcal{H}} \leq 0 \quad (15)$$

Simplifying (14), it can be seen that the following inequality needs to be satisfied:

$$r_i - c_i \geq v_i(\mathcal{H} - 1) \quad (16)$$

According to inequality (11) and the definition of $\alpha_{j,i}$ (i.e. $0 \leq \alpha_{j,i} < 1$), the following holds:

$$0 \leq \sum_{j:S-\{i\}} \alpha_{j,i} < 1$$

Since "$c_a > 0$" and "$v_{a,i} > 0$", according to the definition of $u_{a,i}$ in expression (10), the following holds:

$$0 < \frac{c_a}{v_{a,i}} < 1$$

$\because 0 \leq e_j^{max} \leq 1$

$\therefore\ 0 \leq 1 - e_j^{max} \leq 1$

$\because S = G \cup L, 0 \leq 1 - e_j^{max} \leq 1,\ 0 < \frac{c_a}{v_{a,i}} < 1, \sum_{j:S-\{i\}} \alpha_{j,i} < 1$

$$\therefore\ 0 < \left(\sum_{j\in L-\{i\}} \alpha_{j,i}\left(1-e_j^{max}\right) + \sum_{j\in G-\{i\}} \alpha_{j,i}\frac{c_a}{v_a}\right) < 1$$

$$\therefore\ 0 < \mathcal{H} < 1$$

$$\therefore\ \mathcal{H} - 1 < 0$$

Inequality (16) can be rewritten to

$$v_i \geq \frac{c_i - r_i}{1 - \mathcal{H}} \quad (17)$$

Simplifying (15), the following can be obtained:

$$4v_i(r_i - c_i)\mathcal{H} \geq 0 \quad (18)$$

Since $\mathcal{H} > 0$ and $v_i > 0$, to satisfy (18), the following inequality must hold.

$$r_i \geq c_i \quad (19)$$

In order to ensure that the parabola intersects with the horizontal axis, the three inequalities (13), (17) and (19) must all be satisfied. It can be seen that, if (19) is satisfied, $c_i - r_i \leq 0$ holds. Thus, as long as v_i is a positive value, (13) and (17) can be satisfied. This means that, as long as incentive r_i given by the customer can cover the cost of defence efforts, even if the service provider receives a low payment v_i, the service provider still does its utmost to protect its service.

Observation 8: When $e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}$, the service will use maximum defence effort if $r_i \geq c_i$. □

From observations 6 to 8, the following can be obtained:

Result 2: In the independent partnership game,

- If $e_i^{max} < \frac{v_{a,i}-c_a}{v_{a,i}}$, the customer must ensure that $r_i \geq c_i$ 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 customer must ensure that $b_i > c_i(\frac{v_{a,i}-c_a}{v_{a,i}})$ 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

Rass [16] treated the security provisioning problem as a 2-player zero-sum game. The players are the service provider and the attacker. Using an axiomatic approach, Rass found an optimal balance between service qualities and system performance. Based on this analysis, service providers can formulate their service level agreements with customers. 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. Thus, the terms in a SLA would be more acceptable to both the customer and the service providers.

Varian [15] classified the security of a networked system into three categories, and, analysed the security investment using a public goods game-theoretical framework. Varian used three games, i.e. best effort, weakest-link and total effort games, to discuss how users might contribute to the reliability of the system. Varian focused on two-player

games with heterogeneous effort costs and benefits from reliability. Grossklags et al. [6,2] generalises the work in [15]. Instead of being two-player games, the games in [6,2] are n-player games. They introduced two more complex "weakest-target" games to model a class of security issues not addressed in [15]. Khouzani et al. [8] studied the impact of a regulator on improving the security of the Internet. Their analysis is based on examining the effects that the economic measures used by a regulator can have on the behaviours of the Internet service providers. Mavronicolas et al. [12] investigated the defence of a distributed system by a group of interdependent defenders. They analysed how to optimise the number of attackers caught by a defender in a Nash equilibrium. Apart from the weakest-link game studied in [15], 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. They modelled the security choices problem as a two-stage game and identified the optimal security level for each entity. Fan et al. [3] used a stochastic game model to evaluate attack-defence process in cloud computing. They developed an algorithm for computing the Nash equilibrium of the attack-defence process. 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.

Game theory has been applied to various areas of service computing. Zheng et al. [20] modelled the SLA negotiation as a 2-player bargaining game. Li et al. [10] uses game theory to solve the QoS-aware service composition problem. Khosravifar et al. [9] studied the efficiency of the services that collaborate with each other. Different to the scheme proposed in this paper, none of these schemes addressed how to maximise the security in a service computing environment.

VI. CONCLUSIONS

This paper models the security of two classes of service computing applications as the tightly integrated partners and the independent partnership games. 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 equilibria of the games were analysed from the perspectives of the service providers and the adversary. From the analysis of the Nash equilibria, 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] Khosravifar B., Alishahi M., Bentahar J., and Thiran P. 2011. A Game Theoretic Approach for Analyzing the Efficiency of Web Services in Collaborative Networks. In Proceedings of the 2011 IEEE International Conference on Services Computing (SCC '11), 168-175.

[10] Li H., Zhu Q., and Ouyang Y. 2011. Non-cooperative Game Based QoS-Aware Web Services Composition Approach for Concurrent Tasks. In Proceedings of the 2011 IEEE International Conference on Web Services (ICWS '11), 444-451.

[11] 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

[12] 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.

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

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

[15] 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.

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

[17] 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

[18] Strang G. 1991. Calculus, Wellesley

[19] Watson J. 2013. Strategy: An Introduction to Game Theory, W. W. Norton & Company

[20] Zheng X., Martin P., Powley W., and Brohman K. 2010. Applying Bargaining Game Theory to Web Services Negotiation. In Proceedings of the 2010 IEEE International Conference on Services Computing (SCC '10).