Security by Insurance for Services

Fabio Martinelli
Istituto di Informatica e Telematica,
Consiglio Nazionale delle Ricerche
Pisa, Italy.
Email: fabio.martinelli@iit.cnr.it

Artsiom Yautsiukhin
Istituto di Informatica e Telematica,
Consiglio Nazionale delle Ricerche
Pisa, Italy.
Email: artsiom.yautsiukhin@iit.cnr.it

***Abstract*—It is hard to guarantee proper protection in the Service Oriented Architecture (SOA), when a client outsources a part of its business or sends private data to a services provider. Various solutions proposed so far mostly require evidences of proper protection (e.g., source code for verification or execution traces for monitoring), which are to be provided by the service provider itself, and thus are not fully trusted by the client.**

In this paper we describe both conceptually and formally an approach for guaranteeing proper protection of outsourced data or business using cyber insurance. We discuss several variants of applications of the approach depending on the degree of involvement of different parties. We provide mathematical evidences of benefits of the approach for both client and provider and show how the parameters for the interactions should be computed.

***Index Terms*—Cyber insurance, web services, cloud, security, risk transfer**

I. Introduction

Outsourcing a part of non-core IT business is already an ordinary practice, which helps to save resources, time and money. Such way of conducting business became even more convenient and profitable with emergence of Web Service and Cloud technologies. On the other hand, these technologies significantly decreased the ability of data holders to control and enforce access to their data. Now, cloud and web service providers are responsible for ensuring security of data storage, transmission and processing. In these settings data holders do not have power to affect security provisioning, but only to select the service provider with highest security announced. Such announcement can be done in a form of a Service Level Agreement (SLA), or a part of it [1].

The first problem with this approach is that SLA hardly can be exhaustive, to ensure the needs of all possible customers. Moreover, the service providers are reluctant to reveal details of the quality of protection provided, because this may threaten their security. Thus, currently SLAs contain (in most cases) only the information required for correct connection, i.e., data transmission, without revealing any further details about protection provided. Thus, the protection of data processing and storage is, usually, left for provider choice. Last but not least, there is a big problem with ensuring that specified SLAs are indeed implemented and correctly operated. These problems increase uncertainty of clients about possible risks and restrain the cloud market.

In this paper we provide a simple, yet profitable way to establish trust between the partners without revealing sensitive information. Our core idea is to transfer the responsibility for security accidents from a client, which does not have control over the executing environment any more, to a provider, which has full control. This transfer is achieved by the means of cyber insurance, which is provided by the service provider to its clients in exchange for a premium [2], [3], [4].

Cyber insurance market emerged a bit more than a decade ago [5] and grows rapidly. Betterley report in 2015 [6] predicted the gross premium of cyber insurance in US to be 2,75 billion in that year. The prediction for Europe in 2014 [7] was 150 millions and increase from 50 to 100 per cent each year. Not only does cyber insurance help to transfer risk and smooth the possible losses caused by security breaches for organisations, it is also believed to have a number of additional positive effects. First, cyber insurance may become an incentive for organisations to invest in protection [4], [8], [5], increasing both security level of the protected system and society in general. Also cyber insurance may serve as another generic metric to evaluate and compare the levels of security [9], [8], [22]. Moreover, cyber insurance may lead to advancements in IT security standards[10], [11].

Although cyber insurance is a desirable practice, several negative factors constrain faster development of the market, such as lack of statistical data and experience, information asymmetry (asymmetry in the information available to involved parties), correlated risks and interdependent security [9], [10], [4], [8]. In this paper, we discuss how some of these factors affect the proposed approach.

In short, we propose providers to insure clients against possible threats. Although, a potential implementation of the idea has been mentioned by some practitioners [11], [12], we are unaware about scientific articles providing a model and a formal background for it. Issuing of insurance policy may be performed by the provider itself or in cooperation with an insurance carrier. In our proposal, a client simply pays an insurance premium in addition to the usual service cost. In case of an incident, the client is covered by the provider (and with full insurance does not face any loss). In our approach, a client has to pay additional cost (premium), but this premium simply substitute the losses faced by the client otherwise. A crucial advantage of our approach is that the provider does not have to reveal (and prove) its security practices, but it is interested to keep the attack rate as low as possible to ensure a low price for a client.

A. Contribution

The main contribution of the article is the specification of the approach for provisioning of reliable security with insurance. We describe three models for application of our approach, starting with a simplistic model, suitable for simple client-provider interactions, and ending with an extended model, which allows custom splitting of responsibilities between parties. We show that our approach depends less on availability of genuine information required for operation of the approach, if we compare it with model-checking, security-by-contract, monitoring, etc. Moreover, economical basis makes the responsible entity interested in maintaining high security level (without the need for verification). Furthermore, the proposed approach is even more attractive to clients than the usual one from economic perspective. In the article we do not consider the problem of interdependent security in its full strength, but provide the first (to our knowledge) analysis of the interdependencies within the scope of one service provider.

The article is organised as follows. First, we describe our approach (represented as three models) and its advantages with respect to existing approaches (Section II). Then, we provide a formal theoretical background for analysis of economical impact for both client and provider (Section III). Section IV is devoted to the analysis of the interdependencies of security between clients of the same provider. Finally, we discuss some additional issues in Section V. We conclude the paper with related work (Section VI) and conclusion (Section VII).

II. Security by insurance. Overview

In this section we present our main idea about using cyber insurance to guarantee proper protection of the outsourced business.

A. Core idea

a) Simplistic model: In essence, we propose to a service provider to insure clients against possible security threats. The simplistic model is suitable for simple services with multitude of similar clients, like social networks, hosting services (e.g., Dropbox), etc.

In a very simple case, a client should simply apply for a service, pay its fee and insurance premium. That is it. No security related actions (e.g., property specification, security quality verification, provider monitoring, etc.) are required. In exchange for a premium the client gets full coverage of any losses occurred because of a security breach. Now, it is the responsibility of the provider to ensure proper security level. Moreover, *the provider is now interested to maintain this level*, since this is economically profitable for it. This eliminates the need to control the proper security level, a very hard task in a distributed environment.

In these simplified settings, the service provider estimates expected loss per accident occurrence and its probability depending on the security level provided. Estimation of these values are also considered as a hard task [9], [10]. On the other hand, a service provider has a great opportunity to collect enough statistics for similar hosted systems and derive the required data. In contrast to most of cases when security risk analysis of IT systems is applied, all these data are available to the provider, and the multiplicity of hosted systems should make the derived results significant from the statistical point of view. The provider may also express some conditions for insurance (e.g., maximal coverage limit, exceptions for covering certain threats, penalties for clients involved in self-compromising activities, etc.), but they can be expressed with a natural language, understandable for clients.

b) General model: A general approach is more customised for specific needs of clients. Moreover, clients may have extended capabilities in controlling their business (e.g., maintain their own database) and, thus, be responsible for a part of protection.

In this model, a client and a provider should first agree on the terms and conditions of the insurance: which threats are covered, what coverage limits are, whether insurance is full or partial (i.e., whether clients are responsible for a part of losses), etc. Then, a thorough evaluation of possible losses take place. Finally, the provider and client agree on the level of protection every party is responsible for.Finally, the service provider computes the required premium and charges the client for a usual service fee.

Both simplistic and general models are formally described in Sections III-A and III-B.

c) Extended model: Finally, we would like to consider an extended model, where a provider and an insurer are separated. This can be done from practical reasons. In this model the provider will focus only on provisioning its service, when the insurer will issue the insurance to the client. The insurer may cooperate with the provider, as some insurers do with security providers [13], [14]. In this case the model is similar to the general model, but the profit is split according to the provided businesses.

If an insurer and a provider do not cooperate, the model becomes similar to the usual insurance model and looses some important features. For example, such a non-cooperative model will not encourage the provider to maintain high security level (i.e., increase moral hazard) and will not allow a provider to propose a more competitive product.

B. Advantages of the approach

In the approach we propose, a client and a provider first agree on terms and conditions for service and insurance provisioning. Although, this step is similar to the agreement on an SLA, the main difference is the level of security requirements. The client should no longer specify low level functional requirements, but only the threats (consequences) it would like to be covered from. The provider checks that it can provide the coverage. This step requires a language for underwriting the policy and may require some procedure for negotiation of the terms and conditions suitable for both parties, similar to usual SLA negotiation (if negotiation is an option). Naturally, the simplistic approach is free from these complications, but is much less flexible.

The key advantage of the proposed model, is that there is no need to verify (and for the client to specify) that the provider implements high level of security. This level of security is bound to the premium (as this will be shown further in the formal model). Naturally, the level has to be high enough, to keep premium as low as possible, to attract customers. Moreover, the provider will have an incentive to maintain the same level of protection during the whole time of interaction (rather than stop providing sufficient maintenance after the verification phase), since it will have to reimburse much more to the client because of the raised amount of claims.

When a breach occurs, the provider will reimburse the losses to the client. The key point here is that neither provider should be able to hide the breach, nor the client should be able to cause it deliberately.

Regarding to a possible misbehaviour of the provider, there are several advantages of detecting threats occurrence instead of detecting provisioning of security features. First, threat occurrences are often difficult to hide, since they have immediate impact: service becomes unavailable, data are modified, ransom claims are sent, etc. The problem here is mostly with some confidentiality breaches, i.e., credit card fraud. Second, many accidents have not only contractual, but also legal implications (see for example California Bill [15] and EU data breach regulation proposal [16]). Thus, providers may be less interested in hiding a threat occurrence, since they will be seriously fined when the fact of the breach will be revealed. Naturally, monitoring of activities on the server is of help here as well as it is helpful for monitoring of security requirements in a usual SLA enforcement/monitoring approach. Note, that now there is no need to monitor the activities of the provider, but only an access to the data of the client. Thus, the client has more capabilities to detect the accident (by itself).

III. Formal model

A. Formal simplistic model

Next to many advantages of insurance as a guarantee of security, we are able also to prove that such schema is more attractive for clients.

Let $\boldsymbol{W}$ be a random variable which denotes the amount of wealth of an agent, when W^0 be the initial amount of wealth and a be the cost of the service[1]. Let $U(\boldsymbol{W})$ be a utility function which denotes the utility of wealth for an agent. As it is commonly assumed in the literature studying insurance [17], agents are considered to be risk averse, i.e., an agent prefers to have as less uncertainty as possible; and the expected utility function is a von Neumann-Morgenstern utility function, which is assumed to be twice deferential and concave: $U'(\boldsymbol{W}) > 0$ and $U''(\boldsymbol{W}) < 0$.

Let $\boldsymbol{L}$ be a random variable which denotes the amount of losses from an accident occurrence. Then, the wealth of an agent can be seen as $\boldsymbol{W}_1 = W^0 - a - \boldsymbol{L}$ and the expected utility after using Jensen's inequality is:

$$E[U(\boldsymbol{W}_1)] \leq U(E[\boldsymbol{W}]) = U(W^0 - a - E[\boldsymbol{L}]) \quad (1)$$

If the agent buys insurance it is repaid a portion of the loss, called indemnity $\boldsymbol{I}$ ($\boldsymbol{I} = f(\boldsymbol{L})$), when an accident occurs in exchange to a fixed premium P. The wealth of the agent can be seen as $\boldsymbol{W}_2 = W^0 - a - \boldsymbol{L} + \boldsymbol{I} - P$. Finally, consider the case the service provider/insurer does not get profit out of insurance and repays loss entirely ($\boldsymbol{I} = \boldsymbol{L}$) charging a fair premium ($P = E[\boldsymbol{L}]$). The expected utility is:

$$E[U(\boldsymbol{W}_2)] = E[U(W^0 - a - \boldsymbol{L} + \boldsymbol{I} - P)] = \\ E[U(W^0 - a - \boldsymbol{L} + \boldsymbol{L} - P)] = U(W^0 - a - E[\boldsymbol{L}]) \quad (2)$$

Now, if we compare Equations 1 and Equations 2 we will see that an agent always prefers to buy insurance:

$$E[U(\boldsymbol{W}_1)] \leq E[U(\boldsymbol{W}_2)] \quad (3)$$

This equation also means that the premium may be higher than the fair one and still be acceptable for the agent: $P = E[\boldsymbol{L}]|(1 + \lambda)$, where λ is a loading factor, which may include expenses of the insurer, safe capital, additional profit. Naturally, λ must be low enough to ensure that Equation 3 holds.

Now, we consider a provider and its profit. We assume that the provider is risk neutral, i.e. $U(\boldsymbol{W}) = \boldsymbol{W}$. The provider implements security controls to keep the accident probability low. Let x be the level of security investments.

Let W_p^0 be the initial wealth of the provider, then its wealth could be computed as $\boldsymbol{W}_p = W_p^0 + a - \boldsymbol{I} + P - x$. Then, after engaging into interaction with an agent its expected utility becomes:

$$E[U(\boldsymbol{W}_p)] = E[\boldsymbol{W}_p] = W_p^0 + a + \lambda E[\boldsymbol{I}] - x \quad (4)$$

At the same time, the average utility for the provider which does not insures clients is:

$$E[U(\boldsymbol{W}'_p)] = E[\boldsymbol{W}_p] = W_p^0 + a - x \quad (5)$$

Theorem 1. *A provider which provides insurance and does not maximises its profit is also able to improve security level and still have non-zero profit.*

Proof. We have already shown that a provider which adopts security by insurance approach is more attractive for the clients when the same parameters are applied (see Equation 3). Now, from Equations 4 and 5 we see, that with the same parameters the provider has a surplus $\lambda E[\boldsymbol{I}]$ a part of which it can use to increase security level, and leave a part as profit. □

We would also like to consider whether our provider is *willing* to use the surplus in its benefit to increase its security, while maximising its profit.

Without loss of generality, let $\boldsymbol{L} = L$ when a threat occurs and $\boldsymbol{L} = 0$ when it does not. Let also x be a security level enforced by the provider and $pr(x)$ be the function which returns the probability of an accident when x is enforced. We

[1] The cost of the service may also include the cost for installed protection. This cost changes the magnitude of client satisfaction and benefit of the provider, but does not change the considered relations.

do not know the exact form of this function, but can say, that it is also twice deferential and convex ($pr'(x) < 0$ and $pr''(x) \geq 0$). Then, the average loss can be computed as: $E[\boldsymbol{L}] = pr(x)L$.

Theorem 2. *The proposed model serves as an incentive for the profit-maximising provider to increase the level of protection, if the following relation holds:*

$$-\frac{1}{L} > -\frac{pr(x)U_1' + (1 - pr(x))U_0'}{U_0 - U_1} \tag{6}$$

where $U_1 = U(W^0 - x - L)$ and $U_0 = U(W^0 - x)$

Proof. First, we consider the best possible contract a provider without insurance can offer to the clients, and then find the maximal benefit a provider with insurance will get by offering its clients the contract at least as good as the one proposed by the former provider.

The best contract without insurance the provider is able to offer is when its benefit is zero and from Equation 5: $a^N = x^N$. Now we should maximise the average utility of the client:

$$pr(x^N)U(W^0 - a^N - L) + (1 - pr(x^N))U(W^0 - a^N) \tag{7}$$

After applying the first order condition (FOC) we have that:

$$pr'(x^N) = -\frac{pr(x^N)U_1' + (1 - pr(x^N))U_0'}{U_0 - U_1} \tag{8}$$

On the other hand, if this value results in some maximal utility of customer U^*, provoked by some wealth W^*, by Equation 3:

$$W^* = W^0 - a - pr(x^I)L(1 + \lambda). \tag{9}$$

Now, we can find a and the profit from Equation 4.

$$E[U(\boldsymbol{W}_p)] - W_p^0 = W^0 - W^* - pr(x^I)L - x^I \tag{10}$$

Then, the profit can be further maximised (with FOC) and the solution of the following equation:

$$\begin{aligned} -pr'(x^I)L - 1 &= 0 \\ pr'(x^I) &= -1/L \end{aligned} \tag{11}$$

For x^I to be higher than x^N we should have $pr'(x^I) > pr'(x^N)$, which could be found from Equation 11 and 8. □

The specified condition holds for concave U and not very small $pr'(x)$ [18], while for L much higher than W^0 the condition fails [14].

B. General formal model

Consider the case when a client is responsible for some security settings as well. A provider may apply reasonable security protection for the environment (e.g., firewalls, hardened operational system, timely vulnerability updates, etc.), when the client also has to ensure proper access to its data (enforce access control, manage keys, encrypt the data, etc.).

Let x be a security level enforced by a provider, when x' be the security level enforced by a client. Then, the accident probability function will transform to $pr(x, x')$, which is still twice deferential and convex in both variables ($\frac{\partial pr}{\partial x_i} < 0$ and $\frac{\partial^2 pr}{\partial x_i^2} \geq 0$), where $x_i \in \{x, x'\}$.

Then, the average utilities for a client and a provider be:

$$E[U^c(\boldsymbol{W}_3)] = U(W^0 - a - pr(x, x')L(1 + \lambda) - x') \tag{12}$$

$$E[U^p(\boldsymbol{W}_p)] = W_p^0 + a + pr(x, x')L\lambda - x \tag{13}$$

We again want to maximise the profit of the provider and be at least as well attractive for customers as the providers without insurance. Thus, Equation 12 is to be equal to some U^* and this utility is corresponds to W^*. After finding a out of Equation 12 we put it to Equation 13 and would like to find its maximum. For doing this we should apply FOC for x and x' and we get that:

$$\frac{\partial pr}{\partial x} = -\frac{1}{L} = \frac{\partial pr}{\partial x'} \tag{14}$$

Now, we should solve these two equations with two variables[2] Note, that in some cases no maximum exist for $x \geq 0$ and $x' \geq 0$ and border conditions should be checked.

Example 1. *Let $pr(x, x') = 1/(x + x' + 1)$ and $L = 100$, then using Equation 14 we are able to find that maximum of $E[U^p(\boldsymbol{W}_p)]$ is a line $x = \sqrt{L} - x' - 1$ and any such x and x' will satisfy the client and the provider.*

Finally, we see that when optimal investments are found and agreed, the provider has no intention to deviate from the agreed value (since this will reduce its profit). As for the client, then it may benefit from a dishonest behaviour, but the provider has all capabilities to monitor the actions of the client.

IV. Model with several clients

It is common for a provider to run several systems of its clients on the same platform. In this situation, not only does the direct possibility to attack a client system exist, but also an indirect one, i.e., when an attacker compromises the platform first and then targets client system(s). In this work, we assume that the probability to compromise one client system through another one is negligible, and we leave this more complex scenario for the future work. In other words, the full probability to attack a client system is:

$$pr(x, x_i') = 1 - (1 - \pi(x, x_i'))(1 - m(x)q(x_i')) \tag{15}$$

where $\pi(x_i, x_i')$ is the probability of direct attack on a client system i, $m(x)$ is the probability of compromising the platform, and $q(x_i')$ is the probability to attack the client system i, when the platform is compromised[3]. For simplicity of the following discussion we assume all clients to be equal ($x_i' = x'$), and $pr(x, x_i') = pr$, $\pi(x, x_i') = \pi$, $q(x_i') = q$, and $m(x) = m$ for brevity.

[2] We also should check the necessary condition for checking the maximum.

[3] In this paper, similar to other articles on cyber security, we consider only one possible occurrence per system per the considered period. A more complete and precise model (e.g., modelling accident arrivals as Poisson process) should take into account the possibility for several hits in a considered period.

Moreover, it is not enough to re-define the formula for computation of the probability of accident occurrence, since when one platform hosts several systems, the probabilities of indirect attack are correlated, because after compromising the platform an attacker is able to compromise several systems without the need to compromise the platform again (e.g., a worm). In other words, the estimation of potential losses for the provider (and estimation of premiums, as a consequence) should take into account all clients at the same time, instead of estimating every client separately. We provide the mathematical support of this statement below.

First, consider the formula for estimation of expected losses for the provider in case when every client is estimated separately. Let there be n client systems installed on one platform. Let also the indemnity for every system will be the same $I = L$. First, we remind that the probability to have k hits out of n possible attempts with probability pr can be determined with the binomial distribution:

$$B(pr, k, n) = \frac{n!}{k!(n-k)!} pr^k (1-pr)^{n-k} \tag{16}$$

Then, for calculation of possible damage D^{ind} we need to sum up the multiplications of the probabilities for k compromised systems by the cost to be re-paid $(k * L)$:

$$E[D^{ind}] = \sum_{k=0}^{n} kLB(pr, k, n) \tag{17}$$

When we move L out of the sum then we get a formula for expected number of hits, which is equal to npr. Thus, the expected damage is $E[D^{ind}] = nLpr$ and the portion of damage per one client is Lpr.

Now, consider all clients at the same time, when after compromising the platform an attacker is able to attack any number of systems with probability q. The expected damage is:

$$E[D^{dep}] = \sum_{k=0}^{n} kI\Bigg((1-m)B(\pi, k, n) + \tag{18}$$

$$m \sum_{l=0}^{k} B(\pi, l, n) B(q, k-l, n-l)\Bigg)$$

We see that the first part in brackets refers to the case when the platform is not compromised and only direct attacks count, when the second summand considers all possible variations for attackers to compromise l systems directly and $k - l$ systems indirectly (when $l = 0$, then all systems are compromised indirectly and when $l = k$, then although the platform had been compromised, but no successful indirect attacks had place).

Theorem 3. *The expected damage for independent and dependent cases are equal*[4]*:*

$$E[D^{dep}] = nL(\pi + mq - mq\pi) = E[D^{ind}] \tag{19}$$

It is important to note, that although the expected values are the same for dependent and independent cases, we cannot use the simple formula for independent case (instead of Equation 19). It is possible to see that concrete probability for having a certain amount of hits are *different* for two cases (e.g., one can see this checking the probabilities for 0 hits, i.e., the probability of no attack).

The result has two important implications. First, we see that the portion of the expected damage per client is independent from the amount of clients and the premium can be easily computed as

$$P = (1 + \lambda)L(\pi + mq - mq\pi). \tag{20}$$

In other words, the provider may consider every client separately and without worrying about the changing number of clients per platform in the future, when for a client no additional information is required to correctly estimate possible risks and benefits (i.e., no additional information asymmetry affects the approach). Second, the expectations of a client (who knows only about its system and the platform, and, thus, can compute the damage only with the formula for the independent case) and provider (who considers the total damage for the platform and the plethora of clients on it) coincide, i.e., they independently estimate damage in the same way.

V. Discussion

Here we would like to discuss some issues related to application of the approach.

A. Scope

Although the proposed approach has a number of advantages, it cannot entirely substitute the existing methods. In a number of situations the procedure for maintaining the required level of security is as important as the final outcome. Examples of such situations are the need of an organisation to comply with a certain sets of rules (e.g., standard), or involvement in a more complex process where a failure of a security rule will not have an immediate effect, but will impact the process at the later stage (e.g., separation of duty). In these cases, insurance cannot substitute usual specification of functional security requirements and their enforcement.

B. Interdependent security

In this work we did not discuss the issue of interdependent security thoroughly. Interdependent security has to be taken into consideration in an interconnected environment, where the security level of one node depends on the security level of another one. As it was shown in several papers [19], [20], [14] such interdependence may affect security of a node positively (e.g., a worm attacking the system after compromising a trusted node) and negatively (e.g., an attacker decides to attack the system because its security is lower than security of other systems). The problem is that interdependent security impedes the entities to invest in security optimally.

In our work, we considered only the interdependence between clients and the platform in Section III-B. We assumed that when a client system is compromised it still cannot affect the platform and other client systems running on it. For

[4] The proof is in the Appendix.

example, such situation can be accepted if a provider gives a separate virtual machine to every client. In the situation, when such assumptions are not valid, the formal model must be adjusted. The effect on client's investments in such case can be modelled with a star-shaped topology model (e.g., [21]).

C. Lack of data

Lack of data is a big problem in adoption of cyber insurance. The data are needed to quantify correctly several parameters required for the premium computation. Insurance, in general, solves this problem by collecting huge amount of statistical evidence and deriving the required dependencies. An alternative way to assign values to parameters is to discuss possible threat scenarios with experts [22].

In this respect, our approach has several advantages in comparison with cyber insurance in general. In many cases, a service serves a large amount of similar client systems. The data about accidents are available to the service provider (which is not the case for a general insurer). This helps a service provider to collect the required statistics for an accurate computation of insurance parameters. Second, a provider, usually, has more security knowledge than a client and has more capability to hire security experts to evaluate the system.

D. Incentive for protection

As it has been shown in Section III our approach does not always result in improving the protection when provider is greedy. On the other hand, the provider which insures its clients has the space for a manoeuvre and the capability to provide higher protection. A proper regulation (e.g., by means of fine and rebate [13]) may help to achieve the desired effect.

E. Complex services

Services often play a role of just one activity in a more complex service. Moreover, a service provider may also be a client of another service which provides the infrastructure and so on. Thus, the decision to accept the proposed insurance policy or not, may depend on the effect on the overall structure. This important issue of services has not been tackled in the paper but we are going to investigate the matter in the future work.

VI. Related Work

Several approaches were proposed to guarantee that outsourced business would be properly secured.

A. SLAs

Most approaches have the core idea to specify the agreed security properties to be implemented in a contract, usually, referred as an SLA. In general, an SLA contains any kind of properties agreed between a client and a provider, but in this paper we consider only a security part of SLA. The properties in the SLA are specified with a proper language, which can facilitate document processing, e.g., for machine readable and expressive specification, contract negotiation, properties matching, etc. There are many candidates for formalisation of security requirements, such as XACML [23], ConSpec[24], etc. In our approach, there is a need to specify terms and conditions for cyber insurance, where these results can be applied.

Several techniques for analysis of compliance of specification of the contract and desirable security properties have been proposed [25]. The main challenge for such techniques is to cope with high complexity which grows with the expressiveness of the language and the size of the specification. These techniques can be re-used in our approach to match the terms and conditions of desired and provided insurance coverage.

B. Model-checking

Model-checking techniques (e.g., [26]) are useful for verification that the specified security properties are actually implemented. For this purpose the techniques take the proof, which is linked to the implementation code, follow its steps, and if the steps do not violate the considered properties, validate the conclusion. Although the technique is powerful, it heavily depends on the proof, which must be genuine, complete and correct with respect to the implemented code. These qualities are very hard to ensure in the cloud environment. As we have shown in the paper, adopting our cyber insurance-based approach makes the provider economically interested in providing an appropriate level of protection and facilitates verification of clients' actions.

C. Monitoring/Enforcement

The run-time monitor/enforcement techniques follow the execution of the service step by step and check that the executed operations do not violate defined policies. Enforcement techniques [27] intervene into the course of the execution and prevent the violation from happening. Monitoring techniques [28] only create notifications about occurred events, which can be further analysed. Similar to the model-checking techniques, run-time monitors/enforcers require access to the genuine, correct and precise information, i.e., executed operations, originated from the service. In our approach monitoring techniques can be used in two cases. First, to ensure a provider that an insured indeed made the agreed investments; but since it is the provider who owns the system this information for monitoring is easily obtained. Second, some techniques can be used to assure detection of all occurred accidents.

D. Security-by-Contract

Security-by-Contract [29] is a paradigm that has been created for security assurance in a mobile environment, and then has been applied to Service Oriented Architecture [30], [31]. In essence, this paradigm is a holistic combination of the techniques mentioned above in a unique approach. In general, our approach is easier to implement than the security-by-contract one since it does not require such deep security knowledge from non-experts, i.e., clients, and guarantees supports even if all security precautions fail. Similar to security-by-contract our insurance-based approach may depend on some of the mentioning techniques. On the other hand, as it has been shown above, this dependency is much more relaxed (e.g., a more focused and less expressive language is required, easiness to get proofs of event occurrence, etc.).

E. Cyber insurance

Cyber insurance has got a lot of attention in the scientific community [3], [17], [32]. The researchers studied various challenges in application of insurance to the cyber world. Some of them studied a simple model of interaction between one client and an insurer [33], but a more thorough attention is devoted to a complex model with several clients and their interdependent security [14], [34], [13], [35], [36]. An important question the researchers tried to answer is whether insurance is an incentive for self-protection when security is interdependent and information asymmetry has place.

In our paper, we considered effect of other client systems negligible assuming that the platform cannot be compromised through a client system (and consequently propagate the attack to other client systems). Indeed, with such interdependency, in the general model, a client would have had less incentive to invest in security if there had been a possibility of cyber risk insurance. As for information asymmetry, we have devoted special attention to this problem and have shown that our approach is not significantly impacted by it; at the same time, the provider is not forced to reveal its internal security.

R. Pal et al [37] proposed a model, when a security vendor sells a portion of security and insurance. The authors used a specific utility function for their study and considered a model, where the insurance carrier is monopolistic and insurance is mandatory. Although, this model also can be used in a service oriented architecture, our approach is more generic (not bound to the selected utility function). Not only have we provided the way to analyse the system, but we have shown that the approach itself is more convenient and profitable in the SOA environment, than other existing approaches and techniques.

VII. Conclusion

In the paper, we have discussed in details applicability of cyber insurance for guaranteeing proper security protection in SOA. The approach has the following advantages with respect to existing techniques. It is simple since it requires much less specific security knowledge from the client, who can focus on the core business part instead. The approach is easily applied in practice, since all participants are interested in behaving according to the agreement and most of the data, required for checks are available to the corresponding parties. In contrast, other approaches require information which may be considered by the owner as private (e.g., source code, security settings, or execution logs). Not only does the considered approach ensures proper protection, but it also ensures economical benefits for all parties. The computation of premium for clients is straightforward. Moreover, we have found an interesting case: the premium computed by a provider with several clients is similar to the premium computed for a single client (even if several clients may be affected after a breach of the platform). This finding aligns the views of a client (who is aware about the platform only) and the provider (who knows about the correlated risk).

The current paper is only a general description of application of cyber insurance to SOA. There are a number of issues, which should be tackled to fully adapt the cyber insurance to the service environment. In particular, in the future, we are going to investigate the effect of hierarchical and procedural dependencies on the provided insurance. Another direction of research we are planning is connected with the dynamic nature of the service environment and its effect on insurance.

References

[1] L. Krautsevich, A. Lazouski, F. Martinelli, and A. Yautsiukhin, “Risk-based usage control for service oriented architecture,” in *Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing*. IEEE Computer Society Press, 2010.

[2] T. Moore, “The economics of cybersecurity: Principles and policy options,” *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3–4, pp. 103 – 117, 2010.

[3] R. Anderson, R. Böhme, R. Claytin, and T. Moore, “Security economics and the internal market,”, January 2008.

[4] C. Toregas and N. Zahn, “Insurance for cyber attacks: The issue of setting premiums in context,” The George Washington University, Tech. Rep. GW-CSPRI-2014-1, January 2014.

[5] R. P. Majuca, W. Yurcik, and J. P. Kesan, “The evolution of cyberinsurance,” *The Computing Research Repository*, vol. abs/cs/0601020, 2006.

[6] R. S. Betterley, “Cyber/privacy insurance market syurvey - 2015,” available via http://betterley.com/samples/cpims15_nt.pdf, June 2015.

[7] S. Jones, “Lloyds CEO Sees Cyber Insurance to Surge After Attacks,” Bloomberg Business, October 2014, available via http://goo.gl/kN58LV on 13/07/2015.

[8] National Protection and Programs Directorate. Department of Homeland Security, “Cyber insurance roundtable readout report. health care and cyber risk management. cost/benefit apapproach.” available via http://goo.gl/8hzT80 on 02/12/2014, February 2014.

[9] R. Anderson and T. Moore, “The economics of information security: A survey and open questions,” *Science*, vol. 314, pp. 610–613, 2006.

[10] ENISA, “Incentives and barriers of the cyber insurance market in Europe,” available via goo.gl/BtNyj4 on 12/12/2014, June 2012.

[11] S. Mansfield-Devine, “Security guarantees: building credibility for security vendors,” *Network Security*, vol. 2016, no. 2, pp. 14–18, 2016.

[12] National Protection and Programs Directorate. Department of Homeland Security, “Cybersecurity insurance workshop readout report,” available via https://goo.gl/el8dki on 24/03/2015, November 2012.

[13] M. Lelarge and J. Bolot, “Economic incentives to increase security in the internet: The case for insurance,” in *Proceedings of the 28th IEEE International Conference on Computer Communications*, 2009.

[14] H. Ogut, N. Menon, and S. Raghunathan, “Cyber insurance and it security investment: Impact of interdependent risk,” in *Proceedings of the 4-th Workshop on the Economics of Information Security*, 2005.

[15] C. State, “Senate bill no. 1386 chapter 915,” available http://goo.gl/W8qhb8 on 13/07/2015.

[16] E. Parliament, “European parliament legislative resolution of 12 march 2014 on general data protection regulation,” October 2014.

[17] R. Böhme and G. Schwartz, “Modeling cyber-insurance: Towards a unifying framework,” in *Proceedings of the 9th Workshop on the Economics in Information Security*, 2010.

[18] I. Ehrlich and G. S. Becker, *Market Insurance, Self-Insurance, and Self-Protection*. Dordrecht: Springer Netherlands, 1992, pp. 164–189.

[19] X. Zhao, L. Xue, and A. B. Whinston, “Interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling,” in *Proceedings of the International Conference on Information Systems*, 2009.

[20] W. Shim, “An analysis of information security management strategies in the presence of interdependent security risk,” *Asia Pacific Journal of Information Systems*, vol. 22, no. 1, March 2012.

[21] J. Bolot and M. Lelarge, “A new perspective on internet security security using insurance,” INRIA, Tech. Rep. RR-6329, 2007.

[22] S. Kannry and D. White, *NAVIGATING THE DIGITAL AGE: The Definitive Cybersecurity Guide for Directors and Officers*. CAXTON business & Legal Inc., 2015, ch. Otimizing investment to minimize cyber exposure, pp. 283–287.

[23] OASIS, “eXtensible Access Control Markup Language (xacml) version 3.0,”, January 2013.

[24] I. Aktug and K. Naliuka, “Conspec: a formal language for policy specification,” *Science of Computer Programming*, vol. 74, no. 12, pp. 2 – 12, 2008, special Issue on Security and Trust.

[25] N. Bielova, M. D. Torre, N. Dragoni, and I. Siahaan, “Matching policies with security claims of mobile applications,” in *Proceedings of the Third International Conference on Availability, Reliability and Security*, March 2008, pp. 128–135.

[26] AVANTSSAR, available via http://www.avantssar.eu/ on 15/01/2016.

[27] M. Autili and M. Tivoli, “Distributed enforcement of service choreographies,” in *Proceedings 13th International Workshop on Foundations of Coordination Languages and Self-Adaptive Systems*, 2015, pp. 18–35.

[28] A. Bertolino, E. Marchetti, and A. Morichetta, “Adequate monitoring of service compositions,” in *Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering*, ser. ESEC/FSE 2013.

[29] N. Dragoni, F. Martinelli, F. Massacci, P. Mori, C. Shaefer, T. Walter, and E. Vetillard, *Security-by-Contract (SxC) for Software and Services of Mobile Systems*. MIT Press, 2009, ch. At your service - Service-Oriented Computing from an EU Perspective, pp. 429–455.

[30] N. Dragoni and F. Massacci, “Security-by-contract for web services,” in *Proceedings of the 2007 ACM workshop on Secure web services*, ser. SWS ’07. New York, NY, USA: ACM, 2007, pp. 90–98.

[31] G. Costa, R. Mandati, F. Martinelli, I. Matteucci, and A. Yautsiukhin, *Handbook of Research on Architectural Trends in Service-Driven Computing*. IGI Global, 2014, ch. Mitigating Security Risks in Web Service Invocations: Contract-Based Approaches, pp. 537–552.

[32] A. Marotta, F. Martinelli, S. Nanni, and A. Yautsiukhin, “A survey on cyber-insurance,” Istituto di Informatica e Telematica. Consiglio Nazionale delle Ricerche, IIT TR-17/2015, 2015.

[33] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao, “A model to analyze the unfulfilled promise of cyber insurance: The impact of secondary loss.” *Working Paper*, 2010.

[34] Z. Yang and J. C. S. Lui, “Security adoption and influence of cyber-insurance markets in heterogeneous networks,” *Performance Evaluation*, vol. 74, pp. 1–17, Apr. 2014.

[35] N. Shetty, G. Schwartz, and J. Walrand, “Can competitive insurers improve network security?” in *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing*, ser. LNCS, Springer, 2010, vol. 6101, pp. 308–322.

[36] R. Pal, L. Golubchik, K. Psounis, and P. Hui, “Will cyber-insurance improve network security? a market analysis,” in *Proceedings of the 2014 INFOCOM*. IEEE, 2014, pp. 235–243.

[37] R. Pal, L. Golubchik, K. Psounis, and P. Hui, “On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer,” in *Proceedings of the 12th IFIP Networking Conference*, 2013.

VIII. Appendix

Here we prove that

$$E[D^{dep}] = \sum_{k=0}^{n} kL\Bigg((1-m)B(\pi,k,n)+ \\ m\sum_{l=0}^{k} B(\pi,l,n)B(q,k-l,n-l)\Bigg) = nL(\pi+mq-mq\pi)$$

First, we open all binomial formulas:

$$E[D^{dep}] = L(1-m)\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\pi^k(1-\pi)^{n-k} + \\ mL\sum_{k=0}^{n} k\sum_{l=0}^{k}\left(\frac{n!}{l!(n-l)!}\pi^l(1-\pi)^{n-l}\times \\ \frac{(n-l)!}{(k-l)!(n-l-k+l)!}q^{k-l}(1-q)^{n-k}\right)$$

We see that the sum in the first summand is the expected value of the binominal distribution and is equal to $(1-m)nL\pi$. We also multiply and divide the second summund after the second sum by $k!$ and rewrite it.

$$E[D^{dep}] = (1-m)nL\pi + \\ mL\sum_{k=0}^{n}\left(k\frac{n!}{k!(n-k)!}(1-q)^{n-k}(1-\pi)^n\times \\ \sum_{l=0}^{k}\frac{k!}{l!(k-l)!}q^{k-l}(\frac{\pi}{1-\pi})^l\right)$$

The second sum in the second summand is the expanded version of $(\frac{\pi}{1-\pi}+q)^k$. Then, with a bit of rewriting we get:

$$E[D^{dep}] = (1-m)nL\pi + \\ mL\left[\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\left(\frac{\pi}{1-\pi}+q\right)^k(1-q)^{n-k}\right](1-\pi)^n$$

Consider the following element of the formula separately:

$$\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\left(\frac{\pi}{1-\pi}+q\right)^k(1-q)^{n-k} = \\ n\left(\frac{\pi}{1-\pi}+q\right)\sum_{k=0}^{n}\left[k\frac{(n-1)!}{k!(n-k)!}\times \\ \left(\frac{\pi}{1-\pi}+q\right)^{k-1}(1-q)^{(n-1)-(k-1)}\right] = \\ n\left(\frac{\pi}{1-\pi}+q\right)\sum_{k=1}^{n}\left[\frac{(n-1)!}{(k-1)!((n-1)-(k-1))!}\times \\ \left(\frac{\pi}{1-\pi}+q\right)^{k-1}(1-q)^{(n-1)-(k-1)}\right]$$

Substitute $k-1$ with t and $n-1$ with y we get:

$$\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\left(\frac{\pi}{1-\pi}+q\right)^k(1-q)^{n-k} = \\ n\left(\frac{\pi}{1-\pi}+q\right)\sum_{t=0}^{y}\frac{y!}{t!(y-t)!}\left(\frac{\pi}{1-\pi}+q\right)^t(1-q)^{y-t} = \\ n\left(\frac{\pi}{1-\pi}+q\right)\left(\frac{\pi}{1-\pi}+q+1-q\right)^{n-1} = n\frac{\pi+q-\pi q}{(1-\pi)^n}$$

Now,

$$E[D^{dep}] = (1-m)nL\pi + mLn\frac{\pi+q-\pi q}{(1-\pi)^n}(1-\pi)^n = \\ nL(\pi-\pi m+\pi m+mq-\pi qm) = nL(\pi+mq-\pi qm)$$