Security by insurance for services*

Fabio Martinelli and Artsiom Yautsiukhin

Istituto di Informatica e Telematica,
Consiglio Nazionale delle Ricerche, Pisa, Italy.

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 amount 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.

1 Introduction

Outsourcing a part of non-core IT business is already an ordinary practices, 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 the 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 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.

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 security 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 the specified SLAs are indeed

* This work was partially supported by projects H2020-MSCA-ITN-2015-NeCS 675320 and the PRIN Security Horizons project.

implemented and correctly operated. These problems increase uncertainty of clients about possible risks and restrain the cloud market, as a result.

In this paper we provide a simply, 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 to a premium.

Cyber insurance market emerged a bit more than a decade ago [25, 14, 17] and grows rapidly. Betterley report in 2015 [5] predicted the gross premium of cyber insurance in US to be 2,75 billion in that year. The prediction for Europe in 2014 [13] 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 also believed to have a number of additional positive effects. First, cyber insurance may become an incentive for organisations to invest in protection [30, 19, 17], increasing both security level of the protected system and society in general. Moreover, cyber insurance may lead to advancements in IT security standards.

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. In this paper, we discuss how some of these factors effect the proposed approach.

In short, we propose the provider to insure the client against possible threats. Issuing of insurance policy may be performed by the client 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. On the other hand, 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 the lowest price for a client.

1.1 Contribution

The main contribution of the article is the description 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 the 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 needs for checking this). Furthermore,

the proposed approach is even more attractive to clients than the usual one from economic perspective, and/or leads to higher security.

The article is organised as follows. First, we informally describe our approach (represented as three models) and its advantages with respect to existing approaches (Section 2). Then, we provide the formal background for analysis of economical impact for both client and provider (Section 3). Finally, we discuss some additional issues in Section 5. We conclude the paper with related work (Section 6) and conclusion (Section 7).

2 Security by insurance. Overview

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

2.1 Core idea

Simplistic model. In essence, we propose to the service provider to insure the client 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 the very simply case of our approach, 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. 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.

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 security provisioning.

In this model, the client and the 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. As we show in Section 3.2 proper settings will guarantee that every part is interested in maintaining its security level as specified. Finally, the service provider computes the required premium and charges the client for a usual service fee. Naturally, the process can be simplified with a number of insurance contracts pre-established by the provider with the parameters to be customised for a specific client.

Both models are formally described in Sections 3.1 and 3.2.

Extended model. Finally, we would like to consider an extended model, where the provider and insurer are separated. This can be done from practical reasons. In this model the provider will focus only on provisioning its service, when insurer will issue the insurance to the client. In the model, the insurer may cooperate with the provider, as some insurers do with security providers [16, 21]. 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, when an insurer asks for insurance, but with a combined insured responsible for self-protection: service client and service provider. Thus, it looses most features we focus on and, therefore, we do not considered it in this paper in details.

2.2 Advantages of the approach

In the approach we propose, the client and the 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 the provider has to implement, but only the threats (consequences) it would like to be covered from. The provider checks that it can provide a coverage for the required threats. 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 client should be able to deliberately cause the it.

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 [29] and EU data breach regulation proposal [24, 12]). 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 access to the data of the client. Thus, the client has more capabilities to detect the accident (by itself). Also monitoring by a third party (if applied) is simplified, since it has to monitor usual threats, rather customary security requirements.

3 Formal model

3.1 Formal model for simplistic approach

Next to many advantages of the insurance as the 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. Let also $U(\boldsymbol{W})$ be a utility function which denotes the utility of wealth for an agent. As it is commonly assumed in the literature studying insurance, agents are considered to be risk averse, i.e., an agent prefers to have as less risk as possible; and the expected utility function is a von Neumann-Morgenstern utility of wealth 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 that for a concave utility function is:

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

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:

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

Now, if we compare Equations 1 and Equations 2 we will see that an agent 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 a 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 can consider 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 security level and $C(x)$ be the cost of this level. $C(x)$ is a twice deferential function which is assumed to be strictly convex: $C'(x) > 0$ and $C''(x) > 0$. We may see that the effectiveness of investments in protection decreases with the increase of the protection level x.

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:

$$E[U(\boldsymbol{W}_p)] = E[\boldsymbol{W}_p] = W_p^0 + a - E[\boldsymbol{I}] + E[\boldsymbol{I}](1 + \lambda) - C(x) \quad (4)$$

We have already shown that a provider which adopts security by insurance approach has a competitive advantage against those providers, which do not provide insurance. Now, we consider a competitive environment with several providers, covering losses of a client. Assume for simplicity, that λ is simply additional profit for the insurer and that Equation 3 holds. Let γ be the minimal profit a provider wants to have per case, i.e., no competitors will make a more profitable proposal if this will result in their profit to be lower than γ. Naturally, in this case we have:

$$\begin{aligned} \textit{with insurance} : &\gamma = E[\boldsymbol{W}_p - W_p^0] = a + E[\boldsymbol{I}]\lambda - C(x) \\ \textit{without insurance} : &\gamma = E[\boldsymbol{W}_p - W_p^0] = a' - C(x') \end{aligned} \quad (5)$$

Since $E[\boldsymbol{I}]\lambda$ is a positive value, then in a non-fully competitive market the service provider is able either: 1) reduce the price of its service or 2) spend more on security. Both possibilities are desirable by the clients[1].

In other words, we see that the proposed approach is not only convenient for applications, but is also more profitable.

3.2 Dual model

In some scenarios, a client is responsible for some security settings as well, next to the controls installed by the provider. The provider may provide reasonable security protection (e.g., firewalls, hardened operational system, timely vulnerability updates, etc.) for access to the environment under the control of the client, which also has to ensure proper security (enforce access control, manage keys, encrypt the data, etc.).

Let x be a security level enforced by the provider, when x' be the security level enforced by the client. Let then $pr(x, x')$ be the function which returns the probability of an accident when x and x' are enforced. We do not know the exact form of this function, but can say, that it is also 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 client and provider be:

$$E[U^c(\boldsymbol{W}_p)] = pr(x,x')U(W^0 - a - L + I - P - C(x')) + \tag{6}$$

$$(1 - pr(x,x'))U(W^0 - a - P - C(x')) \tag{7}$$

$$E[U^p(\boldsymbol{W}_p)] = W_p^0 + a + P - pr(x,x')I - C(x) \tag{8}$$

We can show that the optimal investment to security is the solution of the following equation:

$$\frac{\partial pr}{\partial x'} = -\frac{1}{L(1+\lambda)} \tag{9}$$

and the optimal indemnity is:

$$I = L - \frac{\lambda}{r(1+\lambda)(1-pr(x,x'))} \tag{10}$$

where r is a constant greater than 0 and $r = -\frac{U''}{U'}$. The proof is similar to [21].

As for x then we see that having high level of protection is not profitable for provider (see the proof), but it is bound by the market to keep price (premium in particular) as low as possible. On the other hand, it is desirable to have $pr(x, x')$ lower than Equation 9 for the assigned x, since in this case also the client will be interested in investing in protection.

[1] Here we assume that payment cannot be increased, because this will discourage customers.

Dealing with Information Asymmetry With the dual model both client and provider may hide the information about the actual security level.

On the one hand, when we consider client providing incorrect information about its protection level, we have a usual problem for insurance, which has already been studied in the literature [16, 4, 15, 6]. Deducible and partial insurance may help to set up the contract profitable for clients with a specific level of security (and limiting, or eliminating, the amount of clients providing incorrect information). On the other hand, a service provider has much wider capabilities to verify the declared level of protection (e.g., though monitoring installed on its service). Moreover, the portion of security the client is responsible for is often much lower, than the portion of the provider.

For a service provider, it is simply not profitable to claim that its security level is higher than the real one. Consider two situations: a) when the provider honestly declares the provided level of protection and b) when the provider with security level x declares level $\bar{x}$, which is higher ($\bar{x} > x$ and $pr(\bar{x}, x') < pr(x, x')$). Then, Equation 14 can be rewritten for both cases:

$$E[U_1^p(\boldsymbol{W}_p)] = W_p^0 + a + (1+\lambda)pr(x,x')I - pr(x,x')I - C(x) = \tag{11}$$

$$W_p^0 + a + \lambda pr(x,x')I - C(x) \tag{12}$$

$$E[U_2^p(\boldsymbol{W}_p)] = W_p^0 + a + (1+\lambda)pr(\bar{x},x')I - pr(x,x')I - C(x) = \tag{13}$$

$$W_p^0 + a + \lambda pr(\bar{x},x')I + (pr(\bar{x},x') - pr(x,x'))I - C(x) \tag{14}$$

Since $pr(\bar{x}, x') < pr(x, x')$, then $\lambda pr(x, x')I > \lambda pr(\bar{x}, x')I$ and $(pr(\bar{x}, x') - pr(x, x'))I < 0$. Thus, $E[U_1^p(\boldsymbol{W}_p)] > E[U_2^p(\boldsymbol{W}_p)]$ and with honest behaviour provider gets more profit than in case when it is dishonest.

4 Model with several clients

It is often when a provider provides a platform which is used to run several systems of clients. In this situation, there is not only the direct possibility to attack a client system, but also an indirect one, i.e., when an attacker compromises the platform first and then targets the client system(s)[2]. In other words, the full probability to attack a client system is:

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

where $\pi(x_i, x_i')$ is the probability of direct attack on client system i, $m(x)$ is the probability of compromising the platform, and $q(sl_i')$ is the probability to attack the client system i, when the platform is compromised[3]. For simplicity of the

[2] In this work, we assume that the probability to compromise one client system through another one is negligible, though our model may be extended with this possibility in mind.

[3] In this paper, seminar to other articles on cyber security, we consider only one possible occurrence per system per the considered period. A more complete and

following discussion we assume all clients to be equal ($x'_i = x'$), and $\pi(x, x'_i) = \pi$, $q(sl'_i) = q$, and $m(x) = m$ for brevity.

Moreover, it is not enough simple 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, since 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. 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 probability for k compromised systems by the cost to be re-paid $(k * I)$:

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

When we move I out of the sum then we get a formula for expected number of hits, which is equal to $n\pi$. Thus, the expected damage is $E[I^{ind}] = nI\pi$ and the portion of damage per one client is usual $I\pi$.

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

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

We see that the first part in brackets refers to the case when 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 is compromised, but no successful indirect attacks had place).

---

precise model (e.g., modelling accident arrivals as Poisson process) should take into account the possibility for several hits in a considered period.

The solution for Equation 18 is[4] $E[I^{dep}] = nI(\pi+mq)$. We see that $E[I^{dep}] = nI(\pi+mq-mq\pi) = E[I^{ind}]$. 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 18). It is possible to see that concrete probability for having a certain amount of hits *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

$$P = (1 + \lambda)I(\pi + mq - mq\pi). \tag{19}$$

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.

Now, the provider is able to establish the premium and compute its profit with Equation 14. Note, that $C(x)$ in the formula may now refer to the sum of costs of security for the overall platform and security for the a specific client's system. The first cost should be shared by all clients (i.e., divided by the number of clients). In other words, the provider which has more clients will get higher profit than the one with fewer. And since Equation 19 does not depend on the amount of hosted systems, then the providers should be eager to fill the capacity of their platforms with as many systems as possible.

5 Discussion

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

Scope. Although the proposed approach has a number of advantages, it cannot entirely substitute the existing methods. In a number of situation 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 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. Furthermore, also insurance of clients by providers may benefit from the existing approaches as we show in Section 6.

[4] The proof is in Appendix

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 [32, 28, 21] 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 3.2. We assumed that when a client system is compromised it still cannot affect the platform and other client systems running on it. For 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., [7]).

Lack of data is a problem in adoption of cyber insurance. The data are needed to quantify correctly several parameters required for the premium computation. In particular, the amount of possible damage and the dependency of the probability of an accident on the security level are of particular problem. Insurance in general solves this problem by collecting huge amount of statistical evidence and deriving the required dependencies. This is still not the case for cyber insurance, where such data are not available for insurers because of their sensitivity.

On the other hand, our approach has several advantages with respect to cyber insurance in general. In many cases, a service is provided to a large amount of similar clients. The data about accidents are available to the service provider (which is not the case for general insurer). This helps a service provider to collect the required statistics for accurate computation of insurance parameters.

Complex services. Services are often play a role of just one activity in a more complex service. Moreover, 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.

6 Related Work

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

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 client and provider, but in

this paper we consider only 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 [20], Event Calculus [26], PROTUNE [8], ConSpec[1]. In our approach, there is a need to specify terms and conditions for cyber insurance, where these results can be applied.

Contract Matching Several techniques for static analysis of compliance of specification of the contract and desirable security properties have been proposed []. 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. Some authors also proposed to conduct the matching taking into account possible consequences of properties mismatch (i.e., IT security risk). This techniques can be re-used in our approach to match the terms and conditions of desired and provided insurance coverage.

Model-checking Model-checking techniques (e.g., [3]) 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 as a guarantee for cyber protection, in the simplistic case, makes the party responsible for protection (i.e., the provider) interested in providing appropriate security. On the other hand, in the general model, when a client is also responsible for keeping security at a certain level, such techniques can help to guarantee that the level is indeed achieved. As we have shown, in the later case, the provider running the systems has much more capabilities for performing these tests.

Monitoring/Enforcement The run-time monitor/enforcement techniques follow the execution of the service step by step and check that the executed operation do not violate defined policies. Enforcement techniques [**?**] intervene into the course of the execution and prevent the violation from happening. Monitoring techniques [**?**] 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. Our approach does not require such information in a simplistic case, and significantly simplifies acquisition of this information in the general case.

Security-by-Contract Security-by-Contract [10] is an paradigm that has been created for security assurance in a mobile environment, and then has been applied to Service Oriented Architecture [11, 9]. 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, e.i., 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 and execution results, etc.).

Cyber insurance Cyber insurance has got a lot of attention in the scientific community [2, 6, 18]. The researchers studied various challenges in application of insurance to the cyber world. Some of them studies a simple model of interaction between one client and an insurer [4], but a more thorough attention is devoted to a complex model with several clients and their interdependent security [21, 31, 16, 27, 23]. One of the most important questions the researchers tried to answer: how to make insurance an incentive for self-protection in situation 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). Thus, we considered interdependency between the platform an the client system only. We did not show the effect of such interdependency in the paper since there is no difference with respect to a model with two clients (see e.g., [21]). Indeed, in the general model, client would have had less incentive to invest in security if there had been a possibility of outsourcing without positive externalities. In scope of SOA we see no such alternative, unless the probability to compromise a platform is considered close to 0, which is currently unrealistic. As for information asymmetry, we have devote a special attention to this problem and have shown that our approach has a lot of means to reduce it significantly (or even eliminate it at all in the simplistic model).

R. Pal et al [22] 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.

7 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 the provider with several clients is similar as the premium computed for one client (even if several clients may be affected after the 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 the 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. I. Aktug and K. Naliuka. Conspec: a formal language for policy specification. *Science of Computer Programming*, 74(12):2 – 12, 2008. Special Issue on Security and Trust.
2. R. Anderson, R. Böhme, R. Claytin, and T. Moore. Security economics and the internal market. available via `https://www.enisa.europa.eu/publications/archive/economics-sec/at_download/fullReport` on 15/01/2016, January 2008.
3. AVANTSSAR. available via `http://www.avantssar.eu/` on 15/01/2016.
4. 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.
5. R. S. Betterley. Cyber/privacy insurance market syurvey - 2015. available via `http://betterley.com/samples/cpims15_nt.pdf`, June 2015.
6. 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.
7. J. Bolot and M. Lelarge. A new perspective on internet security security using insurance. Technical Report RR-6329, INRIA, 2007.
8. P. A. Bonatti, J. L. D. Coi, D. Olmedilla, and L. Sauro. *PROTUNE: A Rule-based PROvisional TrUst NEgotiation Framework*, 2010.
9. G. Costa, R. Mandati, F. Martinelli, I. Matteucci, and A. Yautsiukhin. *Handbook of Research on Architectural Trends in Service-Driven Computing*, chapter Mitigating Security Risks in Web Service Invocations: Contract-Based Approaches, pages 537–552. IGI Global, 2014.
10. 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*,

chapter At your service - Service-Oriented Computing from an EU Perspective, pages 429–455. MIT Press, 2009.
11. N. Dragoni and F. Massacci. Security-by-contract for web services. In *Proceedings of the 2007 ACM workshop on Secure web services*, SWS '07, pages 90–98, New York, NY, USA, 2007. ACM.
12. D. Heywood. Data breaches what can we expect from the EU?, January 2015. Available via `http://goo.gl/6Sa38Z` on 13/07/2015.
13. 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.
14. M. E. Kabay. ICSA White Paper Threats, Vulnerabilities and Real-World Responses: The Foundations of the TruSecure Process. ICSA, Inc, 1998.
15. J. P. Kesan, R. P. Majuca, and W. J. Yurcik. The economic case for cybersinsurance. Technical Report LE04-004, Illinois Law and Economics, 2004.
16. 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*, pages 1494–1502, Rio de Janeiro, Brazil, April 2009.
17. R. P. Majuca, W. Yurcik, and J. P. Kesan. The evolution of cyberinsurance. *The Computing Research Repository*, abs/cs/0601020, 2006.
18. A. Marotta, F. Martinelli, S. Nanni, and A. Yautsiukhin. A survey on cyber-insurance. Iit tr-17/2015, Istituto di Informatica e Telematica. Consiglio Nazionale delle Ricerche, 2015.
19. 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://www.dhs.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf` on 02/12/2014, February 2014.
20. OASIS. extensible access control markup language (xacml) version 3.0. available via `http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf`, January 2013.
21. 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.
22. 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*, pages 1–9, Brooklyn, New York, USA, May 2013.
23. R. Pal, L. Golubchik, K. Psounis, and P. Hui. Will cyber-insurance improve network security? a market analysis. In *Proceedings of the 2014 INFOCOM*, pages 235–243. IEEE, 2014.
24. E. Parliament. European parliament legislative resolution of 12 march 2014 on general data protection regulation, October 2014.
25. T. Poletti. First-ever insurance against hackers, June 1998. Available `http://goo.gl/SSGArI` on 13/07/2015.
26. M. Shanahan. The event calculus explained. In M. Wooldridge and M. Veloso, editors, *Artificial Intelligence Today*, volume 1600 of *Lecture Notes in Computer Science*, pages 409–430. Springer Berlin Heidelberg, 1999.
27. N. Shetty, G. Schwartz, and J. Walrand. Can competitive insurers improve network security? In A. Acquisti, S. Smith, and A.-R. Sadeghi, editors, *Proceedings of the*

3rd International Conference on Trust and Trustworthy Computing, volume 6101 of *Lecture Notes in Computer Science*, pages 308–322. Springer Berlin Heidelberg, 2010.
28. W. Shim. An analysis of information security management strategies in the presence of interdependent security risk. *Asia Pacific Journal of Information Systems*, 22(1), March 2012.
29. C. State. Senate bill no. 1386 chapter 915. Available `http://goo.gl/W8qhb8` on 13/07/2015.
30. C. Toregas and N. Zahn. Insurance for cyber attacks: The issue of setting premiums in context. Technical Report GW-CSPRI-2014-1, The George Washington University, January 2014. available via `http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/53c3daa5e4b056f825681c72/1405344421345/cyberinsurance_paper_pdf.pdf`.
31. Z. Yang and J. C. S. Lui. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 74:1–17, Apr. 2014.
32. 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, ICIS 2009, Phoenix, Arizona, USA, December 15-18, 2009*, page 49, 2009.

8 Appendix

Here we prove that

$$\begin{aligned} E[I^{dep}] &= \sum_{k=0}^{n} kI((1-\pi)B(\pi,k,n) + m\sum_{l=0}^{k} B(\pi,l,n)B(q,k-l,n-l) \\ &= nI(\pi + mq - mq\pi) \end{aligned}$$

First, we open all binomial formulas:

$$\begin{aligned} &E[I^{dep}] = I(1-m)\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\pi^k(1-\pi)^{n-k} + \\ &Im\sum_{k=0}^{n} k\sum_{l=0}^{k}\frac{n!}{l!(n-l)!}\pi^l(1-\pi)^{n-l} \times \frac{(n-l)!}{(k-l)!(n-l-k+l)!}q^{k-l}(1-q)^{n-k} \end{aligned} \tag{20}$$

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

$$E[I^{dep}] = \tag{21}$$

$$(1-m)nI\pi + mI\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}(1-q)^{n-k}(1-\pi)^n \times \sum_{l=0}^{k}\frac{k!}{l!(k-l)!}q^{k-l}(\frac{\pi}{1-\pi})^l \tag{22}$$

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:

$$E[I^{dep}] = \tag{23}$$

$$(1-m)nI\pi + mI\left(\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}(\frac{\pi}{1-\pi}+q)^k(1-q)^{n-k}\right)(1-\pi)^n \tag{24}$$

Consider the following element of the formula separately:

$$\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\left(\frac{\pi}{1-\pi}+q\right)^k(1-q)^{n-k} = \tag{25}$$

$$n\left(\frac{\pi}{1-\pi}+q\right)\sum_{k=0}^{n} k\frac{(n-1)!}{k!(n-k)!}(\frac{\pi}{1-\pi}+q)^{k-1}(1-q)^{(n-1)-(k-1)} = \tag{26}$$

$$n\left(\frac{\pi}{1-\pi}+q\right)\sum_{k=1}^{n} \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!}(\frac{\pi}{1-\pi}+q)^{k-1}(1-q)^{(n-1)-(k-1)} = \tag{27}$$

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

$$\sum_{k=0}^{n} k\frac{n!}{k!(n-k)!}\left(\frac{\pi}{1-\pi}+q\right)^k(1-q)^{n-k} = \tag{28}$$

$$n\left(\frac{\pi}{1-\pi}+q\right)\sum_{t=0}^{y} \frac{y!}{t!(y-t)!}(\frac{\pi}{1-\pi}+q)^{t}(1-q)^{y-t} = \tag{29}$$

$$n\left(\frac{\pi}{1-\pi}+q\right)\left(\frac{\pi}{1-\pi}+q+1-q\right)^{n-1} = n\frac{\pi+q-\pi q}{(1-\pi)^n} \tag{30}$$

Now,

$$E[I^{dep}] = (1-m)nI\pi + mIn\frac{\pi+q-\pi q}{(1-\pi)^n}(1-\pi)^n = \tag{31}$$

$$nI(\pi-\pi m+\pi m+mq-\pi qm) = nI(\pi+mq-\pi qm) \tag{32}$$