HOW MUCH SHOULD WE PAY FOR SECURITY? (INVITED PAPER)

Sokratis K. Katsikas[1], Athanasios N. Yannacopoulos[2] , Stefanos Gritzalis[1], Costas Lambrinoudakis[1] and Peter Hatzopoulos[2]

[1]Dept. of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, Greece GR-83200; [2]Dept. of Statistics and Actuarial – Financial Mathematics, University of the Aegean, Karlovassi, Samos, Greece GR-83200.

Abstract: Information systems security has become a top priority issue for most organizations worldwide IT managers try to protect their systems through a series of technical security measures. Even though these measures can be determined through risk analysis, the appropriate amount that should be invested in Information Systems security is, by and large, determined empirically. Organizations would also wish to insure their information systems against potential security incidents. In this case both parties, namely the organization and the insurance company would be interested in calculating a fair, mutually beneficial premium. In this paper a probabilistic structure, in the form of a Markov model, is used to provide some insight into these issues.

Key words: Information systems security, security investment, security insurance

1. INTRODUCTION

One of the most crucial steps of any risk analysis exercise, regardless of the method used to carry it out, is the presentation of the findings to the management of the organization whose information systems are the object of the analysis. This is because, in this step, the analysts have to compactly and concisely present their conclusions regarding the risks faced by the organization and the measures that need to be taken to minimize these risks. They have to do so in a language understood by an audience comprising usually high-level and/or mid-level managers, avoiding technical details and

focusing on the potential financial impact of the risks (were they to come true) and on the estimated monetary cost of the proposed security countermeasures.

In such presentations, numerous questions, of a very diverse nature, are usually asked. However, there is one issue that is almost invariably brought up: "We appreciate the need for taking security measures and we realize that these will inevitably bear some cost. We are prepared to undertake some cost towards this direction; however, the estimated cost of the overall security package is beyond our allocated budget." According to the theory, the risk analysis exercise has concluded with a *justified* proposal for installing appropriate countermeasures. Moreover, it is well known that security measures are interconnected into a coherent whole; any partial implementation of the *security puzzle* may render the whole effort ineffective, hence useless. Therefore, in theory, the risk analyst must respond to the issue above stating, more or less, "This is what you should do, and you should do all of it. If your budget is inadequate, and prohibits you from implementing all the necessary measures, then there will inevitably be some risks that you will not be countering, but rather implicitly accepting". This approach is technically flawless; however, in terms of management and finances, it is quite unacceptable. By raising the issue above, any competent management team is actually asking whether there is a way of finding out how much the organization *really* needs to invest in security.

Another issue that increasingly comes up in such presentations is related to the management of the residual risk that will remain after having installed the selected security countermeasures. Until the recent past, organizations were implicitly or explicitly accepting this residual risk, as it was conceived as being rather low. Today, successful attacks against information systems can be (and are) launched by teenagers, using software tools that can be acquired at a minimal (or zero) cost. On the other hand, the value of information stored within organizational information systems has tremendously increased in our networked world. The combination of these two factors leads to the conclusion that we can no longer afford to neglect the residual risk, but we should rather try to handle it in the same way we do in other areas of operation: by mitigating it. Recently, several insurance companies have started insuring information systems against security breaches. The main question when we contemplate mitigating risk by insuring against it is how much should we pay for the insurance premium.

In this paper the two questions identified in the paragraphs above are addressed. The paper combines the findings reported in [1] and [2] and presents them in a more technically and managerially oriented (as opposed to mathematically oriented) way. It is organized as follows: In Section 2 a Markov model describing the information system under study is presented.

In Section 3 the question of calculating an actuarially fair premium for insuring the system against security breaches is taken up. Section 4 attempts to answer the question of what is the optimal security investment. Section 5 summarizes our conclusions and highlights our current and future research directions.

2. A MARKOV MODEL FOR DESCRIBING THE SECURITY OF AN INFORMATION SYSTEM

In this section we provide an overview of the continuous time Markov model proposed in [1]. This model was inspired by a general class of actuarial models for disability insurance, proposed in [3]. The model describes the current state of the information system and its possible transitions to different states of non-full operation as a result of occurrence of security incidents, in the course of time.

Let us assume that the system may result into one of N different states after possible security incidents. We will denote these states by i, where $i = 1, ..., N$. By $i = 0$ we will denote the state where no successful security attack has been made against the system; thus the system is fully operational. We assume that at time $t = 0$ the system is at the fully operational state $i = 0$ and as time passes by it may end up in different states of non-fully operational status, that is it may end up at one of the states $i = 1, ..., N$.

One of the most important steps in the study of various issues related to the function and security of the information system is the determination of the probability of the state of the system at various times. In order to obtain that we propose a Markov model that describes the transition between the various possible states of the system. Let us assume the simplest possible structure in which the only transitions allowed are the transitions $0 \to i$. By $S(t)$ we will denote the state of the system at time t. Clearly, $S(t)$ may take one of the values $0,1, ...,N$. In the framework of the Markov model the most important quantities are the transition probabilities between states, i.e. the quantities $P_{ij}(u,t) = P[S(t) = j / S(u) = i]$. By the general theory of Markov processes in continuous time we know that the model may be fully determined by the transition rates, defined, between states $i \neq j$ as

$$\mu_{ij}(u) = \lim_{t \to u} \frac{P_{ij}(u,t)}{t-u}.$$

Observing that only transition rates of the form μ_{0i} are nonzero, and assuming time-invariant transition rates, the transition probabilities are shown in [2] to be given by

$$P_{00}(z,t) = \exp(-\mu_0(t-z))$$

$$P_{0j}(z,t) = \frac{\mu_{0j}}{\mu_0}(1-\exp(-\mu_0(t-z))),$$

where $\mu_0 = \mu_{01} + \mu_{02} + ... + \mu_{0N}$.

3. HOW MUCH SHOULD WE PAY FOR INSURANCE?

The question we wish to tackle in this section using the simple model of the previous section is how the insurance company can calculate the fair amount of money it will charge, or, in other words, how one may calculate the net or mathematical premium. There is not a unique way to do this; however we will present here a simple, actuarially fair way of determining the cost of the insurance service.

3.1 Actuarial values of premium and benefits

Having obtained the probabilistic structure of the model which will allow us to characterize the state of the system at different times, we may now calculate the actuarial values of the net premium and the benefits [3]. The benefits, as well as the net premium received depend on the state of the information system, which is a random quantity. Thus, the benefits and the net premium received at time I are random variables. The term *actuarial value* denotes the best possible prediction for these random variables, given some information on the system state up to time t. Because of the Markov structure of the model, the information from time 0 to time t is summed up to the information on the state of the system at time t, i.e. it sums up to the information provided by the random variable $S(t)$. As the best possible prediction, we will take the conditional expectation of the random variable given the information provided by $S(t)$. Also note that the benefits and the premium are paid at different times. In order to be able to compare sums of money received or given at different times, we need to evaluate their value at the same time instance. This is done using a properly chosen discounting

factor. We will assume (without loss of generality) that there is a constant deterministic interest rate δ. Thus the discounting factor, relating the value of a payment at time t to the value of this payment at time 0 is $e^{-\delta t}$.

Using the above assumptions, the present value at time t of a continuous benefit at rate $c_j(u)$ given by the insurance company to the owner of the information system at time u as long as $S(u)=j$, is the random sum of money

$$Y_t = e^{-\delta(u-t)} \bullet l_{\{S(u)-j\}} \bullet c_j(u) \bullet du$$

where $l_{\{S(u)-j\}}$ is the indicator of the event $\{S(u)=j\}$ and $c_j(u)$ is the benefit amount paid out in the infinitesimal interval $[u, u+du]$.

In a similar manner, one may calculate the premium. Let us assume that the premium paid varies with the state the system is in. The actuarial value of the net premium at time t, paid at time u if the system is in state j and if $S(t)=i$ is given by the formula

$$P_{t,i,j}(u) = e^{-\delta(u-t)} P_{ij}(t,u) c_j(u) du$$

The total benefits and premium paid will result as the sum over all possible states. Thus the actuarial value of the benefits and premium at time t, paid between time t and T, if the system is in the state $S(t)=i$ at time t will be equal to

$$B_i(t,T) = \int_t^T e^{-\delta(u-t)} \sum_{j=0}^{N} P_{ij}(t,u) b_j(u) du$$

$$P_i(t,T) = \int_t^T e^{-\delta(u-t)} \sum_{j=0}^{N} P_{ij}(t,u) p_j(u) du$$

where T is the term of the contract, i.e. the time when the contract expires.

3.2 Calculation of the premium

For the calculation of the premium one may follow several approaches (giving possibly different results). We present here a simple way for obtaining the premium, which does not involve the use of utility functions.

The insurance contract is entered at time $t=0$, when the system is in state

0. A fair way to calculate the premium would be using the *principle of equivalence,* according to which we choose the premium in such a way so that the actuarial value of the benefits at time $t=0$ and in state 0 is equal to the actuarial value of the total premium paid, again calculated at time $t=0$ and state 0. Mathematically this, means that $B_0(0,T) = P_0(0,T)$.

According to this principle the insured expects to pay to the insurer as much as she expects to get (of course in terms of estimates of the random variables involved). In our simple model the insured pays premium only when the system is in state 0. Also recall that in our model only the transition probabilities P_{0i} are non-zero. Using the equivalence principle and the expressions for the transition probabilities obtained in Section 3.1 and assuming that $P_0(u) = P_0$ we can calculate the net premium as [2]

$$P = \frac{\delta + \mu_0}{\mu_0} \bullet \frac{1}{1 - e^{-(\delta+\mu_0)T}} \bullet \int_0^T e^{-\delta u} \sum_{j=0}^{N} \mu_{0j}(1 - e^{-\mu_0 u}) b_j(u) du$$

4. HOW MUCH SHOULD WE INVEST IN SECURITY?

We now assume that the owner of the information system undertakes some security measures that will have an effect on the transition rate from state 0 to the states $j = 1,..., N$. It is reasonable to assume that one may adopt security measures to reduce the risk of transition to particular states. The cost of the security measure related to the transition to state j will be denoted by Z_j. We will further assume, following the work in [4], that there is also another set of relevant parameters, the vulnerabilities of the various information sets. However, departing from the setup of [4], we assume that an expert may define vulnerability parameters for the various states that the system may end up in. Thus we may assume that the transition rates μ_{0j} are functions of the security cost Z_j and of the vulnerability parameter $v(j).\mu_{0j}(z_j, v_j)$. In general, one expects these functions to enjoy the following properties:

P1. $\mu_{0j}(z_j, 0) = 0$, i.e. if the system is completely invulnerable with respect to the risks related to transition to state j, there will be no such transition.

P2. $\mu_{0j}(0, v_j) = v_j = \overline{\mu_{0j}}$, i.e. if no security measures are undertaken, then the transition rate to state j will be equal to some constant, which may be defined to be the vulnerability v_j.

P3. $\mu_{0j}(z_j, v_j)$ is a decreasing convex function of Z_j. If we assume that μ_{0j} is twice differentiable with respect to Z_j, then

$$\frac{\vartheta \mu_{0j}}{\vartheta z_j} < 0 \text{ and } \frac{\vartheta^2 \mu_{0j}}{\vartheta z_j^2} > 0.$$

This means that the larger the cost of security measures undertaken, the smaller the transition rates become but after a while there is a saturation effect, in the sense that larger security measures have diminishing effect.

Thus, using the above transition rates, we may construct a Markov chain $S^z(t)$, corresponding to the state of the system at time t if the security measures $z = \{z_1, ..., z_N\}$ are adopted.

In order to construct a model for determining the optimal security measures, one must first construct a model for the financial losses caused by the transition of the system to one of the states of malfunction. This can be done with the aid of the Markov chain model proposed in Section 2. We will denote by $X^z(t)$ the stochastic process corresponding to the financial losses (measured in terms of some currency) caused by a possible transition of the system to some state of malfunction. The possible losses may be of various types. For instance, one may assume that there is a lump sum loss $d_j(u)$ at fixed time u if $S^z(u) = j$. This is one of the simplest type of possible losses. Other types of losses are possible and can be treated with similar methods as the ones proposed here. For a simpler exposition of our model we will be content here with the treatment of losses of the above type.

The random wealth of the firm at time t will be

$$w - \sum_{i=1}^{N} z_i - X^z(t)$$

where w is the initial wealth of the firm,

$$\sum_{i=1}^{N} z_i$$

is the total value of the security measures adopted by the firm and $X^z(t)$ are the financial losses that the firm faces as a consequence of transitions to

certain states of malfunction. We assume that $X^z(0)=0$, i.e the system starts at state 0, which corresponds to the state of perfect working order of the system.

The firm will select security measures so as to maximize the intertemporal expected utility of its random wealth. Therefore, the security measures will be chosen so as to solve the problem

$$\max_{z_1,\ldots,z_N} E(U)=E\left[\int_0^T e^{-\delta t}u(w-\sum_{i=1}^N z_i - X^z(t)dt + u(w-\sum_{i=1}^N z_i)\right]$$

possibly subject to the constraint $\sum_{i=1}^N z_i \le K$, where K is a budget constraint corresponding to the maximum amount that may be spent on security. The factor $e^{-\delta t}$ is a discounting factor that models the time impatience properties of the firm and u is a utility function, corresponding to a risk averse agent that is an increasing concave function (see e.g. []). T is the time horizon over which the firm wishes to plan ahead.

We assume that the decision of the security measures adopted is made at time t=0 and is held unchanged throughout the horizon T. A more dynamic model where the decisions are changed over specified time intervals is possible in the above setup, but such a model will not be discussed here.

The Markov structure of the model allows the simplification of the above expectation of the utility function. Assuming losses of the type discussed above and keeping in mind the Markovian nature of the $S^z(t)$ process, one concludes that the optimal security investment program arises as the solution to the set of equations

$$\frac{\vartheta E[u]}{\vartheta z_k}=-\sum_{j=1}^N u'(w-\sum_{i=1}^N z_i - d_j)A_j(z,v)+\sum_{j=1}^N u(w-\sum_{i=1}^N z_i-d_j)\times$$

$$\frac{\vartheta A_j(z,v)}{\vartheta z_k}-u'(w-\sum_{i=1}^N z_i)=0$$

In the general case, these maximization conditions are nonlinear algebraic equations, which have to be treated numerically. Nowadays, the numerical treatment of such equations is fast, accurate and straightforward with the use of standard commercial numerical packages. The use of such methods may yield quite easily the optimal security investment for the firm, taking into account the characteristics of the firm towards risk (the utility

function), the structure of the firm (how much a firm is willing to invest on security) and the structure of the risks the firm is likely to undergo (the probabilistic model for the state of the firm, concerning its security). However, for special cases of utility functions, which are of great practical interest, one may additionally obtain analytic solutions, which help reveal the essential features of our model and allow us to make some observations about possible strategies for optimal security investment. Such types of problems are treated next.

4.1 Some special cases

As a special case of the above general formulation, one may consider the case of the linear utility function. This is equivalent to the criterion of minimization of the expected loss that has been used in related work for the determination of optimal security investment (see e.g. [5].) Further, in order to gain insight into the physical meaning of the mathematical results, consider the case where only two possible states of malfunction exist, one of which is less probable than the other. This can be mathematically modeled by setting $\mu_{01} = \varepsilon\mu_0(z_1)$ and $\mu_{02} = \mu_0(z_2)$ for some function $\mu_0(z_2)$ that enjoys properties P1-P3. In this case, it can be seen [2] that $\mu_0'(z_1) = \mathrm{O}\left(\frac{1}{\varepsilon}\right)$ and $\mu_0'(z_2) = \mathrm{O}(1)$, implying that $z_1 << z_2$, i.e. the organization should spend a negligible amount of money to counter risk 1 (the less probable one) and should concentrate on risk 2.

Under the same assumptions, if we turn our attention to what happens as $T \to \infty$, we can conclude [2] that, when $d_1 = d_2$, and for $\mu_{0i} = A_i v \exp(-a_i z_i)$ (Class I transition rates), then

$$z_1^* = -\frac{1}{a_1}\ln\left(\frac{\mu_{01}^*}{A_1}\right) + \frac{1}{a_1}\ln(v)$$

Using this result one may discuss the dependence of the optimal security investment as a function of the vulnerability parameter. First of all, this quantity must be positive. This will happen only for large enough values of A_1. For small enough values of A_1, it may well be that below a critical value v^* of the vulnerability parameter the optimal security investment is zero. Otherwise, it is a weakly increasing function of the vulnerability parameter.

On the other hand, if we assume that $\mu_{0i} = A_i v^{a_i z_i + 1}$ (Class II transition rates), then

$$z_1^* = -\frac{1}{a_1} - \frac{1}{a_1}\frac{\ln(A_1)}{\ln(v)} + \frac{1}{a_1}\frac{\ln(\mu_{01}^*(v))}{\ln(v)}.$$

Now the behavior of the optimal investment as the vulnerability parameter changes is different. For this kind of transition functions we observe an abrupt increase of the security investment as the vulnerability parameter approaches values near 1.

The conclusions from this simplified version of the model are that the effectiveness of the security measures plays an important role on the optimal security investment. Specifically, for Class I transition rates we notice that a small increase in the invested amount in security leads to a large decrease of the probability of the system to end-up in a non-fully operational state (effective security measures). In this case the optimal investment curve exhibits saturation properties. On the contrary, for Class II transition rates, where the security investments are not that effective, the optimal investment curve does not exhibit saturation properties for large values of the vulnerability parameter.

5. CONCLUSIONS

In this paper we have proposed a Markov model describing the transitions of an information system from the fully operational state to states of non-fully operational status, as a result of a security incident that damages an asset of the information system, using the transition intensity approach. This model has been used for estimating the premium of the insurance contract against the expected losses to the organization that will result from potential security incidents. The model is then improved, being now capable of monitoring the effect of security investment on the probability of a security breach to occur. Insight into practical aspects of risk management is shown to be gained by even this, still simple, model.

Our current research work focuses on extending the model so as to waive the assumption that all non-fully operational states of the information system are absorbing states. In other words, the extended model will be capable of handling cases where there is a transition from some state $i, i \neq 0$ to the fully operational state 0. Another extension will be that all the assets of the information system will be modelled, instead of a single asset that is

currently supported, thus enabling us to account for interdependencies of security incidents or/and security measures operating on different assets and consequently to obtain a more accurate estimate of the insurance premium.

6. REFERENCES

1. Lambrinoudakis C., Gritzalis S., Hatzopoulos P., Yannacopoulos A.N. and Katsikas, S.K., A formal model for pricing information systems insurance contracts, *Computer Standards & Interfaces* **27**, 521-532 (2005).
2. Yannacopoulos A.N., Lambrinoudakis C., Gritzalis S., Hatzopoulos P., and Katsikas, S.K., A dynamic stochastic model for optimizing information systems security investment, *submitted for publication.*
3. Habennan, S. and Pitacco, E., *Actuarial models for disability insurance*, Chapman and Hall, 1999.
4. Gordon, L.A. and Loeb, P., The economics of information security investment, ACM Transactions on Information and Communication Systems Security, **5**, 438-457, 2002.
5. Varian, H.R., *Microeconomic analysis*, Norton and Co., 1992.