Optimizing the selection of information security remedies in terms of a Markov security model

A A Magazev¹ and V F Tsyrlin⁰¹

¹Department of Complex Information Security, Omsk State Technical University, Omsk, Russia, 644050

e-mail: magazev@mail.ru, lera.tsyrlin@mail.ru

Abstract. An information security model expressed in terms of Markov processes is considered. Within this model the functioning of information system as a sequence of failures and recovery actions that appear in response to security threats is described. A detailed investigation of the model is provided, and its important characteristic called the relaxation time is introduced. A permissible range of security parameters is constructed by using the relaxation time. The problem of selection of information security remedies as a problem of non-linear optimization with boolean variables is stated and discussed.

1. Introduction

It is hard to overestimate the significance of modelling in the field of information security. Development and use of mathematical models in this field are needed for the theoretical justification of security methods being employed in the practical design of protected information systems. Moreover, the use of mathematical models allows one to formulate such important characteristics of information security as effectiveness [1, 2] and reliability [3, 4]. It is well known that these characteristics are the quantitative evaluations of the ability of an information security system to perform its required functions.

Among existing information security models that have been used in recent years, the models based on the theory of Markov processes are of special interest. It turns out that the class of problems that can be solved with the help of these models is surprisingly wide: detecting cyber attacks in computer networks [5], modelling the spread of computer viruses [6, 7], anomaly detection in computer systems and networks [8, 9], optimization and reliability growth in security systems [10, 11, 12].

In Refs. [13, 14, 15, 16], the authors investigate the class of Markov models describing information systems as systems with failures and recovery actions. This approach allows one to involve well-developed mathematical tools of reliability theory which are well-established for the development of complex technical systems. In particular, in Ref. [14] the author suggested a Markov model with a finite number of states characterizing the influence of security threats on the information system. Having formulated the basic statements the author, however, limited himself to a perfunctory quantitative analysis of the model. Motivated by this fact, we have decided to investigate the model in more detail. In our previous work [17] we investigated the long-time asymptotic behavior of the model, and introduced its important characteristic called
the relaxation time which has been used to construct a permissible range of security parameters of the model. The present paper continues the study started in [17].

This paper is organized as follows. Section 1 describes the model suggested in Ref. [13] and give the explicit formulas for the probabilities of states of the model. In section 2 we formulate the definition of the relaxation time and briefly present the algorithm for constructing the permissible range of security parameters of the model. In section 3 we employ our model to state and discuss the problem of selection of information security remedies as a problem of non-linear discrete optimization.

2. Model description

Let us consider an information system (here and elsewhere referred to as a system) on which \(n\) independent threats with the probabilities \(q_1, q_2, \ldots, q_n\) act. We assume that the occurrence of two or more threats at the same time is impossible. Furthermore, the next threat can act only after blocking the previous one. Thus, at each moment of time \(t = 0, 1, 2, \ldots\) the system is in one of the states \(s_0, s_1, \ldots, s_{n+1}\). In the state \(s_0\), called the security state, no threats act. The state \(s_i\), where \(i = 1, \ldots, n\), is characterized by the action of \(i\)-th threat. If the system is in the state \(s_i\) at the moment of time \(t\) then there are two alternatives at the next moment of time \(t+1:

- the threat is eliminated with the probability \(r_i\) and the system comes to the security state \(s_0\);
- the threat is not eliminated with the probability \(\bar{r}_i = 1 - r_i\) and the system makes the transition to the final state \(s_{n+1}\).

The state diagram of the system is shown in Fig. 1.

![State diagram of the system](image)

Figure 1. State diagram of the system.

A sequence of transitions between states of the system is a Markov chain with the following transition matrix:

\[
\Pi = \begin{pmatrix}
q_0 & q_1 & q_2 & \cdots & q_n & 0 \\
0 & r_1 & 0 & \cdots & 0 & \bar{r}_1 \\
0 & 0 & r_2 & \cdots & 0 & \bar{r}_2 \\
0 & 0 & 0 & \cdots & 0 & \bar{r}_n \\
0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}.
(1)

Here, we introduce the notation \(q_0 = 1 - \sum_{i=1}^{n} q_i\).
We denote by $p_i(t)$ the probability of state $s_i$ at the moment of time $t$. This probability is defined by the probabilities of states at the previous moment of time $t-1$ as

$$p_i(t) = \sum_{j=0}^{n+1} p_j(t-1) \Pi_{ji}, \quad (2)$$

or in the matrix form

$$\mathbf{p}(t) = \mathbf{p}(t-1) \cdot \Pi. \quad (3)$$

Here, $\mathbf{p}(t) = (p_0(t), p_1(t), \ldots, p_{n+1}(t))$ is the vector of probabilities of system states at the moment of time $t$. By using (3), we can write

$$\mathbf{p}(t) = \mathbf{p}(0) \cdot \Pi^t, \quad t = 0, 1, 2, \ldots, \quad (4)$$

where $\Pi^t$ is the $t$-th power of matrix $\Pi$.

It is natural to assume that the system is in the security state $s_0$ at the initial moment of time $t = 0$, that is $\mathbf{p}(0) = (1, 0, \ldots, 0)$. By simple calculation we derive the following explicit formulas for probabilities $p_i(t)$ [17]:

$$p_0(t) = \frac{1}{w} \left[ \left( \frac{q_0 + w}{2} \right)^{t+1} - \left( \frac{q_0 - w}{2} \right)^{t+1} \right]; \quad (5)$$

$$p_i(t) = p_0(t-1)q_i, \quad i = 1, \ldots, n; \quad (6)$$

$$p_{n+1}(t) = 1 - p_0(t) - p_0(t-1) \sum_{i=1}^{n} q_i. \quad (7)$$

Here, the positive value $w$ called $w$-parameter of the system is defined by

$$w^2 = q_0^2 + 4 \sum_{i=1}^{n} r_i q_i. \quad (8)$$

The absence of any security means that $r_i = 0$ for all $i = 1, \ldots, n$. By virtue of Eq. (8) we have $w = q_0$ in this case, i.e. the $w$-parameter coincides with the probability of absence of threats. Then from (5) – (7) it follows that

$$\lim_{t \to \infty} p_0(t) = \ldots = \lim_{t \to \infty} p_n(t) = 0, \quad \lim_{t \to \infty} p_{n+1}(t) = 1.$$

It is clearly seen that the same limit relations hold in general. To demonstrate this we notice that the absolute values of quantities $(q_0 \pm w)/2$ in the parentheses of Eq. (5) are always less than 1. Indeed, this follows from the fact that the quantities $(q_0 \pm w)/2$ are real roots of the quadratic equation

$$f(x) = x^2 - q_0 x - \sum_{i=1}^{n} q_i r_i = 0$$

which, by virtue of the inequations $f(\pm 1) > 0$ and $f(0) < 0$, lie inside the interval $[-1, 1]$.

From (5) – (7) it follows that the probabilities $p_i(t), i = 1, \ldots, n+1$ are entirely determined by the probability $p_0(t)$. Thus, in the rest of the section we will focus on the function $p_0(t)$.

From (5) we see that $p_0(t)$ decreases as $t \to \infty$. However, in the general case this dependence is not monotonic. Indeed, one can see from (5) that the quantity $p_0(t)$ is the difference between a monotonically decreasing function and a non-monotonically decreasing function (since the value $(q_0 - w)/2$ is negative). The rate of decrease of $p_0(t)$ and the magnitude of its oscillations, in
The graphs of $p_0(t)$ for two different values of parameters $q_1$ and $r_1$ in case of one threat are shown in Fig. 2.

By virtue of the relation
\[
\lim_{t \to \infty} \left| \frac{q_0 - w}{q_0 + w} \right|^t = 0,
\]
we conclude that the magnitude of oscillations of $p_0(t)$ decreases rapidly as $t \to \infty$. Thus, on fairly long time-scales we can assume
\[
p_0(t) \approx p_0^s(t) = w^{-1} \left( \frac{q_0 + w}{2} \right)^{t+1}.
\]
It is not difficult to evaluate the applicability condition for this approximation. Let $\varepsilon > 0$. Then the requirement $|p_0(t) - p_0^s(t)| < \varepsilon$ is equivalent to the inequality
\[
t > \log_{w/q_0} (\varepsilon w) - 1.
\]

3. Relaxation time and construction of the permissible range
Let us consider the dynamics of the system for times satisfying the inequality (10) for given $\varepsilon > 0$. Then, up to the accuracy of the order $\varepsilon$, we can suppose that
\[
p_0(t) \approx w^{-1} \left( \frac{q_0 + w}{2} \right)^{t+1}.
\]
It is important that in this approximation $p_0(t)$ is a monotonically decreasing function.

Now we give the following definition. The relaxation time $\tau$ of the system is the time required for the probability of state $s_0$ to drop from the initial value to $1/2$. By using (11), from the definition we immediately obtain the explicit formula for $\tau$:
\[
\tau = \log_{w/q_0} \left( \frac{w}{2} \right) - 1.
\]
Let $T$ be some fixed moment of time. Our goal is to find values of the security parameters $r_1, \ldots, r_n$ for which $\tau \geq T$. In other words, we are interested in the conditions that guarantee that the relaxation time will not less than a given value.
By using the formula (12), we rewrite the inequality \( \tau \geq T \) in the form:

\[
\frac{w}{2} \leq \left( \frac{q_0 + w}{2} \right)^{T+1}.
\]

Let us consider this inequality as a restriction on the security parameters \( r_1, \ldots, r_n \). Since \( q_0 \) does not depend on \( r_i \), we need to solve (13) for the \( w \)-parameter. The solution of this problem is readily seen to be

\[
w \geq 2x^* - q_0,
\]

where \( x^* \) is a real root of the polynomial equation

\[
x^{T+1} - x + \frac{q_0}{2} = 0,
\]

that belongs to the interval \([q_0, 1]\). Note that (15) is a polynomial equation of degree \( T \) and, therefore, can have more than one real root. However, it is easy to show that the interval \([q_0, 1]\) contains only one real root of (15).

Substituting the explicit expression (8) for the \( w \)-parameter into the inequality (14), we obtain the following restriction on the security parameters \( r_i \):

\[
\sum_{i=1}^{n} q_i r_i \geq x^*(x^* - q_0).
\]

Together with the inequalities

\[
0 \leq r_i \leq 1, \quad i = 1, \ldots, n;
\]

the restriction (16) defines a convex region \( R_T(q_1, \ldots, q_n) \subset R^n \), which we shall call the permissible range for the security parameters \( r_1, \ldots, r_n \). Thus, the relaxation time \( \tau \) is not less than a fixed time \( T \) only for values of \( r_1, \ldots, r_n \) from the permissible range \( R_T(q_1, \ldots, q_n) \).

Let us consider two examples of constructing the permissible range.

**Example 1.** In case of one threat, the system is characterized by two parameters, \( q \) and \( r \). It follows from (16) and (17) that the permissible range \( R_T(q) \) is the interval \([r^*, 1]\), where

\[
r^* = \frac{x^*(x^* + q - 1)}{q}.
\]

Here \( x^* \) is a root of (15) that lies in the interval \([1 - q, 1]\). Some results of numerical modelling for \( r^* \) as a function on \( q \) are shown in fig. 3.

**Example 2.** We consider the system with two threats whose probabilities are \( q_1 \) and \( q_2 \). From (16) and (17) it follows that the permissible range is a convex set

\[
R_T(q_1, q_2) = \{(r_1, r_2) \in R^2: r_1 \leq 1, \quad r_2 \leq 1, \quad q_1 r_1 + q_2 r_2 \leq x^* (x^* - 1 + q_1 + q_2)\}
\]

where \( x^* \) is a root of (15) that lies in the interval \([1 - q_1 - q_2, 1]\). In fig. 4, we have drawn the permissible ranges for \( q_1 = 0.25, q_2 = 0.45 \) and three different times \( T = 10, 20, 30 \).

4. **Selecting an optimal set of information security remedies**

Let us suppose that there are \( m \) different security remedies eliminating the information threats. Denote by \( x_a \) the boolean variable associated with the \( a \)-th security remedy; \( x_a = 1 \) if the \( a \)-th security remedy is used and \( x_a = 0 \) otherwise. Thus, each concrete configuration of security remedies is characterized by an \( m \)-dimensional boolean vector \( x = (x_1, x_2, \ldots, x_m) \in \{0, 1\}^m \).
Denote by $r_{i,a}$ the probability of elimination of the $i$-th information threat by the $a$-th security remedy. Since a few security remedies can eliminate the threat at the same time, the probability of elimination of the threat by all security remedies is

$$ r_i(x) = \sum_{b=1}^{m} (-1)^{b-1} \sum_{a_1 < a_2 < \ldots < a_b} (r_{i,a_1} x_{a_1})(r_{i,a_2} x_{a_2}) \ldots (r_{i,a_b} x_{a_b}). $$

(18)

Obviously, in the general case $r_i(x)$ is a polynomial of degree $m$ in the boolean variables $x_1, x_2, \ldots, x_m$.

From the above, we conclude that the quantities $r_i(x)$ are extremely significant parameters of the information security system characterizing the quality of its functioning. Therefore, it is important to select a security system configuration in which $r_1(x), \ldots, r_n(x)$ satisfy the given restrictions, for instance, mentioned in the previous section. Let us formulate the corresponding problem more rigorously.

Let $c_a$ denote the cost of the $a$-th security remedy. We will consider the linear functional $C : \{0, 1\}^m \rightarrow R$:

$$ C(x) = \sum_{a=1}^{m} c_a x_a. $$

Obviously, the value of $C$ on a vector $x$ gives the full cost of the corresponding configuration of a security system.

Let $T > 0$. Following the previous section, we can restrict the values of the parameters $r_i(x)$ to the permissible range $R_T(q_1, \ldots, q_n) \subset R^n$ such that the relaxation time $\tau$ is not less than $T$. Simultaneously, we require that the full cost of the information security system is minimal.

Therefore, we arrive at the following optimization problem:

$$ C(x) = \sum_{a=1}^{m} c_a x_a \rightarrow \min, \quad x \in X, $$

(19)
where
\[ X = \{ \mathbf{x} \in \{0, 1\}^n : \sum_{i=1}^{n} q_i r_i(\mathbf{x}) \geq x^*(x^*-q_0) \}. \] (20)

Recall that \( q_0 = 1 - \sum_{i=1}^{n} q_i \), and \( x^* \) is a real root of the equation (15) that lies in the interval \([q_0, 1]\).

Since \( r_i(\mathbf{x}) \) are polynomials of degree \( m \) in the boolean variables \( x_1, x_2, \ldots, x_n \), the optimization problem (19), (20) belongs to the class of non-linear discrete optimization problems.

It is well known that currently there are no general effective methods for solving such problems (see, for example, Ref. [18]). However, in practice the number \( m \) of security remedies is not very large, therefore the problem (19), (20) can be solved by the brute-force method. Note that the problem can have one solution, no solutions, or more than one solution. The following example illustrates this remark.

Let us consider an information system on which two threats with the probabilities \( q_1 = 0.59 \) and \( q_2 = 0.18 \) act. We assume that there are \( m = 5 \) different security remedies whose costs are \( c_1 = 600, c_2 = 700, c_3 = c_5 = 400, c_4 = 200 \). Thus, in this example the functional of a security system cost is
\[ C(\mathbf{x}) = 600x_1 + 700x_2 + 400(x_3 + x_5) + 200x_4. \]

The probabilities \( r_{i,a} \) of elimination of threats by the security remedies are given by the matrix:
\[ \|r_{i,a}\| = \begin{pmatrix} 0.96 & 0.50 & 0.47 & 0.50 & 0.07 \\ 0.66 & 0.43 & 0.60 & 0.69 & 0.92 \end{pmatrix}. \]

Let us find solutions of the optimization problem (19), (20) for \( T = 5, 10, 100 \).

The case of \( T = 5 \). The real root of equation (15) from the interval \([q_0, 1]\) is \( x^* = 0.975 \). The domain \( X \), corresponding to (20), has the form
\[ X = \{ \mathbf{x} \in \{0, 1\}^5 : 0.59 r_1(\mathbf{x}) + 0.18 r_2(\mathbf{x}) \geq 0.726 \}, \]
where \( r_1(\mathbf{x}) \) and \( r_2(\mathbf{x}) \) are defined by (18). (The explicit expressions for \( r_i(\mathbf{x}) \) are very cumbersome and are not presented here). The solution \( \mathbf{x} \) of the optimization problem (19), (20) is unique:
\[ \mathbf{x} = (1, 0, 0, 1, 0), \quad C(\mathbf{x}) = 800. \]

The case of \( T = 10 \). In this case \( x^* = 0.988 \), therefore the domain \( X \) has the form
\[ X = \{ \mathbf{x} \in \{0, 1\}^5 : 0.59 r_1(\mathbf{x}) + 0.18 r_2(\mathbf{x}) \geq 0.749 \}. \]

The optimization problem (19), (20) has two solutions \( \mathbf{x}_1 \) and \( \mathbf{x}_2 \):
\[ \mathbf{x}_1 = (1, 0, 0, 1, 1), \quad \mathbf{x}_2 = (1, 0, 1, 1, 0), \quad C(\mathbf{x}_1) = C(\mathbf{x}_2) = 1200. \]

The case of \( T = 100 \). Since \( x^* = 0.999 \), it follows that
\[ X = \{ \mathbf{x} \in \{0, 1\}^5 : 0.59 r_1(\mathbf{x}) + 0.18 r_2(\mathbf{x}) \geq 0.772 \}. \] (21)

In this case the optimization problem (19), (20) has no solutions, because there are no configurations \( \mathbf{x} \in \{0, 1\}^5 \) in the domain (21).

It should be noted that we have developed the Wolfram Language Package MMInfoSec which contains various procedures for investigating the security model presented here. In particular, for \( m \leq 10 \) the optimization problem (19), (20) can be solved by using this package.
5. Conclusions
In this paper, we have investigated one of the models in terms of which the functioning of an information system is considered as a sequence of failures and recovery actions appearing in response to information threats. We give the explicit formulas for the probabilities of the information system states and analyse the long-time behavior of the system. By using the definition of the relaxation time, we describe the algorithm for constructing the permissible range of the security parameters. Finally, we formulate and discuss the problem of selecting information security remedies as a discrete non-linear optimization problem with boolean variables.

Our future work will focus on developing more efficient algorithms for solving the optimization problem (19), (20). We also intend to expand our model by considering the possibility of dependent threats, i.e. threats that generate each other.

6. References
[1] Knapp KJ, Marshall TE, Rainer RK and Ford FN 2007 Information security effectiveness: Conceptualization and validation of a theory International Journal of Information Security and Privacy 1 37
[2] Kankanhalli A, Teo HH Tan BC, and Wei KK 2003 An integrative study of information systems security effectiveness International journal of information management 23 139
[3] Kondakci S 2015 Analysis of information security reliability: A tutorial Reliability Engineering & System Safety 133 275
[4] Burtescu E 2010 Reliability and Security – Convergence or Divergence Informatica Economica 14 68
[5] Pietre-Cambacedes L and Bousso M 2010 Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP) Proceedings of the 8th European Dependable Computing Conference (EDCC-8) (Valencia, Spain) pp 199-208
[6] Van Mieghem P, Omic J, and Kooij R 2009 Virus spread in networks IEEE/ACM Transactions on Networking (TON) 17(1) pp 1-14
[7] Sahneh FD, Scoglio C, and Vann Mieghem P 2013 Generalized epidemic mean-field model for spreading processes over multilayer complex networks IEEE/ACM Transactions on Networking 21(5) 1609-1620
[8] Ye N 2000 A Markov chain model of temporal behavior for anomaly detection Proceedings of the 2000 IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop vol 166 (West Point, NY) p 166
[9] Ye N, Zhang Y, and Borror C M 2004 Robustness of the Markov chain model for cyber attack detection IEEE Transactions on Reliability 53 116-123
[10] Rosenfeld N and Globerson A 2016 Optimal tagging with Markov chain optimization Advances in Neural Information Processing Systems pp 1307-1315
[11] Littlewood B 1975 A reliability model for systems with Markov structure Applied Statistics pp 172-177
[12] Trivedi K S and Medhi D 2009 Dependability and security models Proceedings of 7th International Workshop on the Design of Reliable Communication Networks pp 11-20
[13] Klimenko E S and Rosenko A P 2007 Markov model for the influence evaluation of internal threats on the security of confidential information Izvestiya SFedU. Engineering Sciences 76 123 (in Russian)
[14] Rosenko A P 2008 Mathematical modelling the influence of internal threats on the security of confidential information circulating in an automated information system Izvestiya SFedU. Engineering Sciences 85 71 (in Russian)
[15] Shcheglov K A and Shcheglov Yu A 2015 Markov models for information system security threat Journal of Instrument Engineering 58 957 (in Russian)
[16] Shcheglov K A and Shcheglov Yu A 2016 Modeling of information system security threat using approximating functions Journal of Instrument Engineering 59 50 (in Russian)
[17] Magazev A A and Tsyryun V P 2017 Investigation of a Markov model for computer system security threats Model. Anal. Inform. Sist 24 445 (in Russian)
[18] Onn S 2010 Nonlinear discrete optimization (European Mathematical Society)

Acknowledgments
Dr. S. V. Danilova is gratefully acknowledged for careful reading of the manuscript. This research was partially supported by RFBR (project no. 18-07-00526 A).