Performance Modelling and Evaluation of Enterprise Information Security Technologies

Wen Zeng
School of Computing Science
Newcastle University
Newcastle upon Tyne NE1 7RU, U.K.
Email: wen.zeng.wz@gmail.com

Maciej Koutny
School of Computing Science
Newcastle University
Newcastle upon Tyne NE1 7RU, U.K.
Email: maciej.koutny@ncl.ac.uk

Aad van Moorsel
School of Computing Science
Newcastle University
Newcastle upon Tyne NE1 7RU, U.K.
Email: aad.vanmoorsel@ncl.ac.uk

***Abstract*—By providing effective access control mechanisms, enterprise information security technologies have been proven successful in protecting the confidentiality of sensitive information in business organizations. However, such security mechanisms typically reduce the work productivity of the staff, by making them spend time working on non-project related tasks. Therefore, organizations have to invest a signification amount of capital in the information security technologies, and then to continue incurring additional costs.**

In this study, we investigate the performance of administrators in an information help desk, and the non-productive time (NPT) in an organization, resulting from the implementation of information security technologies. An approximate analytical solution is discussed first, and the loss of staff member productivity is quantified using non-productive time. Stochastic Petri nets are then used to provide simulation results.

The presented study can help information security managers to make investment decisions, and to take actions toward reducing the cost of information security technologies, so that a balance is kept between information security expense, resource drain and effectiveness of security technologies.

Keywords*—*Non-productive Time, Queuing Theory, Stochastic Petri Nets, Security Investment Decision, Information Security Technology.

I. Introduction

Many organizations have to maintain sensitive information or documents that can only be accessed by authorized personnel; for example, personal health records in medical centers, and bank account details in financial organizations. Confidential information leakage and sensitive information distortion have been identified as one of the major information security threats that cause reputation damage, identity theft, and can even undermine the viability of the company [1]. It is therefore essential that companies and organizations keep such information and documents safe. Enterprise information security technologies (e.g., USB access control solutions and digital rights management software) have been developed to address these concerns, for example, by using encryption to restrict the access to protected document.

It is generally accepted that organizations have to invest a signification amount of capital and continue to incur operational expenditure in the area of enterprise information security technologies. Moreover, since these technologies do have negative effects on the efficiency of the organization, it is necessary to demonstrate that the benefits arising from their introduction exceed the costs of the information security investment.

Information security research has been traditionally focused on the technologies and products; for example, the architecture of the system, access control policies, and the functionality of the products. Nowadays, however, human behaviour has been identified as one of the critical factors that determine the effectiveness of security measures, and information security technologies can clearly impact the users in a negative way [2], [3].

Information security technologies use access control measures (e.g., usernames and passwords) to limit unauthorized use of data resources. However, due to various reason, even authorized users might be unable to open a protected resource they want to access. In such a case, they need to seek help from the administrators employed by an organization. In this paper, we will investigate performance both of the service provision and human administrators in the organization, and the productivity loss resulting from the implementation of information security technologies.

There exist different methods for addressing security investment decision; for example, Beres et al. [4] and Beresnevichiene et al. [5] used mathematical models and stochastic simulations to examine the effectiveness of security operation processes and protection mechanisms. Beautement et al. [6] proposed to use economic models based on trade-off between information confidentiality, integrity and availability in order to assess the effectiveness and value of security investment in an information system. However, none of them considered the cost of the administrators in the information help desk and the non-productive time (NPT) in the organization. Zeng et al. [7], [8], [9] proposed to use non-productive time (NPT) as a standard tool to analyze the productivity loss, and the firing delay of stochastic Petri nets to quantitatively evaluate the NPT when implementing Digital Right Management (DRM) products in the organization's network. [9] indicted that an important advantage of the implementation of an information security technology is the reduction of unauthorized attempts to access data resources, and NPT is an important intangible

cost of the organization. Zeng and Koutny [10] proposed a formal model to capture the data loss (cost) in dynamic environments. However, none of these studies analyzed the performance and cost of administrators.

The main aim of the study reported in this paper is to consider the trade-off between performance and security when implementing information security technologies in the organization's network. Firstly, an approximate analytical model of the information security system comprising a server and an administrator is proposed and evaluated using queuing theory. A non-productive time (NPT) function for implementing information security technologies is also given. Moreover, a simulation model based on stochastic Petri nets is proposed and evaluated. Secondly, we consider the case of multiple administrators and provide suitable analytical and simulation models which are then compared. Thirdly, a cost function is proposed to analyze the effect of varying the number of administrators in the information system. This study can help an information security manager to estimate the necessary number of administrators providing system support, and the service capacity that has to be guaranteed by the organization in order to satisfy a given number of users.

II. Implementing Information Security Technologies

In [11], the authors survey the existing enterprise technologies that control access to confidential digital data (e.g., USB access control solutions, digital rights management software, and disk encryption techniques). The researched technologies use endpoint access control as a means of limiting the maintenance overhead introduced by unauthorized devices. The technologies are installed from a centralized security station, sending client-side installations directly to user workstations. They provide auditing options and prevent outsider access through encryption. The various information security solutions follow a model of centralized control, where access policies are recorded at a single location from which they are passed to end users when they interact with the network, and administrators have the highest access rights. The various information security measures rely on the cooperation of various people and system components, thus carrying them out has an impact on the overall productivity of the organization.

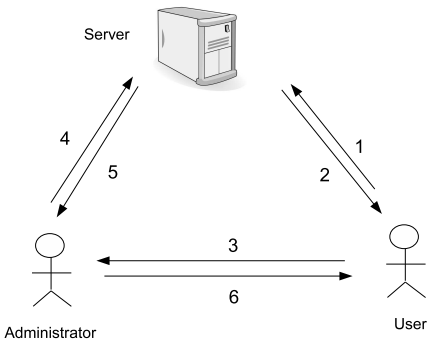

Fig. 1. Relationships between administrators, users and servers.

Figure 1 shows a possible model representing the relationships between users, administrators and servers when implementing information security technologies in the organization's network: (1) When a user tries to access resource, a request is sent to the server. (2) The server attempts to validate the user and, if the user does not pass the authentication procedure, the user is denied the access the resource. (3) If the access is denied, the user contacts the administrator asking for help. (4) The administrator contacts the server. (5) If the user should be allowed to access the resource, the administrator creates the appropriate access rights for the user, or changes the usage policy for this user in the server. (6) Finally, the administrator sends the access rights to the user.

In our models and experiments presented in the rest of this paper, we have adopted a simplified version of the model depicted in Figure 1.

III. Petri nets and Stochastic activity network

Petri nets are a graphical modelling tool for a formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion and conflict [12]. In particular, they have been widely used for structural modelling of work-flows and have been applied in a wide range of qualitative and quantitative analyzes [12], [13], [14], [15].

A basic Petri net N consists of two types of nodes, Pl and Tr, respectively called *places* and *transition*, a set $F \subseteq (Pl \times Tr) \cup (Tr \times Pl)$ of *arcs* that connect the nodes, and the initial marking $M_0 : Pl \to \mathbb{N}$ which is a mapping from the set of places to the set $\mathbb{N}$ of all non-negative integers.

Input arcs start at places and end at transitions, while *output arcs* start at transitions and end at places. Places can contain *tokens*, which are used to simulate the dynamic and concurrent activities of the system modelled by the net. The current state of the modelled system (a *marking*) is given by the number of tokens in each place.

Transitions are the active components of the net. When a transition is executed (or *fired*), it consumes tokens along its input arcs, and produces tokens along its output arcs. The resulting movement of the tokens changes the states of the system. A transitions is only allowed to fire when it is *enabled*, which means that each input place holds at least one token.

One can associate a firing delay with each transition of a Petri net; such a delay specifies the time that the transition has to be enabled before it can actually fire. If the delays are given by a random distribution function, we obtain a stochastic Petri net.

Stochastic Activity Networks (SANs) are a class of stochastic Petri nets [16]. SANs consist of four primitive objects: *places, transitions, input gates* and *output gates*. A place represents a local state of the modelled system; a transition represent an action that take some specified amount of time to complete; input gates are used to control the enabling of activities and define the marking changes that will occur when an activity completes; and output gates are used to define the marking changes that will occur when activities complete (in particular, one can specify a probability with which a token is produced and deposited in an output place).

A. Reward Models

Reward models are used to specify measures of system behaviour [17]. A reward model has two different reward

components: one is concerned with 'rate rewards', that is, the rate at which reward accumulates while the process is in a specified set of markings during an interval of time; and the other is concerned with 'impulse rewards', based on the count of the number of times a transition fires during an interval of time.

The functions used to capture the transition and marking based rewards in a SAN, with places Pl and transitions Tr, are given as follows:

- $\mathcal{C} : Tr \to \mathbb{R}$. For each $a \in Tr$, $\mathcal{C}_a$ denotes the reward obtained due to the completion of transition a.
- $\mathcal{R} : \mathcal{P}(Pl, \mathbb{N}) \to \mathbb{R}$, where $\mathcal{P}(Pl, \mathbb{N})$ is the set of all partial functions from Pl to $\mathbb{N}$. For each $v \in \mathcal{P}(Pl, \mathbb{N})$, $\mathcal{R}_{(v)}$ denotes the rate of reward obtained when there are n tokens in place pl, for every $(pl, n) \in v$.

Impulse rewards are associated with transition completion (via $\mathcal{C}$) and rates rewards are associated with the number of tokens in sets of places (via $\mathcal{R}$):

$$Y_{[t,t+l]} = \sum_{v \in \mathcal{P}(Pl,\mathbb{N})} \mathcal{R}_{(v)} M^{v}_{[t,t+l]} + \sum_{a \in Tr} \mathcal{C}_a N^{a}_{[t,t+l]}$$

In the above, the reward accumulated is related to the number of times each transition completes and time spent in particular markings, during a time interval $[t, t+l]$. For every $v \in \mathcal{P}(Pl, \mathbb{N})$, $M^{v}_{[t,t+l]}$ represents the total time during the interval $[t, t+l]$ that the SAN is in markings such that there are n tokens in pl, for each $(pl, n) \in v$. For each $a \in Tr$, $N^{a}_{[t,t+l]}$ represents the number of completions of transition a during the interval $[t, t+l]$.

IV. Queuing Network Model

Figure 2 shows an information security system modelled by a simple queuing system with two queue stations (the server and the administrator).

In the system, each user's request is assumed to have a duration specified by a negative exponential distribution with a given mean: $1/r_u$ is the frequency for a user send an access request, $1/r_{ser}$ is the average time it takes the server to serve a user's request, and $1/r_a$ is the average time it takes the administrator to help a non-active user. N is the maximum number of users admitted for processing. If there are more than N requests present, the ones that do not occupy a thread wait in an external FIFO queue.

In the diagram, p $(0 < p \leq 1)$ is the probability that a user can pass the user authentication procedure on the server and become an active user, $1-p$ is the probability that a user cannot pass the user authentication and becomes an non-active user who needs help from the administrator.

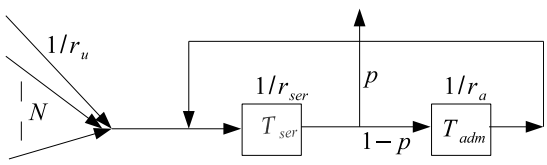

Fig. 2. A queuing theory model of an information security system.

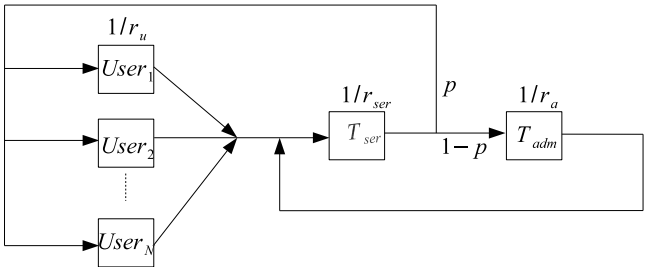

Fig. 3. A closed queuing theory model of an information security system.

When the external queue is non-empty, the system behaves like a closed queuing network (Figure 3), with N requests circulating between the users and the system.

V. Approximate Analytical Solution

Let us assume that there are k user requests circulating between the server and the administrator $(k = 1, \ldots, N)$. Suppose that the circulation continues for a long time, i.e. the system reaches a steady state with k user requests. Then the server queue would behave like an $M/M/1$ queue with a bounded buffer of size k. The load ρ_{ser} on the server is:

$$\rho_{ser} = \frac{r_u k}{r_{ser} p} \tag{1}$$

Using the existing results [18] for the $M/M/1/k$ queue yields the average number of requests in the server:

$$L_{ser} = \frac{\rho_{ser}}{1-\rho_{ser}} \times \frac{1-(k+1)\rho^{k}_{ser} + k\rho^{k+1}_{ser}}{1-\rho^{k+1}_{ser}} \tag{2}$$

The steady state probability Π_k that there are exactly k requests waiting for a response from the server is:

$$\Pi_k = \frac{(1-\rho_{ser})\rho^{k}_{ser}}{1-\rho^{k+1}_{ser}} \tag{3}$$

Therefore, the state-dependent throughput of the server when there are k requests in it, T_{ser}, is given by:

$$T_{ser} = (1-\Pi_k) \times \frac{r_u k}{p} = \frac{1-\rho^{k}_{ser}}{1-\rho^{k+1}_{ser}} \times \frac{r_u k}{p} \tag{4}$$

The probability U_{ser} that the server is busy, given that there are k requests in the system is:

$$U_{ser} = \frac{T_{ser}}{r_{ser}} = \frac{1-\rho^{k}_{ser}}{1-\rho^{k+1}_{ser}} \times \frac{r_u k}{r_{ser} p} \tag{5}$$

The average response time, W_{ser}, of a request that is admitted into the server can be found from Little's theorem:

$$W_{ser} = \frac{L_{ser}}{T_{ser}} \tag{6}$$

The entire system is in a steady state. Thus, the load on the administrator, ρ_{adm} is:

$$\rho_{adm} = \frac{(1-p) r_u k}{r_a p} \tag{7}$$

Therefore, the state-dependent utility of the administrator when there are k requests in the system, T_{adm}, is given by:

$$U_{adm} = \frac{1-\rho^{k}_{adm}}{1-\rho^{k+1}_{adm}} \times \frac{(1-p) r_u k}{r_a p} \tag{8}$$

and the average number of requests on the administrator is given by [18]:

$$L_{adm} = \frac{\rho_{adm}}{1-\rho_{adm}} \times \frac{1-(A+1)\rho_{adm}^{A} + A\rho_{adm}^{A+1}}{1-\rho_{adm}^{A+1}} \quad (9)$$

where, $A = (1-p)k$.

The average response time, W_{adm}, of a request that is admitted into the administrator can be found from Little's theorem:

$$W_{adm} = \frac{L_{adm}}{T_{adm}} \quad (10)$$

The non-productive time (NPT) in the organization is the average number of requests in the server and administrator in an interval of time:

$$NPT = (\frac{L_{ser}}{r_q} + L_{ser} + L_{adm}) \times l \quad (11)$$

where l is the period of time users spend in the system, and $1/r_q$ is the average time taken by a user to send an access request.

A. Comparing Analytical and Simulation Results

We have compared the above approximate analytical solution with simulation results obtained using the Möbius system [16]. The performance of the system under different loading conditions and parameter settings was examined in a series of numerical and simulation experiments. The main purpose of the simulations was to evaluate the accuracy of the analytical solution and, at the same time, to validate the modelling technique based on stochastic Petri nets.

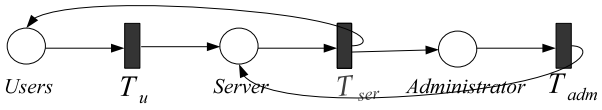

Fig. 4. A stochastic Petri nets model of an information security system. Informally, the middle transition produces a token with in one of the two output places with probabilities p and $1-p$, respectively.

Figure 4 shows the structure of a stochastic Petri nets model representing information security scenario we discussed above. The model consists of three places and three timed transitions. Timed transitions are associated with random exponential distributed firing delays. Authorized *Users* try to access protected resources every $\frac{1}{r_u}$ unit time, each attempt taking $\frac{1}{r_q}$ units of time. We use T_u to control the frequency of access requests sent to the *Server* by a user. The time taken to access the protected resources is given by T_{ser}. If the user can pass the authentication process, then the user can use the resource, but if the user cannot access the resource, the user has to contact the *Administrator* for help. After obtaining such help (the time taken is given by T_{adm}), the user can try to access the resource again.

The behaviour of the model can be measured by the *impulse rewards model* and *rate rewards model*, which are supported by the Möbius software. The throughput of a transition is computed according to the formula which is described in Section III, $\sum_{a \in Tr} \mathcal{C}_a N^a_{[t,t+l]}$. The number of tokens in sets of places is computed according to the formula $\sum_{v \in \mathcal{P}(Pl,\mathbb{N})} \mathcal{R}_{(v)} M^v_{[t,t+l]}$. The time scale of the model is expressed in minutes, i.e., when we run the model one time unit in Möbius represents one minute in real working time.

To measure the throughput of the server, the throughput of a transition per unit of time T_{ser} was computed in average interval of time, and then we could calculate the utility of the server by using the equation (5). To measure the throughput of the administrator, the throughput of the transition per unit of time T_{adm} was computed in average interval of time, and then we could calculate the utility of the administrator by using the equation (8).

As the number of the parameters is quite high, some of them were kept fixed throughout. These were: the probability that a user passes the authentication procedure ($p = 0.7$); the average time a user needs to send an access request ($\frac{1}{r_u} = 100$); and the average time it takes a user to send a request ($\frac{1}{r_q} = 0.25$).

Figure 5 shows the utility of the server against the number of users for both the simulation and approximate analytical approaches for various values of r_{ser} and r_a. Increasing the value of r_{ser} and r_a corresponds to increasing the speed of user access to the resource.

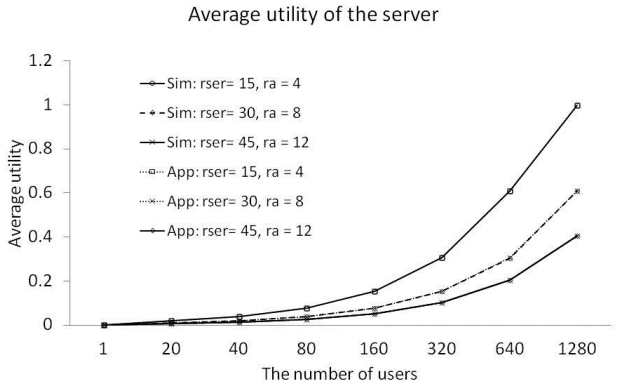

Fig. 5. Utility of the server w.r.t. the number of users in the system. $p = 0.7$, $\frac{1}{r_u} = 100$. The utility increases significantly when the number of users served by the server and administrator increases.

Figure 6 shows the utility of the administrator against the numbers of the users for both the simulation and approximate analytical approaches for various values of r_{ser} and r_a. The results show that there are obvious benefits from increasing the server and administrator speed. If the target utilization of the administrator is 0.72, with $r_{ser} = 15$ and $r_a = 4$ one can serve at most 640 users. After increasing the server rate and administrator's service rate to respectively $r_{ser} = 30$ and $r_a = 8$, the utility of the administrator can increase to 0.71, which is close to the target with 1280 users.

Let us now consider one year of work after the deployment of the information security technologies in the network system of an organization, i.e., we consider 96000 time units in the stochastic Petri net model (this corresponds to 40 weeks of work, each working week having 40 working hours). To measure the NPT, the time users spend in any place other than

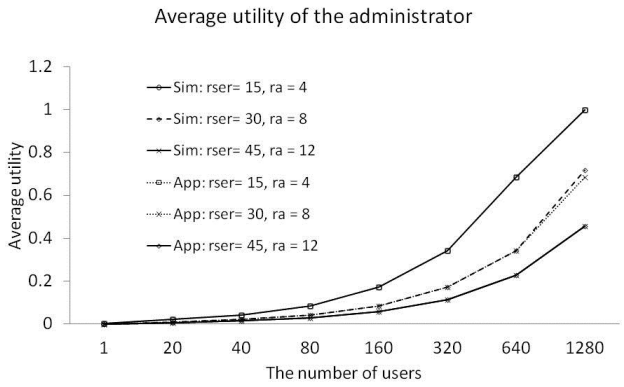

Fig. 6. Utility of the administrator w.r.t. the number of users in the system. $p = 0.7, \frac{1}{r_u} = 100$. The utility increases significantly when the number of users served by the server and administrator increases.

Users is computed. The NPT also includes the time the user takes for sending an access request ($\frac{1}{r_q}$).

Figure 7 shows the NPT of the system w.r.t. the number of users for various values of r_{ser} and r_a. Increasing the value of r_{ser} and r_a is equivalent to increasing the speed of users access to the resource. The NPT includes: the time spent on sending an access request and authentication procedures, and the time spent on waiting for a response from administrator.

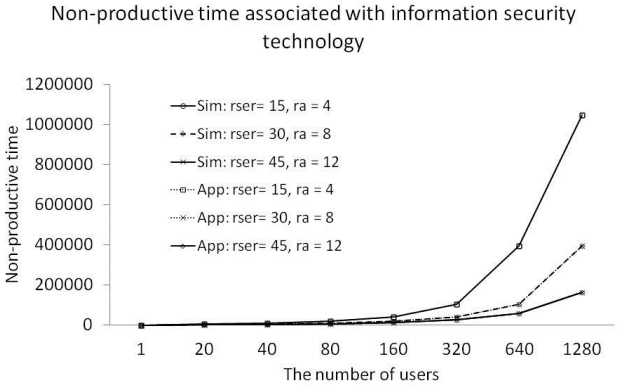

Fig. 7. Total non-productive time (NPT) associated with the deployment of information security technologies. $p = 0.7, \frac{1}{r_u} = 100$. NPT increases significantly when the number of users served by the system increases.

If the target maximum NPT is 120000 time units, one can try to build the system with $r_{ser} = 15$ and $r_a = 4$. Then the system can serve 320 users and the NPT is around 102653 time units which is below the target. However, if we increase the rates to $r_{ser} = 30$ and $r_a = 8$, the system can serve 640 users and the NPT is around 102669 time units.

VI. Multiple Administrators

In the above, we proposed an approximate analytical model for implementing information security technologies. We considered one server and one administrator. In what follows, we consider multiple administrators who provide help with access control problems.

We assume that there are K administrators, each of which can serve one user request at a time, independently of the others (Figure 8). We want to know if it is beneficial to increase the number of administrators, or to increase the operational speed of the administrators. It is well known that for an $M/M/K$ queue, it is preferable to have one administrator serving at the rate μ rather than K administrators serving at the rate μ/K [18]. This is because if there are fewer than K requests in the queue, then some of the administrators will be idle, thus reducing the overall service rate.

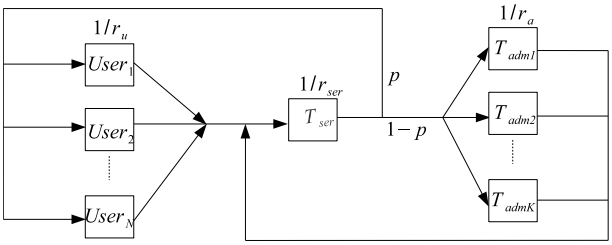

Fig. 8. A closed queuing theory model of an information security system, with *N* users and *K* administrators.

Consider first the administrator subsystem, with j requests circulating between the server and administrators, $j = 0, 1, \ldots, (1-p)N$, where N is the maximum number of user requests, and p is the probability that a user can pass the user authentication on the server.

Suppose that the circulation continues for a long time and the subsystem reaches a steady state with j requests. If there is one administrator in the system and j user requests in the subsystem, the approximation becomes an $M/M/1/./A$ queue ($A = (1-p)N$). Hence the balance equations become [18]:

$$(A-j)r_u\Pi_j = r_a\Pi_{j+1}, \quad 1 \le j \le A \tag{12}$$

where Π_j is the steady state probability that there are exactly j user requests waiting for a response from the administrator.

Now we increase the number of parallel administrators in the model. The model becomes an $M/M/K/./A$ queue, where K is the number of administrators. Therefore, the balance equations become [18]:

$$(A-j)r_u\Pi_j = (j+1)r_a\Pi_{j+1}, \quad 0 \le j < K \tag{13}$$

$$(A-j)r_u\Pi_j = Kr_a\Pi_{j+1}, \quad K \le j < A \tag{14}$$

We can calculate Π_0:

$$\Pi_0 = \left[\sum_{j=0}^{K-1}\frac{A!\rho^j}{(A-j)!j!} + \sum_{j=K}^{A}\frac{A!\rho^j}{(A-j)!K!K^{j-K}}\right]^{-1} \tag{15}$$

The average queue length can then be calculated by [18], [19]:

$$\begin{aligned} L_{adm} &= \sum_{j=1}^{A} j\Pi_j \\ &= A!\Pi_0\left[\sum_{j=1}^{K-1}\frac{\rho^j j}{(A-j)!j!} + \sum_{j=K}^{A}\frac{\rho^j j}{(A-j)!K!K^{j-K}}\right] \end{aligned}$$

Each of the users submits requests to administrators at the rate $\frac{(1-p)r_u}{p}$. Therefore, the throughput T_{adm} is [18]:

$$T_{adm} = (A - L_{adm})\frac{r_u A}{p} \tag{16}$$

and the average response time of administrators, W_{adm}, becomes:

$$W_{adm} = \frac{A}{T_{adm}} - \frac{p}{r_u A} \tag{17}$$

The non-productive time (NPT) in the organization can be calculated using the equation (11).

A. Comparing Analytical and Simulation Results

We again used the Möbius software [16], [20] to simulate the behaviour of the approximate analytical model, and to compare the simulation and analytical results.

Figure 9 shows the structure of a stochastic Petri net for the analytical model we have just discussed, which consists of five places, four timed transitions, and one instantaneous transition. Authorized *Users* try to access resources every $\frac{1}{r_u}$ time units during working hours (the time taken is given by T_{ser}). If the user cannot access the resource, administrators are contacted for help. Here we use T_{help} to control the probability with which the users are handled by different administrators. There are eight administrators (*Adm1*, . . ., *Adm8*), each of which can serve one user request at a time, independently of the others. The throughput and average response time can be computed as in Section V-A.

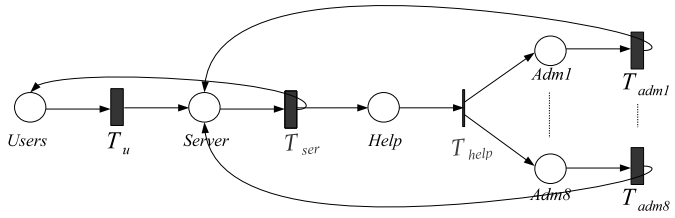

Fig. 9. A stochastic Petri nets model of an information security system with eight administrators. Note that the 'thin' transition with eight output places takes no time to execute, i.e. it is instantaneous.

As before, some parameters were kept fixed: the probability that a user passes the authentication procedure ($p = 0.7$); the frequency with which a user sends access requests ($\frac{1}{r_u} = 100$) (i.e., a user sends a request every 100 time units); and the average time it takes for a user to send an access request ($\frac{1}{r_q} = 0.25$).

Figure 10 shows the average load on the administrators against the number of users for $K = 8$ with $r_a = 0.5$, and $K = 4$ with $r_a = 1$.

Figure 11 shows the average response time of the administrators w.r.t. the numbers of user for $K = 8$ with $r_a = 0.5$, and $K = 4$ with $r_a = 1$.

Consider now one year of the deployment of the information security technology in the network system, i.e., 96000 time units in the stochastic Petri net model.

Figure 12 shows the NPT of the system w.r.t. the numbers of users for $r_a = 0.5$ with $K = 8$, and $r_a = 1$ with $K = 4$. NPT increased significantly when the service speed of the administrators is slow; in other words, increasing the speed of the administrators reduces the NPT of the staff members in the organization.

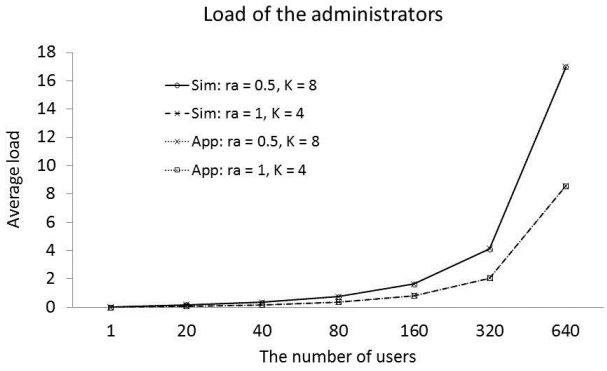

Fig. 10. Average load on the administrators w.r.t. the number of users in the system. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15$.

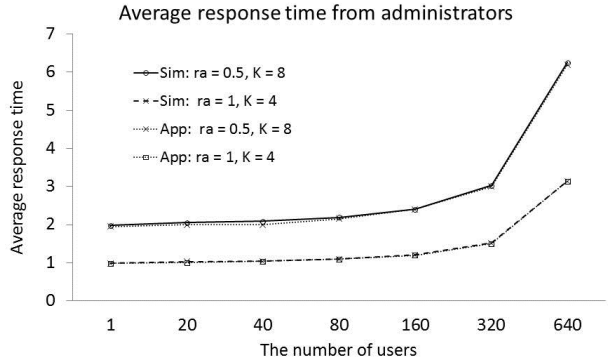

Fig. 11. Average response time of the administrators w.r.t. the number of users in the system. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15$.

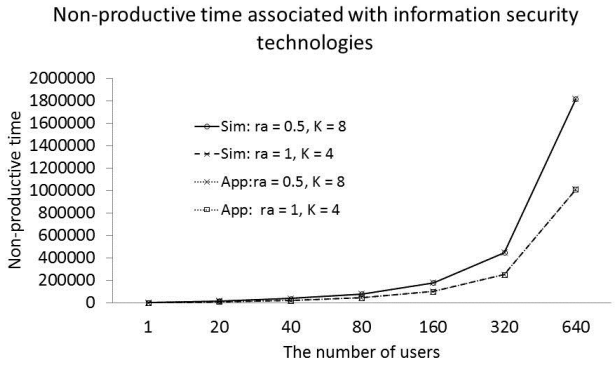

Fig. 12. Total non-productive time (NPT) associated with the deployment of information security technologies. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15$.

Figure 13 shows the NPT of the system w.r.t. the number

of administrators with 400 users in the system. The system reaches a steady state with five administrators in the system. Increasing the number of administrators will reduce the NPT in the organization. However, the administrators will often be idle in such a case.

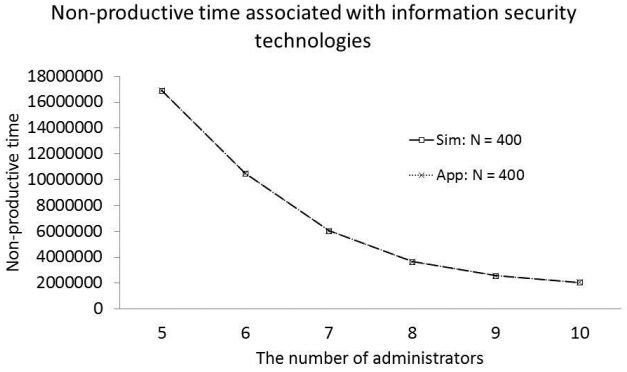

Fig. 13. Total non-productive time (NPT) associated with the deployment of information security technologies. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15, N = 400, r_a = 0.25$.

VII. The Cost Model for Administrators

Now we introduce a cost function which needs to be optimized. This function is based on the assumption that there is a cost of the users' waiting time and a competing cost of providing resources, e.g., salaries of administrators, and administrators' training expenditure. This gives rise to the following simple cost function [18], [19]:

$$C = c_1 L_{adm} + c_2 K r_a, \quad c_1, c_2 \geq 0 \tag{18}$$

The cost rates $c_i (i = 1, 2)$ are non-negative constant, which are dependent on the particular system, or depend on the type of quality of service contract that is in place. If c_1 is large, in order to keep the total cost C low, L_{adm} should be small [18]. At the same time, if c_2 is large, in order to keep the total cost C low, Kr_a should be small [18]. However, the coefficients $c_i (i = 1, 2)$ are not necessarily optimal, because the load of the administrators also plays a key role in determining the best strategy, since the service time and the number of administrators also influence the load of the administrators. In general, if the organizations want to improve the responsiveness of the system, they would increase c_1, and if they want to minimize running costs, they would increase c_2.

A. Analytical Results

We now illustrate the cost function we proposed above using the previous analytical results. Figure 14 shows the cost w.r.t. the number of users. It is clear that under the parameter values with $r_a = 0.25$, the cost rises rapidly at around 320 users, which is the approximate maximum capacity the administrators can handle before the performance starts to degrade. Under the parameter values with $r_a = 0.5$, the cost rises at around 640 users. Therefore, doubling the service rate from $r_a = 0.25$ to $r_a = 0.5$ effectively doubles the capacity of the system. In a small system, when $N < 320$, the cost function is dominated by $c_2 K r_a$. Therefore, the cost is greater for faster administrators. The reason is that the administrators will often be idle, and the system is not making efficient use of resources.

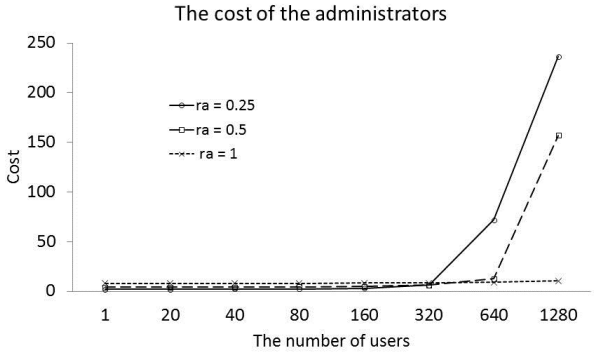

Fig. 14. The cost w.r.t. the number of users calculated by the queuing network model. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15, K = 8, c_1 = 0.5, c_2 = 1$.

Figure 15 shows the cost w.r.t. the number of users. It is easy to see, under the parameter values with $r_a = 0.25$, the cost rises rapidly at around 320 users for all cases ($c_2 = 0.1, 1, 10$).

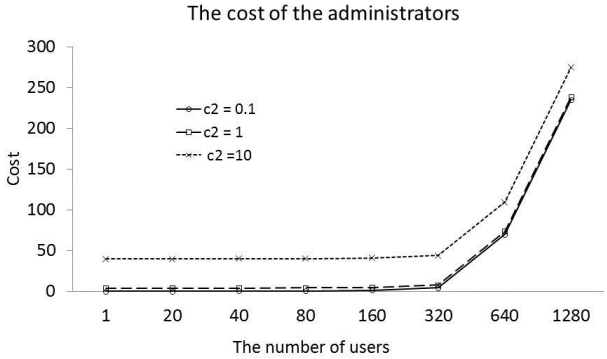

Fig. 15. The cost w.r.t. the number of users calculated by the queuing network model. $p = 0.7$, $\frac{1}{r_u} = 100, r_{ser} = 15, K = 8, r_a = 0.25, c_1 = 0.5$.

Figure 16 shows the cost w.r.t. the number of administrators in the system. In this experiment, the number of users is fixed. The larger c_2 results in a decreasing cost before the optimal point and an increasing rate after the point. For 400 users, in the case of $c_2 = 1$ the optimal value is $K = 17$, which gives the minimal cost of 9.62. In the case of $c_2 = 10$ the optimal value is $K = 10$, which gives the minimal cost of 35.29. When information security managers make the trade-off between security and cost, the balance point here is the value of K where the cost is minimal. Therefore, the security manager could choose $K = 17$ and $K = 10$ when $c_2 = 1$ and $c_2 = 10$, respectively.

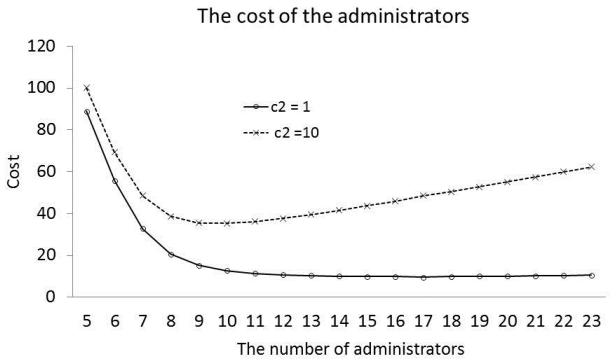

Fig. 16. The cost w.r.t. the number of administrators. $p = 0.7, \frac{1}{r_u} = 100, r_{ser} = 15, N = 400, r_a = 0.25, c_1 = 0.5$.

VIII. Conclusions

In this paper, we provided an approximate analytical model for investigating different implementations of information security technologies. We have also provided a corresponding simulation model based on stochastic Petri nets. The two approaches have been compared through a series of experiments which demonstrated that the results they can supply are very similar. Hence one can conclude that the approximate analytical solution is sound. Moreover, we can conclude that the simulation technique based on stochastic Petri nets can be relied upon when it comes to the evaluation of, e.g., productivity loss caused by the introduction of security technologies. In future we plan to apply it to system organizations which extend the simple scenarios captured by Figure 1; in particular, those that involve a hierarchy of servers and administrators.

We proposed functions to estimate the non-productive time (NPT) in an organization resulting from the implementation of security technologies, and the cost function for the administrators in the information help desk.

Queuing theory was used to numerically analyze the implementaion of information security technologies, and stochastic Petri nets were used to simulate the approach. The effect of several controllable parameters on the performance of the system was examined in a series of numerical and simulation experiments. Such a study can help information security managers to make information security investment decision.

IX. Acknowledgements

We would like to thank the referees for their comments and useful suggestions. This research was supported by the 973 Program Grant 2010CB328102, NSFC Grant 61133001, and EPSRC UNCOVER project.

References

[1] A. Dolya, "Internal it threats in europe 2006," 2006. [Online]. Available: http://www.securelist.com/en/analysis?pubid=204791935

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999. [Online]. Available: http://doi.acm.org/10.1145/322796.322806

[3] B. Schneier, *Secrets and lies: digital security in a networked world*. New York: Wiley Computer Publishing, 2000.

[4] Y. Beres, J. Griffin, S. Shiu, M. Heitman, D. Markle, and P. Ventura, "Analysing the performance of security solutions to reduce vulnerability exposure window," in *Proceedings of the 2008 Annual Computer Security Applications Conference*, ser. ACSAC '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 33–42. [Online]. Available: http://dx.doi.org/10.1109/ACSAC.2008.42

[5] Y. Beres, D. Pym, and S. Shiu, "Decision support for systems security investment," *Manuscript, HP Labs*, 2010.

[6] A. Beautement, R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, A. Sasse, and M. Wonham, "Modelling the human and technological costs and benefits of usb memory stick security," in *Managing information risk and the economics of security*, M. E. Johnson, Ed. Boston, MA: Springer US, 2009, pp. 141–163.

[7] W. Zeng and A. van Moorsel, "Quantitative evaluation of enterprise drm technology," *Electron. Notes Theor. Comput. Sci.*, vol. 275, pp. 159–174, Sep. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.entcs.2011.09.011

[8] W. Zeng and K. Liu, "Sensitivity analysis of loss of corporate efficiency and productivity associated with enterprise drm technology," in *ARES*, 2012, pp. 445–453.

[9] W. Zeng, K. Liu, and M. Koutny, "Cost-benefit analysis of digital rights management products using stochastic models," in *SpringSim (ANSS)*, 2013, p. 1.

[10] W. Zeng and M. Koutny, "Data resources in dynamic environments," in *TASE*, 2014.

[11] S. E. Parkin, R. Y. Kassab, and A. van Moorsel, "The impact of unavailability on the effectiveness of enterprise information security technologies," in *Proceedings of the 5th international conference on Service availability*, ser. ISAS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 43–58. [Online]. Available: http://dl.acm.org/citation.cfm?id=1788594.1788603

[12] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, *Modelling with generalized stochastic Petri Nets*. Wiley Series on Parallel Computing, 1995.

[13] N. R. Adam, V. Atluri, and W.-K. Huang, "Modeling and analysis of workflows using petri nets," *J. Intell. Inf. Syst.*, vol. 10, no. 2, pp. 131–158, Mar. 1998. [Online]. Available: http://dx.doi.org/10.1023/A:1008656726700

[14] K. Salimifard and M. Wright, "Petri net-based modelling of workflow systems: An overview," *European Journal of Operational Research*, vol. 134, no. 3, pp. 664 – 676, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0377221700002927

[15] W. M. P. van der Aalst, "The application of petri nets to workflow management," *The Journal of Circuits, Systems and Computers*, vol. 8, pp. 21–66, 1998.

[16] W. H. Sanders, "Möbius user manual," 2013.

[17] W. H. Sanders and J. F. Meyer, *A unified approach for specifying measures of performance, dependability, and performability*. Springer-Verlag, 1991, vol. 4, pp. 215–237.

[18] I. Mitrani, *Probabilistic Modelling*. Cambridge university press, 1998.

[19] Y. Zhao and N. Thomas, "Efficient solutions of a pepa model of a key distribution centre," *Perform. Eval.*, vol. 67, no. 8, pp. 740–756, 2010.

[20] D. D. Deavours and W. H. Sanders, "Möbius: Framework and atomic models," in *Proceedings of the 9th International Workshop on Petri Nets and Performance Models (PNPM'01)*, ser. PNPM '01, 2001, pp. 251–260.