Modelling and Analysis of Corporate Efficiency and Productivity Loss Associated with Enterprise Information Security Technologies

Wen Zeng[1] and Maciej Koutny[2]

[1]*School of Computer Science and Informatics, De Montfort University*
Leicester LE1 9BH, U.K.
Email: wen.zeng.wz@gmail.com
[2]*School of Computing, Newcastle University*
Newcastle upon Tyne NE1 7RU, U.K.
Email: maciej.koutny@ncl.ac.uk

Abstract

By providing effective access control mechanisms, enterprise information security technologies have been proven successful in protecting the 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 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. Moreover, sensitivity analysis is applied to develop a cost-effective strategy for mitigating the negative impact of implementing information security technologies. 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: access control, non-productive time, queuing theory, stochastic Petri nets, security investment decision

1. 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 centres, and bank account details in financial organizations. Sensitive information leakage and 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 (Dolya (2006)). 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 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 (Adams and Sasse (1999); Schneier (2000); Kirlappos and Sasse (2014); Sasse et al. (2016); Beautement et al. (2016)).

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 enterprise information security technologies, especially we focus on the impact of failed access control in the organization.

There exist different methods for addressing security investment decisions; for example, Beres et al. (2008, 2010) used mathematical models and stochastic simulations to examine the effectiveness of security operation processes and protection mechanisms. Beautement et al. (2009) 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 administrators in the information help desk and the productivity loss in the organization. Parkin et al. (2008) indicated that the unavailability of system components and staff members would bring productivity loss in the organization. However, the measurement of productivity loss is very vague in this study. Reinecke et al. (2010) proposed a framework for the definition of benefit-based adaptivity metrics. However, they did not consider the metrics to evaluate the productivity loss. In addition, Wolter and Reinecke (2010) present standard performance metrics and discuss proposed security metrics that are suitable for quantification. However, the authors only considered the metrics to evaluate the server components, they did not consider the users. Zeng and van Moorsel (2011) 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. Zeng (2019) 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. 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. An 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. Fourthly, sensitivity analysis is applied to determine which of the parameters exerts the most influence on the NPT of the organization. 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.

This document is organized as follows: Section 2 will introduce the working mechanism of the enterprise information security technologies; Section 3 will present a queuing network model to analyse the implementation of information security technologies; Section 4 is an approximate solution of the system comprising the server and an administrator in the information help desk; Section 5 is background on stochastic activity networks; Section 6 is a stochastic activity network model for information security technologies; Section 7 will analyse the value of variables in the model and the sensitivity of non-productive time of the system; Section 8 will compare the approximate analytical solution with simulation results; Section 9 will analyse multiple administrators in the system; A cost function will be proposed in Section 10 to analyse the information help desk; Section 11 is the conclusions.

2. The Implementation of Information Security Technologies

Parkin et al. (2008) 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.

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 a 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 administrator asking for help. (4) The administrator contacts the server. (5)

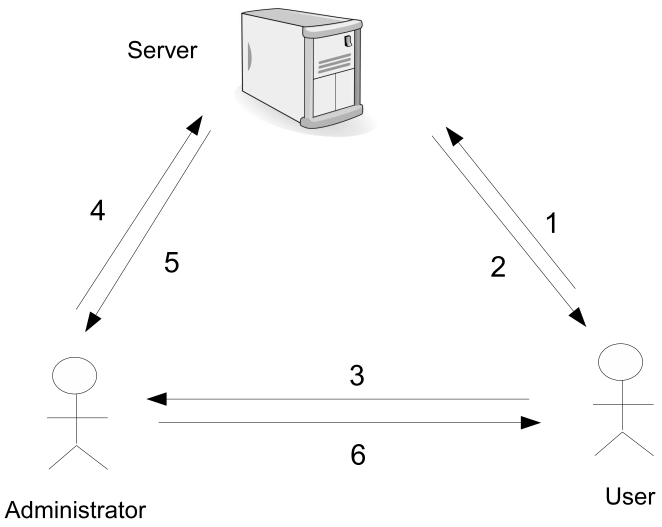

Figure 1: Relationships between administrators, users and servers.

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.

3. Queuing Network Model

In this section, we will introduce a queuing network model to describe the relationship between users, administrators and servers. Queuing network models is an important tools in design and analysis of computer systems, due to the fact that, queuing network models achieve a favourable balance between accuracy and efficiency (Mitrani (1998)).

Figure 2 shows an enterprise information security system modelled by a simple queuing system with two queue stations – a single server T_{ser} and a single administrator T_{adm}. User's request arrive at the server, wait in the *queue* if necessary, receive service from the server, and depart.

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 first in first out 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.

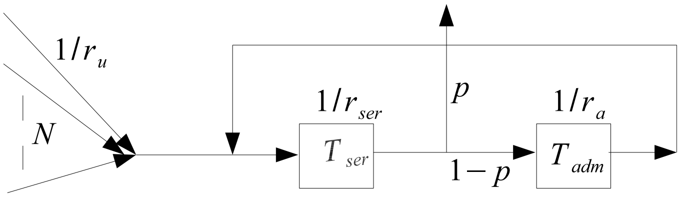

Figure 2: A queuing theory model of an information security system.

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.

4. 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

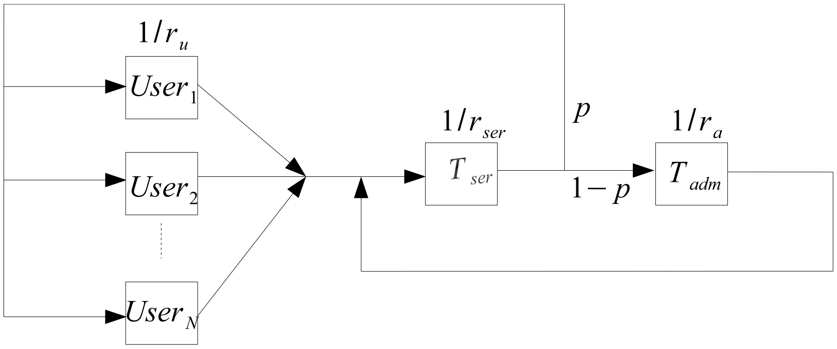

Figure 3: A closed queuing theory model of an information security system.

a bounded buffer of size k. Therefore, the frequency for users send access requests in the system is $\frac{k}{r_u}$.

The load ρ_{ser} on the server is:

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

Using the existing results (Mitrani (1998)) for the $M/M/1/k$ queue yields the queue length (the average number of requests, both waiting and receiving service) in the server:

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

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

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

Therefore, the state-dependent throughput (the rate at which users pass through the service) of the server when there are k requests in it, T_{ser}, is given by:

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

The utility U_{ser} (the proportion of time the server is busy), given that there are k requests in the system is:

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

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:

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

and the average number of requests on the administrator is given by (Mitrani (1998)):

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

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:

$$W_{adm} = \frac{L_{adm}}{T_{adm}} \tag{10}$$

NPT is the average time taken by users to send the requests, the time of requests queue in server station and administrator station, and the time services provided by the server and administrator during a time interval.:

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

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

5. Petri Nets and Stochastic Activity Network

Queuing theory has been used extensively for the evaluation of computing systems, but their application to systems that exhibit complex concurrency, fault tolerance and degradable performance is not straightforward (Sanders (1988)). Extensions to Petri net, on the other hand, have proved to be valuable tools for evaluation of systems that exhibit these properties. Many of these extensions have included the addition of an explicit representation of time. This permits the representation of both performance and dependability related characteristics, depending on the interpretation given to the tokens in the model.

In this section, we will show the definition of Petri nets and stochastic activity nets which is a class of stochastic Petri nets.

5.1. Petri Nets

Petri nets are a graphical modelling tool for a formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion and conflict (Marsan et al. (1995); Murata (1989)). 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 (Marsan et al. (1995); Salimifard and Wright (2001); van der Aalst (1998)).

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 $M_0 : Pl \rightarrow \mathbb{N}$ 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.

5.2. Stochastic Activity Networks

Stochastic Petri nets extend the classic Petri nets with timing and probability features, and stochastic activity networks (SANs) are a class of stochastic Petri nets (Sanders (1988, 2018)).

SANs consist of four primitive objects: *Activities, places, input gates* and *output gates.* Activities ('transitions' in Petri net terminology) are two types, *timed* and *instantaneous.* Elongated ovals represent *timed activities* and solid bars represent *instantaneous activities.* Timed activities are used to represent activities of the modeled system, whose duration impact the system's ability to perform. Instantaneous activities represent system activities which, relative to performance variable in question, complete in a negligible amount of time. Places are depicted as circles and, as with Petri nets, each place can hold a non-negative number of tokens.

Cases (a generalization of probabilistic arcs) can be associated with both timed and instantaneous activities and are represented by small circles. Cases permit the realization of two types of spatial uncertainty. Uncertainty about which activities are enabled in a given marking is realized by cases associated with intervening instantaneous activities. Uncertainty about the next marking assumed upon completion of a timed activity is realized by cases associated with that activity. Input gates contain both an enabling predicate and input function (on the marking of the places). The enabling predicate must be true for the activity associated with that gate to be enabled. Upon completion of the associated activity, the input function is executed, possibly changing the marking of the net. Output gates have a single output function (on the marking of the places) associated with them, which is executed upon completion of the associated activity.

The stochastic nature of the nets is realized by associating an activity time distribution function with each of the timed activities and a probability distribution with each set of cases.

Reward models are used to specify measures of system behaviour. A reward model consists of a stochastic process and a reward structure. The stochastic process represents the dynamics of the system and can be constructed by hand or, automatically, from some network level description. The reward structure is typically a set of one or more functions defined on the states or transitions between states in the process.

A reward model in SANs 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 an activity fires during an interval of time.

The functions used to capture the activity and marking based rewards in a SAN, with places Pl and activities A, are given as follows:

- $\mathcal{C} : A \to \mathbb{R}$. For each $a \in A$, $\mathcal{C}(a)$ denotes the reward obtained due to the completion of activity a.
- $\mathcal{R} : \mathcal{P}(Pl, \mathbb{N}) \to \mathbb{R}$. For each $v \in \mathcal{P}(Pl, \mathbb{N})$, $\mathcal{R}(v)$ denotes the rate of reward obtained when for each $(pl, n) \in v$, there are n tokens in place pl.

where $\mathbb{N}$ is the set of natural numbers, and $\mathcal{P}(Pl, \mathbb{N})$ is the set of all partial functions from Pl to $\mathbb{N}$.

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

In the following, variable types of the interval category are denoted by 'Y' while variables types of the time-averaged category are denoted by 'W', each with the appropriate subscript. We let

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

$$W_{[t,t+l]} = \frac{Y_{[t,t+l]}}{l}$$

In the above, the reward accumulated is related to the number of times each activity completes and time spent in particular markings, during a time interval $[t, t+l]$.

- $J^{v}_{[t,t+l]}$ is a random variable representing the total time that the SAN is in a marking such that for each $(pl, n) \in v$, there are n tokens in pl during $[t, t+l]$.

- $N^{a}_{[t,t+l]}$ is a random variable representing the number of completions of activity a during the interval $[t, t+l]$.

6. Stochastic Activity Network Model

Figure 4 shows the structure of a stochastic activity network model representing information security scenario we discussed. The model consists of eight places, three timed transitions and three instantaneous 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. Place *Users* contains the users that may arrive to the queue. The tokens in *Users* are the authorized users. We use T_u to control the frequency of access requests sent by a user, thus each completion of activity T_u represents the arrival of a request to the waiting room. Idle servers are represented by

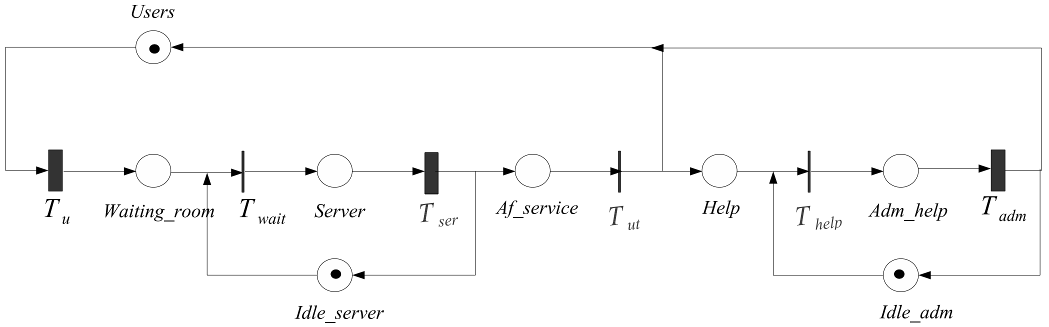

Figure 4: A stochastic activity network model of an information security system. Note that the 'thin' transition with output places takes no time to execute, i.e., it is instantaneous. Informally, the middle transition T_{ut} produces a token with in one of the two output places with probabilities p and $1-p$, respectively.

tokens in place *Idle_server*, busy servers are represented by tokens in place *Server*. The time taken to access the protected resources is given by T_{ser}. The marking of *Users* determines the firing rate of the transition modelling users arrivals, and the marking of *Server* determines the firing rate of the transition modelling user departure.

If the user can pass the authentication process, then the user can use the resource, however, if the user cannot access the resource, the user has to contact the administrators for help. Place *Af_service* contains all users who went through the server, the probabilities on immediate transition T_{ut} represents the users passed the authentication process and the users did not pass the authentication process. Idle administrators are represented by tokens in place *Idle_adm*, busy administrators are represented by tokens in place *Adm_help*. The time taken to help the users is given by T_{adm}. After obtaining such help, 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 (Sanders (2018)).

The throughput of a transition is computed according to the formula which is described in Section 5,

$$\sum_{a\in A} \mathcal{C}(a) \cdot N^{a}_{[t,t+l]}.$$

The number of tokens in sets of places is computed according to the formula

$$\sum_{v \in \mathcal{P}(Pl,\mathbb{N})} \mathcal{R}(v) \cdot J^{v}_{[t,t+l]}.$$

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 $[t, t + l]$, 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).

This model will be used as base case model for sensitivity analysis later in Section 7.

7. Sensitivity Analysis of Productivity Loss in the Organization

From the models we can see that NPT associated with enterprise information security technologies is related to a variety of parameters, which are affected by the security policies and user behaviour in the organization. Since these parameters have an impact on the organization efficiency loss, it is of critical business importance for corporations to find out which parameter results in a large contribution to the overall output variability, so that enterprise-wide security budget can be optimized to these factors in order to minimize the cost (Anderson and Choobineh (2008)). Therefore, sensitivity analysis is particularly useful in this situation.

We analyze the relative importance of each parameters by applying sensitivity analysis to the stochastic activity network model. To get the aim of the sensitivity analysis, three main steps are proposed:

Step 1 Building a base case model to simulate the business process by implementing an enterprise information security technology. The base case should incorporate the best bet values of all the input parameters. Following an initial run with the base case model, a belief about the optimal strategy can be formed (Pannell (1997)). This belief is also based on the modeler's perceptions of probability distribution of profit for the preferred strategy.

Step 2 Identify the base case, maximum and minimum value of the parameters which we are interested in. If we analyze the sensitivity of $\{x_1 \ldots x_n\}$, we use x_i^{bas} denotes the base case value of input parameter x_i, x_i^{max} denotes the maximum value of x_i, and x_i^{min} denotes the minimum value of x_i. The output of the base case model is y^{bas}.

Step 3 Analysing the sensitivity of x_i, x_i is varied by using its maximum or minimum value, while leaving all other parameters at their base values. We calculate the output of the model, and assess the influences of each input parameter relative to the output of the model [1]. Thus, the sensitivity of x_i can be calculated as:

$$Positive\ part: \ \frac{y_i^{max} - y^{bas}}{x_i^{max} - x_i^{bas}}$$

$$Negative\ part: \ \frac{y^{bas} - y_i^{min}}{x_i^{bas} - x_i^{min}}$$

where x_i^{max} and x_i^{min} correspond to the output values y_i^{max} and y_i^{min} respectively.

7.1. Base Case Model

Enterprise digital rights management (EDRM) is used as a case study (Zeng and van Moorsel (2011)). When authorized users try to open protected documents, the user needs a username and password in order to login to the system. If the user can open the document they become an active user. If the user cannot pass the document authentication or the user cannot pass the user authentication, the user would contact the administrators for help. After the user gets help from the administrators, the user would try to use the document again.

The model we use is in Section 6. There are nine input parameters in the model (Table 1). The first five parameters: The number of authorized users

[1] The units of measurement of different parameters might not be comparable, so there cannot be absolute scopes with respect to changes in different parameters. This problem can be overcome by measuring the percentage change in the output, divided by the percentage change in the input parameter. Therefore, the sensitivity coefficient is the ratio of the change in output to the change in input while all other parameters remain constant

Table 1: The input parameters of the model.

	Parameters	Value
1	Number of authorized users in the organization	50
2	Number of documents, a user might use every day on average	4
3	Number of normal working hours per day	8
4	Number of working weeks per year	52
5	Number of administrators in the organization	1
6	Average time service need to serve each user	0.01s
7	Average time administrators need to help each user	4.5 min
8	Average time users need to pass user authentication	7.33 s
9	Percentage of time when authorized users experience a login system failure and attempt ask administrator for help	0.70 %

in the organization, the number of documents that an authorized user might use every day on average, the number of normal working hours per day, the number of working weeks per year, and the number of administrators, these five parameters depend entirely on the size and business type of different organizations. Therefore, the values of these parameters are determined by literature based assumptions. Other four parameters of the model can be gathered by previous research works and experiments.

Average time service need to serve each user: The values of this parameter are the measurements from a real Google service (Dean and Barroso (2013)). The Google search system updates query results interactively as the user types, performing the search and showing the results within a few tens of milliseconds. From a real Google service (Dean and Barroso (2013)), each server typically responds in 10 ms (i.e. $0.01sc$). The maximum response time is 140 ms (i.e. $0.14sc$), and the minimum response time is 1ms (i.e. $0.001sc$).

Average time administrators need to help each user: This interview is taken in Newcastle University. All the students in the university have their own username and password to access facilities, computers, and network in the campus. When students experienced username and password issues, they would go to the information help desk of the university and ask for help.

In the interview, the technical staff member in the information help desk claimed that: It takes 1 or 2 min for the staff change a student's password, after changing the password, the password is available for use immediately. Creating a new account for a student would take 5 or 10 min, which would also be available for immediate use. If the username and password of enterprise Digital Rights Management product (EDRM) belong to the campus domain, the procedure to creating or changing the username and password would be the same as normal password changing and creating procedure.

In our study, the following assumption is made: after help desk staff change or create a username and password for a user, the user can use the username and password to open protected documents immediately and the values of this parameter are uniform in distribution, thus we have $(1+2+5+10)/4 = 4.5$, which means the average time technical staff spend to change or create a username and password is 4.5 min. The maximum time cost is 10 min and the minimum time cost is 1 min.

Average time users need to spend to pass user authentication: The participants in the experiment were 30 students in Newcastle University: 5 Ph.D students, 3 MSc students and 22 undergraduate students. Participants used their username and password to log into their web based e-mail accounts, and check their e-mail in the summer term at a computer cluster and students' offices.

From the username and password setting rules in the Newcastle University: *The login name is made up of 'a' or 'n' followed by the middle seven characters of the Student Number .... The way to set a password: you need something which is memorable, but not guessable. Think of a phrase of eight words (or more) which contains at least one upper case (capital) letter and at least one number, and then use the initial letters of the phrase.*

Out of the 30 participants, the minimum time cost to login into their student account is 4 s. The maximum time cost is 17 s, and the average time cost is 7.33 s. We noticed that time cost of each student depended on the length of the username and password, the strength of the password, the character restrictions of the password and the frequency of using and changing the username and password.

Percentage of time when authorized users experience a login system fail-

ure: This parameter is based on the experiment in University College London. They found that there are approximately 0.7% of login attempts that can be expected to result in a help desk call, where passwords are re-set via the information help desk (Brostoff and Sasse (2003)). The highest percentage of password reminder is 26.1%, and the lowest percentage of password reminder is 0%.

The system reaches steady state under the parameters in Table 1, based on equation (1) and (7):

$$\begin{aligned} \rho_{ser} &= \tfrac{r_u k}{r_{ser} p} &&= 0.003497398 < 0 \\ \rho_{adm} &= \tfrac{(1-p) r_u k}{r_a p} &&= 0.000024481 < 0 \end{aligned}$$

where the frequency for a user send an access request $\frac{1}{r_u} = \frac{8 \times 60}{50 \times 4} = 2.4$, number of users $k = 50$, the average time it takes the server to serve a user's request $\frac{1}{r_{ser}} = 0.0001667$ time unit, the average time it takes the administrator to help a non-active user $\frac{1}{r_a} = 4.5$, the probabilistic users can pass the authentication process $p = 0.993$.

Let us now consider one year of work after the deployment of EDRM in the network system of an organization, i.e., 124800 time units in the stochastic Petri net model (this corresponds to 52 weeks of work, each working week having 40 working hours). We measure the NPT, using equation (11), the time users spend in any place other than *Users* is computed. The NPT also includes the time the user takes for sending an access request $(\frac{1}{r_q})$.

We increase the number of users up to tens of thousands, using a discrete approximation to keep the state space limited. That is, we assume 50 active users circle around in the model, each representing a group of users as determined by a model multiplier. By incorporating the multiplier correctly in the various transition rates, we can approximate the behaviour of a system with tens of thousands of users by a model that has less than one million states. One million states is easily manageable with Möbius tool (Sanders (2018)).

Figure 5 shows the NPT of the system, for up to 25600 users. 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. Once the number of users rises above two thousand, the system starts to deteriorate. A middle-size corporation that has 50 authorized users will incur about 133.32 h of NPT.

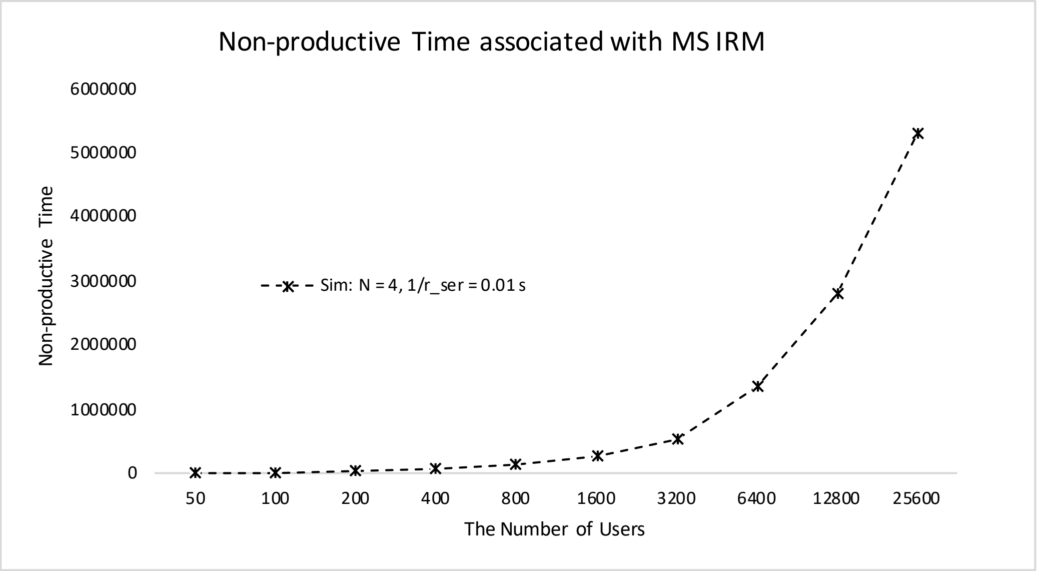

Figure 5: Total non-productive time (NPT) associated with the deployment of information security technologies. NPT increases significantly when the number of users served by the system increases.

7.2. Define Key Parameters

Table 2 lists the four parameters that will be investigated, more information can be found in Section 8. They are variable numbers and could be adjusted independently, which can be changed by the security policies of the organization.

7.3. Sensitivity Analysis

Figure 6 shows the results of sensitive analysis for the parameters in Table 2. Sensitivity is calculated as the ratio between the relative change of model output and the relative change of an input parameter. It has been found that a small change of *parameter 3 - Average time users need to spend to pass user authentication* contributes most to output variability. *Parameter 1 - Average time service response time* gives the smallest relative change in the NPT.

8. Comparing Analytical and Simulation Results

We put the parameters in Table 1 into the model in Figure 4, and compare the approximate analytical solution with simulation results obtained using

Table 2: The Parameters for Sensitivity Analysis.

Parameters	Highest Value	Base Value	Lowest Value
1. Average time service response time	0.14 s	0.01 s	0.001 s
2. Average time administrators need to help each user	10 min	4.5 min	1 min
3. Average time users need to spend to pass user authentication	17 s	7.33 s	4 s
4. Percentage of time when authorized users experience a login system failure and attempt ask administrator for help	26.1%	0.7 %	0%

the Möbius system (Sanders (2018)). The performance of the system under different loading conditions and parameter settings was examined in a series of numerical and simulation experiments.

Figure 7 shows the utility of the server against the number of users for both the simulation and approximate analytical approaches for various values of N (number of documents, a user might use every day on average). Increasing the value of N corresponds to increasing the utility of the server.

Figure 8 shows the utility of the administrator against the numbers of the users for both the simulation and approximate analytical approaches for various values of N. Increasing the number of documents, a user might use every day on average, corresponds to increasing the utility of the administrator in the organization.

9. Multiple Administrators

In the above, we proposed an approximate analytical model for implementing information security technologies. We considered one server and one administrator. However, in a real life situation, the administrator would have multiple tasks, which make them too busy to handle the access control

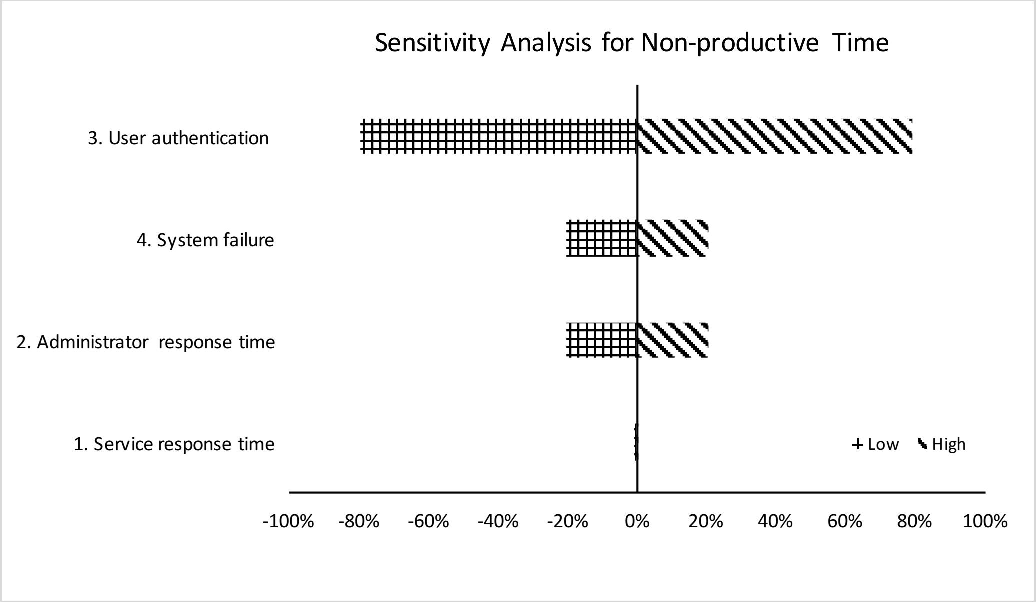

Figure 6: The tornado chart is the sensitivity of four key variant parameters in the model. The x-axis is the percentage change from the base case model of the sensitivity analysis. This analysis is associated with the parameters in Table 2.

problems for information security technologies. 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 9). 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 (Mitrani (1998)). 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.

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

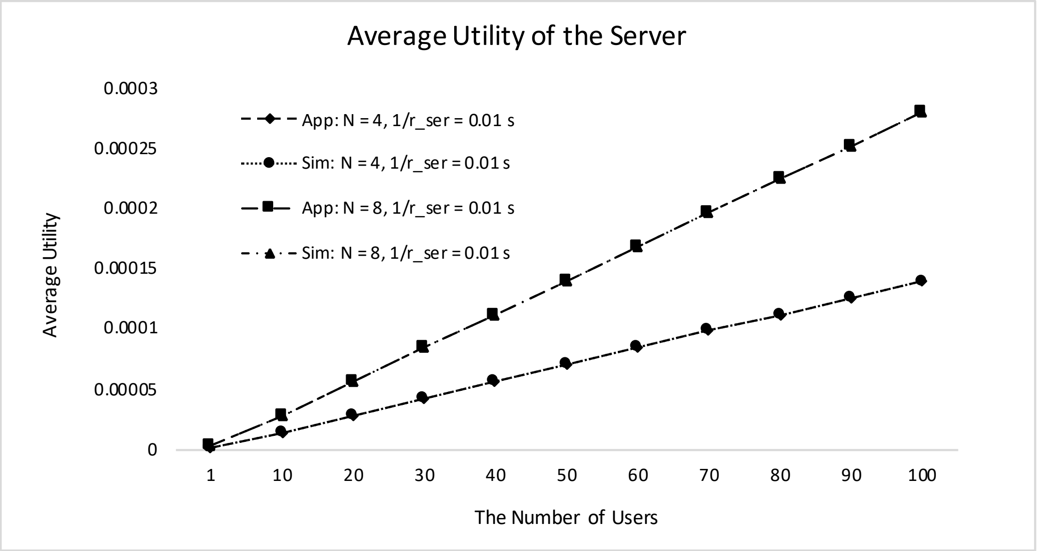

Figure 7: Utility of the server w.r.t. the number of users in the system. The utility increases significantly when the number of users served by the server and administrator increases.

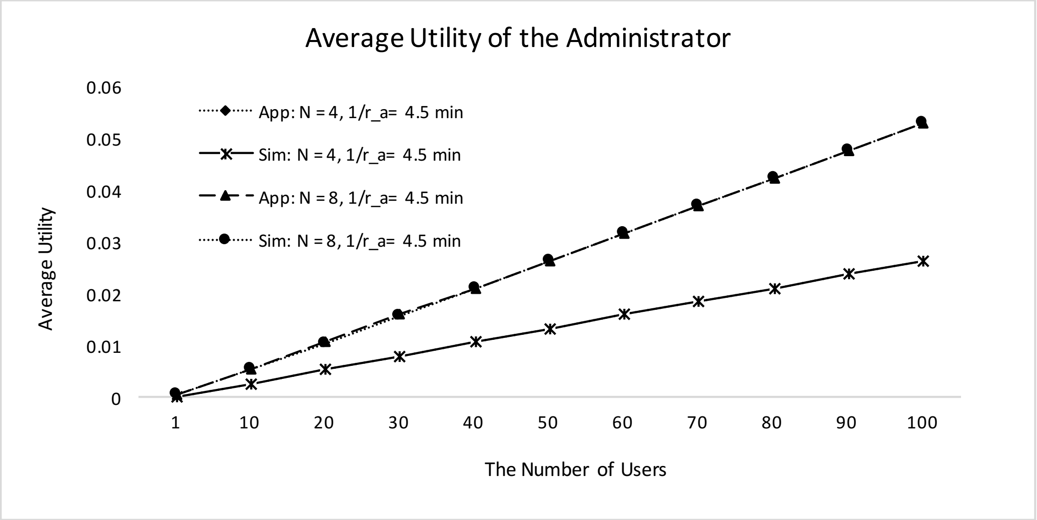

Figure 8: Utility of the administrator w.r.t. the number of users in the system. The utility increases significantly when the number of users served by the server and administrator increases.

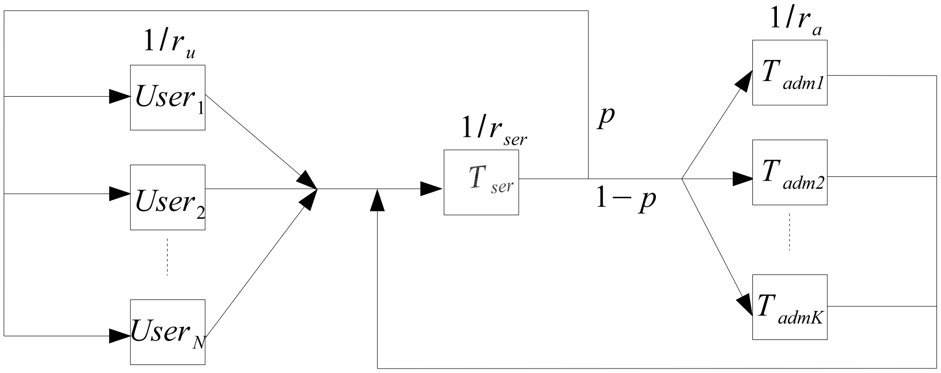

Figure 9: A closed queuing theory model of an information security system, with N users and K administrators.

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 (Mitrani (1998)):

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

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 (Mitrani (1998)):

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

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

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 (Mitrani (1998); Zhao and Thomas (2010)):

$$\begin{aligned} L_{adm} &= \textstyle\sum_{j=1}^{A} j\Pi_j \\ &= A!\Pi_0 \left[\textstyle\sum_{j=1}^{K-1} \frac{\rho^j j}{(A-j)!j!} + \sum_{j=K}^{A} \frac{\rho^j j}{(A-j)!K!K^{j-K}}\right] \end{aligned} \tag{16}$$

Each of the users submits requests to administrators at the rate $\frac{(1-p)r_u}{p}$. Therefore, the throughput T_{adm} is (Mitrani (1998)):

$$T_{adm} = (A - L_{adm})\frac{r_u A}{p} \tag{17}$$

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

$$W_{adm} = \frac{A}{T_{adm}} - \frac{p}{r_u A} \tag{18}$$

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

We again used the Möbius software (Sanders (2018); Deavours and Sanders (2001)) to simulate the behaviour of the approximate analytical model, and to compare the simulation and analytical results.

We recall Figure 4, shows the structure of a stochastic Petri net for the analytical model we have just discussed. Here the number of administrators are represented by the tokens in place *Idle_adm*, the number of servers are represented by the tokens in place *Idle_server*, the number of users are represented by the tokens in place *Users*.

Consider now one year of the deployment of the information security technology in the network system, i.e., 124800 time units in the stochastic Petri net model. Figure 10 shows the NPT of the system w.r.t. the numbers of users for numbers of administrators $K = 2$, and $K = 1$. NPT increased significantly when the numbers of users increase. The non-productive time are similar due to the low load on the administrators and the administrators often be idle in such a case.

10. The Cost Model for Administrators

Now we introduce a cost function which needs to be optimized. This function is very useful when the numbers of protected documents and users are high in large organizations. 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 (Mitrani (1998); Zhao and Thomas (2010)):

$$C = c_1 L_{adm} + c_2 K r_a, \quad c_1, c_2 \geq 0 \tag{19}$$

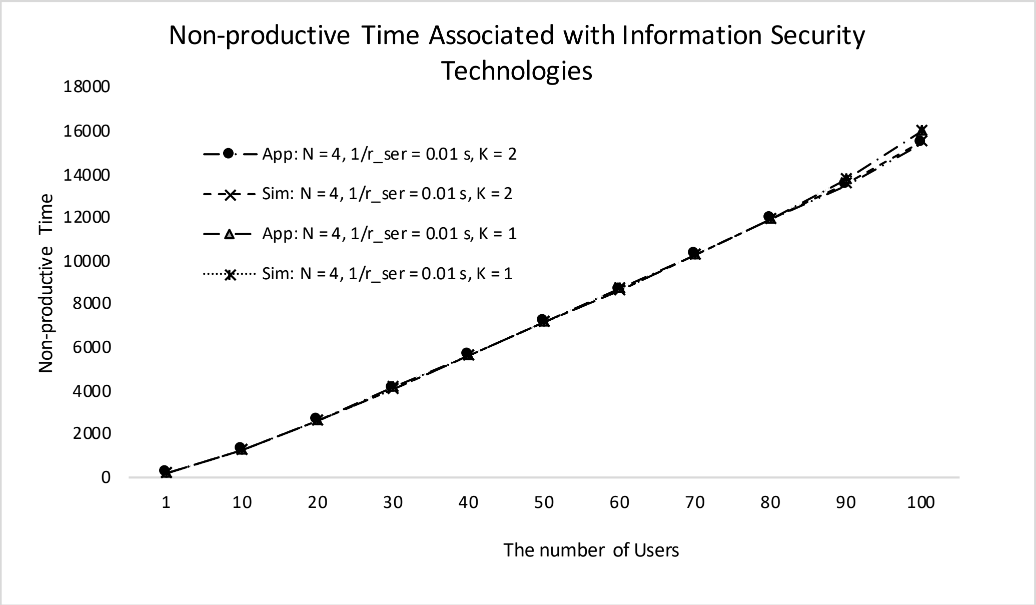

Figure 10: Total non-productive time (NPT) associated with the deployment of information security technologies.

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} (the average number of requests on the administrator) should be small (Mitrani (1998)). At the same time, if c_2 is large, in order to keep the total cost C low, Kr_a should be small (the rate administrators need to help the users) (Mitrani (1998)). 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.

10.1. Analytical Results

We now illustrate the cost function we proposed above using the analytical results we can get from previous section. Figure 11 shows the cost w.r.t. the number of users. It is clear that under the parameter values with $1/r_a = 4.5, c_1 = 1, c_2 = 0.5$, more administrators bring more cost to the organization.

However, when the number of users reach 640, the costs start to close towards each other. In a small system, when $N < 640$, the cost function is dominated by $c_2 K r_a$. The reason is that the administrators will often be idle, and the system is not making efficient use of resources.

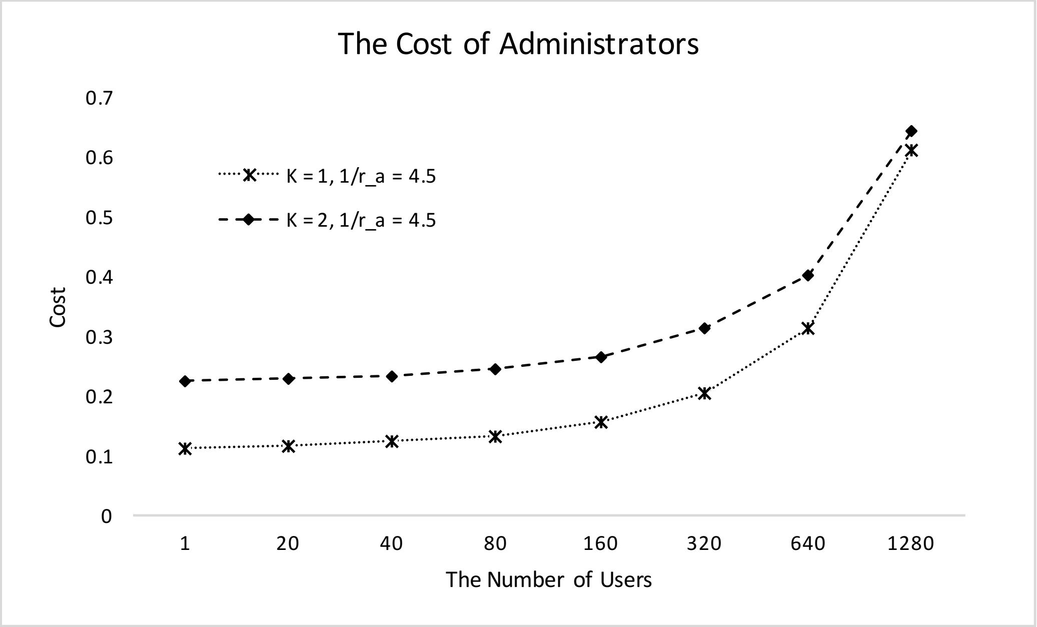

Figure 11: The cost w.r.t. the number of users calculated by the queuing network model when $c_1 = 1, c_2 = 0.5, \frac{1}{r_a} = 4.5$.

Figure 12 shows the cost w.r.t. the number of users. It is easy to see, under the parameter values with $1/r_a = 4.5$, the cost rises rapidly at around 640 users for all cases $(c_2 = 0.05, 0.5, 5)$.

11. Conclusions

In this paper, we provided an approximate analytical model for investigating the previous models test the aforementioned user-server-admin model. We have also provided a corresponding simulation model based on stochastic activity networks. 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

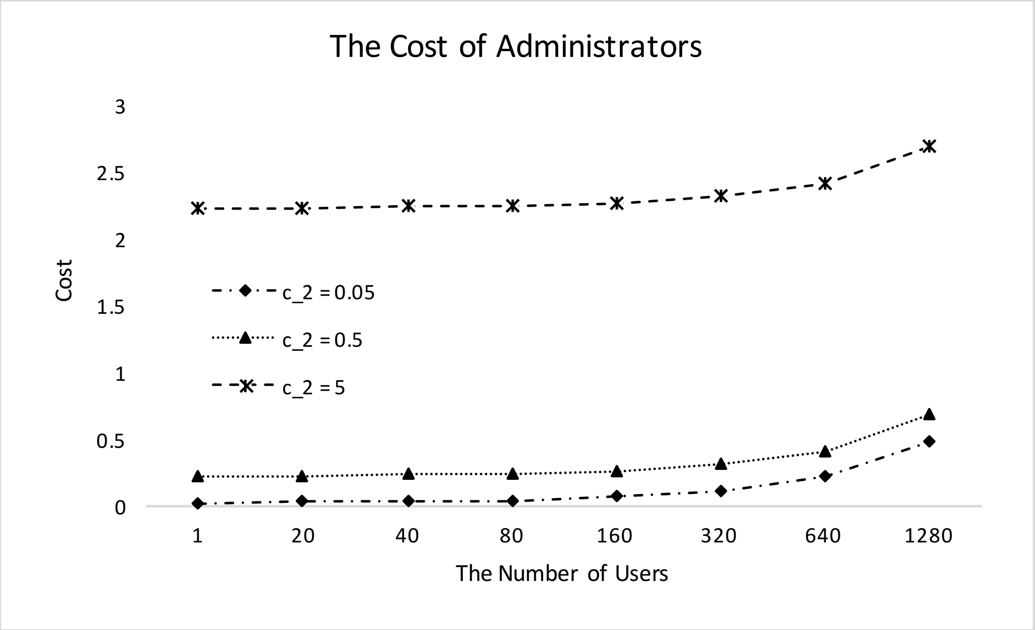

Figure 12: The cost w.r.t. the number of users calculated by the queuing network model. $K = 2, \frac{1}{r_a} = 4.5, c_1 = 0.5$.

based on stochastic activity networks 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 implementation of information security technologies, and stochastic activity networks 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.

Sensitivity analysis is used to determine which of the parameters exerts the most influence on the NPT of an corporation, in order to help information security managers to balance the weight of information security expenses, and make well informed security investment decisions. In this study, each parameter is assigned by value. Different values of the input parameters would lead to different results. Such a study can help information security managers to make information security investment decision.

12. Acknowledgement

We would like to thank the referees for their comments and useful suggestions. This research was supported by EPSRC Uncover project.

13. References

Adams, A., Sasse, M. A., December 1999. Users are not the enemy. Communications of the ACM 42 (12), 40 – 46.

Anderson, E. E., Choobineh, J., 2008. Enterprise information security strategies. Computers & Security 27 (1- 2), 22 – 29.

Beautement, A., Becker, I., Parkin, S., Krol, K., Sasse, M. A., 2016. Productive security: A scalable methodology for analysing employee security behaviours. In: Twelfth Symposium on Usable Privacy and Security, SOUPS 2016, Denver, CO, USA, June 22-24, 2016. pp. 253 – 270.

Beautement, A., Coles, R., Griffin, J., Ioannidis, C., Monahan, B., Pym, D., Sasse, A., Wonham, M., 2009. Modelling the human and technological costs and benefits of usb memory stick security. In: Managing Information Risk and the Economics of Security.

Beres, Y., Griffin, J., Shiu, S., Heitman, M., Markle, D., Ventura, P., 2008. Analysing the performance of security solutions to reduce vulnerability exposure window. In: Proceedings of the 2008 Annual Computer Security Applications Conference. ACSAC '08. IEEE Computer Society, Washington, DC, USA, pp. 33 – 42.

Beres, Y., Pym, D., Shiu, S., 2010. Decision support for systems security investment. Manuscript, HP Labs.

Brostoff, S., Sasse, M. A., 2003. "ten strikes and you're out": Increasing the number of login attempts can improve password usability. In: Proceedings of CHI 2003 Workshop on HCI and Security Systems. John Wiley.

Dean, J., Barroso, L. A., 2013. The tail at scale. Communications of the ACM 56, 74 – 80.

Deavours, D. D., Sanders, W. H., September 2001. Möbius: framework and atomic models. In: Proceedings 9th International Workshop on Petri Nets and Performance Models. pp. 251 – 260.

Dolya, A., 2006. Internal it threats in europe 2006. SECURELIST 2010 (November).

Kirlappos, I., Sasse, M. A., 2014. What usable security really means: Trusting and engaging users. In: Human Aspects of Information Security, Privacy, and Trust - Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings. pp. 69 – 78.

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

Mitrani, I., 1998. Probabilistic Modelling. Cambridge university press.

Murata, T., 1989. Petri nets: Properties, analysis and applications. Proceedings of the IEEE 77 (4), 541 – 580.

Pannell, D. J., 1997. Sensitivity analysis: strategies, methods, concepts, examples. School of Agricultural and Resource Economics, University of Western Australia.

Parkin, S. E., Kassab, R. Y., van Moorsel, A., 2008. The impact of unavailability on the effectiveness of enterprise information security technologies. In: Proceedings of the 5th international conference on Service availability. ISAS'08. Springer-Verlag, Berlin, Heidelberg, pp. 43 – 58.

Reinecke, P., Wolter, K., van Moorsel, A., 2010. Evaluating the adaptivity of computing systems. Performance Evaluation 67 (8), 676 – 693, special Issue on Software and Performance.

Salimifard, K., Wright, M., 2001. Petri net-based modelling of workflow systems: An overview. European Journal of Operational Research 134 (3), 664 – 676.

Sanders, W. H., 1988. Construction and solution of performability models based on stochastic activity networks. Ph.D. thesis, University of Michigan.

Sanders, W. H., 2018. Möbius user manual. University of Illinois.

Sasse, M. A., Smith, M., Herley, C., Lipford, H., Vaniea, K., 2016. Debunking security-usability tradeoff myths. IEEE Security & Privacy 14 (5), 33 – 39.

Schneier, B., 2000. Secrets and Lies: Digital Security in a Networked World, 1st Edition. John Wiley & Sons, Inc., New York, NY, USA.

van der Aalst, W. M. P., 1998. The application of petri nets to workflow management. The Journal of Circuits, Systems and Computers 8, 21 – 66.

Wolter, K., Reinecke, P., 2010. Performance and security tradeoff. In: Proceedings of the Formal Methods for Quantitative Aspects of Programming Languages, and 10th International Conference on School on Formal Methods for the Design of Computer, Communication and Software Systems. SFM'10. Springer-Verlag, Berlin, Heidelberg, pp. 135 – 167.

Zeng, W., 2019. A methodology for cost-benefit analysis of information security technologies. Concurrency and Computation: Practice and Experience 31 (7).
URL `https://doi.org/10.1002/cpe.5004`

Zeng, W., van Moorsel, A., September 2011. Quantitative evaluation of enterprise drm technology. Electronic Notes in Theoretical Computer Science 275, 159 – 174.

Zhao, Y., Thomas, N., 2010. Efficient solutions of a pepa model of a key distribution centre. Performance Evaluation 67 (8), 740 – 756.