Available online at www.sciencedirect.com

SciVerse ScienceDirect

Electronic Notes in Theoretical Computer Science

Electronic Notes in Theoretical Computer Science 275 (2011) 159–174

www.elsevier.com/locate/entcs

Quantitative Evaluation of Enterprise DRM Technology

Wen Zeng [1,2] Aad van Moorsel[3]

Centre for Cybercrime and Computer Security
School of Computing Science
Newcastle University
Newcastle, U.K.

Abstract

It is of critical business importance for organizations to keep confidential digital documents secure, as the potential cost and damage incurred from the loss of confidential digital documents have increased significantly in recent years. Digital Rights Management (DRM) was developed to help organizations keep digital documents secure, as one of many digital information security solutions.
In this study, the functions of eight popular DRM products currently available on the market are reviewed, and the impact of using of these DRM products is evaluated quantitatively. A group of metrics is defined reflecting the potential costs and impact to the organization incurred by implementing DRM products. Stochastic models are used to quantitatively evaluate the costs and impact of implementing a particular DRM product. In this study, it is found that although DRM products protect digital assets by encryption and by providing central control on information within the organization, this comes at a cost, since these security mechanisms typically reduce the productivity of the staff. The reduction in productivity is in turn measured in the form of non-productive time (NPT) which is an inherent part of the stochastic modeling process.

Keywords: Petri-nets, stochastic modeling, DRM products, digital security, non-productive time, information help desk

1 Introduction

Many organizations maintain sensitive information or documents that should be accessed only by authorized personnel, for example, personal health records in health institutions, bank statements and account balances for financial organizations. Confidential information leakage and sensitive information dissertation have been iden-

[1] The authors want to express their sincere appreciations to Simon Parkin and Rouaa Yassin Kassab at Newcastle University for their constructive suggestions and feedbacks during both the research and writing stages of this work. Detailed, critical reviews by four anonymous reviewers from the workshop committee significantly improved the quality of this manuscript. The authors feel deeply obliged to their contributions.

[2] Email: wen.zeng@ncl.ac.uk. Corresponding author.

[3] Email: aad.vanmoorsel@ncl.ac.uk. The second author has been funded in part by UK Technology Strategy Board (TSB), grant nr. P0007E (Trust Economics).

doi:10.1016/j.entcs.2011.09.011

tified as major information security threats that cause reputation damage, identity theft and even threaten the viability of the organization[1].

Although hacker attacks, virus epidemics and system vulnerabilities have been identified previously as the main causes of loss of sensitive information, the number of security incidents caused by internal attacks has increased significantly in recent years[2]. In a comprehensive survey conducted by[2], 400 surveyed organizations admitted to 6244 incidents of employee negligence, 5794 incidents of excessive privilege and access control rights. The number of internal security incidents totaled 57,485[2]. Therefore, the behavior of internal staff has a significant impact on information security and attacks associated with the inappropriate behavior of internal staff are on the rise and are posing a great threat. For example, some staff members save sensitive information on laptops, USB devices or smart phones for convenience purposes. When these devices are lost, organization will not be able to exert any control on the information saved in these devices. In addition, employees in the company might occasionally send e-mail messages that contain confidential files as attachments without noticing that the files should not be distributed, or otherwise that the recipient should not see the files or is an unintended recipient who has been incorrectly (accidentally or otherwise) chosen to receive the e-mail. All of these behaviors could cause digital information to leak outside the company. It is essential that companies and organizations keep these information and document safe. Digital Rights Management (DRM) systems are developed to address these concerns and needs.

The term, Digital Rights Management (DRM), is used to describe any technology that delivers the capability of controlling the access rights of digital content both within and outside a digital environment[3]. Commercial DRMs are DRM systems that protect digital content in music, film and print industry. Enterprise DRM is one of many information security products and DRM claims to have the ability to protect the confidentiality, integrity and availability of information in the organization. Since organizations have to invest a significant amount of capital and continue to have operational expenditure on enterprise DRM products and enterprise DRM products might have negative effects on the efficiency of the organization, it is necessary to demonstrate that the benefits from DRM products exceed the costs of information security investment. However, it is challenging to quantitatively evaluate the potential impact of DRM products on the organization. For example, DRM technologies use access control (username and password) to limit unauthorized use of sensitive documents. However, authorized users might be unable to open a document and lose significant amount of time in finding the correct password to open the protected document. Thus, the business process is halted and productivity of employees is reduced.

Therefore, the contributions of this study are, 1) to review popular DRM products currently available on the market in terms of their common features; 2) to develop a methodology so that the impact of DRM technology can be evaluated quantitatively by stochastic modeling techniques. These techniques include defining metrics and constructing and running Petri-nets stochastic models.

2 DRM technology

Eight of the currently popular DRM products are selected and reviewed in this document from the following four aspects: administrative models, content management, users monitoring, rights management[4]. Most of these products are developed by leading computer technology firms. The aim of this part is to understand the common features of DRM products and the working of DRM within the business processes of an organization. This serves as the fundamental work to analysis their effectiveness and costs.

- Adobe LiveCycle Policy Server[5]
- Oracle Information Rights Management (formerly SealedMedia E-DRM)[6]
- Microsoft Windows Rights Management Services for Windows Server 2003[7]
- Documentum IRM Services[8]
- Liquid Machines Document Control[9]
- Secure2Trust[10]
- PDF Document Security[11]
- Workshare Protect[12]

2.1 Administrative models

All eight DRM products reviewed have a similar centralized administrative model (Fig.1). Documents are stored in a centralized space[4]. Each document has a unique identifier, which is linked with users and rights[13]. Only administrators who do not have access limitations can access the space to manage protected documents. Administrators can define the rights for each document and each user.

The organization also can control all the encrypted information centrally regardless of its location[4]. Dynamic policy centralized control allows the administrators to change the policy of the document no matter it has been distributed or not. The policy becomes effective immediately, when users open the document. This helps preventing unauthorized users from accessing documents.

Through centralized administration, organizations can manage digital information more effectively (Fig.1). Administrators have the highest access rights, and can define policies for all the documents and change policies for users. They can control the usage policies, revocation and exclusion. They can centrally define who can access the documents, what kind of things they can do with the content of the document after authorized user access, and the expiry date of the document.

When authorized user can not open a document, the user will have to contact the administrator, who will then check the status and rights of the user and make appropriate changes (Fig.2). This process might take some considerable time thus delay due business process and create non-productive time (NPT) for the employee.

When a user tries to open a protected document, access right request is sent to the DRM server, which records this request. If the user does not pass the authentication on the server, the user will not be able to use the document. The user

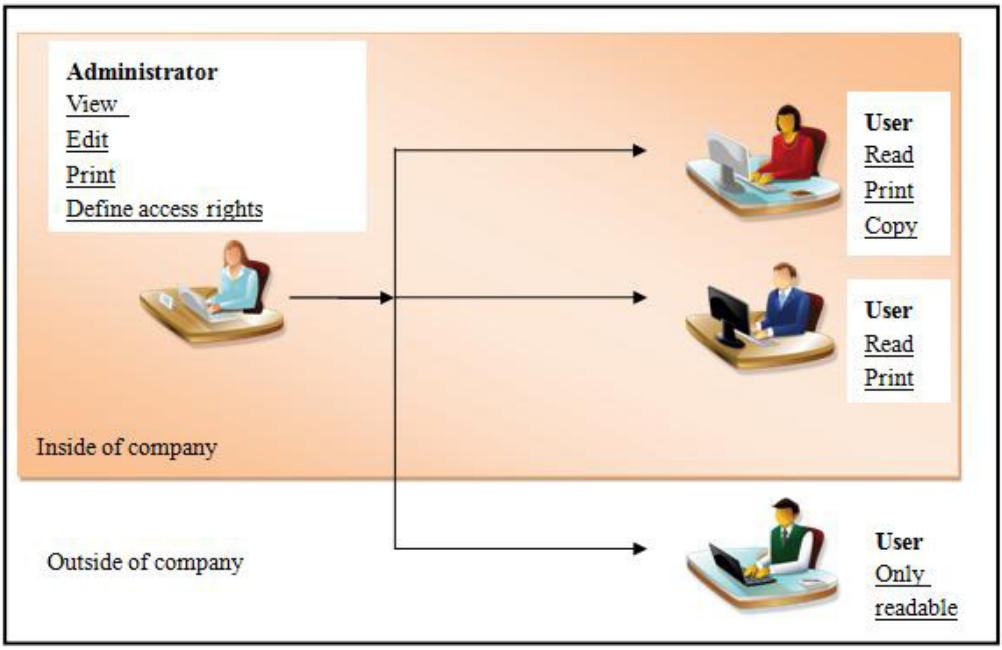

Fig. 1. An Example of Centralized administration of end users

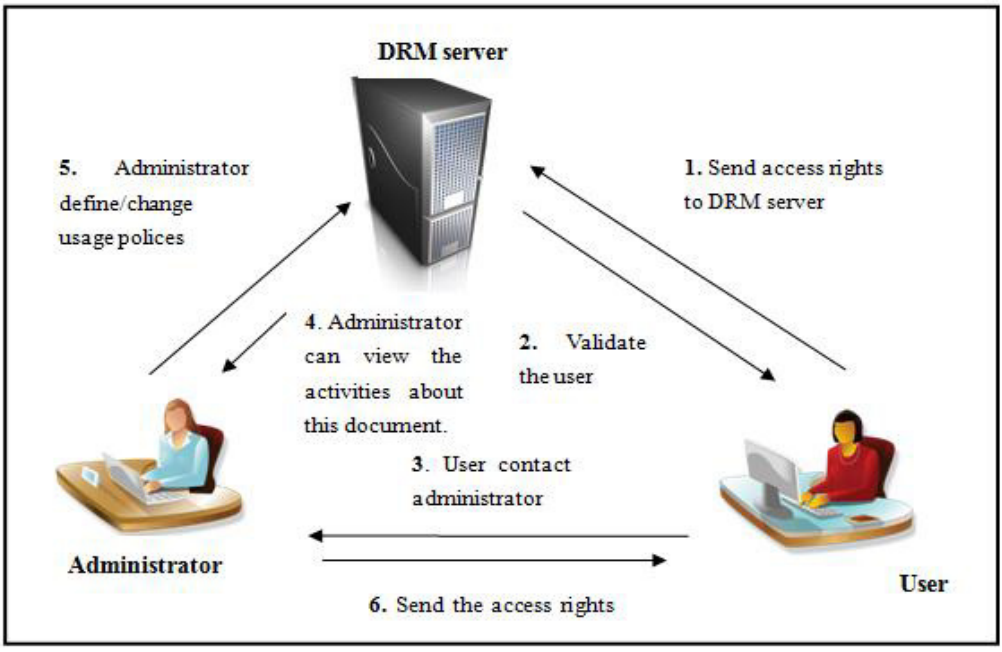

Fig. 2. Workflow of authorized users to open protected document when access is denied

will have to contact the administrator and ask for access rights. The administrator then views the activities associated with this document and checks the user's role. If the user is allowed to access the document and the user has not been given access rights or the access rights are not enough for this user to use the document, the

administrator will create the access rights for the user or change the usage polices for this user via the DRM server. Finally, the administrator sends the access rights to the user.

2.2 Content Management

All eight DRM products reviewed use encryption to keep the information secure no matter where it has been transferred[4]. Authorized users use decryption keys to open the document and access the information. This helps organizations comply with government regulations. All of the products provide creation functions for each authorized user so that they have the ability to create various types of digital documents with unique identity for each document and secure these documents with rights for other users[13].

2.3 Users Monitoring

All eight DRM products reviewed provide the function to manage user lists for every document, so administrators can create new users or delete existing users from the user list of the document[4]. All the products provide unique identity for each user, e.g. user name and password, email address and password, fingerprint, and etc. In addition, administrators have the ability to restrict the usage of documents by defining usage policies for the documents; for example, number of times accessing document, expiration date of access rights to the document, and etc.[13].

2.4 Rights Management

All eight DRM products reviewed provide functions for organizations to provide rights for each document and each user[4]. Full control, modify, read, print are basic rights for DRM products. All DRM products can provide limited document usage by using expiration dates. After expiration date, only administrators can access an expired documents.

Digital content and the rights assigned to each user can be dynamically changed[4]. Users who own full control accounts have the ability to change the rights for digital content[13].

3 Background on Stochastic Models

Stochastic modeling is used to create an abstraction of a business process so that organizations can understand how DRM technologies change employees working processes, and evaluate the benefits, costs and impact of implementing a DRM solution. Therefore, stochastic Petri-net theory methodology is introduced in this section.

3.1 Classic Petri Net

Petri net is a graphical and mathematical modeling tool for the formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion and conflict, which are typical features of distributed environments[14]. Petri nets have been widely used for structural modeling of workflows and have been applied to a wide range of qualitative and quantitative analysis[14,15,16,17].

A definition of a classic Petri Net:

A Petri net is a 5-tuple(P, T, F, W, M_0), where:

- P = $\{p_1, p_2, p_3, ..., p_n\}$, P is the set of places, p_n is the name of each place;
- T = $\{t_1, t_2, t_3, ..., t_n\}$, T is the set of transitions, t_n is the name of each transition;
- F $\subseteq (P \times T) \cup (T \times P)$ is a set of arcs;
- W: F$\rightarrow$ {1, 2, 3,.....} is a weight function;
- M_0: P $\rightarrow$ {0, 1, 2,.....} is the initial marking;
- $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$

A petri net consist of *place, transition* and *arcs* that connect them. *Input arcs* start at places and end at transitions, while *output arcs* start at a transition and end at a place. Places can contain *tokens*, which are used in the network to simulate the dynamic and concurrent activities of the system. The current state of the modeled system (the *marking*) is given by the number of tokens in each place. Transitions are active components, when a transition fires, the model activates, then tokens move in the model, which changes the states of the system. Transitions are only allowed to fires when they are enabled, at least a token in every input place. More rules of transition enabling and firing are defined at[18,14].

3.2 Stochastic Activity Networks

For Petri net, if a firing delay associated with each transition, which specifies the time that the transition has to be enabled. Before it can actually fire, if the delay is a random distribution function, the Petri net is called Stochastic Petri net. Stochastic Activity Networks (SANs) are stochastic extensions to Petri nets[19]. SANs consist of four primitive objects: *places, transitions, input gates* and *output gates*. A place represents each state of the modeled system; transitions represent actions of the modeled system 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.

3.3 Reward Formalism

Reward models are used to specify measures of system behavior[20]. Reward model has two different reward structures: one is *rate rewards*, which is the rate at which reward accumulates while the process is in the state during an interval of time;

another is *impulse rewards*, which is used to count the number of times an transition fires during an interval of time.

Reward Structure:

The functions to express transition and marking oriented reward structure of a SAN with places P and transitions A:

C: $A \to R$, where for $a \in A$, C(a) is the reward obtained due to completion of activity a.

R: $P(P,N) \to R$, where for $v \in P(P,N)$, R(v) is the rate of reward obtained when for each $(p,n) \in v$, there are n tokens in place p.

N is the set of natural numbers, P(P, N) is the set of all partial functions between P and N. Impulse rewards are associated with transition completions(via C) and rates of rewards are associated with number of tokens in sets of places (via R).

$$Y_{[t,t+l]} = \sum_{v \in p(p,N)} R(v) M^{v}_{[t,t+l]} + \sum_{a \in A} C(a) N^{a}_{[t,t+l]}$$

$$RW_{[t,t+l],t\to\infty} = \frac{Y_{[t,t+l]}}{l}$$

In this function, reward accumulated is related to the number of times each transition completes and time spend in particular markings during an interval of time [t, t+l]. $M^{v}_{[t,t+l]}$ represents the total time that the SAN is in a marking such that for each $P(p,n) \in v$, there are n tokens in p during [t, t+l].

$N^{a}_{[t,t+l]}$ represents the number of completions of transition a during [t, t+l].

3.4 Möbius software

Möbius is a software tool for modeling the reliability, availability and performance of complex systems [19]. It supports majority of modeling techniques, specifically supports SANs[19]. It works by making different modeling processes (SANs modeling formalisms, compositional formalisms, reward formalisms, solvers) modular. Möbius provides simulation and numerical solvers for obtaining solutions on measures of interest. The simulation solver can be used to solve models using discrete event simulation[19]. Numerical solvers can be used on only models that have only exponentially and deterministically distribution transitions[19].

4 Quantitative Evaluation of DRM

As a firm moves towards planning security strategies, some questions security managers would ask are: Is the document control necessary? Will the document control bring high costs to the organization? To answer these questions, metrics should be defined as a standard to evaluate the effectiveness and the effect of using DRM[21]. The data of metrics can help security managers make sound security investment decisions[22].

All eight DRM products provide centrally defines policies for each document, and centralized administration that allows organizations to manage authorization information from a single facility or location. Centralized administration also allows

organizations to keep a minimum number of IT staff (administrators). However, if a significant number of users are trying to seek help from the administrators at the same time, some users will have to wait. This result in non-productivity time (NPT) and reduces the operational efficiency of the organization. In some cases, users might give up waiting and choose to proceed in their work without appropriate information.

In addition, since IT resources are not unlimited, it is necessary for organizations to classify documents into different levels of confidentiality so that higher-value documents will have higher levels of security[23]. In this study, documents are divided into two levels: normal and high-value (classified documents). Users only need a username and password to open normal documents; on the other hand, users need to have the particular password of each classified document in addition to user's own username and password.

Table 1
Metrics are defined as standards to help evaluate DRM

	Executive	Document Type
1	authorized users can read documents	with document classification
2	authorized users cannot read documents	with document classification
3	authorized users can read documents	without document classification
4	authorized users cannot read documents	without document classification
5	authorized users can change documents	with document classification
6	authorized users cannot change documents	with document classification
7	authorized users can change documents	without document classification
8	authorized users cannot change documents	without document classification

In this document, three aspects are considered to evaluate DRM: the number of users that can read protected documents under the encryption mechanism; the number of users that can change protected documents under the usage policy, and how the document classification strategy impacts the effect of using the DRM. Therefore, eight metrics are defined to measure the effect of using DRM from these three aspects (Table 1), e.g. the percentage of authorized users can read documents under documents classification.

Microsoft information rights management (MS IRM) is used as the case study in this document. From the experiment and information provided by Microsoft technical centre, a model is built in this part to evaluate the effect of using MS IRM[24,25]. This model focuses on function utility and user's tasks when they use data. The core feature of MS IRM is: protected documents are centrally managed. In order to ensure access permissions of employees successfully, a number of IT staff (administrators) are needed in the organization to help employees solve problems, when users cannot use protected documents properly. In this document, two help desks are defined. One help desk helps users deal with the access issue, the other help desk helps users deal with the usage issue. Documents in the organization are divided into two levels: normal documents and high-value documents.

A stochastic Petri-net model is built to simulate this business process and quantitatively evaluate the effect of using MS IRM on organizations operational efficiency.

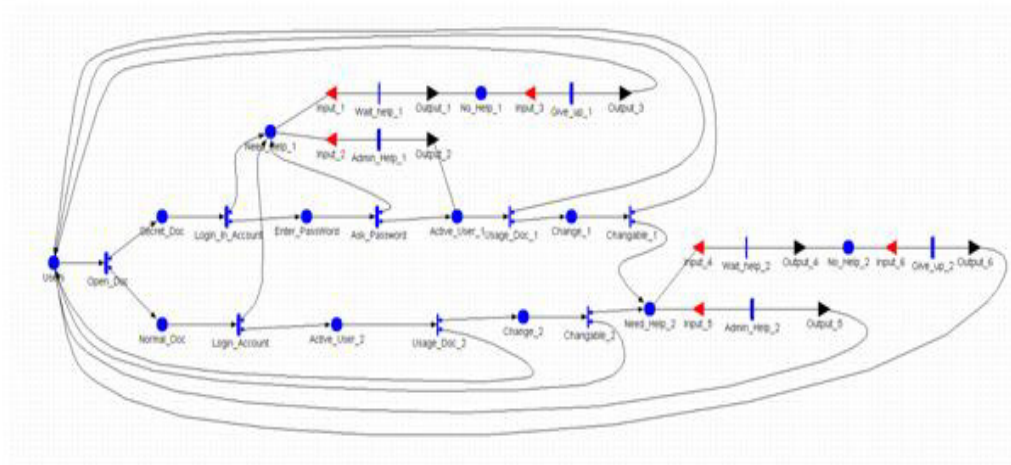

Fig. 3. A Petri net model representing authorized users' access protected documents

The model (Fig.3) consists of six input gates, six output gates, twelve places, and fourteen transitions, eight timed transitions and six immediate transitions. Timed transitions are associated with random exponentially distributed firing delays, and immediate transitions are fired in zero time.

Authorized users (*Users*) use four documents per day during working hours (the time taken to use the documents is given by *Open_Doc*). When authorized users try to open documents, two things might happen, if the document is a secret document (*Secret_Doc*), firstly, the user needs a username and password in order to login to the system (given by the time taken by *Login_In_Account*). If the user passes user authentication, the user needs to input in a document password (*Enter_PassWord*), which takes time (given by the time taken by *Ask_Password*). If the user passes the document authentication, then the user can open the document and become an active user (*Active_User_1*), but if the user cannot pass the document authentication or the user cannot pass the user authentication, the user would contact the administrators (*Need_help_1*) for help. If the user can get help from the administrators (the time taken is given by *Admin_help_1*), the user inputs the document password to

open the document. If the user cannot get help from the administrator (*No_Help_1*), the user would give up (*Give_up_1*). Active users might change protected documents (*change_1*), but they might have not enough usage authority to change documents, so they will contact administrators to ask for help (*Need_Help_2*). If users can get help from the administrators (the time taken given by *Admin_Help_2*), they can change documents, if they cannot receive help (*No_Help_2*), they might be give up.

If the document is a normal document (*Normal_Doc*), the user just needs to input a username and a password to open the document (the time taken for this is given by *Login_Account*). If the user can open the document, the user can open the document (*Active_User_2*). Otherwise the user needs to contact the administrators (*Need_Help_1*) for help. Active users might change protected documents (*change_2*), but they might not be given enough usage authority to change documents, so they will contact administrators to ask for help (*Need_Help_2*).

All of the input parameters in this model are in Table 2. The time scale of the model is in minutes. It assumes that administrators need spend 10 minutes on average to help each user, if less than seven users are in the queue waiting for help, the users would be patient enough until they get help from administrators. But if more than seven users are in the queue, users only at most can wait for one hour. If after one hour users still cannot get help, they would give up.

The behavior of the model can be measured by the Impulse Rewards model and Rates Rewards model, which is supported by the Möbius software. The throughput of transitions are computed according to the formula which is described in Section 3.3:

$$\sum_{a \in A} C(a) N^a_{[t,t+l]}$$

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

$$\sum_{v \in p(p,N)} R(v) M^v_{[t,t+l]}$$

To measure the number of authorized users that can read documents, the sum of the throughput of transitions: *Usage_Doc_1 (case1&2), Usage_Doc_2 (case1&2)* are computed. To measure the number of documents that authorized users can change, the sum of the throughput of transitions: *Changble_1 (case1), Changeable_2 (case2), Admin_Help_2 (case2)* are computed. To measure the numbers of documents that authorized users have tried to use, the sum of the throughput of transition: *Open_Doc (case1&2)* is computed. To measure the non-productive time (NPT), the fraction of time users spend in any place other than (*Users*) are computed, it is considered time loss because of MS IRM provide identity and access control technology.

4.1 Result analysis

The deployment of the DRM product has a significant impact on the operational efficiency of the organization. Within six months of the deployment of MS IRM in

Table 2
Input parameters of the Petri-net model

Parameters	Value
Number of documents, an user might use every day on average	4
Number of normal working hours per day	8
Number of working weeks per year	40
Number of help desk help to solve documents access issue	1
Number of help desk help to solve documents authority issue	1
Number of documents an user uses per working hour on average	0.5
The average time users need to spend to pass user authentication	0.5 minutes
The average time users need to spend to pass document authentication	0.5 minutes
The average time administrator spends to help one user	10 minutes
The percentage of secret documents, if the organization uses a document classification strategy	50%
The percentage of time when users experience a login system failure or users cannot remember the password for secret documents	5%
The percentage of documents that can be changed by authorized users	40%

the network system in this case study (48000 time units in the model), a middle-sized organization that has 500 authorized users will incur about 9000-11000 hours, or about 375-458 days, of non-productive time (Fig.4), under the assumptions made in Table 2. This total loss of productive time has two components: the time spent on authentication procedures and the time spent on waiting for responses from the administrators. In this case study, under the assumption made in Table 2, the total authentication time loss amounts to 2500-3000 hours (Fig.5) and the total waiting time loss amounts to 6500-8000 hours (Fig.6).

The total non-productive time (NPT) is closely related to three factors: user behaviors, the number of employees supported by the administrators and the company document classification process (Table 2 and Fig.4). User behavior statistics are critical inputs into this Petri-nets model (Table 2), for example, the average time that users have to spend to pass user authentication and the frequency with which users forget the proper password and have to seek assistance. User behavior statistics can be improved by proper security awareness training[26]. The number of employees served by each administrator is another important factor. The larger the ratio between the number of employees to administrators, the more difficult it is for employees to get timely assistance.

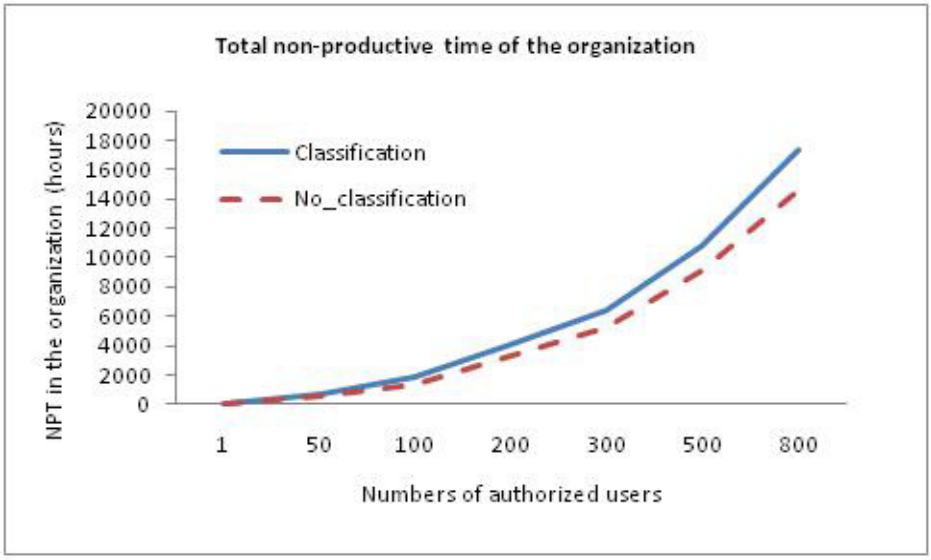

Fig. 4. Total non-productive time (NPT) associated with the deployment of MS IRM under the assumptions made in Table 2. NPT increases significantly when the number of authorized users served by each administrator increases. Proper classification of the company documents will reduce the NPT impact from the DRM deployment.

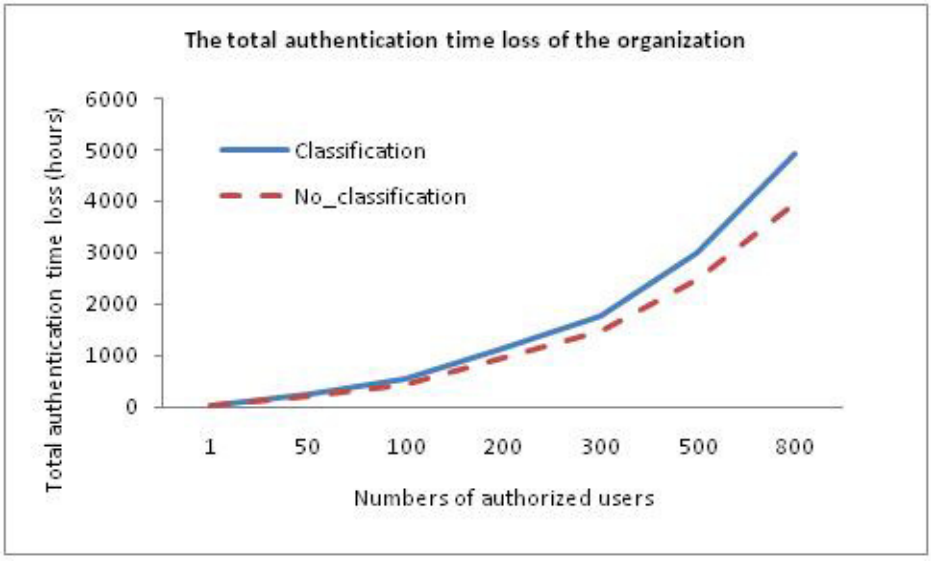

Fig. 5. Total authentication time loss associated with the deployment of MS IRM under the assumptions made in Table 2. Proper classification of the company documents will reduce the authentication time loss impact from the DRM deployment.

In addition, if the organization adopts a proper classification system, the non-productive time and availability of documents associated with the deployment of DRM products will be reduced (Fig. 4,5,6,7,8). That is, a proper document classification will help offset part of the negative effect that DRM products have on the efficiency of the organization. However, when the size of the organization is smaller than 100 staff members per administrator, the difference in NPT and availability

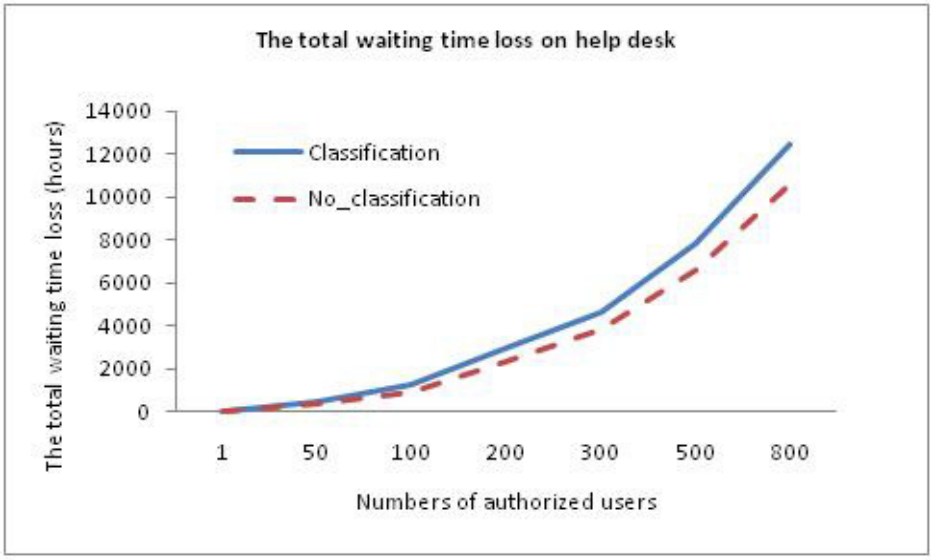

Fig. 6. Total waiting time loss associated with the deployment of MS IRM under the assumptions made in Table 2. The total waiting time loss increases significantly when the number of authorized users served by each administrator increases.

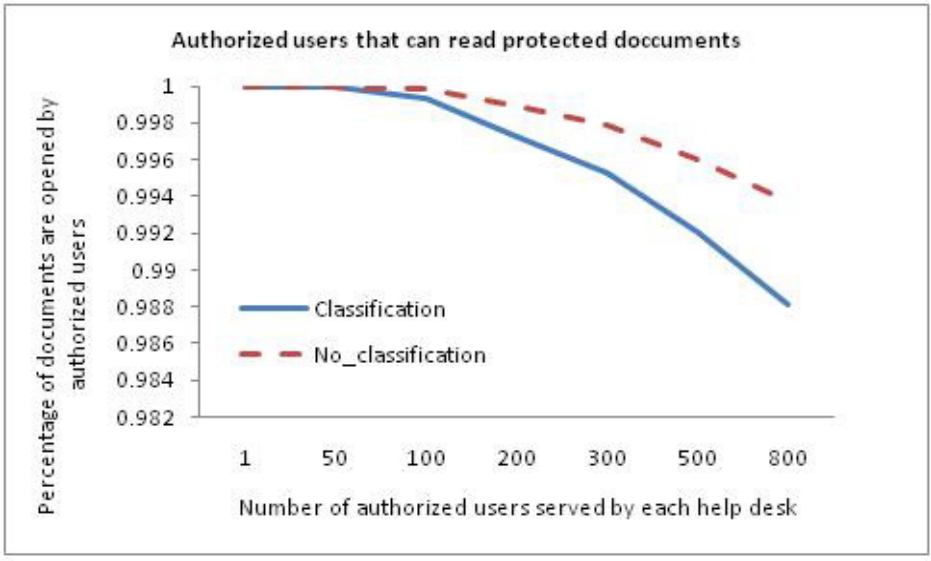

Fig. 7. The total numbers of documents users can read associated with the deployment of MS IRM under the assumptions made in Table 2. The number of documents users can read decreases significantly when the number of authorized users served by each administrator increases. Classification of the company documents will reduce availability of documents impact from the DRM deployment.

of documents between the modeled two scenarios, with and without a document classification, is not significant (Fig. 4,5,6,7,8). Therefore, when an organization makes decision on whether to adopt a more complex digital file classification system when planning the deployment of a DRM product, both the size of the organization and the number of administrators have to be taken into consideration.

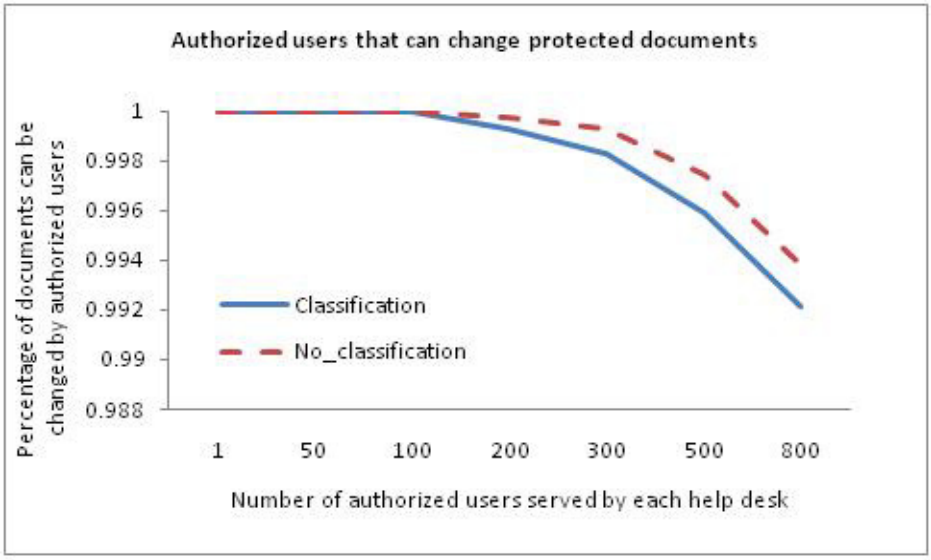

Fig. 8. The total numbers of documents users can change associated with the deployment of MS IRM under the assumptions made in Table 2. The number of documents users can change decreases significantly when the number of authorized users served by each administrator increases.

5 Conclusions

The stochastic Petri-net method is applied in this case study to build a model for the purpose of simulating the business process of deploying a DRM product. This model is used to quantify the potential impact of DRM products on the efficiency of the organization.

DRM products use encryption to make information in the organization secure so that only authorized users can access the documents. However, it is found that DRM products reduced the availability of documents within the organization even to authorized users. The authentication processes will result in non-productive time (NPT) for the employees, therefore, reducing the overall operational efficiency of the organization. This is particularly the case when authorized users cannot open secured documents for various reasons and have to wait the assistance from the administrators.

The stochastic Petri-net model quantified the NPT incurred by the deployment of the DRM product, and assisted in identifying the three major factors that affect the NPT: user behavior, the number of authorized users served by each administrator and document classification.

User behavior statistics are part of the input data into the Stochastic Petri-net model. They have direct impact on the amount of NPT incurred by the DRM products, as is output from the simulation model.

The NPT associated with the waiting for responses from the administrators increases significantly when the number of authorized users served by each administrator increases, although centralized control functionality of DRM helps to limit the number of administrators within an organization.

In addition, a proper document classification process can help reduce the negative impact of the deployment of DRM products on operational efficiency, although the benefit from classifying documents is limited, when the organization is small, or there are a large number of DRM administrators within the organization.

In summary, it is demonstrated that this stochastic Petri-net based business model has the potential to be used to help organizations to quantify the benefit and cost of implementing DRM products in order to make sound information security investment decisions.

References

[1] Kaspersky Lab,Internal IT Threats in Europe 2006, http://www.viruslist.com/en/analysis?pubid=204791935 (2006).

[2] IDC,Insider Risk Management: A Framework Approach to Internal Security, http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf (2009).

[3] J. C. Umeh, The World Beyond Digital Rights Management, *Swindon: The British Computer Society* , (2007).

[4] W. Zeng, S.E. Parkin and A. van Moorsel, Digital Rights Management, *Technical Report: CS-TR-1223, School of Computing Science, Newcastle University*(2010).

[5] Adobe Systems Inc., Adobe LiveCycle Rights Management ES, http://www.adobe.com/products/livecycle/rightsmanagement/ (2009).

[6] Oracle Corporation, Oracle Information Rights Management, http://www.oracle.com/technology/products/content-management/irm/index.html (2009).

[7] Microsoft Corporation, Microsoft Windows Rights Management Services for Windows Server 2003, http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx (2009).

[8] Authentica (EMC), Documentum IRM Services, http://uk.emc.com/products/category/intelligent-information-management.htm (2009).

[9] Liquid Machines, Liquid Machines Document Control, http://www.liquidmachines.com/document-control?id=1063(2009).

[10] Avoco Secure, Secure Documents, http://www.avocosecure.com/htmlpages/products/secureDocuments.html (2009).

[11] LockLizard, PDF Document Security/Web Content Security, http://www.locklizard.com/ (2009).

[12] Workshare Inc., Workshare Protect, http://www.workshare.com/products/wsprotect/default.aspx (2009).

[13] M.H. van Beek, Comparison of Enterprise Digital Rights Management systems, *Advice report, Aia Software*(2007).

[14] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli and G. Franceschinis,Modelling with Generalized Stochastic Petri Nets,*Wiley Series on Parallel Computing*(1995).

[15] W. M. P. Van der Aalst, The application of Petri Nets to Workflow Management, *The journal of Circuits, System and Computers* **8**(1998)21-66.

[16] N. R. Adam, V. Atluri and W. K. Huang, Model and analysis of workflow using Petri nets, *Journal of Intelligent Information System* **10**(1998)131-158.

[17] K. Salimifard and M. Wright, Petri net-based modeling of workflow system: An overview,*European Journal of Operational Research* **134**(2001)664-676.

[18] T. Murata, Petri nets: Properties, Analysis and Applications,*Proceedings of the IEEE* **77**(1989)541-580.

[19] W. H. Sanders, Mobius User Manual, *Version 2.2.1, University of Illinois*(2008).

[20] W. H. Sanders and J. F. Meyer, A Unified Approach for Specifying Measure of Performance, Dependability, and Perform ability, *Dependable Computing for Critical Applications***4**(1991)215-237.

[21] D. Sohn, Evaluating DRM: Building a Marketplace for the Convergent World, *Version 1.0* (2006).

[22] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty and Doubt, *Pearson Education. Inc.* (2007).

[23] E. Humphreys, Information Security Risk Management, *British Standards Institution* (2010).

[24] Microsoft Corporation, Active Directory, http://technet.microsoft.com/enus/library/bb742424.aspx (2010).

[25] Microsoft Corporation, Information Rights Management in the 2007 Microsoft Office system, http://office.microsoft.com/enus/help/HA101029181033.aspx#1 (2010).

[26] A. Stephanou, The Impact of Information Security Awareness Training on Information Security Behavior, *Research report in University of the Witwatersrand*(2008).