Evaluating Usage Control Deterrents

Keshnee Padayachee[1], J.H.P. Eloff[2]

[1]School of Computing, University of South Africa
[2]Information & Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria

ABSTRACT

This paper explores the effectiveness of usage control deterrents. Usage control enables finer-grained control over the usage of objects than do traditional access control models. Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. In this context, an adaptation of usage control is assessed as a proactive means of deterrence control to protect information that cannot be adequately or reasonably protected by access control. These deterrents are evaluated using the design science methodology. Parallel prototypes were developed with the aim of producing multiple alternatives, thereby shifting the focus from purely usability testing to model testing.

CATEGORIES AND SUBJECT DESCRIPTORS

D.4.6S [Security and Protection]

KEYWORDS

Access Control, Usage Control, Deterrent Control

1. INTRODUCTION

In general, the following countermeasures are employed to discourage the misuse of information systems – security policies, security awareness programs, computer monitoring and preventive security software [1]. The current research evaluated usage control deterrents deployed by a software system. Deterrence theory is based on certainty, severity and celerity of punishment that affects people's decisions about whether or not to commit a crime [2]. In an information systems security context, these may be visualised in terms of an employee's assessment of the consequences of a security threat and the probability of exposure to a substantial security threat [3]. According to D'Arcy and Hovav [1], the success of security countermeasures as a deterrence mechanism ultimately depends on the actions and awareness of end-users, and managers should understand the effect of controls from the perspective of end-users. Such an understanding would produce a more realistic evaluation of the effect of security countermeasures on end-users' computing behaviour. Furthermore, an access control system should provide countermeasures that dissuade users from committing data abuse.

Industry surveys confirm that a substantial portion of computer security incidents are due to the intentional actions of legitimate users. The consequences of these include negative publicity, competitive disadvantage and the loss of consumer confidence [1]. Hence it is vital that access control systems oblige the user to comply with the access control policies propagated by the system. Padayachee and Eloff [4] presented a model for addressing the inadequacies of access controls, which involved a reformulation of usage control as a mechanism to deter users from information abuse, rather than one that is entirely dependent on denial of access. Padayachee and Eloff's [4] approach towards deterrence control is an application of optimistic access control, which is useful in cases where openness and availability are more important than complete confidentiality [5]. Optimistic access control involves a combination of audit and accountability aspects as deterrent mechanisms to encourage trustworthy behaviour. This approach is characteristically retrospective, rather than proactive. However, the application of usage control within an optimistic access control context may provide a proactive means of deterrent control. Usage control enables finer-grained control over the usage of objects than do traditional access control models [6]. Within traditional access control models, usage control would offer an extra layer of restriction to prevent unauthorised usage. However, under the optimistic access control paradigm, usage would not be restricted, but users would rather be deterred from illicitly accessing and misusing information. Furthermore, the risk of denial of access in an emergency situation is averted. In terms of the optimistic access control paradigm, the user must ultimately be able to access the required information. Although this model may solve the problem of implementing and maintaining complex access control policies, its flexibility may render it vulnerable to exploitation. The issue at hand is whether system deterrents are considered to be an effective mechanism for controlling illicit access in an open architecture such as optimistic access control.

This paper presents an evaluation of usage control deterrents to determine whether this type of implementation indeed increases an end-user's propensity towards compliant security behaviour. The rest of the paper is structured as follows: Section 2 elaborates on access control models in general. Section 3 deals with the research methodology chosen to evaluate usage control deterrents, while the results of the evaluation are presented in Section 4. Finally, Section 5

[1] Email: padayk@unisa.ac.za,

[2] eloff@cs.up.ac.za

suggests possible future research opportunities and Section 6 concludes the paper with a summary.

2. BACKGROUND TO ACCESS CONTROLS

Access control is a fundamental part of computer security where every requested access must be governed by an access policy that states who is allowed access to what. The request must then be mediated by an access policy enforcement agent [7]. Traditional access control models assume that human beings cannot behave in a trustworthy manner and that the system has to prevent them from behaving in an undesirable manner. Traditional models such as mandatory access control (MAC) or role-based access control (RBAC) are based entirely on denial of access. For instance, with MAC [8], access control policy decisions are made beyond the control of the individual owner of the object and a central authority determines what information is to be accessible by whom. The user cannot change access rights [9]. With RBAC, system administrators create roles according to the job responsibilities assumed in a company, they grant permissions (access authorisation) to those roles, and then assign users to the roles on the basis of their specific job responsibilities [10]. For instance, a patient's medical information can be accessed by any health professional assigned to the role of ward physician [11]. However, this does not guarantee that an authorised user demonstrates integrity or acts professionally.

Optimistic access controls address this gap where access control is not preconfigured and the user is essentially trusted to behave ethically. While traditional access controls such as MAC or RBAC may be highly appropriate in certain contexts, optimistic access controls may be more appropriate in other circumstances. A field study conducted by Stevens and Wulf [12] who considered the cooperation between two engineering offices and a steel mill is a case in point. Within this real-world inter-organisational cooperation scenario, it was found that traditional access controls do not comply with the organisation's requirements and that cooperation and competitive reasons motivate the use of interactive and optimistic access controls [12]. Since the flexibility offered by optimistic access control may well be exploited, Padayachee and Eloff [4] proposed that optimistic access control should be complemented with usage control.

The optimistic access-control-with-usage-control model, designated the $OAC_{(UCON)}$ model, is a formalisation and consolidation of the work by Padayachee [13]. The $OAC_{(UCON)}$ model employs usage control as a deterrent mechanism to proactively prevent users from committing data misuse (see Figure 1). Usage control (UCON) considers the missing components of traditional access control, such as the concepts of obligations and conditions. *Obligations* require some action by the subject (user) so as to gain or sustain access, for example by clicking on the ACCEPT button in a licence agreement or agreeing not to distribute a confidential document. *Conditions* represent system-oriented factors such as time-of-day, where subjects are allowed access only within a specific time period. With traditional access control, authorisation is assumed to be done before access is allowed. However, the UCON model extends these conditions with continuous enforcement by re-evaluating usage requirements throughout usages (ongoing evaluation) [6]. The $OAC_{(UCON)}$ model does not initially depend on the subject attributes or object attributes as do traditional access models. It is an open architecture that becomes increasingly constrained to users that have demonstrated that they are undeserving of being trusted with information. For the most part, it is assumed that data is freely available. As such, the user is expected to behave in a trustworthy manner. Consequently, trust is maintained by the user's acceptance of the *pre-obligations*, the *ongoing obligations* and the *post-obligations* that are coupled with accessing the information. However, the subject will not be allowed to access information unless the conditions are valid before usage (*pre-conditions*). If the conditions become invalid during usage (*ongoing conditions*), then access is immediately revoked. As the present model is based on optimistic access control, there must be a means to override these conditions under special circumstances. Hence the model provides a facility such as a *break-the-glass* mechanism to supersede the system in an emergency. With the $OAC_{(UCON)}$ model the user must ultimately be able to access the information unless his/her rights to information in the optimistic access control domain have been downgraded based on prior misdemeanours. This task is performed by the *Post Update Module*. The *Audit Module* checks for red flags and unjustified breaches, for example an unfulfilled post-obligation. The *Roll-back Module* may be deployed if an unjustified breach resulted in the data being compromised. The current research does not promote the notion that traditional access control models are inferior to optimistic access control. Rather, it was suggested that the two approaches might work well together in a complementary approach. The $OAC_{(UCON)}$ model is flexible and reduces the burden of setting preconfigured security policies for every subject-object relationship. Thus it decreases the load on system administrators. However, the model acknowledges that the gains realised by flexibility should not be negated through data misuse. Therefore, the model provides sufficient deterrents against data misuse by leveraging the security mechanisms offered by usage control. It is proposed that data that cannot be reasonably protected within traditional access control could be protected by these usage control deterrents. In the next section, this approach is evaluated.

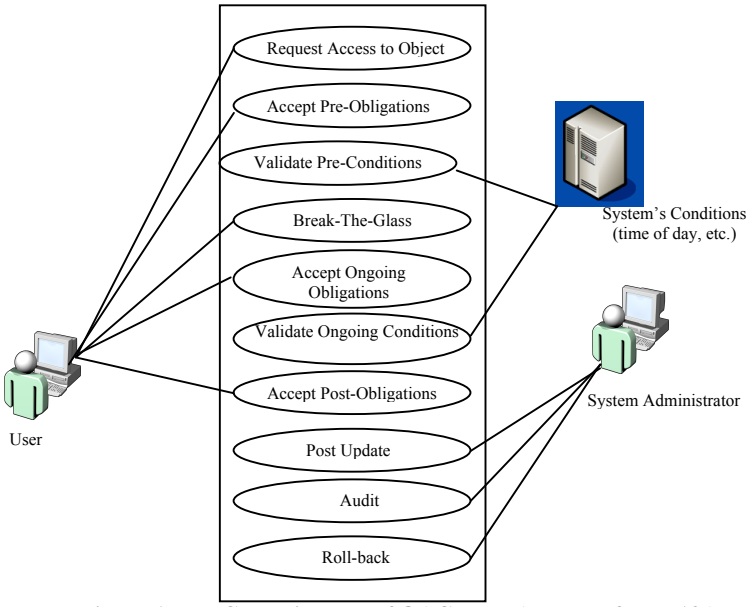

Figure 1. Use Case Diagram of $OAC_{(UCON)}$ (adapted from [13])

3. RESEARCH METHODOLOGY

The design science research methodology was used to conduct a small-scale experiment based on the following activities: build, evaluate, theorise and justify [14]. Figure 2 demonstrates the steps taken in the model. Design science is a pragmatic research paradigm that calls for the 'creation of innovative artefacts to solve real-world problems' [15]. A proof-of-concept prototype was developed by the author. However, in order to remove researcher bias, the product concept was introduced to 14 Honours students at the University of Pretoria. They were not shown the working version so as not to bias their judgement of the concept.

Purposive sampling was used, as the participants had to be advanced programmers. As this was not purely a usability study rather it involved reasoning about the model concept. It was posited that participants that developed the model could provide more in-depth analysis than an end-user perspective. Parallel prototypes have value in terms of producing multiple alternatives thereby adding to the diversity [16] of perception. The authors assert that developing a parallel prototypes and having several testers shifts the focus from pure usability testing to proof-of-concept testing.

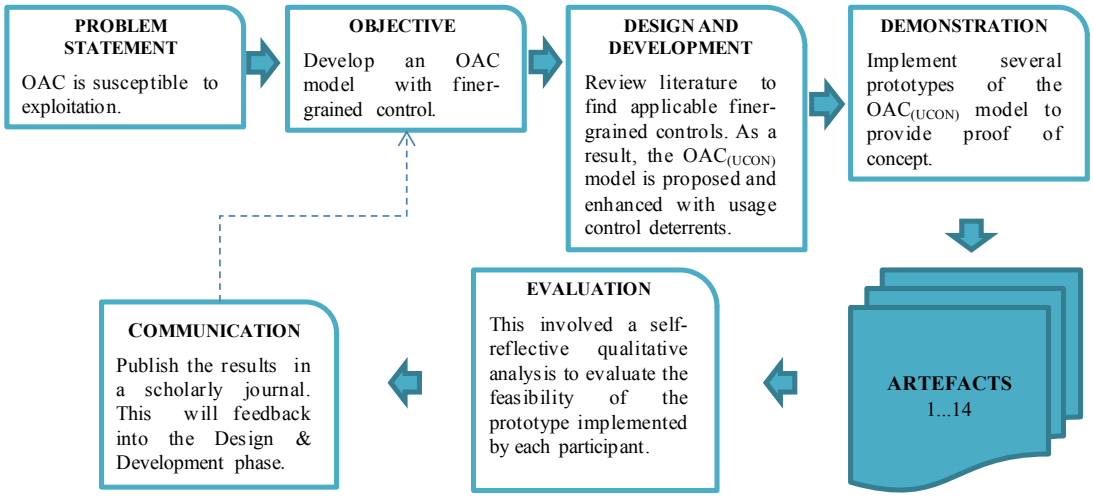

Figure 2. The Phases in the Research Design (adapted from [17])

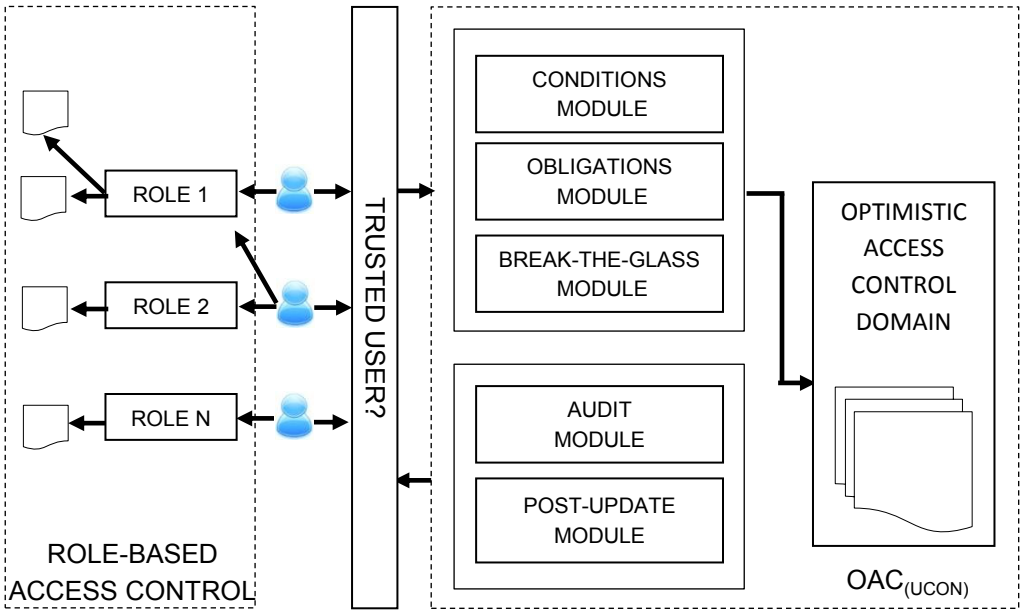

Figure 3. The $OAC_{(UCON)}$ model complemented by RBAC and Trust (adapted from [13] and [18])

According to [17], the process of design science research involves defining the following phases: *Problem Statement*, *Objectives*, *Design and Development*, *Demonstration* and *Evaluation,* and finally *Communication,* which is evidenced by this article. The problem statement essentially is concerned with the susceptibility of OAC. The objective is to enhance OAC with finer-grained controls such as usage control. The *Design and Development* phase led to the creation of the $OAC_{(UCON)}$ model. The *Demonstration* phase employed postgraduate Computer Science students from the University of Pretoria and involved them in the implementation of the evaluative prototypes. Each participant had to implement an operational prototype. In the *Evaluation* phase, fourteen artefacts were evaluated with respect to each participant's perceptive on the model as well as his/her design decisions. The concept specification was scaled up to a real-world scenario and included an RBAC component together with a trust component. Figure 3 shows how data may be managed by using two types of access control: RBAC (on the left) and optimistic access control enforced with usage control deterrents such as obligations and conditions (on the right). This is moderated by a trust component that may downgrade a user's privileges to information in the optimistic access control domain. The latter occurs through the process of auditing and then performing an update on the user's access rights using fuzzy logic. Only the aspects specifically related to access control were considered.

Participants were given the following specifications (summarised from [13]) as a term assignment:

- Create database to store information on a typical organisation with employees and clients.
- Client information is relegated to the public domain, while the employee data is protected by role-based access controls.
- The employee records are protected by role-based access controls. There are three roles: *manager*, *administrator* and *user*. The manager can *read*, *delete* and *update* an employee record, whereas an administrator can *read* and *update* an employee record. Users can only *read* employee records.
- User authentication and access control policies for the data in the database are required and a policy file is used to grant permissions to authenticated users.
- If the user attempts to access data in the public domain, then he/she is subject to the following usage control mechanisms:
  - Pre-obligation: The user must click on a button in a dialogue box, thereby indicating that he/she agrees not to distribute this information.
  - Pre-condition: This information must be accessed during business hours only.
  - Ongoing obligation: A window with the following warning "This dataset must be used EXCLUSIVELY for work-related purposes" is to remain open while the user accesses the information.
  - Ongoing condition: This information may be accessed during business hours only.
  - Post-obligation: The user must send an e-mail to the administrator if he accessed these databases outside of business hours.
  - Break-the-glass (BTG): While the user will not be permitted to access the information unless the obligations have been satisfied, he/she will under special circumstances be allowed to access it by utilising the BTG facility even if the pre-conditions or ongoing conditions are invalid.
  - Post-update: A user's rights to information in the public domain can be modified based on prior usage. The program should log all access in such a way that there is a secure audit trail. At the onset, each user has a trust level of high. However, as he/she demonstrates untrustworthiness, this level is downgraded to medium and finally to low. As the trust level drops, the user loses his/her right to information in the public domain – i.e. the information to which he/she is

allowed access is constrained. Users with a medium trust level can access most information except for account information. Users with a low trust level are not allowed to view account information or contact details. They can be limited to view less sensitive details such as the client's name, occupation, etc.

- After the user has accessed the database, his/her trust level is updated by using fuzzy logic. For test purposes, each access can be given a random priority [0, 1]. If the BTG facility was deployed by the user, then the trust level [0,1] is updated, dependent on the priority of the task and the user's previous trust level using the fuzzy matrix given below (Table 1).

Table 1. Fuzzy Matrix for Trust Levels

Previous Trust Level	Priority of the Task		
	High	**Medium**	**Low**
High	Trust level remains High	Trust level downgraded to Medium	Trust level downgraded to Medium
Medium	Trust level remains Medium	Trust level downgraded to Low	Trust level downgraded to Low
Low	Trust level remains Low	Trust level remains Low	Trust level remains Low

During the evaluation stage, the participants interacted with their individual evaluative prototypes and provided value judgements on them in terms of the effectiveness of the security mechanism provided by the $OAC_{(UCON)}$ model. In the following section, only the issues relating to the effectiveness of usage control deterrents are synthesised from the study by Padayachee [13]. The design science methodology was selected as it provides more than a mere usability study of usage control deterrents. It also allows participants to reason about the implementation and operational requirements of the system, as well as possible deficiencies of the model. In order for suitable interpretations of the model to emerge, participants were not given a formal design as to how to implement usage control deterrents. However, most participants naturally expressed usage control deterrents by means of dialogue boxes or pop-ups with explicit warning messages.

In this synthesis of the evaluation three main factors were extrapolated: risk, compliance and the usability of usage control deterrents as shown in Figure 4. There was considerable debate about the proper definition of an information security risk, which may be defined as 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation' [19]. The risk of relying entirely on usage control deterrents such as conditions and obligations is reviewed within this context. On the opposing side of the continuum, the risk of using access control policy based entirely on denial of access is not considered in this study.

With regard to usability (according to Whitten and Tygar [20]), security software is usable if the individuals who are expected to use it

- are reliably made aware of the security tasks they need to perform;
- are able to figure out how to successfully perform those tasks;
- do not make dangerous errors; and
- are sufficiently comfortable with the interface to continue using it.

From this standpoint, usability is viewed as the extent to which the system is usable within the bounds of usage control deterrents. It is important to note that, as the design science methodology was used, this evaluation focused on implementation issues relating to the interface rather than on aesthetic issues.

It is hypothesised that usage control deterrents should increase an end-user's compliance intention. In this regard, the compliance mindset subscribes to what might be called a deterrence theory of motivation, which employs mandates, procedural controls and threats of punishment to manage and motivate people [3]. In terms of this evaluation, compliance is viewed as the extent to which usage control deterrents compel a user to comply with access control policies.

The participants were given value statements about the model concept they had to implement and they had to indicate whether they agreed or disagreed with the statements. These statements emphasised the compliance intention, risks and usability of the model concept in terms of its implementation. In addition, the researcher conducted a qualitative interview with each participant to determine his/her perception of the viability of the model concept with respect to deterrent control. Participants had to consider the model concept in terms of the following: weaknesses, strengths, potential improvements, viability, applicability and scalability.

4. DATA ANALYSIS

The participants were given statements based on the sample items listed Table 2. For each value statement, participants had to provide a value judgement (agree/disagree) and justify their response. All the participants agreed that the model specifications were viable. However, the priorities of task specification were criticised as they were assigned randomly in the specification. In addition, the specification 'did not give explicit rules for the break-the-glass option'. This notion would be an additional improvement to the model in future studies.

Table 2. Responses to the value judgements synthesised from [13]

	Value Statements	*% Agree*	*Causative Responses*
Compliance	*(1) Other non-technical mechanisms would be more effective than system deterrents.*	21.5%	Other mechanisms – in combination – will increase the security overall. The training and policy documents are "simpler to ignore" and "not a constant reminder" as is the case with an automated system.
	(2) Specifying system conditions deters users from abusing their privileges.	78.5	These conditions may give users the feeling that they are "doing something wrong" and that they will be deterred as a result. The threat of punishment and losing trust may motivate users not to abuse their privileges.
	(3) Fulfilling obligations will compel users to comply with the established rules of behaviour.	85%	Using obligations will prevent users from claiming ignorance as an excuse for not complying. As users are intimidated by warnings, user responsibility can be expected to increase.
	(4) The risk of losing one's rights to information may deter one from abusing one's privileges	84.6%	The threat of being caught and losing one's trust is a strong motivator. However, if the user's premeditated goal is to steal data, these mechanisms will not prevent such incidences.
Risk	*(5) The flexibility offered under the optimistic access control domain is a security risk.*	78,5%	This depends on the nature of the organisation and its data, and the fact that some environments such as the medical industry actually require the proposed level of flexibility.
	(6) The break-the-glass facility is vulnerable to abuse.	71%	The threat of being discovered after the event is a way of preventing the Break-the-Glass facility from being misused.
Usability	*(7) An individual who interacts with the system will recognise that access is dependent on user responsibility as well as technical access control.*	71.4%	Although this is probably true, users are irresponsible and untrustworthy.
	(8) Most users will ignore the messages about conditions and obligations relating to access.	50%	Users will eventually pay no attention to these messages. Users will ignore these messages unless the consequences are clearly specified.
	(9) System deterrents may be distracting to a user.	43%	After some time most users will ignore these pop-ups anyway. However, all of this will depend on how the user interface was designed.

According to our study the greatest deterrent appears to be the risk of losing privileges. The results indicated that the specifying of obligations would deter end-users more than would the specifying of conditions. The latter gives the user an indication that he/she is 'doing something wrong' and as a consequence he/she may decide rather to comply. Using obligations would prevent users from claiming ignorance as an excuse for not complying. Furthermore, given that users are intimidated by warnings, user responsibility could be expected to increase. Overall, most participants agreed that system deterrents would be effective. Some participants indicated that this does not negate the need for security training and policy documents. However, usage control deterrents were harder to ignore than were non-technical mechanisms. Relying entirely on system deterrents seemed to be considered a high risk, although some participants indicated that various organisations, such as those in the medical industry, might actually require an open architecture. Most of them, though, indicated that the threat of being discovered after the event was a way of preventing users from misusing their privileges.

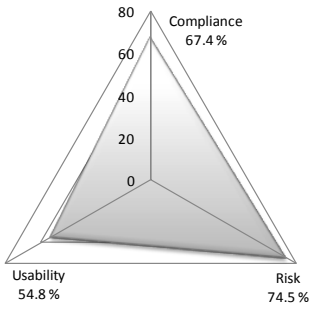

Figure 4. Evaluating Usage Control Deterrents with regard to Compliance, Risk and Usability

The security usability of system deterrents was ranked as intermediate. Participants felt that end-users would understand the purpose of system deterrents and take responsibility for their actions. However, they also felt that system deterrents would be distracting to users and over time they would probably become complacent about the warning messages. It was proposed that there be a way for users to respond to the messages in such a way that they cannot simply ignore the implications of the warnings. In addition, the consequences of non-compliance should be indicated clearly. The findings discussed above were extrapolated from Figure 4. It consolidates the percentage of the participants who agreed with the value statements in Table 2 and places them into three categories – Compliance, Risk and Usability.

In general, most participants regarded relying entirely on proactive system deterrents to be a considerable security risk. However, they reasoned that the additional facilities of obligations and conditions might deter users from abusing their privileges. In order to lower the risk, participants indicated that there must be discernible and adequate monitoring of usage. Although the risk of relying on end-users to comply is high, usage control deterrents should have a positive influence on compliance. In terms of improvements, it was suggested that the conditions be more dynamic and based on user profiles. The evaluation exercise revealed that usage control deterrents would be suitable to environments where users were transitory. They would furthermore be more suitable in environments where damage was reversible or in small organisations that relied on data that was not highly sensitive. With regard to security usability, usage control deterrents were argued to be potentially distracting and to impact negatively on the productivity of users. Perhaps, as the user became more 'trustworthy', some obligations or conditions could be relaxed or negotiated. It is important to note that participants felt that users should be meticulously authenticated before system deterrents could be entirely relied upon. The sample size was small (14 participants), hence the limitations of the experiment need to be heeded when making generalisations from the research. A small sample size however allowed for a more in-depth analysis of each participant's value judgement on the prototypes produced.

5. FUTURE RESEARCH

In this study, usage control deterrents were evaluated on the basis of three factors, namely risk, compliance and usability. Future studies could involve research into other intrinsic factors that influence compliance. Workman, Bommer and Straub [21] already considered several intrinsic factors in terms of non-compliant behaviour. The *response efficacy* factor relates to a user's perception of the effectiveness of preventive software measures correlated with evaluating the effectiveness of an access control system. The present study considered behavioural factors that relate to employees who ignore security countermeasures, such as being monitored. According to Workman, Bommer and Straub [21], s*elf-efficacy* and *locus of control* are intrinsic motivators that may offer a useful framework to assist organisations in determining the reasons that influence a user to change his/her behaviour and take security precautions.

6. CONCLUSION

According to Siponen, Pahnila and Mahmood [22], the results of a study of this nature are relevant for both researchers and practitioners. It is useful to obtain empirically proven information as to how organisations can improve their employees' adherence to information security policies and hence improve information security in their organisations. The $OAC_{(UCON)}$ model has not been tested within a large distributed system with several end-users in an organisational setting. However, participants who tested the model concept may be considered the representatives of stakeholders in the information technology industry. As postgraduate students, they have extensive knowledge of information systems and are currently employable or employed within the information systems sector. The model concept was found to be highly viable as all participants were able to implement the scaled-up version of the concept. The risks of having an open architecture were rated as high, but the proposed usage control deterrents were considered to be an effective way of limiting the risks posed. Consequently, the complexity of implementing and maintaining preconfigured access control policies was shifted to the way the user interacts with the system. Adapting usage control as a deterrent has provided a proactive mechanism over and above the retroactive methods of auditing and accountability. By using the $OAC_{(UCON)}$ model, a larger subset of information may be relegated into the public domain. However, the usability of usage control deterrents needs to be addressed. These deterrents need to be enforced in such a way that the end-user is always cognisant of access control policies. In the final analysis: in determining whether to implement usage deterrents in an organisation, it would be useful to weigh the risk of denying access for a legitimate purpose against the risk of using open-ended architecture such as the $OAC_{(UCON)}$.

ACKNOWLEDGEMENTS

The author (affiliated with the University of Pretoria) would like to acknowledge the support of SAP Research and the SAP Meraka Unit for Technology Development.

REFERENCES

[1] D. D'Arcy and A. Hovav, "Deterring internal information systems misuse", Communications of the ACM, vol. 50, pp. 113-117, 2007.

[2] G. E. Higgins, A. L. Wilson, and B. D. Fell, "An Application of Deterrence Theory to Software Piracy", Journal of Criminal Justice and Popular Culture, vol. 12, pp. 166-184, 2005.

[3] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations", European Journal of Information Systems, vol. 18, pp. 106-125, 2009.

[4] K. Padayachee and J. H. P. Eloff, "Adapting usage control as a deterrent to address the inadequacies of access controls", Computers and Security, vol. 28, pp. 536-544, 2009.

[5] D. Povey, "Optimistic Security: A New Access Control Paradigm", in Proceedings of the 1999 workshop on New Security Paradigms. Caledon Hills, Ontario, Canada, 1999.

[6] R. Sandhu and J. Park, "Usage Control: A Vision for Next Generation Access Control", in Computer Network Security, vol. 2776, Lecture notes in Computer Science, V. Gorodetsky, L. J. Popyack, and V. A. Skormin, Eds. Berlin/Heidelberg: Springer, 2003, pp. 17-31.

[7] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3rd ed. Prentice Hall, Upper Saddle River, New Jersey, 2003.

[8] R. Ramachandran, D. J. Pearce, and I. Welch, "AspectJ for Multilevel Security", presented at the 5th AOSD Workshop on Aspects, Components and Patterns for Infrastructure Software (ACP4IS), Bonn, Germany, 2006.

[9] C. P. Pfleeger, Security in Computing, 2nd ed. United States of America: Englewood Cliffs, NJ.: Prentice Hall, 1997.

[10] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models", IEEE Computer, vol. 29, pp. 38-47, 1996.

[11] P. Pudney, "e-Consent in consumer health & telemedicine," in Telemedicine Research Center: University of South Australia, 2003.

[12] G. Stevens and V. Wulf, "A New Dimension in Access Control: Studying Maintenance Engineering across Organizational Boundaries", in Proceedings of the ACM conference on Computer Supported Cooperative Work (CSCW). New Orleans, Louisiana, USA, 2002.

[13] K. Padayachee, "An Aspect-Oriented Approach towards enhancing Optimistic Access Control with Usage Control", in Computer Science. Pretoria: University of Pretoria [Online] Available: http://upetd.up.ac.za/thesis/available/etd-07262010-142652/ (Last accessed 5 November 2010), 2009.

[14] M. T. March and G. F. Smith, "Design and natural science research on information technology", in Decision Support Systems, vol. 15, pp. 251-266, 1995.

[15] A. Hevner and S. Chatterjee, "Design Science Research in Information Systems," in Design Research in Information Systems, Integrated Series in Information Systems: Springer US, 2010, pp. 9-22.

[16] S. P. Dow, A. Glassco, J. Kass, M. Schwarz, and D. L. Schwartz, "Parallel Prototyping Leads to Better Design Results, More Divergence, and Increased Self-Efficacy", ACM Transactions on Computer-Human Interaction, vol. 17, pp. 18:1-18:24, 2010.

[17] K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen, and J. Bragge, "The design science research process: a model for producing and presenting information systems research", presented at Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, USA, 2006.

[18] P. Samarati and S. de Capitani di Vimercati, "Access control: Policies, models, and mechanisms", in Foundations of Security Analysis and Design, vol. 2172, Lecture Notes in Computer Science, R. Focardi and R. Gorrieri, Eds. Berlin: Springer-Verlag, 2001, pp. 137-196.

[19] J. R. Vacca, Computer and Information Security Handbook. Burlington, USA: Elsevier Science and Technology, 2009.

[20] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", in Proceedings of the 8th USENIX Security Symposium. Washington DC, America, 1999.

[21] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test", Computers in Human Behavior, vol. 24, pp. 2799-2816, 2008.

[22] M. Siponen, S. Pahnila, and A. Mahmood, "Employees' Adherence to Information Security Policies: An Empirical Study", presented at IFIP International Federation for Information Processing, 2007.