Towards information sharing in virtual organisations: The development of an icon-based information control model

Shada Al-Salamah[1], Jeremy Hilton[1], Pete Burnap[1]

[1]Department of Computer Science & Informatics, Cardiff University, Cardiff, UK

S.A.Salamah@cs.cardiff.ac.uk, Jeremy.hilton@cs.cardiff.ac.uk, p.burnap@cs.cardiff.ac.uk

Keywords

Information security, Access control model, Information sharing, Collaboration and virtual organisation

1. Introduction

Today, innovation in information technology has encouraged contribution among different fields, including healthcare, business, government, and science. This is to tackle large-scale scientific problems or introduce novel inventories which, in both cases, demand extensive sharing of different resources, including data and information, among collaborating organisations in order to achieve the overall goal [1-3]. In such environments, such contribution consists of distributed resources used and shared by users from geographically and administratively distributed physical organisations that own the resources, and this contribution forms Virtual Organisations (VOs) [2, 3]. To facilitate collaboration among users in a VO, the resources should be available across organisations seamlessly [2]. The term “seamlessly”, in this context, means that when an authenticated user from one of the participating organisations grants access to the environment controlled by another organisation, the user can access and use the resource through direct communication. This is important because seamless resource sharing significantly improves the effectiveness and efficiency of collaborations among various organisations [2].

However, VOs have raised a number of information security issues that limit the effectiveness, dynamism, and potential of collaborative working. A major obstacle preventing these kinds of collaborations from being widely adopted is the ability to govern remote access to sensitive information during the time of contribution and control its usage after access has been granted, either when disseminated electronically, transformed into paper format, or even shared verbally. Therefore, massive information security research has been conducted to control access and usage of resources and hence, a number of theories and technologies have attempted to provide information access and usage control solutions to facilitate the distribution and sharing of information in such environments. This includes, but is not limited to, traditional access controls, digital rights management, trust management, and usage control. Nonetheless, they focused on the research’s own target problems and provided detailed solutions with consideration only to these problems, and thus, there is a lack of comprehensive, systematic approaches for controls on usage of information shared electronically regardless of specific circumstances [1]. The three key information security issues investigated and identified in this paper are, firstly, most access control models are based on a system-level protection of information in which users are either granted full access to information (once they have been authenticated) or rejected [4]. This, consequently, may result in restricting the information sharing if any information encompasses a small amount of high-level sensitive content that demands restricted access to [4]. Secondly, the solutions attempt to protect information as long as it exists within the secured boundaries of the organization, and when this information is shared across the secured information system and network, the information is no longer secured or controlled [4]. Finally, although a few solutions were able to protect digital content after distribution (such as digital rights management), they are constrained by a limited number of uses and/or users [5]. However, even if some solutions sustained control over information, the control policy associated with the content cannot be changed by the owner of the information after dissemination [4]. In fact, this is a vital issue that would prevent the adaption to virtual organisations' dynamic environment, for example, when the VO working group may disperse or, simply, the VO users and/ or physical organizations participating need to be changed, and thus, there will be a persistent need to deny access to information previously shared [6].

2. Methods

This paper proposes an information control model that is built on two previous research works, SPIDER solution [4] and Protective Commons (PC) [7], and is demonstrated in the Microsoft Office Word 2007 application. This was achieved in three different and interrelated stages: First, SPIDER solution was explored. SPIDER (short for Self Protecting Data for De-perimeterised Information Sharing) is an access control model that investigated the constraints and weaknesses of the existing access control models, and addressed the information security issues mentioned previously by simply believing that information has different levels of sensitivity, and thus, different levels of protection are required. As a result, it used a classification scheme to assign and sustain the right protection level to the exact amount of information that requires that protection. This scheme is based on the Traffic Light Protocol philosophy, which comprises four marking colours (red, amber, green, and white) to reflect the level of information sensitivity and protection needed. Second, SPIDER capabilities were extended by initially defining three different access control permissions associated with information content (read, write, and ownership), then distinguishing between the information owner and user, and finally, adopting a labeling scheme, proposed by PC, instead of the classification scheme. This labeling scheme is not only categorized based on the protection level needed, but additionally, the usage of the information after it is accessed by the right users in the VO. PC produced a set of nine complementary icons as visual information labels and suggested a number of associated information security controls with these icons based on the meaning they attempt to convey. Each control represents a license that is described in three different levels of information formats: lawyer-readable, human-readable, and machine-readable license. Finally, Microsoft Office Word 2007 application has been selected as the platform for demonstrating this information control model.

3. Results

The information control model proposed in this paper adopted the icons provided by PC to generate an icon-based information labeling scheme. Every time the user labels a selected range of information with an icon before distribution, an Access Control Policy (ACP) is created/ updated. This ACP considers the type of user accessing the information, the permission associated with that user, the selected icon, and the associated control(s). It is embedded in the information range before distribution, linked to it thereafter, and can be updated at any time only by the information owner(s) (i.e. a user or a group with ownership permission to the information range).

This model was represented in a developed plug-in software, named Information Labeling Palette (ILP), into Microsoft Office World 2007 application that is believed to be a comprehensive platform for information exchange among the VO users, and is one of the leading word processors with security features. This makes it a secured environment for hosting ILP. ILP is in its early development stages, and so far it has implemented two of the nine icons: *Restricted Access and Authorised-by* icons. The former icon is used for highly sensitive information ranges that can only be shared with nominated user(s) by the information owner, and should be encrypted for the recipient(s) when stored or shared outside the controlled environment. The latter is used for information ranges that needs to be digitally signed with a qualified electronic signature compliant with the EU Digital Signature Directive. Each icon is used to assign its control rules to the labeled information at three different levels with a single button-click: an 'expert'-level policy which contains full rules in 'legal code' for an information security officer; human-readable rules contained in an electronic description within the icon and the controls associated with them; and machine-readable rules, which are transparent to the user, that generate machine-level commands to programmatically enforce the control to the information range.
The Information Labeling Palette plug-in software is illustrated in Figure1 and 2.

4. Conclusion

The aim of this paper was to investigate and present a novel information control model that would keep information self-protected in dynamic collaborative environments not only by enforcing different levels of protection controls within the same information content for electronic dissemination, but also to inform usage when the information is transferred into a paper format, or shared verbally. Although ILP is in its early stages of development, unit and system-level tests showed that the early-defined system requirements of the two developed icons were met. In addition, Microsoft Word has been widely used in different platforms, including Windows and Mac operating systems. This facilitates the use of the developed model by a wide range of users around the globe with no technical experience or knowledge. Furthermore, different complex environments such as healthcare have different information security requirements and issues, and this novel information control model can be widely applicable for addressing the issues and tailored for meeting the needs. Finally, it is believed to lay a good foundation for future work in the area of information security and control policy enforcement in collaborative environments.

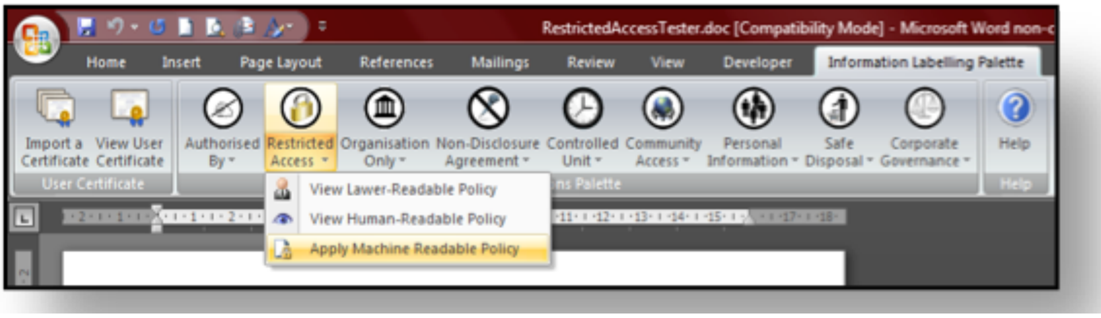
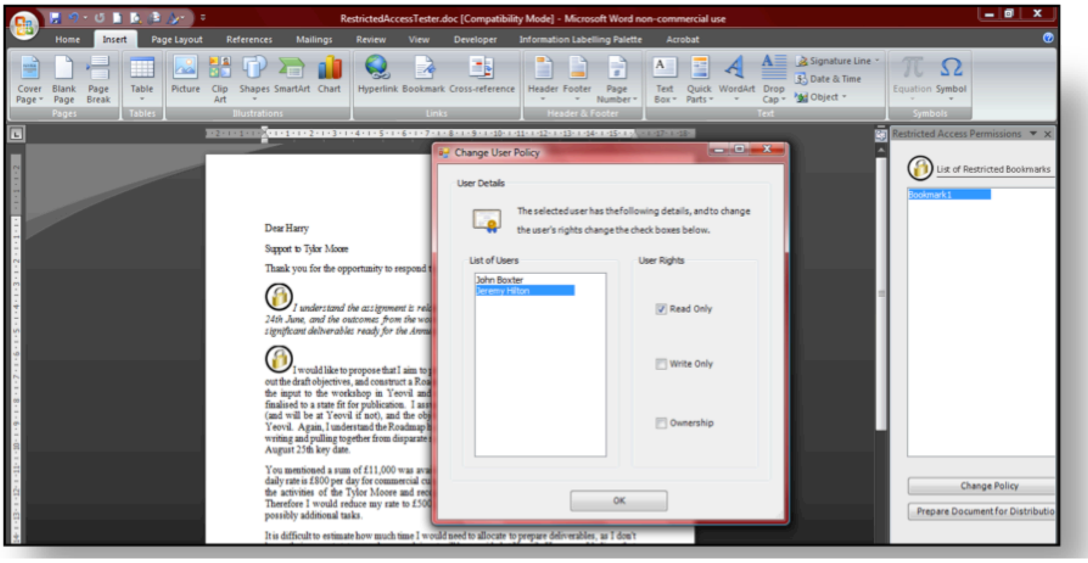


Figure 1 Information Labelling Palette plug-in and the three levels of control license



The selected user has thefollowing details, andto change the user's rights change the check boxes below.

☑ Read Only

☐ Write Only

☐ Ownership

Dear Harry

Support to Tylor Moore

Thank you for the opportunity to respond t

I understand the assignment is rel
24th June, and the outcomes from the wo
significant deliverables ready for the Annu

I would like to propose that I aim to p
out the draft objectives, and construct a Roa
the input to the workshop in Yeovil and
finalised to a state fit for publication. I ass
(and will be at Yeovil if not), and the obj
Yeovil. Again, I understand the Roadmap h
writing and pulling together from disparate
August 25th key date.

You mentioned a sum of £11,000 was ava
daily rate is £800 per day for commercial cu
the activities of the Tylor Moore and rec
Therefore I would reduce my rate to £500
possibly additional tasks.

It is difficult to estimate how much time I would need to allocate to prepare deliverables, as I don't

Figure 2 Restricted range of information with nominated users and permission(s) assigned to them

References

[1] Park J and Sandhu R. (2002). Towards Usage Control Models: Beyond Traditional Access Control Proceedings of SAMAT 2002, Monterey, California. 3th-4th June 2002, ACM.

[2] Yau S. S. and Chen Z. (2008). Security Policy Integration and Conflict Reconciliation for Collaborations among Organizations in Ubiquitous Computing Environments. L. F.E. Sandnes et al. (Eds.): UIC 2008. Berlin, Heidelberg, Springer-Verlag (2008): PP.3-19.

[3] Wasson G. and Humphrey M. (2003). Policy and Enforcement in Virtual Organizations. In Proceedings of the 4th international Workshop on Grid Computing . International Conference on Grid Computing. Washington D.C., USA, IEEE Computer Society: 125.

[4] Burnap P. and Hilton J. (2009). Self Protecting Data for De-perimeterised Information Sharing. Proceedings of the Third International Conference on Digital Society. ICDS 2009, Cancun, Mexico. 1st-7th Feb 2009.

[5] Safavi-Naini R and Sheppard P. (2003). Digital Rights Management for Content Distribution. In Australian Information Security Workshop 2003, Adelaide, Australia.

[6] Burnap P. and Hilton J. (2008). Information Assurance for Collaborative Working in Deperimeterised Environments. Presented at the UK All Hands Meeting 2008, Edinburgh, United Kingdom. 8th-11th September 2008.

[7] Hilton J. (2009). Privacy in Multi-Agency Data Sharing (Unpublished Report). Cardiff University. Cardiff, United Kingdom.