Evaluating the Effects of Security Usability Improvements in Word 2007

M.Helala and S.M.Furnell

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

It has been argued in the literature that integrating security features with user goals and increasing their visibility would improve the usability of these functionalities. This paper investigates how these approaches affect the efficiency of use and subjective user satisfaction. The impacts of the combination of these two methods are evaluated as well. In order to do this the user interface of Word 2007 is modified according to these principles and usability tests are carried out with both the original and the modified user interfaces. The results suggest that integrating security features with user goals would improve the efficiency of using them but the impacts on user satisfaction cannot be clearly identified based on the collected data. No indications of any major improvements in the efficiency of use or user satisfaction are found when the visibility of security features is increased. The combination of these two methods seems to improve both the efficiency of use and the subjective user satisfaction.

Keywords

Security, Usability, Visibility, User Goals

1 Introduction

Several usability studies have been conducted in order to evaluate different security tools and security features in other applications. In some cases these have even suggested improvements to the studied applications and tools. However, solutions that could be applied to a wide range of applications would be more beneficial for user interface (UI) designers and software developers. Therefore this paper concentrates on presenting common usability issues and solutions that could be used in several everyday applications. The impacts these solutions have on efficiency of use and user satisfaction are also considered.

2 Common usability issues in security features

2.1 Security tasks are not integrated with user goals

Dourish *et al.* (2004) and Smetters and Grinter (2002) have criticised the way security features are presented in many applications. They have argued that the features are not integrated well enough with the tasks users need to do. This can lead to situations in which users cannot use applications or tools in a way that would be natural to them or to the tasks they are trying to complete.

Smetters and Grinter (2002) mentioned an example of this kind of situations. They found in their study that from time to time users had to manually change relevant security settings before carrying out certain tasks and then restore the previous settings afterwards. Clearly, having to turn off or bypass security features in this way increases the risk of user errors which can potentially compromise security. It can be argued that if security aspects of a task that users wish to do were integrated with other aspects of the task, it would be easier for them to complete the task successfully.

In addition, according to Balfanz *et al*. (2004) users tend to think about security in the context of the tasks they need to do rather than as security terms, such as certificates or encryption keys. Hence it could be beneficial to integrate security with these tasks so that users do not need to take separate steps in order to achieve the security aspects of their tasks.

2.2 Lack of visibility

It has been claimed that in many cases the visibility of security related functionalities is not good enough for users to notice them easily (Furnell, 2005). Therefore users might not utilise some important security features simply because they have not come across them (Furnell, 2005). In addition, Tognazzini (2003) stated that users of any applications should not be expected to search for features and functionalities. This clearly implies that if average users are expected to utilise different security features in everyday applications these features should be presented in a way that users will become aware of them while using other aspects of these applications.

Also, Dourish *et al.* (2004) have argued that security is not the main concern for most users when they are using IT in their everyday life. Furthermore, according to a research conducted by De Witt and Kuljis (2006), users often try to get their work done quickly even at the cost of security. The results of their research indicated that this common attitude was not dependent on users' security awareness. Even users who were aware of the security consequences of this kind of behaviour often had the same approach. These findings provide further support for the idea that security should be given enough emphasis when designing UIs. If these features are hidden in different menus user can easily give up searching for them or might not even look for them in the first place.

3 Usability test methodology

Based on the findings presented above it was decided to test how integrating security features with user goal, increasing the visibility of security features and the combination of these improvements would affect their usability in everyday applications. The effects of these improvements were tested using some of the security features available in Microsoft Word 2007. In order to do this the UI regarding these features was modified with a Word 2007 add-in.

3.1 User interface modifications

The visibility of protecting documents against unauthorised access and modifications was increased. This was achieved by adding a *Security Options* button to the *Save As* dialog and removing the *General Options…* menu item from the *Tools* menu. The *General Options* dialog that presented the protection settings was also replaced with a new *Document Level Security Options* as shown in Figure 1. The original and modified dialogs are shown in Figures 1 and 2 respectively.

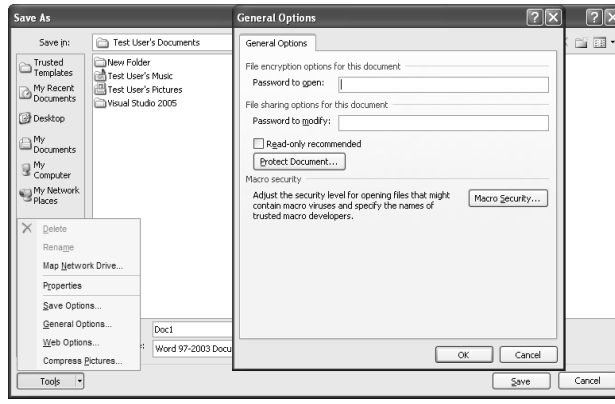

Figure 1: The origianl *Save As* and *General Options* dialogs.

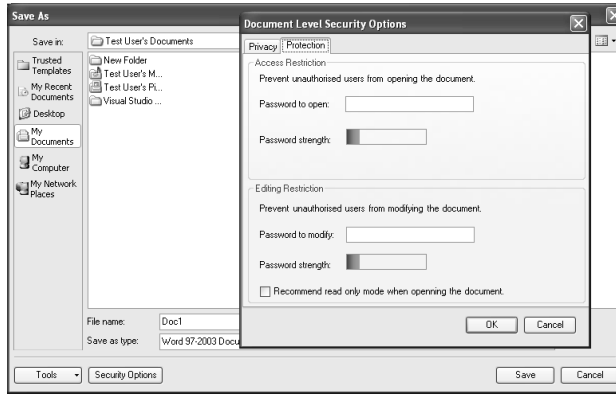

Figure 2: The modified *Save As* dialog and the new *Document Level Security Options* dialog.

An effort was made to integrate security features and user goals in three cases. Users were given an option to create documents with access and editing restrictions as well as documents with increased privacy level. This was done by adding relevant buttons to the *Office Menu* as shown in Figure 3.

Both of the improvements were tested in two cases: controlling metadata, such as author name and revision number, that is saved with an existing document and controlling the metadata that is saved with all new documents by default. In this

paper these are referred to as document level privacy settings and application wide privacy settings respectively.

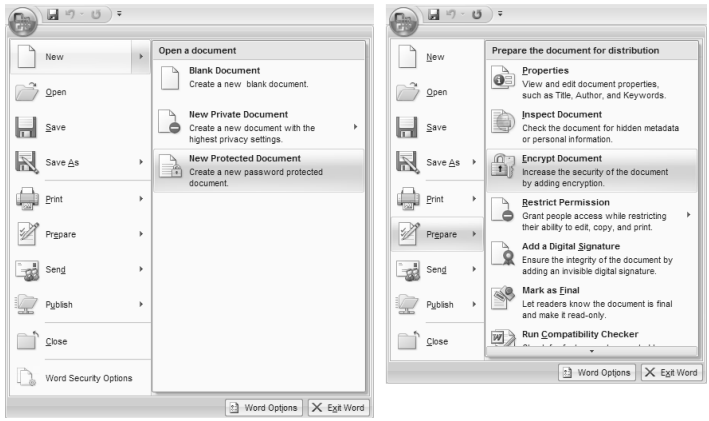

Figure 3: The new *Office Menu* (left) and the original version (right)

In the case of document level privacy settings users were able to select the metadata they wanted to be saved with a document instead of having to inspect the document and then remove the unwanted details with the *Document Inspector*. This was made possible through a privacy tab in the *Document Level Security Options* dialog as illustrated on the left side of Figure 4. This was done in order to integrate the user goals and the security functionality. In addition the *Security Options* button that was mentioned earlier was used for increasing the visibility of this feature.

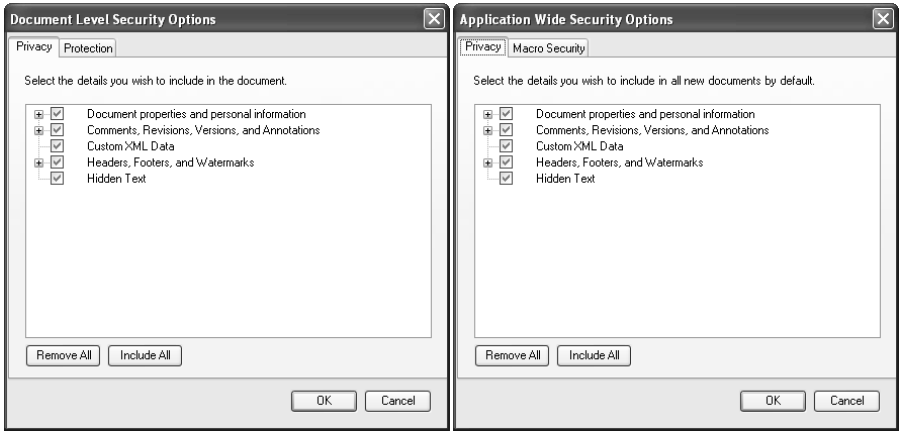

Figure 4: The privacy tabs of the new *Document Level Security Options* and *Application Wide Security Options* dialogs.

The visibility of application level privacy settings was increased by adding a *Word Security Options* button into the *Office Menu* as shown in Figure 4. Clicking this button opened a dialog shown on the right side the Figure. The same approach of integrating this functionality with user goals was used as in the case of document level privacy settings. In the original solution there was no straightforward way of controlling all the metadata described above. It was only possible to remove the

default author name through the *User name* field in the *Word Options*. In order to do anything beyond this users were required to modify the *Normal.dotx* template, which is by default used as a template for all new documents. The new approach saved users from inspecting this template with the *Document Inspector* and removing any unwanted metadata this way.

3.2 Usability tests

Ten users participated in the practical tests. Most of the users were students at the University of Plymouth and the rest had at least a higher education qualification. Six of the participants rated themselves as advanced IT users and the rest regarded themselves as intermediate users. All participants used computers daily. In addition all but two of them had prior experience with the Word 2007. Even the two users who had not used this version were users of Word 2003.

The usability tests consisted of seven different security related tasks, as shown in Table 1, that users might encounter in their day-to-day use of any word processor. In each of these tasks users were required to utilise the features described earlier in this chapter. In addition the users were asked to do all tasks with both the original Word 2007 UI and the modified UI. If users had been divided into two groups each testing only one UI, the variation in the skills and performance of individual users could have caused significant difference between the groups (Nielsen, 1993, pp.178-9). In order to avoid bias caused by this, within-subjects testing was used. In addition, the problems caused by skills transferred between the two UIs was controlled by asking half of the participants to test the modified UI first and the other half to test the original one first as suggested by Nielsen (1993, p.179). In practice every other user tested the modified UI first and the rest tested the original one first.

Task number	Task description
1	Create a new document with restricted access.
2	Restrict access to an existing document.
3	Create a new document that does not contain any personal details in the metadata.
4	Remove personal details from the metadata of an existing document.
5	Create a new read only document.
6	Convert an existing document to a read only document.
7	Change the privacy settings so that by default no personal details will be included in the metadata of new documents.

Table 1: Description of the test tasks used in the usability tests.

The efficiency of use was estimated by measuring the completion times and success rates for all tasks. In addition subjective user satisfaction was estimated by recording user opinions regarding the ease of use and preference on certain areas of the UIs. The ease of use was measured with the following 5-point scale: *very difficult*, *difficult*, *neither easy nor difficult*, *easy*, and *very easy*. To make comparison between the two UIs easier geometric means were calculated for the completion times and the ease of use. In order to do this for the ease of use, the 5-point scale was represented with a linear numeric scale so that *very difficult* was given the value 1 and *very easy* the value 5.

4 Results

Overall consideration of the results needs to examine the effects upon the efficiency of the users' operations when using the new interfaces, as well as how they felt about them in the process. These aspects are discussed in the sub-sections that follow.

4.1 Efficiency

In terms of completion times the only major difference between the two UIs was noticed in task 3 in which the modified UI was faster to use as it can be seen on the right side in Figure 5. When success rates presented on the left side in Figure 5 were considered, differences were notices in tasks 1, 3 and 7. In all of these users performed better with the modified UI.

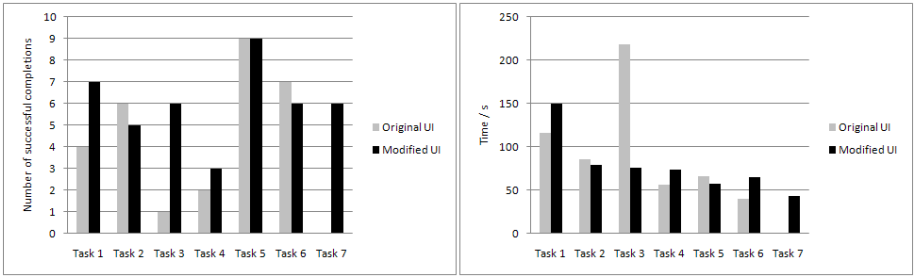

Figure 5: Task success rates on the left and geometric means of task completion times on the right.

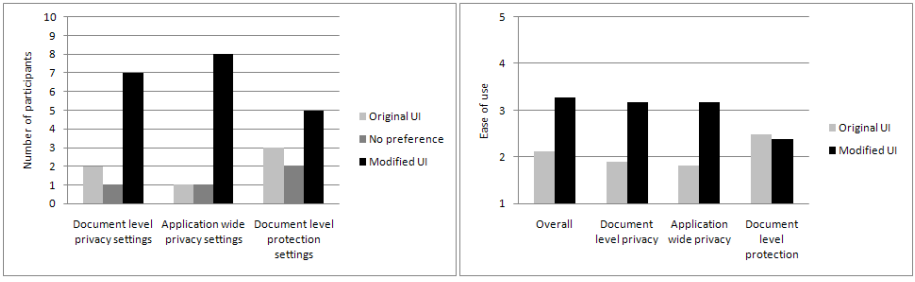

Figure 6: User preference regarding specific areas of the user interfaces on the left and geometric means of user opinion regardig the ease of use on the right.

4.2 User satisfaction

The results considering user opinions regarding ease of use are presented on the right side in Figure 6. This shows that users felt that the modified UI was easier to use in most cases. Only in the case of document level protection settings there was no major difference between the two interfaces. Furthermore, the number of user who preferred the modified UI was higher in all considered cases as it can be seen from the graph on the left side in Figure 6. However, again the difference was quite small in case of document level protection settings.

5 Discussion

5.1 Integrating security features with user goals

Integrating security features and user goals was tested in tasks 1, 3 and 5. The completion times for task 3 suggested that this approach would improve the efficiency of using the functionality in question. In addition, the success rates were higher for the modified UI which supports this finding. However, only one participant managed to complete the task 3 successfully with the original UI while only three participants out of ten failed the task with the modified one. Hence the task completion times might not be comparable. On the other had the poor success rate shows that the original UI was not very efficient in this respect. The success rates for task 1 support the effectiveness of the improvements used in the modified UI regarding this task. Thus it can be argued that integrating security features and user goals increases the efficiency of using them.

User satisfaction concerning document level privacy settings was higher for the modified UI as it scored higher in terms of users' opinions regarding ease of use and user preference. Tasks 3 and 4 involved document level privacy settings. Task 3 tested the impacts of unifying security features with user goals while task 4 tested the effects of combining this modification with increasing the visibility of the relevant functionality. However, due to the phrasing of the questions presented to the participants, it was not possible to say which one they referred to when rating the ease of using or preference regarding document level privacy settings.

5.2 Increasing visibility of security features

The results did not show any major differences between the two UI in the tasks 2 or 6 which tested the effects of increasing visibility of security features. Similar task completion times and success rates were recorded for both UIs in these tasks. Similarly no indications were found that this approach would increase subjective user satisfaction. Nevertheless, there were no indications of decreased level of usability when this method was used.

5.3 Combining the two improvements

Tasks 4 and 7 tested the combination of integrating security features with user goals and increasing their visibility. In task 7 more users completed the task successfully with the modified UI. In fact none of the participants managed to complete this task successfully with the original user interface. Thus the completion times could not be compared. In task 4 no major differences were found between the two UIs in terms of efficiency of use.

Tasks 3 and 4 involved controlling document level privacy settings. As mentioned earlier in this chapter, it could not be determined from the collected data which task users referred to when giving their opinion regarding ease of use and preference. Therefore, based on task 4 conclusions could not be made regarding the effectiveness of the combination of these modifications. In case of task 7, however, users rated the modified UI higher in terms of ease of use. In addition most users preferred the

modified UI in this case. Hence it can be argued that the combination of integrating security features with user goals and increasing their visibility improves both the efficiency of use and subjective user satisfaction.

6 Conclusion

The results presented in this paper have indicated that at least in some cases integrating security features with user goals would improve the efficiency of using these features. Two out of three test cases showed improvements in efficiency of use when this approach was used. It could not be clearly identified from the collected data if this approach improved subjective user satisfaction. No indications of improvements in efficiency of use or subjective user satisfaction were found when the visibility of security features was increased. On the other hand this approach does not seem to decrease the usability either. The combination of the two improvements mentioned above seemed to increase the efficiency of use and user satisfaction in one of the two test cases.

In order to verify the results presented in this paper, further studies should be carried out with larger and more diverse groups of test users. In addition, the reliability of the results could be increased by testing the effects that different improvements have on the same functionalities and by carrying out similar tests with other applications as well.

7 References

Balfanz, D., Durfee, G., Smetters, D.K. and Grinter, R.E., (2004), "In search of usable security: five lessons from the field", *IEEE Security & Privacy*, Vol. 2, No. 5, pp19—24.

DeWitt, A.J. and Kuljis, J., (2006), "Aligning usability and security: a usability study of Polaris", *Proceedings of the second symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, USA: ACM, pp. 1-7.

Dourish, P. Grinter, E., Delgado de la Flor, J. and Joseph, M., (2004), "Security in the wild: user strategies for managing security as an everyday, practical problem" *Personal Ubiquitous Comput.*, Vol. 8, No. 6, pp.391— 401.

Furnell, S., (2005), "Why users cannot use security", *Computers & Security*, Vol. 24, No. 4, pp.274—279.

Nielsen, J., (1993), Usability Engineering, Academic Press, San Diego, ISBN: 0-12-518405-0

Smetters, D.K. and Grinter, R.E., (2002), "Moving from the design of usable security technologies to the design of useful secure applications" *NSPW '02: Proceedings of the 2002 workshop on new security paradigms,* New York, NY, USA: ACM, pp.82—89.

Tognazzini, B., (2003), "First Principles of Interaction Design", http://www.asktog.com/basics/firstPrinciples.html, (Accessed 14 January 2008)