available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The challenges of understanding and using security: A survey of end-users

*S.M. Furnell**, *A. Jusoh*, *D. Katsabas*

Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Plymouth, United Kingdom

ARTICLE INFO

Article history:
Received 26 October 2005
Revised 14 December 2005
Accepted 14 December 2005

Keywords:
Security
Usability
Human–computer interaction
Internet Explorer
Word
Outlook Express

ABSTRACT

Many applications contain security features that are available for end-users to select and configure, as well as the potential to place users in situations where they must take security-related decisions. However, the manner in which these aspects are implemented and presented can often serve to complicate the process, such that users cannot actually use the security that they desire, or which may be expected of them. This paper presents the results of a survey of over 340 end-users in order to determine their understanding of the security features within Windows XP and three popular applications (Internet Explorer, Outlook Express, and Word). The study reveals some significant areas of difficulty, with many standard security features presenting apparent usability challenges for large proportions of the respondents. The results highlight the need for a more considered approach towards the presentation of security functionality if users are to have a realistic chance of protecting themselves.

1. Introduction

It is now widely accepted that security requirements cannot be addressed by technical means alone, and the chances of success will be significantly influenced by the people involved. As an example, the 2004 survey of IT abuse from the Audit Commission in the UK suggested that the majority of reasons that abuse is possible can be traced back to factors relating people (Audit Commission, 2005). Of particular note was that more than a third cases were attributed to a lack of 'security awareness' (22%), or 'inadequate or insufficient training' (13%), evidencing that people need to know what is expected of them if they are to uphold security effectively. Unfortunately, even with appropriate awareness, further barriers to security will be encountered if users do not understand the approaches that they are expected to use. This can often be the case with technology-based solutions, with features being presented in such a way that users cannot understand them. Indeed, this can often represent the downfall of such solutions, because the good safeguards that are available are not used effectively.

The need for technology to be presented to its users in an appropriate manner is by no means a new idea. Indeed, a whole discipline within the IT field is dedicated to human–computer interaction (HCI), and a wealth of information is available to inform and guide the appropriate implementation of modern systems (Shneiderman, 1998; Carroll, 2001). Nonetheless, it is still possible to identify many examples of systems that have been implemented in ways that are less than conducive to usability. In some cases, this may merely prevent people

* *Corresponding author*. Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom. Tel.: +1 752 233 521; fax: +1 752 233 520.
E-mail address: nrg@plymouth.ac.uk (S. M. Furnell)
0167-4048/$ – see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.12.004

from using functionality that they would otherwise find useful. In others, however, it may prevent or impede the use of features that could actually be regarded as essential – an example of which would be the features that users ought to be using to protect themselves.

This paper examines the possible usability challenges posed by security features in end-user software. The discussion begins by outlining some of the challenges to be faced in achieving usable security, with reference to examples of prior works in the area. It then proceeds to the main focus of the paper, presenting the results from a survey conducted to assess end-user understanding of security features in common software applications. The findings suggest that users face some significant impediments, leading to some general recommendations for future systems.

2. The challenge of usable security

When considering the inclusion of security functionality within end-user software, a number of desirable criteria can be identified that will influence the overall usability of the resulting protection. Some key points include the following:

- Understandable – Options and descriptions should be presented in a manner that is meaningful to the intended user population. Security offers a great deal of potential for the use of technical terminology and other jargon, but this could easily come at the cost of excluding a proportion of the users. Sufficient help and support should be available to assist novices to achieve the level of security that they need.
- Locatable – Users need to be able to find the features they need. If casual users have to spend too long looking for security, it increases the chances that they will give up and remain unprotected.
- Visible – The system should give a clear indication of whether security is being applied. Appropriate use of status indicators and warnings will help to remind users in cases where they may have forgotten to enable appropriate safeguards.
- Convenient – Although visibility is important, the provision of security should not become so prominent that it is considered inconvenient or intrusive. Users are likely to disable features that become too much of an impediment to legitimate use.

Examining current implementations of security can reveal deficiencies in these regards. Indeed, usability difficulties have already been well-documented within security-specific tools and utilities, with Whitten and Tygar (1999) having evaluated the problem in the context of PGP, and Johnston et al. (2003) having more recently conducted an examination of the Internet Connection Firewall within Microsoft Windows.

The issue of usability was also flagged as a major research challenge in a 2003 report from the Computing Research Association. Identifying the fact that 'human error' is often cited as a major cause of configuration errors, the CRA report suggested that this problem often "has its roots in the design of the system and its corresponding administrative interface", and proceeded to identify the requirement for understandable, deployable and usable security. Citing the specific example of encryption technology, the report suggested that the protection is under-utilised because users have difficulty dealing with it – "There is a 'usability gap' that translates directly into a 'usage gap'" (CRA, 2003). Unfortunately, encryption is far from the only aspect of security that is likely to suffer in this way.

Although the aforementioned examples have considered security-specific tools, the issue extends beyond these contexts, and there is also potential to encounter problems with the presentation and usability of security within more general applications. Here the features are included to provide protection for specific tasks, and the usage is often at the discretion of the end-users themselves. As such, if the related functionality is not presented in an accessible manner, then the very people that it is intended to protect will end up missing the opportunity.

3. A survey of end-users

With the above points in mind, a survey was mounted in order to assess users' understanding, and hence the potential usability, of security-related interfaces within a number of well-known software packages. The chosen programs were Windows XP, Internet Explorer, Word, and Outlook Express. Although these selections are drawn exclusively from Microsoft products, this is not intended to imply that the usability of security features within Microsoft's software is specifically poor. The choices were actually made to reflect the widespread usage and popularity of the programs concerned – thus maximising the chances of potential respondents also being end-users of the software (although this was not a prerequisite for completing the related section of the survey, it was considered that respondents would feel more comfortable and interested in answering questions about programs they were familiar with).

Rather than attempt to conduct an exhaustive assessment, respondents were asked to consider representative examples of the security features found within the four environments, with the survey aiming to assess their interpretations or understanding of related interfaces and dialogs. Particular focus was given to aspects that end-users would be likely to find if they were to search for security options, as well as a few examples of how security might be encountered during general use. The questionnaire included screenshots of the relevant aspects, and thus it was intended that even respondents who did not use the associated software would be able to offer a meaningful opinion about whether they understood the information.

The survey was mounted online during July and August 2005, and promoted via targeted emails and subsequent word-of-mouth from the respondent group. A total of 342 responses were received during the survey period, providing a good basis for the subsequent analysis. It should be noted that all of the percentages reported in the next sections are based upon proportions of this total group. However,