Chapter XII
Security Usability Challenges for End-Users

Steven Furnell
Centre for Information Security & Network Research, University of Plymouth, UK

ABSTRACT

This chapter highlights the need for security solutions to be usable by their target audience, and examines the problems that can be faced when attempting to understand and use security features in typical applications. Challenges may arise from system-initiated events, as well as in relation to security tasks that users wish to perform for themselves, and can occur for a variety of reasons. This is illustrated by examining problems that arise as a result of reliance upon technical terminology, unclear or confusing functionality, lack of visible status and informative feedback to users, forcing users to make uninformed decisions, and a lack of integration amongst the different elements of security software themselves. The discussion draws upon a number of practical examples from popular applications, as well as results from survey and user trial activities that were conducted in order to assess the potential problems at first hand. The findings are used as the basis for recommending a series of top-level guidelines that may be used to improve the situation, and these are used as the basis assessing further examples of existing software to determine the degree of compliance.

INTRODUCTION

End-users are faced with an increasing requirement to use security, with recent years witnessing a significant surge in the range and volume of security threats that can affect their IT systems. Highly publicized incidents involving malware, spyware, phishing, and denial of service have all served to heighten general awareness of Internet threats, with the consequence that users at all levels (be they at work or at home) are likely to have at least some appreciation of the need to keep their systems secure. However, adequate protection will rarely be achieved by default, and here we often find that even the security technologies that *are* used are often used badly (classic examples

being bad practice with passwords, and poorly maintained anti-virus protection). In some cases, the blame for this clearly resides with careless or irresponsible end-users. However, it is important to realize that another significant factor is often the underlying unfriendly nature of the technology.

Security-related functionality can be found in both specific tools and embedded within general applications, and users will frequently encounter the requirement to make security-related decisions during routine use of their system. However, provision of security functionality is only of value if the target audience can understand and use it. Unfortunately, the manner of presentation, and the implicit assumptions about users' abilities, can often hamper usage in practice. This can represent a particular problem in contexts where users are required to fend for themselves, and may result in necessary protection being under-utilized or misapplied.

Although much security-related functionality is now presented via the ostensibly friendly context of a graphical user interface, if we look beyond the surface, the user-friendliness can quickly disappear. For example, a series of apparently simple check boxes or low-medium-high settings can soon become more complex if you have to understand the actual functionality that they control (Furnell, 2004). As a result, many users will ultimately remain as baffled as they would have been by a command line interface. Those most likely to suffer are non-technical users, who lack the knowledge to help themselves, or any formal support to call upon. Should they be implicitly denied the level of protection that they desire simply because they are not technology experts? Clearly, the answer is no. As such, the usability of security is a crucial factor in ensuring that it is able to serve its intended purpose. Although this requirement is now beginning to achieve much more widespread recognition (CRA, 2003; Cranor & Garfinkel, 2005), usable security remains an area in which current software is often notably lacking.

This chapter examines the nature of the usability problem, presenting examples from standard end-user applications, as well as supporting evidence from current research. Having established the existence and nature of the problem, the discussion proceeds to consider specific issues that can present obstacles from the usability perspective. Particular consideration is given to problems at the user interface level, and how we may consequently find our attempts to use security being impeded (or entirely prevented) as a result of inadequate attention to human-computer interaction (HCI) aspects. The discussion then proceeds to present a brief examination of means by which the situation can be improved, and the chapter concludes with a summation of the main issues.

BACKGROUND

If we consider the factors that may prevent users from securing their systems then, perhaps unsurprisingly, lack of knowledge and inability to use the software concerned are amongst the prominent reasons, particularly for the novice community. Evidence here can be cited from a study of security perceptions amongst 415 personal Internet users who were asked to identify the factors that prevented them from carrying out security practices (Furnell, Bryant, & Phippen, 2007). The overall findings are illustrated in Figure 1, and although 41% considered that they devoted sufficient attention to security, a variety of reasons were seen to be impeding the remainder. Although there is no single issue that stands out as an obstacle to all users, there are clearly some reasons that can be related to the users' knowledge and the usability of the software (e.g., "I don't understand how to use security packages" clearly shows that some users find the protection challenging to use, whereas "Security impedes the use of my computer" illustrates a usability constraint from a different perspective). When specifically considering the main reasons cited by respondents that classed