INFORMATION SCIENCE PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8879

Chapter XVIII

Security and Online Learning: To Protect or Prohibit

Anne Adams
Middlesex University, UK

Ann Blandford
UCL Interaction Centre, UK

ABSTRACT

The rapid development of online learning is opening up many new learning opportunities. Yet, with this increased potential come a myriad of risks. Usable security systems are essential as poor usability in security can result in excluding intended users while allowing sensitive data to be released to unacceptable recipients. This chapter presents findings concerned with usability for two security issues: authentication mechanisms and privacy. Usability issues such as memorability, feedback, guidance, context of use and concepts of information ownership are reviewed within various environments. This chapter also reviews the roots of these usability difficulties in the culture clash between the non-user-oriented perspective of security and the information exchange culture of the education domain. Finally an account is provided of how future systems can be developed which maintain security and yet are still usable.

INTRODUCTION

The World Wide Web is facilitating new forms of remote education. These online environments provide a wealth of possibilities for supporting learning throughout the world. Yet, with the many opportunities come a myriad of risks. Risks to the system and its data can dramatically affect users' perceptions of a system's reliability and trustworthiness. Whether these infractions are malicious or accidental, they can have serious repercussions for a system and its administrators. Security is therefore essential to retain users' trust in an online learning program.

Although security is an essential part of any system it should not impede the original objectives of that system. However, security mechanisms and their poor implementation have been found to present serious usability problems. There are two principal security issues, authentication and privacy, where usability is a source of problems for online learning systems (OLS). Initially, users encounter a variety of usability problems with authentication procedures, such as passwords, which incur high user overheads or are simply unworkable. The result is that users either try to circumvent the mechanisms or use other systems to complete their task (Adams & Sasse, 1999c; Adams, Sasse, & Lunt, 1997; Holmström, 1999; Preece, 2000; Whitten & Tygar, 1999). Users seeking to protect their privacy encounter further complex usability problems. These usability issues often relate to concepts of ownership (e.g., intellectual property rights, copyright, privacy rights). Many OLS, however, do not provide adequate feedback or control rights (Adams, 1999a; Bellotti & Sellen, 1993; Preece, 2000). Although some usability issues only relate to specific online settings, others are more universal.

For security mechanisms in OLS to effectively protect our information they must be designed appropriately to the users' needs. Usability, in this sense, would relate to providing users with adequate control to protect their data. In this context, users may be the providers of learning materials, in which case the concern is commonly over authorised access to proprietary learning materials. Alternatively, users may be learners, in which case the concern may be over their answers to questions, their results or even their images (notably in videoconferencing systems, where even matters as apparently trivial as the quality of a video image can affect perceptions enormously). Various OLS, however, do not provide adequate feedback or control rights to allow this control.

This chapter details why we need security in OLS and the factors underpinning how that security is provided within various environments. A review is also provided of the fundamental differences between the culture of security and online learning that produce clashes between the two disciplines. These clashes are often the root cause of usability issues in security mechanisms for OLS. Finally, an account is provided of how future systems can be developed which maintain security and yet are still usable.

Ultimately, this chapter seeks to review three important concerns: