Chapter 5.3
Human Factors in Information Security and Privacy

Robert W. Proctor
Purdue University, USA

E. Eugene Schultz
High Tower Technologies, USA

Kim-Phuong L. Vu
California State University, USA

ABSTRACT

Many measures that enhance information security and privacy exist. Because these measures involve humans in various ways, their effectiveness depends on the human factor. This chapter reviews basic components of information security and privacy with an emphasis on human factors issues. It provides an overview of empirical investigations that have been conducted regarding the usability of security and privacy measures. These studies show that users have difficulty interacting with complex interfaces and that users' performance can be improved by incorporating human factors principles into the designs. The authors conclude by discussing how human factors analyses can lead to the design of usable systems for information security and privacy assurance.

INTRODUCTION

Human Factors will be critical in resolving issues surrounding privacy, the construction of usable profile interfaces, and many other issues. Marc Resnick, 2006

Information security and privacy are essential for the functioning of e-commerce and many other Web-based services. Security breaches ("security-related incidents") have become commonplace. A security breach is an event in which a vulnerability is exploited to subvert or bypass security mechanisms. Some of the most frequent types of attacks that occur are Web page defacements, data security compromises, password-guessing attacks, and buffer overflow attacks in which an excessive amount of input is sent to a system or application to cause systems' memory capacity to be exceeded to allow malicious commands to be

DOI: 10.4018/978-1-61350-323-2.ch5.3

executed (see Viega, 2005). These incidents often result in considerable disruption and financial loss.

Information security means protecting the confidentiality, integrity and availability of data, applications, systems, and networks, as well ensuring that electronic transactions cannot be falsely repudiated ("non-repudiation"). Confidentiality means protection against unauthorized access to and reading of information, whereas integrity means protection against unauthorized changes in systems, networks, and information. Availability refers to the ability to gain uninterrupted access to systems, networks, and/or information. Non-repudiation denotes providing reasonable proof that the initiator of an electronic transaction was a certain person, even if that person denies having initiated that transaction. Securing a Web site necessitates securing the Web server itself, the application(s) that run on the Web server, data transmitted between the Web server and the client (browser), and the system on which the Web server runs.

Once a system's information is secure, the issue of privacy assurance needs to be addressed. Users should be assured that their personal information will be used in its intended manner and that their preferences regarding use of this information will not be violated. Information privacy refers to protection against unauthorized disclosure of information about individuals. Privacy assurance has become a topic of considerable interest due to numerous highly publicized incidents of personal information being stolen, sold, or otherwise made available to unauthorized parties. Consequently, many organizations hosting Web sites now post privacy policies that are intended to inform users about how their personal information will be stored and used, and organizations may certify that a site's policy adheres to good privacy practices. Also, protocols have been developed for standardizing Web privacy policies in machine-readable form so that client-based applications can automatically determine whether a site's policy conforms to specified needs and preferences.

Human factors plays an important role in information security and privacy, but this role often is overlooked when designing secure systems (Proctor & Vu, 2004; Schultz, 2005). Because ensuring security and privacy relies on the cooperation and performance of end users, system administrators, and other authorized personnel, the maximal benefit of security and privacy measures cannot be achieved unless interactions between all types of users and the systems with which they interact are simple and user-friendly. People will not use security features and functionality if they find them intrusive or non-intuitive. Although user resistance to security- and privacy-related methods and tasks suggests that usability problems abound, too little research examining the relationship between usability and those methods and tasks has been published.

In this chapter, we discuss human factors issues, research, and challenges in both information security and privacy. In the first major section, we examine usability issues associated with each of the major areas of information security. We provide examples of usability problems in security-related tasks, as well as some well-designed interaction sequences. An analysis of each area of information security suggests that usability and security methods are often at least to some degree orthogonal to each other. Solutions discussed include elevating the default level of security in Web servers, offering simple settings that result in groups of related security parameters being set, and making available more security-enhancing reusable software routines and tools that integrate with Web servers and applications. The section concludes with an example focusing on password generation that shows how security can be improved through increased usability.

In the second major section, we consider usability issues associated with information privacy and assurance. We review research on users' privacy concerns and preferences to assess the extent to which such preferences are accommodated by existing Web sites and privacy policies.