IDEA GROUP PUBLISHING ITB11308

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the book, *Advanced Topics in End User Computing, vol. 4* edited by M. Adam Mahmood © 2005, Idea Group Inc.

Chapter XIV

A TAM Analysis of an Alternative High-Security User Authentication Procedure

Merrill Warkentin, Mississippi State University, USA

Kimberly Davis, Mississippi State University, USA

Ernst Bekkering, Northeastern State University, USA

ABSTRACT

The objective of information system security management is information assurance, which means to maintain confidentiality (privacy), integrity, and availability of information resources for authorized organizational end users. User authentication is a foundation procedure in the overall pursuit of these objectives, and password procedures historically have been the primary method of user authentication. There is an inverse relationship between the level of security provided by a password procedure and ease of recall for users. The longer the password and the more variability in its characters, the higher the level of security is that is provided by the password, because it is more difficult to violate or crack. However, such a password tends to be more difficult for an end user to remember, particularly when the password does not spell a recognizable

word or when it includes non-alphanumeric characters such as punctuation marks or other symbols. Conversely, when end users select their own more easily remembered passwords, the passwords also may be cracked more easily. This study presents a new approach to entering passwords that combines a high level of security with easy recall for the end user. The Check-Off Password System (COPS) is more secure than self-selected passwords and high-protection, assigned-password procedures. The present study investigates tradeoffs between using COPS and three traditional password procedures, and provides a preliminary assessment of the efficacy of COPS. The study offers evidence that COPS is a valid alternative to current user authentication systems. End users perceive all tested password procedures to have equal usefulness*, but the perceived* ease of use *of COPS passwords equals that of an established high-security password, and the new interface does not negatively affect user performance compared to a high-security password. Further research will be conducted to investigate long-term benefits.*

BACKGROUND

Despite continuing improvements in computer and network technology, computer security continues to be a concern. One of the leading causes of security breaches is the lack of effective user authentication, primarily due to poor password system management (The SANS Institute, 2003), and the ease with which certain types of passwords may be cracked by computer programs. Yet even with today's high-speed computers, an eight-character password can be very secure, indeed. If a Pentium 4 processor can test 8 million combinations per second, it would take more than 13 years on average to break an eight-character password (Lemos, 2002). However, the potential for password security has not been fully realized, and a security breach can compromise significantly the security of information systems, other computer systems, data, and Web sites. Furthermore, the increasing degree to which confidential and proprietary data are stored and transmitted electronically makes security a foremost concern in today's age of technology. This is true not only in civilian use, but also in government and military use.

A primary objective of information system security is the maintenance of confidentiality, which is achieved in part by limiting access to valuable information resources. Historically, user authentication has been the primary method of protecting proprietary and/or confidential data by preventing unauthorized access to computerized systems. User authentication is a foundation procedure in the overall pursuit of secure systems, but in a recent e-mail to approximately one million people, Bill Gates (chairman of Microsoft Corporation) referred to