Chapter I
Human and Social Aspects of Password Authentication

Deborah S. Carstens
Florida Institute of Technology, USA

ABSTRACT

With the increasing daily reliance on electronic transactions, it is essential to have reliable security practices for individuals, businesses, and organizations to protect their information (Vu, Bhargav, & Proctor, 2003; Vu, Tai, Bhargav, Schultz, & Proctor, 2004). A paradigm shift is occurring as researchers are targeting social and human dimensions of information security, as this aspect is seen as an area where control can be exercised. Since computer security is largely dependent on the use of passwords to authenticate users of technology, the objectives of this chapter are to (a) provide a background on password authentication and information security, (b) provide a discussion on security techniques, human error in information security, human memory limitations, and password authentication in practice, and (c) provide a discussion on future and emerging trends in password authentication to include future research areas.

INTRODUCTION

With the increasing daily reliance on electronic transactions, it is essential to have reliable security practices for individuals, businesses, and organizations to protect their information (Vu et al., 2003; Vu et al., 2004). A paradigm shift is occurring as researchers are targeting social and human dimensions of information security, as this aspect is seen as an area where control can be exercised. Since computer security is largely dependent on the use of passwords to authenticate users of technology, the mission of this chapter is to addresses the human and social aspects of password authentication (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Users are challenged to remember long and random passwords and therefore too often choose passwords that may have low security strength or be difficult to remember (Wiedenbeck et al., 2005; Yan, Black-

well, Anderson, & Grant, 2004). As the number of individuals using computers and networks has increased, so has the level of threat for security breaches against these computers and networks. Carnegie Mellon's computer emergency response team (CERT) (2007) has collected statistics showing that six security incidents were reported in 1988 compared to 137, 529 in 2003. Furthermore, CERT (2007) reported that 171 vulnerabilities were reported in 1995 in comparison to 8,064 in 2006. In addition, the Federal Bureau of Investigation (FBI) conducted a survey in which 40% of organizations claimed that system penetrations from outside their organization had increased from the prior year by 25% (Ives, Walsh, & Schneider, 2004).

The rapid expansion in computing and networking has thus amplified the need to perpetually manage information security within an organization. Events such as 9/11 and the war on terrorism have also underscored an increased need for vigilance regarding information security. Organizations, government, and private industry are currently trying to adjust to the burden of this heightened need for information security, and, as an example of this, the U.S. Department of Homeland Security (2002) has focused particular efforts on ensuring information security. In light of the current context of universal computing and the realistic threats that exist to organizations' information systems, there is a strong need for more research in the field of information security. The main objectives of this chapter are to (a) provide a background on password authentication and information security, (b) provide a discussion on the main thrust of the chapter, human and social aspects of password authentication, which include the topics of security techniques, human error in information security, human memory limitations, and password authentication in practice, and (c) provide a discussion on future and emerging trends in password authentication to include future research areas and concluding remarks in the area of human and social aspects of password authentication.

Password Authentication Background

In this world of ever increasing technological advances, users of technology are at risk for developing information overload as the number and complexity of passwords and other electronic identifiers increase. Previous investigations of the National Institute of Standards and Technology (NIST, 1992) have suggested that more than 50% of incidents that occur within government and private organizations have been connected to human errors. The role that people play in maintaining information security is an important one that the literature has only begun to address. As researchers improve their understanding of how social and human factors limitations affect information security, they can provide organizations with insight into improving information security policies. Passwords adopted by users are too easily cracked (Proctor, Lien, Vu, Schultz, & Salvendy, 2002). In particular, organizations can benefit from research revealing how best to minimize the demands that passwords place on the human memory system while maintaining the strength of a password (Carstens, McCauley-Bell, Malone, & DeMara, 2004).

The application of human factors and specifically, cognitive theory principles, can be used to positively influence system security when organizations follow password guidelines that do not exceed human memory limitations. Ultimately, user memory overload can be minimized when all aspects of a password authentication system have been designed in a way that capitalizes on the way the human mind works and also recognizes its limitations. As Hensley (1999) wrote, "Password(s) do little good if no one remembers them." Nevertheless, the exponential growth in vulnerabilities and security incidents as suggested by the CERT (2007) underscores that the design