Chapter 47
An Evaluation of User Password Practice

John Campbell
University of Canberra, Australia

Kay Bryant
University of Canberra, Australia

ABSTRACT

Maintaining the security of information systems and associated data resources is vital if an organization is to minimize losses. Access controls are the first line of defense in this process. The primary function of authentication controls is to ensure that only authorized users have access to information systems and electronic resources. Password-based systems remain the predominant means of user authentication despite viable authentication alternatives. Research suggests that password-based systems are often compromised by poor user security practices. This chapter presents the results of a survey of 884 computer users that examines user practice in creating and reusing password keys, and reports the findings on user password composition and security practices for email accounts. Despite a greater awareness of security issues, the results show that many users still select and reuse weak passwords keys that are based on dictionary words and other meaningful information.

INTRODUCTION

While there have been significant technological developments in online authentication methods especially in biometrics and graphics-based approaches (Ratha, Connell, & Bolle, 2001; Man Hong, Hayes, & Matthews, 2004; Jain, Ross, & Prabhakar, 2004; Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005; de Paula et al., 2005), passwords remain the most common means of authenticating a user. Unfortunately, users can compromise password security by forgetting passwords, writing them down, sharing them with other people, and selecting easily guessed words (Spafford, 1992; Stanton, Stam, Mastrangelo, & Jolton, 2005; Trček, Trobec, Pavesić, & Tasič, 2007; Yan, Blackwell, Anderson, & Grant, 2004).

DOI: 10.4018/978-1-4666-2136-7.ch047

These weaknesses are known to seriously undermine the efficacy of password access systems (Conklin, Dietrich, & Walz, 2004; Carstens, 2004). In particular, the issue of password reuse is an area that remains under researched and is, therefore, the major focus of this study. This chapter explores aspects of user password management practice within the context of email usage by profiling email account usage, password reuse, and user management practice.

PASSWORD SECURITY ISSUES

Password-based authentication remains the most common way to control access to computer-based resources. Passwords remain in widespread use because they are conceptually simple for both system designers and end users and provide cost effective protection for many systems if used correctly. Unfortunately, effective passwords are by nature complex and difficult to for users to remember (Ma, Campbell, Tran, & Kleeman, 2007). Prior research has shown that users are one of the main risks to the effectiveness of security measures (Rhodes, 2004). Organizations often rely on password composition policies to force users to create more secure passwords. These policies are usually implemented in such a way as to provide an explicit framework that constrains user choices during the password creation and replacement process. While this approach may help improve password security, these restrictions make the composition and memorizing of passwords complex and less intuitive (Campbell, Kleeman, & Ma, 2007).

Further, due to the predominance of password authentication systems, many users are required to remember passwords for a range of different systems and applications. As earlier research has demonstrated, the requirement to remember such a large number of passwords can cause a major problem for users (Yan et al., 2004; Zviran & Haga, 1999). Unfortunately, typical users are capable of managing a small number of unique passwords, generally less than five (Adams & Sasse, 1999). Also, remembered information can simply be forgotten, so users typically resort to using information that is easy to recall (Vu et al., 2007). One consequence of this is that while the information is easy to recall, it is also relatively easy to guess. Passwords that are more difficult to remember may be written down, thereby compromising password and system security (Stanton, et al., 2005).

A SURVEY OF EMAIL PASSWORD SECURITY

Remembering unique passwords for different systems and applications is difficult in practice and it is therefore no surprise that many users select dictionary words, personal names or other meaningful information as the basis for their passwords. For similar reasons users frequently select the same password for multiple accounts (Ives, Walsh, & Schneider., 2004). Password reuse can compromise the security of all of the password systems that a user might access. Cognitive limitations mean that many users will choose easy to remember passwords that are based on some meaningful combination of names and/or numbers (Brown, Bracken, Zoccoli, & Douglas, 2004). If the security of one system is breached, then all other password-based systems may become vulnerable.

Electronic mail is the most widely adopted password-protected application and affects the daily life of almost every working person in the industrialized world (Rudy, 1996; Bälter, 2000). Electronic mail systems provide a useful research context for studying the password behavior of users because of its widespread social and organizational impact. A preliminary study was undertaken to gain insight into password behaviors and to test our initial survey instrument (Campbell & Bryant, 2004). The pilot study involved 82 computer