Chapter 1.9
Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security*

Merrill Warkentin
Mississippi State University, USA

Kimberly Davis
Mississippi State University, USA

Ernst Bekkering
Mississippi State University, USA

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 significantly compromise 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 passwords as "the weak link" in computer security, noting that most passwords are either easy to guess or difficult to remember (*Gates pledges better software security,* 2003). Gates correctly identified a classic trade-off that system and network administrators must face when considering various password procedures for adoption. Specifically, there is an inverse relationship between the level of security provided by a password procedure and ease of recall for end users. When end users select their own easily remembered passwords, they are easier to crack than longer passwords with a greater variety of characters. The longer the password and the more variability in the characters, the higher the level of security provided by such a password. However, human memory has significant limitations, and such passwords tend to be more difficult for end users to remember. Typically, human short-term memory can only store seven plus or minus two (7 ± 2) "chunks" of information (Miller, 1956), and alphanumeric characters such as punctuation marks and other symbols are not easily combined in a chunk with other characters. For example, the letters "b," "a," "n," and "d" can be easily stored together as a single chunk, but it is difficult for humans to combine symbols such as the vertical bar (|) and tilde (~) with other characters to form a chunk. The problem of striking a balance between security and ability to remember passwords will become more acute as the number of passwords per user increases.

In a survey with 3,050 distinct respondents (Rainbow Technologies Inc., 2003), the following picture emerged:

- Respondents used, on average, almost 5 ½ passwords
- 23.9% of respondents used eight or more passwords
- More than 80% were required to change passwords at work at least once a year
- 54% reported writing down a password at least once
- 9% reported always writing down their passwords
- More than half had to reset business passwords at least once a year, because they forgot or misplaced the password

The 352 participants in the present study reported using an average of 3.90 passwords at the time of the study and 4.53 passwords in the six months. Further, 35.5% reported writing down at least one password. Clearly, the use of multiple passwords constitutes a burden to users.

PASSWORD STRATEGIES

Because of the trade-offs detailed above, and because methods and technologies employed by crackers are constantly improving, new security strategies with improved password procedures are required. Traditional methods include allowing users to select their own password and assigning passwords to them, both of which may be subject to restrictions on password length and character choices. The efficacy of both systems depends on the ability of end users to recall such passwords without writing them down. The Federal Information Processing Standards (FIPS) publication 112 includes guidelines for different levels of password security (National Institute of Standards and Technology, 1985). At the highest