IDEA GROUP PUBLISHING

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

ITP4550

Towards Powerful, User-Friendly Authentication: The Check-Off Password System ("COPS")

Ernst Bekkering, Merrill Warkentin, and Kimberly Davis
Department of Management & Information Systems
College of Business and Industry, P.O Box 9581
Mississippi State University, MS STATE, MS 39762-9581
(662) 325-8475, (662) 325-1955, (662) 325-8066–Fax: (662) 325-8651
tjb6@msstate.edu, mwarkentin@acm.org, kdavis@cobilan.msstate.edu

ABSTRACT

Passwords have always been the dominant method of information system user authentication. The level of security provided by passwords has been an ongoing concern. Strong security requirements mandate that users are issued passwords of sufficient length and with sufficient variability in characters, but these passwords tend to be difficult to remember. Conversely, when users select their own, more easily-remembered passwords, the passwords may also be easier to violate or "crack." The proposed study presents a new approach to entering passwords, which combines a high level of security with easy recall for the user. The Check-Off Password System (COPS) is more secure than user-selected password systems, as well as high-protection, assigned password systems. However, we hypothesize that users will prefer this system to traditional assigned-password systems despite the more cognitively involved input mechanism, because it is easier to recall the COPS "password." Our findings will establish COPS as a valid alternative to current user authentication systems.

BACKGROUND

Despite continuing improvements in computer and network technology, computer security continues to be a concern. At the recent 2002 PC Expo, 74% of respondents stated that they would be working on computer security in 2003, and 80% consider security products a "hot" technology (Ames, 2002). A recent study found that the average cost of security breaches is currently $193,000 (Yager, 2002). That survey also reported that 24% of IT leaders are delaying deployment of Web services and 18% are delaying the implementation of wireless networks due to security concerns (Yager, 2002). In a different study, 90% of respondents detected computer security breaches within the last twelve months, but only 34% of intrusions were reported to law enforcement (Computer Security Institute, 2002).

One of the causes of these security breaches is the lack of effective user authentication, primarily due to poor password system management. Poor password practices occupy the number 2 spot on the Top 20 list of General Vulnerabilities (The SANS Institute, 2002). 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, breaking an eight-character password would take more than 13 years on average (Lemos, 2002). Clearly, the potential for password security is not fully utilized.

PASSWORD STRATEGIES

The Federal Information Processing Standards (FIPS) publication 112 (National Institute of Standards and Technology, 1985) includes requirements for different levels of password security. At the highest level, these criteria include passwords with 6 to 8 characters composed from the full 95 printable character ASCII set. Furthermore, the guidelines specify using an automated password generator, individual ownership of passwords, use of non-printing keyboards, encrypted password storage, and encrypted communications with message numbering. The theoretical number of passwords is approximately 6.7×10^{15} ($= 95^8 + 95^7 + 95^6$). However, to utilize the full set of characters, all non-alphanumeric characters must have an equal chance of selection as the alphanumeric characters. But passwords with non-alphanumeric characters can be hard to remember. Consider, for example, passwords such as " ,swFol=; " or " >_F<"Yjz ". To avoid having to use such awkward passwords, we have devised a new password interface for user authentication, described below.

When allowed to select their own password, users tend to select passwords which may be easy to remember, but may also be easy to crack. On the other hand, when they are assigned a cryptographically strong password, users will generally find them difficult to remember, and will frequently record them in writing. To remedy these potential security problems, various strategies are currently used. Some organizations attempt to reduce the number of passwords needed by using a single system sign on (SSO) (Boroditsky & Pleat, 2001). Others are researching the possibility of using graphical mechanisms (Real User Corporation, 2002) (Bolande, 2000) (Jermyn, Mayer, Monrose, Reiter, & Rubin, no date) or combining passwords with keystroke dynamics (Monrose, Reiter, & Wetzel, 1999). Organizations can instruct their members in the proper selection of passwords to varying degrees, from simple instructions regarding the minimum number of positions and the minimum variability of characters, to extensive instructions and even feedback mechanisms where weak passwords are rejected immediately (Bergadano, Crispo, & Ruffo, 1998) (Jianxin, 2001). Weirich and Sasse (2001) advocate proper instruction and motivation of users, as well as a flexible approach depending on the organization and type of work for which the security is needed.

In a study of password usage, Adams and Sasse (1999) identified the following four factors that negatively influence the use of passwords:

- the need to remember multiple passwords due to the use of different passwords for different systems and the requirement to change passwords at intervals;
- lack of user awareness regarding the requirements for secure password content;
- perceived lack of compatibility of passwords with work practices; and
- incorrect user perception of organizational security and information sensitivity.

Though the latter three factors can be remedied with organizational measures such as review of password policies and user education, the first factor remains grounded in the limitations of human memory. Since the number of secure systems used by each individual is bound to increase rather than decrease, memory limitations must be accommodated.

HUMAN MEMORY

A heuristic for the capacity of the human short-term memory system states that an individual can recall seven plus or minus two (7 ± 2) chunks of information (Miller, 1956). This rule of thumb applies only to information to be recalled for relatively brief periods without rehearsal. Information can be maintained for longer periods of time, but elaborate rehearsal is required for transfer to long-term memory (Hewett, 1999) (Newell & Simon, 1972). A recent model describes a *working memory*, which is part of the larger memory system and not distinct from long-term memory (Anderson, 1994). In this model, memory limitations also depend on the ability to retrieve information from long-term storage to working memory. Regardless of the cognitive model, a capacity limitation exists. The proposed password system addresses this memory capacity limitation by offering a process that is easier than FIPS-compliant password systems, yet is more secure.

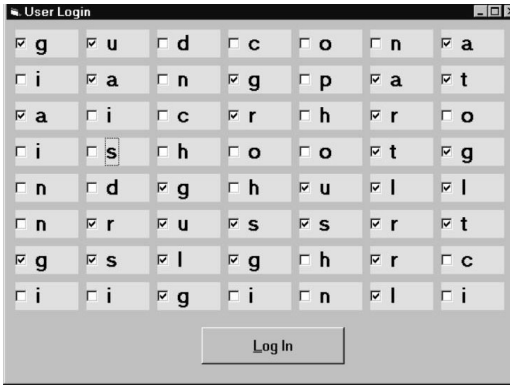
THE CHECK-OFF PASSWORD SYSTEM (COPS)

Traditional password systems either assign an ordered series (sequence) of characters which may or may not spell something meaningful to the user, or users are allowed to select their own ordered sequence of characters. In either case, the order of the characters is significant and must be maintained. A strength of the Check-Off Password System (COPS) is that the order of characters within the password is irrelevant, and therefore the user can choose to remember them in many ways. COPS balances the security of system-selected passwords with the memorability of meaningful character combinations. It assigns each user a set of 8 different characters (the "COPS password") selected from the sixteen most commonly used lower case characters (AskOxford.com, 2002) (the "COPS Superset"), including all five major vowels (e a r i o t n s l c u d p m h g). The user is able to form any word or words from these 8 characters, and may use any of the characters more than once in doing so. For example, suppose a user were issued the characters, "ulatsreg" (in no particular order), which we will refer to as the "Example Password." Using the characters in the Example Password, one user might form the compound word "starglue" in order to remember the eight characters, whereas another user may select "gluerats", "slugtears", or "restgulag". In other words, while the Example Password (and every COPS password) consists of a random selection of 8 alphabetic characters without repetition, users may reorder those characters (and use characters more than once) to form their own "password" (similar to an anagram) to facilitate recall. The user may even use characters not found in the COPS Superset (b f y w k v x z j q) to form a memorizable password, since those characters will not be included on the input interface (the COPS selection grid, as described below). For example, by using the "b" character, a music aficionado could form the password "greatblues" from the Example Password. Finally, an automated password generator might include a facility for suggesting words from a dictionary.

To authenticate the user, COPS presents an 8-by-7 grid of checkboxes, each with a character randomly selected from the COPS Superset. The user checks off only the boxes showing the assigned characters in the COPS password. With 56 grid cells (boxes) and only 16 characters to choose from, characters will appear more than once, requiring an average of 3.5 check-offs.

Consider the Example Password again ("ulatsreg"). To enter the password, the user would be presented with a grid such as the one shown in Figure 1 below, which demonstrates a failed attempt to enter the Example Password. To successfully enter the Example Password, the user would need to check the box for every "u" appearing in the grid (i.e., three checkboxes with a "u" would need to be checked), and the user would need to check the box for every "l" appearing in the grid (i.e., four checkboxes with an "l"), etc. If the user fails to successfully check all of the necessary boxes, she will be presented with a new grid in a randomized layout (which will almost certainly be different than the preceding layout). In Figure 1, the user has neglected to check off the "s" box in the fourth row of the second column. The login attempt will fail, and on the next attempt, a completely new grid layout will be presented.

Figure 1: Representative COPS Selection Grid



Without the ever-changing grid interface, the number of possible combinations would be no higher than C(16,8) or 12,870, because the presence of one instance of a character would determine the result for all other instances of the same character. In other words, if one "t" is selected, all other boxes with a "t" on the same interface should also be selected. Even with a new layout on each login attempt, a human cracker can manually try to enter all 12,870 combinations, because he can see the characters in the checkboxes. Of course, time considerations would make this impractical. A computer can run through combinations much faster, but if the characters are blended into a background graphic for each new login interface, the computer could only "see" them with Optical Character Recognition (OCR). This is much more processor-intensive than entering a simple string. As long as the layouts are randomly generated and OCR cannot be used effectively, the number of possible combinations with 56 check-off boxes either selected or not selected will remain 2^{56} or 7.2×10^{16}.

Although the semi-self-selected passwords using COPS are easy to remember, the system also requires user input which is more cognitively challenging than traditional password systems. If only one check-off box is erroneously missed or selected, an entirely new check-off grid must be generated and completed, thereby increasing the cognitive load of the activity. This may generate resistance to adoption on the part of the system user. In new technology implementations, the Technology Acceptance Model (TAM) indicates that perceived ease of use (PEOU) and perceived usefulness (PU) are considered antecedents of intention to use, which in turn is an antecedent to actual use (Davis, 1989). Therefore, it is imperative that we test the PEOU and PU of COPS in order to evaluate its actual potential as a preferable alternative to current user authentication methods.

PROPOSAL AND DISCUSSION

In order to evaluate the efficacy of COPS, we will conduct a controlled empirical study of COPS and existing alternatives, comparing user perceptions and measures of efficiency. Users will be experienced system users who have previously used multiple password systems. Treatment groups include those with (1) self-selected passwords without restrictions, (2) system-assigned passwords from the list of common passwords found in Spafford (1988), (3) system-assigned passwords following the FIPS standard for high protection (National Institute of Standards and Technology, 1985), and (4) system-assigned "passwords" in the Check-Off Password System (COPS). Standard pre-test and post-test research instruments for the Technology Acceptance Model (TAM), modified as appropriate, will be applied to the various treatment groups, and short-term and medium-term recall performance will be measured. Results will be evaluated with standard tests of variance and covariance to determine the effectiveness of each password strategy in terms of both performance and user acceptance. Whereas COPS may be mathematically more secure than the alternatives, the research questions are: (1) to what extent will users accept this system, and (2) will users be able

to successfully remember their COPS password and be able to log into the system? We will also employ software routines to attempt to crack the COPS password-protected systems and compare those results to the results from similar tests performed on the alternative password systems.

When completed, this study will expand our knowledge of password system acceptance by users by comparing users' perceptions of various alternatives along with the effectiveness of each system as a strong user authentication protocol. Only when viewed in their entirety can the alternative techniques be reasonably compared. The results of this study will be reported at the conference.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40—46.

Ames, B. B. (2002). PC developers worry about security. *Design News, 57*(16), 29.

Anderson, J. R. (1994). *Cognitive Psychology and Its Implications* (4th ed.). New York, NY: W. H. Freeman.

AskOxford.com. (2002). *What is the frequency of the letters of the alphabet in English*. Available: http://www.askoxford.com/asktheexperts/faq/aboutwords/frequency [2002, 9/29/2002].

Bergadano, F., Crispo, B., & Ruffo, G. (1998). High dictionary compression for proactive password checking. *ACM Transactions on Information and System Security (TISSEC), 1*(1), 3—25.

Bolande, H. (2000, November 26, 2000). *Forget passwords, what about pictures?* Available: http://zdnet.com.com/2102-11-525841.html [2002, 9-18-2002].

Boroditsky, M., & Pleat, B. (2001). *Security @ The Edge - Making Security and Usability a Reality with SSO*. Available: http://www.passlogix.com/media/pdfs/security_at_the_edge.pdf [2002, 9-18-2002].

Computer Security Institute. (2002). *Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row*. Available: http://www.gocsi.com/press/20020407.htmlApril 7, 2002].

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(Issue 3), 318.

Hewett, T. T. (1999). *Cognitive factors in design (tutorial session): basic phenomena in human memory and problem solving.* Paper presented at the Proceedings of the third conference on Creativity & cognition, Loughborough, United Kingdom.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (no date). *The Design and Analysis of Graphical Passwords*. Available: http://www.usenix.org/publications/library/proceedings/sec99/full_papers/jermyn/jermyn_html/camera3.html9/18/2002].

Jianxin, J. Y. (2001, 2001). *A note on proactive password checking.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico.

Lemos, R. (2002). *Passwords: the Weakest Link?* Available: http://news.com.com/2009-1001-916719.html [2002, 9-18-2002].

Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review, 63*, 81-97.

Monrose, F., Reiter, M. K., & Wetzel, S. (1999, 1999). *Password hardening based on keystroke dynamics*. Paper presented at the Proceedings of the 6th ACM conference on Computer and communications security, Kent Ridge Digital Labs, Singapore.

National Institute of Standards and Technology. (1985). *Federal Information Processing Standards Publication 112*. Available: http://www.itl.nist.gov/fipspubs/fip112.htm9-18-2002].

Newell, A., & Simon, H. A. (1972). *Human Problem Solving*. Englewood Cliffs, NJ: Prentice-Hall.

Real User Corporation. (2002). *The Passface™User Authentication System*. Available: http://www.realuser.com/cgi-bin/ru.exe/_/homepages/users/passface.htm [9/18/2002.

Spafford, E. H. (1988). *The Internet Worm Program: An Analysis* (Technical Report Purdue Technical Report CSD-TR-823). West Lafayette, IN 47907-2004: Purdue University.

The SANS Institute. (2002). *The Twenty Most Critical Internet Security Vulnerabilities (Updated)*. Available: http://www.sans.org/top20.htmMay 2, 2002].

Weirich, D., & Sasse, M. A. (2001, 2001). *Pretty good persuasion: a first step towards effective password security in the real world.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico.

Yager, T. (2002). Security Part 1: Strategies. *InfoWorld, 24*(Issue 33), 1.