Behavior Research Methods, Instruments, & Computers
2002, 34 (2), 163-169

Improving computer security for authentication of users: Influence of proactive password restrictions

ROBERT W. PROCTOR
Purdue University, West Lafayette, Indiana

MEI-CHING LIEN
NASA Ames Research Center, Moffett Field, California

KIM-PHUONG L. VU
Purdue University, West Lafayette, Indiana

E. EUGENE SCHULTZ
University of California, Berkeley, California

and

GAVRIEL SALVENDY
Purdue University, West Lafayette, Indiana
and Tsinghua University, Beijing, China

Entering a username–password combination is a widely used procedure for identification and authentication in computer systems. However, it is a notoriously weak method, in that the passwords adopted by many users are easy to crack. In an attempt to improve security, proactive password checking may be used, in which passwords must meet several criteria to be more resistant to cracking. In two experiments, we examined the influence of proactive password restrictions on the time that it took to generate an acceptable password and to use it subsequently to log in. The required length was a minimum of five characters in Experiment 1 and eight characters in Experiment 2. In both experiments, one condition had only the length restriction, and the other had additional restrictions. The additional restrictions greatly increased the time it took to generate the password but had only a small effect on the time it took to use it subsequently to log in. For the five-character passwords, 75% were cracked when no other restrictions were imposed, and this was reduced to 33% with the additional restrictions. For the eight-character passwords, 17% were cracked with no other restrictions, and 12.5% with restrictions. The results indicate that increasing the minimum character length reduces crackability and increases security, regardless of whether additional restrictions are imposed.

Engaging in electronic transactions has become a significant part of people's daily activities. A large amount of personal information, such as social security numbers and credit card numbers, is accessible on line or in data systems. Organizations also have their own proprietary resources that need protection. Violations of security can be extremely costly, both financially and personally, making information security a central concern of many individuals, businesses, and organizations. Although the financial risks for individuals, such as psychologists and other academicians, are not as large as those for businesses and organizations, the liabilities are still significant. For example, many transactions conducted by psychologists involve the usage of computer networks for teaching, research, and practice, with many sensitive documents and data files accessible to an intruder. Threats to information security include eavesdropping on user sessions, masquerading as another user, manipulating data without authorization, misrouting communications, and repudiating a recently initiated electronic commerce transaction, among others (see, e.g., Bernstein, Bhimani, Schultz, & Siegel, 1996). Not surprisingly, considerable knowledge concerning these and many other threats, and how to counter them, has been published in the area of information security, which, among other things, attempts to ensure that authentic and accurate information is stored, retrieved, and transmitted through any computing system.

Traditionally, issues concerning methods of improving information security have been restricted primarily to the realm of computer science. Many sophisticated

This research was supported by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. Correspondence concerning this article should be addressed to R. W. Proctor, Department of Psychological Sciences, Purdue University, West Lafayette, IN 47907-1364 (e-mail: proctor@psych.purdue.edu).

methods have been developed to increase information security, but these methods do not take into account the end-users and system administrators who must interact with the system in the intended manner if the optimal level of security is to be achieved (Schultz, Proctor, Lien, & Salvendy, 2001). Users often do not interact with the security method as intended, because (1) they circumvent the procedures, (2) they do not know what impact their behaviors have on system security, or (3) the demands placed on the users exceed their capabilities. In other words, the limiting factor in computer security often is the human user, rather than the security method itself. Consequently, there has been growing recognition of the need for the designers of information security methods to draw on the knowledge and techniques of cognitive psychology and related disciplines to provide the basis for interactions between users and the security method (e.g., Schultz et al., 2001).

The major types of security controls that exist today apply to several areas (Schultz et al., 2001). Many controls focus on the importance of maintaining the integrity, confidentiality, and availability of data for the users. Any information stored on computers is subject to being deleted, altered, or stolen, and each of these outcomes has an associated cost that may be quite high. Consequently, considerable effort in information security is devoted to protection of data and systems. Another area in which security controls exist is that of intrusion detection, which focuses on mechanisms for detecting the activity of intruders and the steps to be taken when an attack is detected. A final area of concern, which is the focus of the present study, is that of identification and authentication, the method used to allow or deny the user access to systems and/or networks. Identification refers to means for confirming the user's identity, and authentication generally requires additional steps, such as entry of the user's account name.

The most commonly used form of identification and authentication is the username–password entry method. Usernames provide a mechanism for confirming the user's identity, or identification. Passwords are used for authentication, establishing one's identity for the purpose of access to systems and networks. For example, in order to receive personal e-mails, the username identifies which account should be accessed, and the password determines whether access to that account is permitted. Although the username–password entry method is widely accepted (e.g., logging into the university system, accessing on-line course material, using an e-mail account, etc.), it does not provide much security, because users typically fail to select crack-resistant passwords. Many users do not know what are good choices for passwords, and those who do know what choices are safe will often select easy-to-remember passwords, such as variations of their own names or meaningful words, because much less effort is required than to generate safe passwords (Bishop & Klein, 1995). Moreover, a user is likely to have more than one account for which a username–password combination is required; having to remember several "nonmeaningful" but crack-resistant passwords will likely require much more effort on the user's part than simply remembering a single safe password.

In many universities, students, faculty, and staff log into numerous network systems (library account, course account, etc.) by using the person's last name and social security number as the username–password combination. However, it is relatively easy for another person to obtain this information, because social security numbers are often used as student/faculty identification numbers and are printed on a variety of documents (e.g., identification cards, class rosters, posted grades, pay stubs, etc.). Because knowledge of this information would allow anyone to access confidential information, security will be enhanced if the individuals are required to generate different passwords to access their university accounts or are required to use another method of authentication.

Other authentication methods include biometric measures, such as fingerprints (Jain, Hong, & Pankanti, 2000), smart cards (credit-card–sized plastic cards that carry information via an embedded computer chip), and tokens (small cards used to provide authentication through a "log-on challenge" in which users must first connect to a service provider and use an authentication token, such as a number displayed on a special device, in order to gain access to the system). However, such methods have historically tended to be expensive, obtrusive, difficult to implement on a large scale, and low in user acceptance (see, e.g., B. Miller, 1994; Proctor, Lien, Salvendy, & Schultz, 2000).

Another approach to this problem is to improve security by imposing additional requirements within the identification–authentication framework. Systems have been designed to include additional security measures, such as having users identify themselves multiple times during a session, providing computer-generated passwords, and using one-time passwords. However, requiring users to log in multiple times greatly disrupts their task. The use of computer-generated passwords and one-time passwords also raises problems, because users will likely have difficulty remembering them. A technique that is relatively easy to implement and, hence, relatively widely used is proactive password checking (Stallings, 1995). With this technique, users are allowed to generate their own passwords, but restrictions are placed on the passwords that will be accepted. The system checks to determine whether a generated password satisfies certain criteria (e.g., contains at least one uppercase and one lowercase English alphabet character in addition to a digit) and accepts the password if it does. If it does not, the password selection is rejected, and the user must generate a new password. Even though restrictions limit the acceptable passwords, users should be able to remember them more easily than computer-generated passwords, because the password can still be meaningful to the user. In addition, recall of the same material usually is better if users generate the material, rather than merely having it provided for them (Neath, 1998; Slamecka & Graf, 1978).

It is generally assumed that password restrictions of the type imposed in proactive password checking will improve the security of a system by making the passwords more difficult to crack. However, to our knowledge, it has not yet been demonstrated that the passwords generated under commonly used restrictions are any more difficult to crack than those generated under minimal restrictions. Moreover, any gain in security is extremely likely to be accompanied by a decrease in usability. Some drawbacks of imposing restrictions on passwords are that more time may be needed to generate an acceptable password, passwords generated under restrictions may be less memorable than those generated without restrictions, and the additional restrictions may cause more entry errors and lengthened the log-in procedure.

Despite the widespread use of password restrictions, the extent to which they increase security, relative to the costs associated with initial generation and later retrieval, is not known. In the present study, we examined how proactive restrictions on passwords affected the passwords that users generated and the ease with which they could be cracked. In two experiments, we evaluated the ease of generating and remembering passwords under conditions of minimal and additional restrictions for passwords with a minimum length of five characters (Experiment 1) or eight characters (Experiment 2). The time required to generate the passwords and to recall and enter them in later log-in sessions was measured. In addition, user ratings of the difficulty involved in generating and recalling passwords under the two conditions of restriction were obtained, and a cracking tool was used to test the crackability of the passwords.

EXPERIMENT 1

In Experiment 1, we evaluated how generation of the initial password and recall of the password on subsequent log-ins were affected when additional restrictions were imposed on a password that had to have a minimum of five characters. This minimum length was chosen because it is within a user's working memory capacity (e.g., G. A. Miller, 1956).

Method

Subjects. Twenty-four Purdue University undergraduates participated in partial fulfillment of an introductory psychology course requirement. All the subjects had their own personal accounts set up with the University computer network and were familiar with general log-in procedures.

Apparatus. The study was conducted using two personal computers, with one being used for the primary password generation and authentication task and the other one for a word-naming task. Trinity Client and Enterprise authentication software, Version 3.0 (American Biometric Company, Ontario; now known as the Ankari Company), was used for the generation and authentication of passwords and log-ins. The word-naming task, described below, was presented as a distracting task, using Micro Experimental Laboratory 2.0 software (Schneider, 1995).

Procedure. All the subjects were told that they were setting up a new account on a workstation. They were also asked to generate a password for that account that would represent one they would typically use for a real computer account. Each subject generated and recalled passwords under minimal restrictions (only a length requirement) and additional restrictions, with the minimal and additional restriction conditions counterbalanced for order across subjects. The length restriction was that the password should have at least five characters. The additional restrictions consisted of the following: It must contain an uppercase letter; it must contain a lowercase letter; it must contain a numeric character; it must not repeat a character two times in a row; it must not contain two characters from the username. These restrictions are the maximum allowed by the software for generating one reusable password.

The subject entered the generated password into the dialog box, with the restrictions listed. As the entry fulfilled each criterion, the symbol next to the restriction changed from a red "x" to a green checkmark (see, e.g., Figure 1). The experimenter sat next to the subject and recorded the time spent generating an acceptable initial password, using a stopwatch, and the number of errors committed.

After generating the password, the subject was asked to log off the workstation and to log into the system using the username–password combination that initially had been generated. The experimenter recorded the time from when the password dialog box appeared until the user clicked or entered "OK" to finish the log-in procedure and also recorded the number of errors. The subject then engaged in a distractor task of reading aloud 60 words presented for 500 msec each, to prevent rehearsing the password between log-ins. This standard procedure ensured that the to-be-remembered items were not in working memory (e.g., Neath & Crowder, 1990). Four additional log-in trials were performed, with the distractor task administered between each trial.

At the end of the experiment, the subjects were given a questionnaire in which they were asked to rate the difficulty of generating and remembering the password for each task condition. The subjects used a 7-point scale (1 = *very low*; 7 = *very high*) to rate each of the following: (1) the difficulty of initially *generating* the password when the only restriction was that it must be at least five characters, (2) the difficulty of *remembering* the password when the only restriction was that it must be at least five characters, (3) the difficulty of initially *generating* the password when it had to satisfy the additional restrictions, and (4) the difficulty of *remembering* the password when it had to satisfy the additional restrictions.

Determining the crackability of passwords. The passwords generated by the subjects in Experiment 1, as well as those generated in Experiment 2, were entered as passwords to accounts on a Sun Solaris 7 system, which used crypt(3), a variant of the data encryption standard (DES) algorithm, to encrypt the passwords. The passwords were then run through John the Ripper 1.6 password-cracking software on a 400-MHz Pentium II computer running on a Red Hat Linux system. John the Ripper 1.6 is a powerful and fast cracking program used for Unix passwords. Initially, the passwords were tested with the standard Solaris/usr/dict/words dictionary, and the remaining uncracked passwords were tested with the "brute force" feature. This feature tests possible character combinations and, if given an unlimited amount of time, will eventually crack the password. The initial test lasted for approximately 22 min, and the brute force test was run for approximately 1 day. Across the two experiments, all except two of the passwords cracked by the brute force feature were identified within the first half hour.

Results

Generation and recall. The subjects generated passwords until they had entered a valid password that satisfied all the restrictions. We recorded the number of invalid passwords generated, as well as the total time taken to generate a valid password. We also measured the average response time and the number of errors on five subsequent log-in trials for each subject. The average

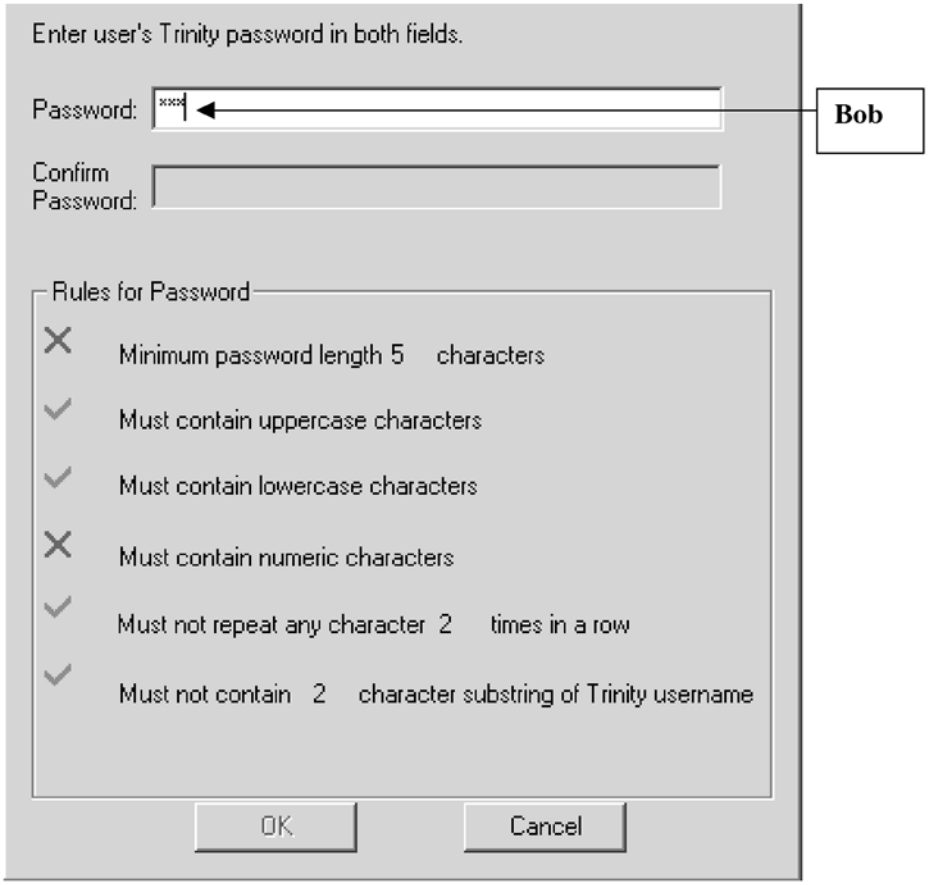

Figure 1. Screen shot of the password generation dialog box for the condition with passwords with a length of five characters and additional restrictions.

password length was 0.5 characters shorter in the *minimal* condition ($M = 6.0$) than in the *additional* condition ($M = 6.5$). Mean time to generate the password was 7.8 sec for the *minimal* condition and 18.6 sec for the *additional* condition [$F(1,23) = 15.99$, $MS_e = 86.6$, $p < .001$]. The subjects averaged 0.2 errors in generating a password that met the five-character criterion and 1.6 errors with the additional restrictions [$F(1,23) = 11.64$, $MS_e = 1.95$, $p = .002$].

The subjects averaged 2.3 sec to recall and enter the password in the *minimal* condition and 3.2 sec in the *additional* condition [$F(1,23) = 79.11$, $MS_e = 0.13$, $p < .001$]. The mean number of entry errors was 1.0 for the *minimal* condition and 1.3 for the *additional* condition [$F(1,23) < 1$].

Questionnaire. The mean rating for the difficulty of generating a password was 1.6 for the *minimal* condition and 3.6 for the *additional* condition [$F(1,23) = 26.46$, $MS_e = 1.89$, $p = .001$]. The mean rating for the difficulty of remembering the password was 1.9 for the *minimal* condition and 2.8 for the *additional* condition [$F(1,23) = 15.13$, $MS_e = 0.55$, $p < .001$].

Password crackability. Overall, 18 of 24 passwords were cracked by John the Ripper for the *minimal* condition, as compared with 8 out of 24 passwords for the *additional* condition. For the *minimal* condition, 10 of the cracked passwords were obtained from the dictionary procedure, and 8 were obtained from the brute force attempts. The 6 passwords that were not cracked tended to be longer than those that were cracked, with 4 of them having seven or eight characters and one having six characters. For the *additional* condition, 6 of the cracked passwords were obtained from the dictionary procedure, and 2 were obtained from the brute force attack. Out of the individuals who generated the 8 cracked passwords in the *additional* condition, 7 of their passwords were also cracked for the *minimal* condition.

Discussion

It was considerably more difficult to generate passwords when more restrictions were imposed. The time to generate the password was more than twice as long (10 sec longer) in the *additional* condition than in the *minimal* condition, and errors were more frequent. However, the subjects had little difficulty recalling the passwords for logging into the account. They took only about 1 sec longer, on average, to log in for the *additional* condition than for the *minimal* condition, and the number of errors

Table 1
The Passwords Generated in Experiment 1

Minimal Condition		Additional Condition	
Password	Cracked?	Password	Cracked?
megan	+	Rocket3	+
final	+	Maestro7	+
password	+	Quasney1	
dragon	+	Davion2	
seger	+	1Time	
dogwood	+	Squeak24	
fifth	+	Asd1n	
jacob33		Ryan525	
doggy	+	Dogie7	
hands	+	Lester5	+
drummer	+	1candyG	
666girly		6aGirl	
271toaster		271Toast	
meijer	+	Fender8	+
pusher9		Noland8	
miles	+	Mito1	+
anarchy	+	Total1	+
goette		abcd4E	
corona	+	April1	+
mikey	+	Dra4230	
kishm		Love5	+
mike2	+	recoN23	
chewy	+	Chewy3	
jjjjj	+	boscO9	

Note—A "+" sign next to the password indicates that it was cracked by John the Ripper v 1.6.

was not different across conditions. Thus, although it was difficult to generate the passwords initially when restrictions were imposed, there was little cost of these restrictions with respect to the ease of recalling the passwords.

Although the generated passwords satisfied the additional restrictions, they typically consisted of a meaningful word beginning with a capital letter and ending with a number (e.g., Rocket3; Maestro7; Dogie7; see Table 1). Thus, to some extent, the users were defeating the intent of the restrictions by imposing a simple strategy that would still yield meaningful and memorable strings. Even so, John the Ripper was not able to crack as many of the passwords from the *additional* condition as from the *minimal* condition in the designated amount of time. Thus, there was some increase in security, but still a third of the passwords were cracked. Moreover, the successfulness of the cracking software probably could be increased substantially by incorporating the simple algorithms that the subjects were using to generate many of the passwords.

EXPERIMENT 2

Most often, password length restrictions require passwords longer than five characters, with a minimum of seven or eight characters being common. Performance may be substantially different with passwords of this longer minimum length, since the larger number of characters imposes a greater working memory load (Baddeley, 1992). Therefore, in Experiment 2, the minimum number of characters was increased to eight. In other respects, the method was similar to that of Experiment 1.

Method

Twenty-four new subjects from the same subject pool as that in Experiment 1 participated. The apparatus and procedure were identical to those in Experiment 1, except that the minimum number of characters was eight instead of five.

Results

Generation and recall. The mean length of the passwords generated was similar in the *minimal* condition ($M = 8.7$) and the *additional* condition ($M = 8.8$). Mean time to generate the password was 24.7 sec for the *minimal* condition and 74.8 sec for the *additional* condition [$F(1,23) = 22.40$, $MS_e = 1, 344$, $p < .001$]. The subjects made no errors in generating a password that met the criterion in the *minimal* condition and 0.8 errors in the *additional* condition [$F(1,23) = 25.00$, $MS_e = 0.33$, $p < .001$].

For the log-in trials, the subjects spent 4.4 sec entering the password in the *minimal* condition and 5.7 sec in the *additional* condition [$F(1,23) = 7.32$, $MS_e = 2.79$, $p = .013$]. The mean number of errors was 0.1 for the *minimal* condition and 0.2 for the *additional* condition [$F(1,23) = 1.49$, $p > .05$].

Questionnaire. The mean rating on the difficulty of generating a password was 2.0 for the *minimal* condition and 4.7 for the *additional* condition [$F(1,23) = 98.22$, $MS_e = 0.92$, $p < .001$]. The mean rating on the difficulty of remembering the password was 1.6 for the *minimal* condition and 3.5 for the *additional* condition [$F(1,23) = 56.59$, $MS_e = 0.78$, $p < .001$].

Password crackability. The 48 passwords were run through John the Ripper 1.6, with a standard dictionary or a brute force attack, as in Experiment 1. Overall, 4 of 24 passwords for the *minimal* condition were cracked. This outcome was similar to the 3 out of 24 passwords cracked for the *additional* condition. The brute force attack accounted for no additional passwords for either the *minimal* or the *additional* condition. Only 1 subject had both passwords cracked by John the Ripper (see Table 2).

Discussion

As in Experiment 1, it was more difficult to generate passwords when more restrictions were imposed. In this case, the increase in generation time was nearly 50 sec, which is approximately three times longer in the *additional* condition than in the *minimal* condition. Again, as in Experiment 1, the subjects did not show much increase in the difficulty of recalling and logging in under the restrictions. The additional time to log in was only about 1.5 sec, and the error rate was not significantly higher in the *additional* condition than in the *minimal* condition.

The passwords generated for the *minimal* condition were easy-to-remember words (e.g., princess) or combinations of words (e.g., lifehouse), and for the *additional* condition, they were easy-to-remember word–number

Table 2
The Passwords Generated in Experiment 2

Minimal Condition		Additional Condition	
Password	Cracked?	Password	Cracked?
protractor	+	Tractors2	+
luckyblh		4iuUrocE	
princess	+	Texas4u2	
jklein69		4130Jwk01	
26altair		9Aurelia	
gllcontrol		twin1Ghs	
pyramida	+	Sr59d4n5	
yia557720		CHen1820	
opendammit		Jobe0909	
225ds7RK		MK2ds25rk	
vonRyan4		Waterford4	
boiler02		Thegrub1	
Rodoki98		Blrmkr03	
tootsiroll		Tractor1	+
lifehouse		9297isHome	
gregkamer		August01	
9288181		Psych120	
Gramvoxd		Indagation1	
password	+	Purple23	
mousserr		Mahjong1	
ilovejune		Oh12hap12py	
vickim50		Cin5five	
wilson1970		Ivote4ja	
sparrowfoot		Biochemistry1	+

Note—A "+" sign next to the password indicates that it was cracked by John the Ripper v 1.6.

combinations (e.g., Tractor1, Thegrub1) or complex arrangements of characters (e.g., Sr59d4n5, 4iuUrocE). However, even with the additional brute force attack, John the Ripper was able to crack only four passwords in the *minimal* condition and three in the *additional* condition. Thus, increasing the minimum string length alone was sufficient to reduce the number of crackable passwords, and the additional restrictions had minimal effect on crackability for John the Ripper. Because John the Ripper was not able to crack many of the passwords in the *minimal* condition, there was little opportunity to show a benefit for the *additional* condition. The possibility exists that a difference in the ease with which the passwords in the two conditions could be cracked would become evident if the brute force routine were run for longer than 24 h.

GENERAL DISCUSSION

Password restrictions greatly increase the difficulty of generating an acceptable password. With a five-character minimum in Experiment 1, the time it took to generate a password increased by more than 10 sec when additional restrictions were imposed, with the time being more than twice that required than when they were not. With an eight-character minimum in Experiment 2, the increase was approximately 50 sec, so that the amount of time needed to generate a password when the additional restrictions were imposed was more than three times that needed when they were not. The subjects also judged password generation to be considerably more difficult when additional restrictions were in effect than when they were not, more so in Experiment 2 than in Experiment 1. It is clear that any imposition of restrictions beyond a minimum length drastically increases the cognitive demands for generating a password and will likely be met with user resistance.

In contrast, for log-in time, password restrictions had only small effects. With a five-character minimum in Experiment 1, the time it took to recall and enter the password increased only a small amount, from slightly more than 2 sec under minimal restrictions to slightly more than 3 sec when additional restrictions were imposed. With an eight-character minimum in Experiment 2, the increase in time was from 4.4 sec with minimal restrictions to 5.7 sec with additional restrictions. Although the increase in retrieval time was not large, it was statistically significant. Moreover, in both experiments, the subjects judged retrieval as more difficult with the passwords generated under additional restrictions than with those generated with minimal restrictions, although the differences in judged difficulty for retrieval were not as large as those for initial generation of the password. For most uses of computers, users do not log in only at short intervals after first generating the password, and different passwords must be used for different accounts. It is possible that, under those conditions, password restrictions would have a stronger effect on performance than was evident in the present study.

The reason that restrictions did not have much effect on log-in time is that the generated password was often a relatively meaningful string of characters. To a large extent, particularly with the five-character minimum, the subjects circumvented the intent of the restrictions by generating a word or name with a capital letter at the beginning and a number at the end. With the five-character minimum, although John the Ripper cracked 33% of the passwords, this was substantially less than the 75% that were cracked when no restrictions were in effect. Thus, although restrictions improved security, the ease with which many strings could be cracked indicates that the system could hardly be considered secure. With the eight-character minimum, the percentage of cracked passwords was reduced substantially to 17% without restrictions and to 12.5% for passwords generated to satisfy the restrictions.

It is interesting that increasing the minimum length from five to eight characters was more effective at reducing the number of cracked passwords than was placing other restrictions on the acceptable passwords. Moreover, this relatively greater effectiveness of an increase in minimum length was accompanied by only a relatively small increase in the time it took to retrieve the passwords when logging in. Thus, the simplest way to increase the average effectiveness of passwords is to increase the minimum length of strings that are acceptable. Given that people are adept at creating and combining meaningful chunks of information (G. A. Miller, 1956;

Simon, 1974), an even better way to improve security for the username–password combination without decreasing usability and user acceptance may be to have a long minimum character restriction and to instruct users to generate word combinations instead of single words.

Perhaps the most important message of this study is that restrictions on user-generated passwords may not accomplish their intended goals. The restrictions imposed by the software used in this study could reasonably be expected to produce passwords that have little meaning and will be difficult to crack. Although the resulting passwords are somewhat more difficult to crack, at least for five-letter strings, it is clear that users tend to follow certain relatively systematic procedures to satisfy the constraints. Any time that systematic patterns appear in passwords, this information can be incorporated into the routines used by a cracker. Thus, although proactive restrictions may increase the difficulty of password cracking, they result in sets of passwords that can hardly be described as extremely secure.

REFERENCES

Baddeley, A. D. (1992). Working memory. *Science*, **255**, 556-559.

Bernstein, T., Bhimani, A. B., Schultz, E. E., & Siegel, C. A. (1996). *Internet security for business*. New York: Wiley.

Bishop, M., & Klein, D. V. (1995). Improving system security via proactive password checking. *Computers & Security*, **14**, 233-249.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, **43**, 91-98.

Miller, B. (1994, February). Vital signs of identity. *IEEE Spectrum*, pp. 22-30.

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.

Neath, I. (1998). *Human memory: An introduction to research, data, and theory*. Pacific Grove, CA: Brooks/Cole.

Neath, I., & Crowder, R. G. (1990). Schedules of presentation and temporal distinctiveness in human memory. *Journal of Experimental Psychology: Learning, Memory, & Cognition*, **16**, 316-327.

Proctor, R. W., Lien, M.-C., Salvendy, G., & Schultz, E. E. (2000, April). A task analysis of usability in third-party authentication. *Information Security Bulletin*, pp. 49-56.

Schneider, W. (1995). *MEL professional: User's guide* (Version 2.0) [Computer software]. Pittsburgh: Psychology Software Tools.

Schultz, E. E., Proctor, R. W., Lien, M.-C., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, **20**, 620-634.

Simon, H. A. (1974). How big is a chunk? *Science*, **183**, 482-488.

Slamecka, N. J., & Graf, P. (1978). The generation effect: Delineation of a phenomenon. *Journal of Experimental Psychology: Human Learning & Memory*, **4**, 592-604.

Stallings, W. (1995). *Network and internet security*. Englewood Cliffs, NJ: Prentice-Hall.

(Manuscript received November 13, 2001;
accepted for publication February 24, 2002.)