A Comparison of Password Techniques for Multilevel Authentication Mechanisms

M. ZVIRAN AND W. J. HAGA

Department of Administrative Sciences, Naval Postgraduate School, Monterey, CA 93943, USA

Various mechanisms for authenticating users of computer-based information systems have been proposed. These include traditional, user-selected passwords, system-generated passwords, passphrases, cognitive passwords and associative passwords. While the mechanisms employed in primary passwords are determined by the operating systems' manufacturers, system designers can select any password mechanism for secondary passwords, to further protect sensitive applications and data files. This paper reports on the results of an empirically based study of passwords characteristics. It provides a comparative evaluation on the memorability and users' subjective preferences of the various passwords mechanisms, and suggests that cognitive passwords and associative passwords seem the most appropriate for secondary passwords.

1. INTRODUCTION

Access control based on verification of a person's identity is a commonly used method in computer installations. The most popular method is to provide authorized users with passwords, which serve as the 'key' for authorized use of a computer systems and try to make unauthorized access virtually impossible [2, 5, 8, 9, 10, 12, 13, 15, 17, 19].

Commonly, passwords are used as a sole authentication mechanism to a computer-based information system, controlling access to an entire set of computing resources through the operating system [1, 15]. These passwords are referred in the literature as *primary passwords*. However, passwords can also be used to further control access to segments of these resources [13]. These are called *secondary passwords* and are used with particular resources such as specific applications or data files. Figure 1 presents a multilevel security environment, where primary passwords are used to limit the accessibility of the operating system and secondary passwords are used as an additional security mechanism to further protect sensitive software applications and data files.

The format of primary passwords is determined by the operating systems' manufacturers and the use of traditional, user-selected, passwords is common to most of them. However, their use at lower levels of a security system is not mandatory and it is possible to incorporate alternative password mechanisms as secondary passwords at the application level.

A partial list of methods includes system-generated passwords [13], passphrases [16], cognitive passwords [6, 25] and associative passwords [17]. However, no comparative evaluation or analysis of user preferences have yet been reported. This research is based on empirical data and aims at evaluating the characteristics of the various authentication techniques.
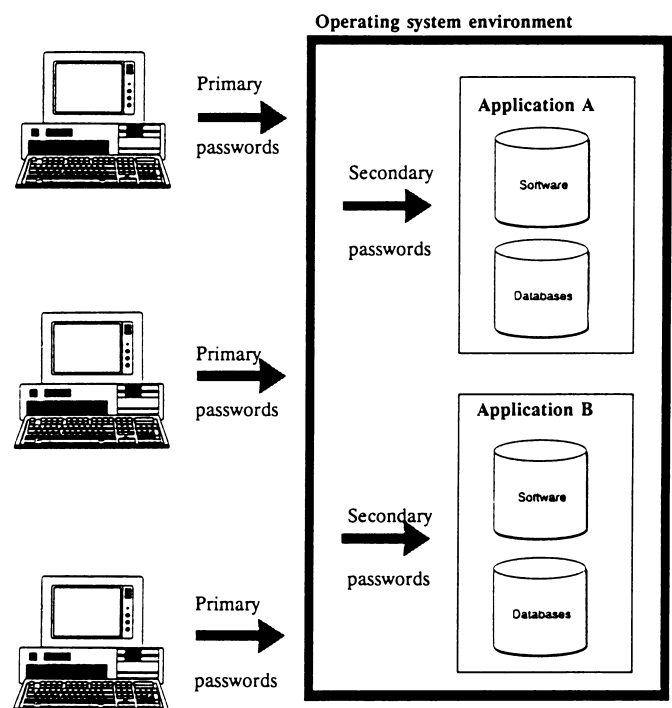
Operating system environment

FIGURE 1. A multilevel security environment.

2. TRADITIONAL PASSWORDS

Traditional passwords are the most commonly used authentication method in existing operating systems [7, 8, 13, 15]. With this mechanism, a new user is introduced to the system by a given user-ID and instructed to select a password to be known only to him. This user-ID and password pair serves for user authentication and authorizing use of a computer system while trying to block unauthorized access to the computing resources. Despite their widespread use, passwords are known to suffer from several pitfalls. First, the tradeoff between memorability and safety poses a dilemma in the generation of passwords. Passwords should be difficult to guess and

easy to remember [11, 15, 16]. For passwords to be difficult to guess, they should be selected from a large domain. Nevertheless, if passwords are chosen to make them difficult to guess, they may also be difficult to remember. The most secure type of password is a random string of characters [3, 16, 20]. Although such passwords are difficult to guess by others, users generally dislike them because random, arbitrary passwords are difficult to remember. Instead, most users will resort to meaningful details, such as name, nickname, initials, birthdate, etc. [3, 13].

A password that is difficult to remember compels a user to write it down, ensuring they will not forget them but compromising its secrecy [14]. On the other hand, if a difficult password is not written down, it may well be forgotten, resulting in serious inconvenience [2, 16]. Therefore, an organization should establish a password policy that strikes a balance between ease of remembrance and susceptibility to compromise [20].

3. ALTERNATIVE PASSWORD TECHNIQUES

3.1. System-generated passwords

With a system-generated password, a password is automatically generated by the operating system and assigned to a user. A common practice in this method is that a pseudo-random number generator arbitrarily creates a string of alphanumeric characters as the password [3, 4, 13].

The basic characteristics of system-generated passwords make them more difficult to guess than traditional passwords [14]. However, being composed of a random sequence of alphanumeric characters, these passwords are usually more difficult to remember since there is no meaningful relation to the user [13]. As a result, the high degree of complexity may cause the user to write down or even forget the password, thus failing to provide secure access control [18]. Also, this method may result in friction between the user and the administrator's need to meet security requirements.

3.2. Passphrases

A variation of the traditional password system is an extended password, known as a passphrase. A passphrase consists of a meaningful sequence of words, e.g. 'to be or not to be'. Because it becomes more difficult to guess or find out a password as its length increases, a passphrase is designed to form a compromise between ease of memorability and difficulty in figuring out. The longer, extended password of 30–80 characters becomes difficult to guess [16]. Unlike system-generated passwords, the passphrase is generated by a user, allowing a selection of a meaningful sequence of words for ease of memorability. In the passphrase method the sheer length of the passphrase provides the desired security, so having the passphrase unrelated to the user is not as stringent a requirement. The following example shows how length

thwarts a possible intruder. If a user were to use a minimum of 30 alphabetic characters, over 1 000 000 000 000 possible combinations exist. This definitely makes the brute force attempt of trying all possible character combinations a formidable obstacle to an intruder [15].

3.3. Cognitive passwords

Another alternative to the traditional password system is a the cognitive passwords mechanism. This method is based on a question-and-answer mode, where, instead of a user entering just one password, he is required to enter several passwords, one at a time, when prompted by the computer. Cognitive passwords are based on an individual user's perceptions, personal interests and personal history. This information is unique to the individual and is neither commonly associated with the user by others, nor could it easily be found in personal records [21]. Examples of questions for cognitive items include: 'What is the first name of your favorite uncle', 'what is the name of the elementary school from which you graduated', 'What is your favorite type of music' or 'what is your favorite color'.

In order to make the cognitive password mechanism effective, the system should consist of non-trivial questions as the stimulus for user responses. If trivial questions, such as 'What is your name?', are chosen, then an intruder will more easily break into the system than if, for example, 'What was the name of your first girlfriend/boyfriend?' is used.

A cognitive password system combines both system-generated and user-defined characteristics. It is system-generated in the sense that the system creates the questions to stimulate a response from a user. The exact responses to these questions would entirely be user-determined. As such, the password system is set up basically as an access quiz. If the user responds correctly to a series of questions concerning himself, then he would be authorized access to the system [6].

Every new user is assigned with a user-ID by the system administrator and asked to create his or her a user profile by answering a set of 20 cognitive items [6]. In a typical session, a user desiring access enters his or her assigned user-ID. Having passed the user-ID validity test, a user is presented with five randomly selected questions from the same set that was user to create the profile. The questions are presented sequentially, one at a time. Upon gathering all five answers, they are compared against the stored cognitive data in the user's profile database, using the evaluation mechanism. If correct, access is granted. If one or more answers do not match, a user might be given a second chance but presenting another set of five questions to be answered.

Like the other password methods described, responses to these questions need to be entered exactly for a user to gain access. Because the responses vary in length, cognitive passwords have no preset length associated

with them. They also would be meaningful items, as opposed to a random string of alphanumeric characters.

Since cognitive passwords consist of meaningful details, they are likely to be easy for a user to remember, but difficult for an intruder to guess or find out. Cognitive passwords may be of such length that a brute force method of trying all character combinations would be thwarted. Also, a cognitive password system requires several questions to be answered correctly, adding further security to the system.

On the other hand, there are some disadvantages in the use of cognitive passwords. In a traditional password system it is difficult for a user to remember one password, therefore remembering many cognitive passwords would seem to be harder for the user [17]. Also, it is unlikely that a user would remember all of his responses so establishing an acceptable miss percentage may be difficult to do. If set too low, intruders may penetrate the system; if set too high, authorized users may be denied access.

3.4. Associative passwords

Another password mechanism requiring a series of passwords to verify user identity is associative passwords [17]. In this alternative, the user constructs a list of cues and responses that would be unique to the individual. A trivial example would be the cue word 'high' which would require the response 'low'. Smith [17] designed this model with the thought that an initial list of 20 cues and responses per user would be sufficient to allow flexibility in changing the cues presented to the user when logging in to the system. Depending upon the security of the system, a user would be required to give from one to several correct responses.

The actual structure is based on a single-word cue and a one-word response. Doing so allows for ease of memory for the user. Similarly, the user is responsible for constructing all 20 cues and responses making it user-friendly [17].

In order to make this method a stronger impediment to intrusion, the word associations should be non-trivial. For example, a list of 20 opposites (e.g. 'good' and 'bad', 'yes' and 'no', 'black' and 'white') would be easy to penetrate [17]. To make construction of the list easier and to make it easier for the user to remember the responses, it is helpful for a particular user to choose one central theme [17]. For instance, a user may associative passwords profile around the Beatles. In this case, cues may include 'abbey', 'john', 'yellow' and 'george' and have responses of 'road', 'Lennon', 'submarine' and 'Harrison', respectively.

Finally, a user is expected to generate correct responses to gain access to the system. As with cognitive passwords, every new user is assigned with a user-ID and asked to create 20 word associations which compose his or her a user profile. Then, a user desiring access enters his or her assigned user-ID which is matched

against his or her profile. Having passed the user-ID validity test, a user is presented with five randomly selected cues from the a set of 20 word associations in his or her profile. The cues are presented one at a time and responded by the matching word association. Upon gathering all five responses, they are compared against the stored user's profile database. If correct, access is granted. If one or more answers do not match, a user might be given a second chance and another set of five cues is randomly selected from the database.

Smith postulated several advantages to this method:

1. The responses would be easy to remember.
2. Without knowledge of the theme and non-trivial associations, the responses would be resistant to intrusion.
3. Since the cues and responses are selected by the user, there would be little user resistance to such a method.
4. The cues and responses would uniquely identify each individual user.
5. If a need arises to change a cue and response, it could easily be altered without altering or compromising the rest of the list. [17]

On the other hand, If a user is not careful in constructing the word associations, the responses may be easily guessed. Also, a user may be tempted to write down the cues and responses or the central theme since there would be so many responses to remember. This would lead to compromise. Finally, like cognitive passwords, a user would likely not remember all the responses so an acceptable margin of incorrect responses would have to be established.

4. RESEARCH METHODOLOGY

4.1. Instrumentation

To assess the ease of recall for the various password mechanisms, two nearly identical versions of a self-administered questionnaire (Form-1 and Form-2) were developed. Using Form-1 (see Appendix A), respondents created their passwords for the various methods. Form-2 questionnaires were answered by the same group of respondents three months later and aimed at assessing their ability to recall the different types of passwords. The questionnaires consisted of the following.

4.1.1. Demographic items

The first part of Form-1 asked for each respondent's age, sex, years of computer usage, the types of computer which they have used (mainframe, personal computer (stand-alone or linked to a mainframe) and the last four digits of their US Social Security number (SSN). Form-2 asked only for the SSN digits, so that each copy could be matched with its counterpart Form-1. The SSN digits were used to mask the identity of individual respondents in this study, while letting us match Form-1 and Form-2 for each of respondent.

4.1.2. Creation and assignment of passwords and passphrases

The second part of Form-1, but not Form-2, asked each respondent to construct a password consisting of any combination of up to eight alphanumeric characters. They were urged to memorize and safeguard this password as they would any other password. They were then asked how they devised this password. For example, did they use a meaningful detail such as a name, a date or a number? Did they use a combination of meaningful details? Did they use a random choice of characters or some other means?.

The second part of Form-1 contained a unique eight character password that was assigned to each respondent. Here the Form-1 questionnaires were split into two groups. Fifty-five of the Form-1 questionnaires had a system-generated random alphanumeric password. The other 48 questionnaires had a pronounceable system-generated password. To distinguish between the two versions of Form-1, the random alphanumeric form was designated Form-1R and the pronounceable password form was designated Form-1P. The respondents were urged to safeguard this password as well.

Also included in the second part of Form-1 was a segment requesting each respondent to create a passphrase consisting of any combination of up to 80 alphanumeric characters. There was no requirement as to the minimum number of characters or words in the passphrase. The respondents were again urged to memorize and safeguard this passphrase as they would any other password. Then they were asked how they devised this passphrase. Five choices were given:

1. Nonsensical phrase.
2. A quotation.
3. A piece of advice.
4. A common phrase.
5. Other means.

4.1.3. Cognitive passwords

Both Form-1 and Form-2 are identical in their third part. It consisted of 20 open questions which asked for items of information that were described as cognitive passwords. These items were classified into two categories of responses. The first group contained six items of personal facts assumed to be known only by the respondent or someone socially close to the respondent, e.g., elementary school attended, mother's maiden name or father's occupation. The second category consisted of 14 opinion-based items which ask the respondent to choose a favorite item, for example, favorite vacation place, favorite restaurant or favorite fruit. Once again, it was assumed that these responses would be known only by the respondent or someone socially close to him.

4.1.4. Associative passwords

The last part of the Form-1 requested the user to come up with a list of 20 word associations. In formulating these 20 cues and responses, the respondents were advised to centralize them around a common theme but this was not set as a mandatory requirement. There was no limitation or minimum number of alphanumeric characters in either the cues or responses.

4.1.5. Items for recall of passwords

The Form-2 questionnaire was designed to assess the ability of the respondents to recall those passwords used on Form-1. It was administered to the same group three months after the administration of Form-1.

Where Form-1 assigned passwords to the respondents (either random or pronounceable), asked each respondent to create a password, and also a passphrase, the later Form-2 asked them to recall those passwords. First, it asked each person to recall the password of his or her own making. It then asked them whether they recalled their password from memory or had resorted to writing it down. Secondly, the respondents were asked to recall the password that we assigned to them on Form-1. Next, they were asked to recall the passphrase they used in Form-1. They were also asked whether they recalled it from memory or had written it down.

4.1.6. Items for recall of cognitive passwords

The cognitive passwords section of the Form-2 version was identical to Form-1. The same respondents were asked the same questions again. In examining a system of passwords based upon cognitive information, the correlation between the Form-1 and Form-2 responses to cognitive items 3 months apart was of interest.

4.1.7. Items for recall of associative passwords

In the identical Form-2 version of the word association section, the same respondents were asked to regenerate their list of 20 cues and responses. As soon as the respondent had generated as many associations from memory as possible, they were given a list of their original 20 cues as a memory aid. They were then asked to write down as many of their responses as they remembered. If, at this point, they were still unable to remember their responses, they were given the central theme (taken from their corresponding Form-1 questionnaire), if any, to aid them in correctly remembering their responses.

4.1.8. Items concerning ranking of the various password methods

The last section of Form-2 requested the respondents to rank the various password methods—user-generated passwords, system-generated passwords, passphrases, cognitive passwords and associative passwords—by two distinct characteristics: ease of recall and how they liked them.

4.2. Sample and data collection design

The Form-1 questionnaire was administered to 103 graduate students, majoring in management information systems. The average age of the participants was 33 years, in a range of 25–42. Of them, 85% were male and 15% were female. They averaged 5 years of experience with computers. Twelve percent said they had no computer experience before starting graduate studies. Forty-eight percent reported that they used some combination of personal computer and mainframe, 32% said their computer experience was limited to personal computers, while 8% claimed to have only used a mainframe.

The Form-2 version of the questionnaire was administered to the same user respondents three months after the Form-1 administration. All of the original 103 Form-1 respondents participated in the Form-2 administration.

5. FINDINGS

5.1. Recall of self-generated passwords

Of the 103 respondents, 27.2% were able to recall correctly the password they had created themselves 3 months earlier. Among the respondents who recalled their password, 42.9% said they remembered it without aid, 7.1% said they wrote it down even though they were instructed not to and 17.9% said it was the only password they ever used so it was easy to remember. Finally, 32.1% gave 'other means' as the basis for recall.

The characteristics of the self-generated passwords were examined according to three attributes: selection method, format and length. Table 1 shows how the respondents constructed their self-generated password and their recall success. The majority of the respondents (67%) used some form of meaningful detail in creating their password.

Cramer's V statistical test was performed to test the null hypothesis that there is no difference in recall success between methods of choosing self-generated passwords. The results (Cramer's $V = 0.1683$; $P = 0.404$) suggest that the null hypothesis cannot be rejected at $P \leqslant 0.05$ level. Thus, the methods for selecting self-generated passwords had no statistically significant association with success in recalling the passwords.

The format of the self-generated passwords and recall success is depicted in Table 2. The respondents mainly

TABLE 2. Format of self-generated password and recall success

	Alphabetic only	Alphanumeric	ASCII	Total
Total selected	76	23	3	103
Failed recall	50	22	3	75
Succeeded recall	26	2	0	28

used alphabetics in creating their passwords. More interesting is the fact that 93% of the 28 respondents who recalled their password used alphabetics only.

The null hypothesis in this case suggested no difference in recall success between formats used in creating self-generated passwords. The Chi-squared test results ($\chi^2 = 7.324$; $P = 0.022$) allow us to reject this hypothesis at $P \leqslant 0.05$ level and accept the alternative hypothesis that the formats used in creating self-generated passwords had a statistically significant association with success in recalling the passwords.

The distribution of self-generated passwords according to their length and recall success is presented in Table 3. Since most operating systems support a password length of up to eight characters, there were eight spaces on the Form-1 questionnaire. Most of the respondents (54%) tended to use all the spaces when making up their passwords.

There was no statistically significant association between the number of characters in a self-generated password and a respondent's success in recalling it. The results of the statistical test (Cramer's $V = 0.228$; $P = 0.374$) could not reject the null hypothesis of no statistical difference between passwords of different character lengths at $P \leqslant 0.05$ level.

5.2. Recall of system-generated passwords

Table 4 reflects the ability of respondents to recall either the assigned random alphanumeric password or the pronounceable password. As expected, more respondents were able to recall a pronounceable, system-generated, password than a random character password. The Chi-squared test results ($\chi^2 = 7.898$; $P = 0.005$) provide evidence that this difference is statistically significant at $P \leqslant 0.01$ level.

The increased memorability of pronounceable passwords is further supported in Table 5. While 83% of

TABLE 1. Method of choosing self-generated passwords and recall success

	Meaningful detail	Combination of meaningful details	Randomly chosen characters	Other	Total
Total selected	46	23	1	33	103
Failed recall	34	19	1	21	75
Succeeded recall	12	4	0	12	28

TABLE 3. Number of characters in self-generated password

	3	4	5	6	7	8	Total
Total	1	8	10	17	11	56	103
Failed recall	1	4	8	10	8	44	75
Succeeded recall	0	4	2	7	3	12	28

TABLE 4. Pronounceability and recall success

	Not pronounceable	Pronounceable	Total
Total selected	54	49	103
Failed recall	47	31	78
Succeeded recall	7	18	25

TABLE 5. Method of recall of system-generated passwords

	Method of recall	Number recalled	Percentage
Pronounceable passwords	unaided memory	15	83
	written down	3	17
Random passwords	unaided memory	0	0
	written down	7	100

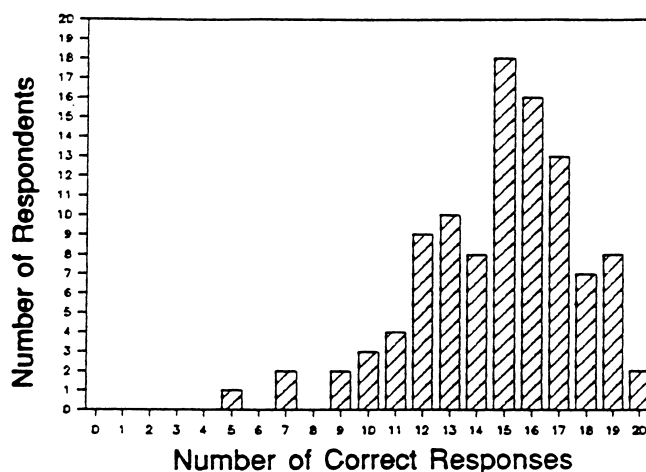**FIGURE 2.** Distribution of correct matches on cognitive passwords.

those remembering their pronounceable password claimed to recall it from unaided memory, no one was able to recall their random-character, system generated password from memory. Moreover, 67% of the respondents who recalled their pronounceable password stated that they remembered it precisely because it was pronounceable.

5.3. Recall of passphrases

Of the 103 respondents, only 21.4% were able to recall the passphrase which they had created 3 months earlier. As expected, a long string of characters, even though it formed an expression familiar to a respondent, made it difficult to remember. There was no marked difference between the general characteristics of the passphrases chosen and those that were recalled. The average length of all passphrases was 23 characters, compared to an average of 21 characters in recalled passwords. The average number of words in a passphrase was 5 while the number of words in recalled passwords averaged 4.4, compared with an average of 21 characters in recalled passwords. For those respondents who did remember their passphrase, 20 of 22 (91%) recalled it from unaided memory while only two (9%) had written it down.

5.4. Recall of cognitive passwords

These respondents, on average, recalled 14.8 out of their 20 cognitive items between Form-1 and Form-2; 68% recalled between 12 and 18 cognitive items. This average is somewhat lower than the 82% match reported in previous research by Zviran and Haga [21]. Figure 2 reflects this distribution. Of interest is the grouping of the respondents at the high end of the continuum. While

outliers at the low end of the continuum lowered the mean, 62.1% of the respondents had 15 or more correct responses.

Besides the overall match, respondents' performance for each individual question is of interest. As noted earlier, the cognitive questions were split into six fact-based questions and 14 opinion-based questions. The success of the respondents in recalling cognitive passwords over a three month period is expressed in the percentage of correct matches that were produced on Form-2. Table 6 shows that the recall for the fact-based questions was high, 83.7%. On average, these respondents recalled five out of their six fact-based cognitive items; 68% recalled between four and all six of the fact-based items. Even the lowest cognitive question had a recall rate of 74.8%, twice the recall rate for any of the previous password methods.

The success rate for the recall of the opinion-based questions is lower than for the fact-based questions. The average percentage of correct responses here was 70%. There was a fairly wide variance with the number of correct responses ranging from 49.5 to 87.4%. On average, these respondents recalled 9.8 out of their 14 opinion-based items; 68% recalled between seven and 12 of opinion-based items. Table 7 presents the recall results of the opinion-based cognitive questions.

TABLE 6. Respondents' recall on fact-based cognitive items

Fact-based item	Percent matched correctly
What is the name of the elementary school from which you graduated?	85
What is the name of your favorite uncle?	86
What is the name of your best friend in high school?	85
What is your mother's maiden name?	93
What was the first name of your first boyfriend/girlfriend?	75
What is the occupation of your father?	79

TABLE 7.   Respondents' recall on opinion-based cognitive items

Opionon-based item	Percent matched correctly
What was the name of your favorite class in high school?	78
What is the name of your favorite music performer or group?	80
What is your favorite type of music?	86
What is the name of your favorite vacation place?	66
If you could travel to any country in the world, which would it be?	71
What is the last name of your favorite actor or actress?	58
What is your favorite flower?	87
What is your favorite dessert?	66
What is your favorite vegetable?	75
What is your favorite fruit?	66
What is your favorite color?	75
If you could change occupations, which new occupation would you choose?	55
What is the name of your favorite restaurant?	50
What is the last name of your favorite college instructor?	67

The questions that had the lowest success rate dealt with an individual's favorite restaurant, actor or actress and choice of alternative profession. Two possible explanations for missing these questions are: (1) at the time of administration of Form-1, a respondent may have wavered between a couple of answers, failing to remember which one he or she had chosen three months earlier and selecting a different answer on Form-2 and (2) these questions call for answers that may have changed for the respondent since the administration of Form-1. Therefore, a respondent may have answered the question according to his opinion at the time of the administration of Form-2, as opposed to responding as he or she did when first answering the question.

The question of possible differences between recall success of fact-based items and opinion-based items is of particular interest since the initial results show that fact-based items had a better recall rate (83.7% on average) than opinion-based items (70%, on average). Table 8 depicts the comparative recall pattern of the two types of cognitive passwords. The null hypothesis claims for no difference in recall success between fact-based and opinion-based cognitive items. However, the results of the statistical analysis ($\chi^2 = 99.40$; $P = 0.000$) reject the null hypothesis at $P \leqslant 0.01$ level and suggest that the difference between the recall success rate of the fact-based cognitive items and the opinion-based items is statistically significant.

5.5. Recall of associative passwords

The overall average number of correct matches by the respondents on all the word associations between Form-1 and Form-2 was 13.8 out of 20 (69%). These respondents fell anywhere in the continuum from 0 to 20 correct responses as shown in Figure 3. Of note is that 60 respondents (58.3%) got 14 or more matches correct.

As expected, when first asked to recall both their cues and responses, the respondents on average were able to generate only 4.1 out of the 20 (20.5%). However, when presented with their list of cues they were able to recall responses albeit with some errors. Not one respondent requested to know their theme. Either they had no theme or the list of 20 cues brought it back to them remember their theme. While it was expected that few would need their theme to generate responses, it was surprising that not one respondent, including the one who got no responses correct, requested the theme to help figure out the answers.
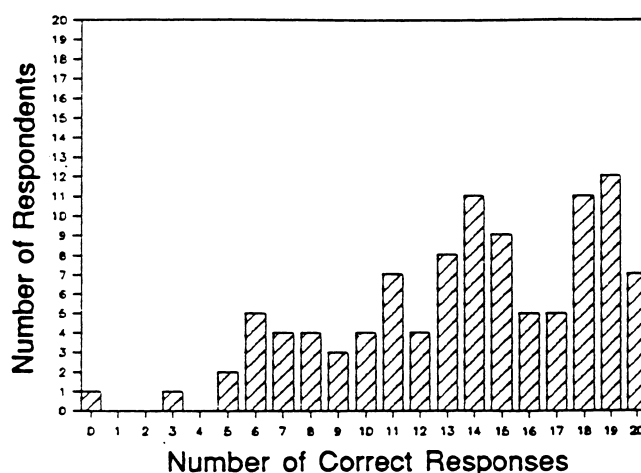
FIGURE 3.   Distribution of correct matches on associative passwords.

TABLE 8.   Comparative recall success of fact-based and opinion-based cognitive passwords

Number of fact-based items recalled	3	4	5	6	7	8	9	10	11	12	13	14	Row totals
2	1		1					1					3
3		1		1		1	2	2		1			8
4				3	2	3	1	3	3	1	2		18
5		1		1	3	4	2	7	5	4		3	30
6					3	3	7	10	7	7	5	2	44
Column totals:	1	2	1	5	8	11	12	23	15	13	7	5	103

5.6. Ranking of the various methods

As a last task, the respondents were asked to rank the various methods of user authentication. First, they were asked to rank the five methods based on their ease-of-recall. The password method perceived to be the easiest to remember was ranked '1' and the most difficult to remember passwords were ranked '5'. Next, respondents were then asked for their subjective ranking of the various methods according to how they liked them. Similarly, the password method perceived to be most liked was ranked '1' and the most unliked passwords were ranked '5'. Table 9 presents the users' ranking of passwords and the averages on these two characteristics.

Ranking by ease of recall, self-generated passwords were ranked first 50 times. Second was authentication by word association with 29 first place rankings. Third was cognitive passwords with 14 first place rankings. Passphrases were fourth with two first places. Finally, system-generated passwords (no distinction was made between random or pronounceable) were ranked last with no one choosing it as easiest to remember.

Ranking password mechanisms by liking, the order was the same, as reflected from Table 9. Self-generated passwords received 47 first place rankings, word association had 30, cognitive passwords had 16, passphrases had three and one person liked system-generated passwords the best.

Table 10 compares the rankings of respondents' opinions about ease of recall and liking of different types of passwords with their actual success at recalling the different types. The two subjective rankings are identical, yielding a perfect Spearman's rank order correlation

(1.00). However, neither of the subjective rankings agree with the objective measure of recall success. Spearman's rank order correlation of opinion rank (ease-of-recall as well as liking) with actual recall (Spearman's $\rho = 0.50$; $P = 0.20$) was not statistically significant at $P \leqslant 0.05$ level, suggesting no relationship between the actual ranking and the subjective ranking.

6. DISCUSSION

6.1. Recall of passwords and passphrases

Over a 3 month period, only 27.2% of the respondents could recall a password they had created themselves. Worse, only 12.7% of the respondents could remember their system-generated random alphanumeric password. However, 38% of the respondents who were assigned a pronounceable password were able to recall it, compared with 13% for a random passwords. Thus, pronounceable passwords, although unrelated to a user's life or a meaningful detail, seem to be more memorable to a user than a self-generated password. The statistical tests performed lend further support to these findings. As for random, alphanumeric, system-generated passwords, not one respondent was able to recall such a password from memory after a three-month period.

Of the survey respondents, 21.4% were able to recall their passphrases. Most of the respondents (77.7%) chose passphrases consisting of fewer than the minimum recommended 30 characters [16]. Nevertheless, they still had little success in recalling the passphrase.

6.2. Recall of cognitive passwords

Using sets of fact-based and opinion-based questions, the respondents recalled an average of 74% of their cognitive passwords after 3 months. Only two of these respondents were able to recall all 20. When the fact-based cognitive passwords were analyzed separately, the recall averaged over 83%. The recall performance on the opinion-based cognitive passwords was far lower than for the fact-based passwords, resulting a 74% recall on the average. The difference between these two types was also found to be statistically significant at $P \leqslant 0.01$ level.

A previous study [21] reported a better rate of recall for the same set of cognitive passwords. Nevertheless, the recall of the cognitive passwords in this study was noticeably better than for any of the previously described password alternatives. Overall, the finding support the notion that the ease of recall of cognitive passwords is superior to that of traditional passwords [21].

6.3. Recall of associative passwords

After 3 months, the respondents recalled, on average, 69% of their associative passwords. Seven of the respondents remembered all 20 responses and almost a third could recall 90% or more of their responses. While there was success at the high end of the spectrum, there

TABLE 9. Respondents' opinions about liking types of passwords and ease-of-recall

Type of password	Ease of recall rank		Liking rank	
	rank	average score	rank	average score
Self-generated	1	1.98	1	1.96
Associative	2	2.41	2	2.39
Cognitive	3	2.61	3	2.79
Passphrase	4	3.45	4	3.38
System-generated	5	4.46	5	4.54

TABLE 10. Correlation of opinion rank verses recall success of password mechanisms

Type of password	Ease of recall rank	Recall success score (%)	Actual recall success rank
Self generated	1	27.2	3
Associative	2	69.0	2
Cognitive	3	74.0	1
Passphrases	4	21.4	5
System-generated	5	24.0	4

was a fairly uniform distribution of respondents remembering from 30 to 90%. An explanation for this distribution is that the respondents were given free reign in making up their word associations. Unlike the cognitive password section, in which all the respondents answered the same set of questions, the word associations had various degrees of difficulty depending upon how challenging each respondent decided to make them.

Even with this wide variance, the average success rate was over twice as that of the traditional self-generated password method. In comparison with the overall success rate of cognitive passwords, the recall of associative passwords was somewhat less (69% compared with 74%). However, there were almost twice as many respondents (30 versus 17) scoring 90% or more correct responses on the word associations than on the cognitive passwords.

Smith's research [17] used a smaller sample size and showed that after 6 months the four respondents in his survey group could recall 94% of their word associations [17]. This is considerably higher than the 69% success rate after 3 months from the sample in this study. The difference in sizes of the two samples probably accounts for the difference in success rate. Smith concluded that authentication by word association seemed promising for finding a better method for user authentication. The results of this study support his conclusion.

6.4. Ranking of the various methods

When asked to rank the various methods as to how easy they were to remember, the respondents clearly chose self-generated passwords as the one that they thought was easiest. However, this method was one of the worst for recall by the respondents. Other than this, the rankings generally reflect how the respondents actually did in recalling their passwords from the different methods.

When the respondents ranked the methods by how they liked them, those that were user-oriented were ranked highest. Of interest are two facts: (1) there was no difference between the two subjective rankings and (2) no relationship was found between the subjective ranking of the various password mechanisms and the actual recall rate. This shows that the respondents may have interpreted that how they liked a certain method meant that it was easy to remember. It could also explain why the respondents chose self-generated passwords as easiest to remember when in reality they were not.

7. CONCLUSION

While primary passwords mechanisms, serving as a basic authentication mechanism in most operating systems, are determined by the operating systems' manufacturers, the selection of a password mechanism to be employed for secondary passwords is determined by the designers of the specific applications. The underlying question in

this selection process is which of the various password mechanisms is the most suitable for this purpose.

Several user authentication mechanisms were examined in this study, resulting two ratings. When user ability to recall the different types of passwords is examined, pronounceable passwords, cognitive password and associative password proved to be much better than passphrases, random system-generated passwords, or even user-selected passwords. The respondents subjective judging of the password mechanisms, both for ease-of-remembrance and how they liked it, ranked traditional passwords first, followed by the two handshaking mechanisms (cognitive and associative passwords) and then the others. A third rating focuses on ease of guessing or brute-forcing. Previous research [2–4, 13, 14, 21] suggests that this characteristic depends on the password length, the character set from which it was drawn and frequency of changing the password. Based on these characteristics, cognitive and associative passwords are ranked first, followed by passphrases, system generated passwords and traditional passwords being last.

When deciding on a particular password mechanism to be employed as for secondary passwords, two major considerations need to be taken in account: the desired security level of the application policy and user convenience of logging-in (ease-of-use). If an organization desires just to upgrade its traditional password system, without making radical changes, then eight-character pronounceable passwords, usually consisting of one word, are be used. These passwords, either user-selected or system-generated were proven easiest to remember. One pitfall they have is that users dislike system-generated passwords; so by allowing the users to choose them, this password method should be more desirable to the user. Pronounceable passwords also offer a high degree of security as they are a mix of alphanumeric characters that do not form an actual word or phrase [3, 13].

If an organization desires to extend its present user authentication method to make it the best possible, then authentication by cognitive or associative passwords should be selected. These two mechanisms have shown to be the easiest to remember of the various methods discussed here. Yet, previous research [17, 21] demonstrated their high level of security, difficulty of guessing and applicability. Moreover, users ranked them second and third as both easiest to remember and the one they liked.

Both authentication by word association and cognitive passwords provide better security than traditional password systems [17, 21]. They proved to be user-friendly and offer ease of memorability. Thus, these two mechanisms seem to be the most appropriate for implementation at a secondary authentication level. The implementation experience reported by Haga and Zviran [6] lends further support to the applicability of handshaking techniques for this purpose.

Two avenues for future research are proposed. First, a comparative evaluation is needed to further explore

the ease-of-use and the ease of-guessing of cognitive and associative passwords. Second, real-life experience with these mechanisms, providing additional evidence for their feasibility and applicability is also required.

ACKNOWLEDGEMENTS

REFERENCES

[1] N. Ahituv, Y. Lapid and S. Neumann, Verifying the authentication of an information system user. *Computers and Security*, **6**, pp. 152–157 (1987).

[2] S. Avarne, How to find out a password. *Data Processing & Communication Security*, **12**(2), pp. 16–17 (1988).

[3] B. F. Barton and M. S. Barton, User-friendly password methods for computer-mediated information systems. *Computers and Security*, **3**, pp. 186–195 (1988).

[4] *Department of Defense Password Management Guideline*. National Computer Security Center, CSC-STD-002-85, Washington, DC (1985).

[5] R. P. Fisher, *Information Systems Security*. Prentice-Hall, Englewood Cliffs, NJ (1984).

[6] W. J. Haga and M. Zviran, Cognitive passwords—from theory to practice. *Data Processing & Communications Security*, **13**(3), pp. 19–23 (1989).

[7] L. J. Hoffman, *Modern Methods for Computer Security and Privacy*. Prentice-Hall, Englewood Cliffs, NJ (1977).

[8] D. K. Hsiao, *Computer Security*. Academic Press, New York (1979).

[9] D. L. Jobusch and A. E. Oldhoeft, A survey of password mechanisms: weaknesses and potential improvements. Part 1. *Computers and Security*, **8**, pp. 587–601 (1989).

[10] D. L. Jobusch and A. E. Oldhoeft, A survey of password mechanisms: weaknesses and potential improvements. Part 2. *Computers and Security*, **8**, pp. 675–689 (1989).

[11] S. Kurzban, A dozen gross 'mythconceptions' about information processing. In: *Security, IFIP/sec '83*, V. Fak (ed.), pp. 15–25. North Holland, Amsterdam (1983).

[12] C. E. Landwehr, The best available technologies for computer security. *IEEE Computer*, **16**,(7) pp. 86–99 (1983).

[13] B. Menkus, Understanding the use of passwords. *Computers and Security*, **7**, pp. 132–136 (1988).

[14] R. Paans and I. S. Herschberg, Computer security: The long road ahead. *Computers and Security*, **6**, pp. 403–416 (1987).

[15] C. P. Pfleeger, *Security in Computing*. Prentice-Hall, Englewood Cliffs, NJ (1989).

[16] S. N. Porter, A password extension for human factors. *Computers and Security*, **1**, pp. 54–56 (1982).

[17] S. L. Smith, Authenticating users by word association. *Computers and Security*, **6**, pp. 464–470 (1987).

[18] J. C. Spender, Identifying computer users with authentication devices (tokens). *Computers and Security*, **6**, pp. 385–395.

[19] W. H. Ware, Information system security and privacy. *Communications of the ACM*, **27**, pp. 315–321 (1984).

[20] C. C. Wood, Effective information system security with password controls. *Computers and Security*, **2**, pp. 5–10 (1983).

[21] M. Zviran and W. J. Haga, Cognitive passwords: the key for easy access control. *Computers and Security*, **9**, pp. 723–736 (1990).

APPENDIX A: FORM-1 QUESTIONNAIRE

Part A: personal information

Please answer the following questions:

  Sex (Circle one): Male   Female
  Last 4 digits of the your SSN _____
  Number of years of computer usage:_____
  Type of computer(s) you have used prior to NPS (check any that apply):
    Microcomputer _____
    Microcomputer linked to a mainframe _____
    Mainframe terminal_____

Part B: passwords and passphrases

For the purpose of this survey anytime you are requested to memorize something **do not write it down**. This is for all parts of this survey—passwords, passphrases, cognitive passwords and word association.

1. Please create and write in the boxes below a password, up to eight alphanumeric characters. Please memorize and safeguard it as you normally do your passwords.

   As with other parts of this survey, you will later be asked to recall what you have been requested to memorize.

   |__|__|__|__|__|__|__|__|

2. How did you choose the password above? (Circle one)

   A. A meaningful detail (name, date, number, etc.)
   B. A combination of meaningful details (JIM1989, etc.)
   C. A randomly chosen combination of characters
   D. Other (please specify)
   _____

3. The following password has been assigned to you for this study. Please memorize and safeguard it as you would any other password. This password is pronounceable, which may help you remember it. For instance, UN4TUNE8 would be unfortunate.

   |__|__|__|__|__|__|__|__|

4. A passphrase is a string of up to 80 alphanumeric characters. Theoretically, it is more secure than a normal password since it is unlikely that someone will guess it. The passphrase can be silly like "Susie sells seashells by the seashore," or it can be a quotation or a common phrase. Please construct a passphrase of your choice in the space below. Please memorize it and safeguard it as you would any other password.

   _____

5. How did you choose your passphrase above? (Circle one)

   A. Nonsensical phrase that I can remember

B. A quotation
C. A piece of advice
D. A common phrase
E. Other (please specify)_____

Part C: cognitive passwords

Cognitive passwords suggest that use of fact, interest and opinion-based cognitive data, that are known only to the user as an authentication mechanism. Please answer the following questions using a maximum of 20 characters.

1. What is the name of the elementary school from which you graduated? _____
2. What is the first name of your favorite uncle? _____
3. What is the first name of your best friend in high school? _____
4. What is your mother's maiden name? _____
5. What was the name of your first boyfriend/girlfriend? _____
6. What was the name of your favorite class in high school? _____
7. What is the name of your favorite music performer or group? _____
8. What is your favorite type of music? _____
9. What is the name of your favorite vacation place? _____
10. If you could travel to any country in the world, which would it be? _____
11. What is the last name of your favorite actor or actress? _____
12. What is your favorite flower? _____
13. What is your favorite dessert? _____
14. What is your favorite vegetable? _____
15. What is your favorite fruit? _____
16. What is your favorite color? _____
17. If you could change occupations, which new occupation would you choose? _____
18. What is the name of your favorite restaurant? _____
19. What is the occupation of your father? _____
20. What is last name of your favorite college instructor? _____

Part D: word association

Another form of access control is a challenge-and-response query after a user has logged on. When the user correctly responds to the queries, the system ensures that it is the authorized user who has logged on. One such method is a series of word associations. Each user creates 20 word associations peculiar to him. For instance a user could decide to set up a table composed of queries that remind him of musical artists. The partial table is listed:

QUERY	RESPONSE
Virgin	Madonna
Deaf	Beethoven
Eliminator	ZZTop
Glasses	Elton_John
Lips	Mick_Jagger

So, after initial logon, the system would query: Glasses? The authentic user would then respond: Elton_John

1. Now construct a set of word associations for yourself. Please list 20 associations. While it is helpful for memory purposes to use one theme throughout it is not mandatory. Here are some other suggestions for possible themes: comic strips, authors, TV shows, movies, family members.

QUERY	RESPONSE
1. _____	_____
2. _____	_____
3. _____	_____
4. _____	_____
5. _____	_____
6. _____	_____
7. _____	_____
8. _____	_____
9. _____	_____
10. _____	_____
11. _____	_____
12. _____	_____
13. _____	_____
14. _____	_____
15. _____	_____
16. _____	_____
17. _____	_____
18. _____	_____
19. _____	_____
20. _____	_____

Theme (if any) _____

Thank you for your cooperation!