User-Friendly Password Methods for Computer-Mediated Information Systems

Ben F. Barton
Department of Electrical and Computer Engineering, University of Michigan, Ann Arbor, MI 48109, USA

and

Marthalee S. Barton
College of Engineering, University of Michigan, Ann Arbor, MI 48109, USA

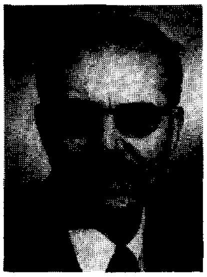
Violations of published strictures on password use have led to widespread unauthorized access to computer systems. The problem may compound as inexpert users, handicapped by inadequate guidance and ignorance of computers, are increasingly involved on networked, supposedly "user-friendly" workstations. The literature on password methods reflects a technocentric focus emphasizing security without due regard for user comfort, i.e., a "user-hostile", system perspective. We present a "user-friendly" model for the password selection and re-creation processes rooted in cognitive psychology. The model suggests two approaches to password selection – one rooted in a nomothetic, or particularized, the other in an idiographic, or generalized, treatment of experience – that exploit principles of recall, memory aids and simple formal transformations. A third approach, exploiting environmental cues – hence recognition rather than recall – is also considered. Intermediate approaches enable tradeoffs between password security and memorability appropriate to the context and cognitive style of the user. The reduction of the approaches to practice is illustrated in numerous examples. The approaches yield passwords more vulnerable to discovery than those envisioned in system-oriented theory, yet operationally superior to many prompted by strictures reflecting a technocentric system perspective. We recommend that guidance materials on password use be made available on systems.

Keywords: Keywords: passwords, user authentication, user-friendly, cognitive psychology, human-memory model

North-Holland
Computers & Security 3 (1984) 186–195

1. Introduction

Two recent phenomena suggest the value of a new look at password methods of controlling access to computer systems. First, the widely publicized escapades of the Milwaukee-based "414's" and others dramatize the ease of unauthorized access to many computer systems based on password compromises. For example, testifying recently before a House subcommittee, seventeen-year-old Neal Patrick claimed that he simply "kept trying passwords until one worked" [1]. Password compromises have resulted from information on computer bulletin boards, from guesses based on personal vitae and environmental cues, and from systematic trials. Incredibly, many intruders – including Neal Patrick – have simply exploited knowl-



Ben F. Barton is a Professor of Electrical and Computer Engineering at the University of Michigan. He has extensive industrial experience and has consulted with numerous private organizations and governmental units. He was formerly Director of the Cooley Electronics Laboratory at the University, where he was involved in research programs dedicated to electronic countermeasures and communications. His teaching areas range from electronic circuits and communications to computer applications. He has published widely on such topics as electronic circuits, technical communication, and computers. He has co-authored numerous publications with the joint author of the article.

Marthalee Barton is a Lecturer in Humanities in the College of Engineering of the University of Michigan. She earned a Ph.D. in comparative literature from that university, and has taught there in such diverse fields as English, literary theory and technical communication. She also teaches a course in communications, technology and public policy focussing on the role of computers in society. Her background includes extensive experience as a technical editor and consultant. She was an associate editor of *Alternative Futures*, and has published articles on the cooperative teaching of engineering project courses, the distinctions between academic and professional problems in engineering, the case method, communication models for computer-mediated information systems, and computer-mediated cases.

edge of obvious passwords (e.g., "test" and "system") in common use among field personnel of computer manufacturers. Thus, even some computer professionals have used deficient passwords.

We may well be apprehensive, then, over a second recent phenomenon, the dramatic increase in the number of novices using computers, for novices may be especially prone to use deficient passwords due to their limited understanding of computers. Their use of computers has been fostered through the development of so-called "user-friendly" workstations – workstations now being "networked", or interconnected, along with central equipment to facilitate information-sharing and communication. Still, considerations of personal privacy, proprietary interests and administrative confidentiality dictate control of information access – we thus exclude direct consideration here of measures addressing national security – and the problems of controlling access are compounding, as systems become increasingly distributed and as inexpert users are involved in ever greater numbers.

The nature of these problems is exposed by examining the literature on password methods of controlling access, and its relation to practice. Most current methods of controlling system access involve user selection of passwords; yet the literature provides the computer novice – or the expert, for that matter – with few guides for password selection [2]. Rather, contributions have often featured lists of *ad hoc* "dos" and "don'ts" focussing on security [3]. The lists of "dos" generally recommend passwords that are long, composed of random characters, and frequently changed. The "don't" lists usually reject the use of names, initials, dates and numbers prominent in the user's life, in particular, and of words, in general. They often forbid the use of reverse transcriptions of these items as well as environmental cues. They also counsel against keeping records of passwords in card decks, computer files or work areas as well as on one's person. In practice, however, these strictures are largely ignored: Parker observes, for example, that most users select as passwords names, initials, dates or numbers prominent in their lives, or their reverse transcriptions [4]. Moreover, much of the formal theory in password literature fails to accord with common practice. In particular, combinatorial analyses pertaining to random character strings, though a popular topic, have little relevance to most current passwords as characterized above.

That users generally ignore published strictures on password selection is hardly surprising, since they cannot be reconciled with the "user-friendly" basis of system operation now widely sought. The traditional emphasis on system security at the expense of password memorability reflects a technocentric, "user-hostile" perspective. Thus, the literature gives short shrift to the user's problems of selecting passwords that can be reliably recalled and of coping with serious information overload – problems compounded with suggested password methods. For example, it fails to recognize that the use of *transistory* passwords without transcription represents a departure from common experience, for people routinely use cards to store even relatively *permanent* personal information of comparable complexity and sensitivity, including social-security, driver's license, credit-account and bank-account numbers [5].

The disparity between published wisdom and practice indicates a broad need for suggestions on methods of selecting relatively secure passwords that are acceptable to users. A spectrum of unresolved user problems should be confronted. Critical questions include: Are there effective general methods of password use "friendly" to novice users? [6] Can such methods provide for reinforcing memory of selected passwords, for combatting interference from mental "clutter" such as discarded passwords? In this article, we consider how password methods can be made more consistent with the over-arching goal of "user-friendliness" for systems. First, we develop a "user-friendly" model for the password selection and recreation processes. Subsequently, we discuss password methods especially adapted to the needs of inexpert users. In particular, we recommend some simple methods of selecting passwords that are easily recalled but not easily discovered. We then consider how systems can ease the user's plight.

2. A Model for the Password-Selection Process

Password methods of controlling system access would be facilitated by a "user-friendly" process of password selection, that is, a process yielding passwords visible to the user, yet invisible to others.

In effect, then, memorability and security of passwords should *both* be made critical issues. Further, a model of the process should accommodate the need for a typical user to select a *sequence* of passwords. Such a requirement is likely for several reasons. First, users should anticipate sudden password changes warranted by possible compromise, as when keyboard scrutiny may have occurred during password entry. Second, routine changes of password are desirable to end any undetected intrusions. Third, a user may need, or elect, to have several accounts with different passwords, particularly since partitioning of information among several accounts with different passwords can limit the implications of a password compromise.

A model of the selection process for passwords clearly ought to accommodate also to the process for their re-creation. In the absence of direct environmental cues, a case considered subsequently, re-creation of a previously selected password involves recall, or appeal to long-term memory (LTM). The representation of LTM in terms of so-called "semantic" and "episodic" memories – a distinction more or less accepted by cognitive psychologists – has great utility for a model of the password re-creation process [7]. Semantic memory is deemed to hold information closely tied to language use, including models, whereas episodic memory is thought to store information more directly descriptive of individual experience. Semantic memory provides rapid access to information stripped of contextual details, while episodic memory provides slower access to information on contextualizing details, e.g., on temporal and spatial relations among events. Semantic memory is, then, largely a repository of widely shared information, whereas episodic memory is a store of information that is largely unshared, being so closely tied to personal experience. Thus, in relation to passwords, recourse to semantic memory implies use of information framed in a broad social context that favors recall, but also apprehension by others. On the other hand, recourse to episodic memory implies use of information framed in a limited personal context that *may* suffice to ensure recall but *does* limit risk of apprehension by most others. To enhance password security, the appeal should be made as nearly as possible to episodic memory. However, the issues of recallability and the user's preferred cognitive style will dictate compromises of varying degree [8].

The use of environmental cues to foster password re-creation is itself "user-friendly", since humans find recognition easier than recall; indeed, such cues can reduce the degree of dependence on information in LTM [9]. In fact, such cues are so "user-friendly" – especially for users with recall problems, or in controlled areas – that they cannot be lightly dismissed. However, since the user clearly risks that information drawn from the environment will be apprehended by a prospective intruder more or less aware of the same environment, environmental cueing of passwords is viable only if done discreetly.

Whatever the source of information, a model for the password-selection process should also accommodate "user-friendly" methods for meeting security requirements. For this purpose, users need congenial ways of transforming information to produce passwords distanced enough in form from ordinary experience to make discovery unlikely. Congeniality implies that the transformation process is easy both to remember and to execute. Happily, semantic memory functions as a rich storehouse of formal, model-related transforms employed continuously in mediating experience. Such transforms, and their use, are subjects of subsequent sections of this presentation.

Last, a model of the password-selection process should also account for the user's physical context. For users in public areas, even keyboard characteristics must be considered: For example, the use of characters requiring an unusual reach for entry, e.g., the numerals, risks their apprehension through visual monitoring. At the other extreme, the exclusive use of characters demanding little reach, e.g., the "home" keys, risks apprehension of different, also potentially useful, information. Similarly, the number of password characters may well be discerned through monitoring of audible "clicks" – clicks that, ironically, are often made to accompany actuations on noiseless keyboards as a service to the user [10]. The use of relatively long passwords – say, of six to twelve characters – reduces the risk that such specific information will lead to password compromise [11]. For users in private quarters, e.g, home-based telecommuters, direct dependence on environmental cues may be appropriate.

3. User-Friendly Approaches to Password Selection

The cognitive model for password use just described suggests three general "user-friendly" approaches to password selection. The first approach trades initially on information stored largely in semantic memory, the second on information stored in episodic memory, and the third on information prompted by the environment. In each approach, the initial information is then transformed to produce passwords distanced enough in form from ordinary experience to resist discovery.

Adopting the first approach, the user initially appeals to *semantic* memory by choosing a well-known set of character strings as a basis for producing a sequence of passwords. Two general principles can profitably guide the choices. First, the user should choose character strings – provisionally, as developed later – that are widely shared, in the interest of recallability [12]. The strings, however, should not strongly reflect the user's public life: That is, they should not strongly reflect such user characteristics as age, sex, ethnicity, geographical origin, social class, occupational role, group membership or personal attitudes [13]. Second, the user should have demonstrated a strong capacity, even a predilection, to recall the character strings and may well elect to heighten their recallability using methods suggested later. The number of suitable strings available is far greater than might first appear. Each of us involuntarily retains, for example, a vast store of marginally functional trivia that persist in semantic memory but that are not likely to be closely associated with us by others. Possible choices include: aphorisms; titles, lines, or names from movie or television scripts; titles or segments of lyrics, poems and other literature; tunes; quotations; childhood verses; advertising jingles; recipes; names, numbers or expressions related to historical and current events; descriptors related to recreational activities, furnishings, apparel, etc.

Table 1
Illustrative sequence of passwords associated with the lines of a chosen childhood verse.

Verse Line	Password
1. One for the money	14MUNNY
2. Two for the show	24SHOW
3. Three to get ready	32REDDY
4. Four to go (to)	42GOTO

The second step of the suggested approach involves processing of the chosen character strings, using information also stored largely in semantic memory, to produce passwords distanced in form from ordinary experience. One such approach exploits memory-based models to transform the strings at some level, e.g., character, phoneme, syllable, word, phrase, clause, or sentence. Several principles can profitably guide the choice of a transform procedure. First, the procedure should be congenial for the user, i.e., easy both to remember and to execute. Second, it should yield passwords with structural details facilitating re-creation, hence error discovery and control of inter-password interference. Third, it should yield passwords that resist discovery based on informed guesses or systematic trials. Consider the following two examples of the proposed approach.

Example 1. Table 1 summarizes steps in producing a set of passwords closely related to a childhood verse. The verse selected is easily recalled, yet distanced from a given professional – and perhaps known personal – situation. The use of numeric representations of the first word, and of homo-

Table 2
Summary of relations among chosen names of cities, intermediate expressions and selected passwords.

City	Intermediate Expression	Password
1. Paris	I Love Paris in the Springtime	ILPITST
2. Rome	Three (Bright) Coins in the (Trevi) Fountain	TBCITTF
3. New York	The Sidewalks of New York (City)	TSWONYC
4. San Francisco	I Left My Heart In San Francisco	ILMHISF

phones of the second word, in each verse line leads to passwords combining numeric and alphabetic characters in a shared pattern, as a memory aid. Dropping dispensable words in the first three lines helps produce passwords of convenient length. Transliterations of the last word of two verse lines are used in passwords, and the last password has been extended rather arbitrarily using a congenial alliteration. The patterns of the passwords, especially their sequential initial numerics, may help avoid confusion during, say, their concurrent use on different accounts. The strong underlying relation among the passwords may warrant reserving them for non-critical uses.

Example 2. Table 2 illustrates steps in the production of passwords tied to a list of "favorite cities" easily recalled by its author, who is concerned that his use of the list information might be anticipated, e.g., based on his resume. He therefore masks his use of the list by first choosing congenial expressions closely associated by him with list elements. In this process, he interpolates the words in parentheses in popular song titles; as a result, passwords formed from the initial characters of words – including both components of compound words – each contain seven characters. This pre-planned structural detail serves as a convenient check at password re-creation. The results are ill-suited to pronunciation as "words", hence to acoustic coding at that level. Nevertheless, the passwords are easily re-created by their inventor and reasonably "safe" from discovery. (Two password options, the choice of case for letters and the use of non-alphanumeric characters, are neglected in our initial examples but considered subsequently.)

Both examples illustrate a judicious initial appeal to shared information that is demonstrably recallable in full and immutable detail. In a second step, formal transformations lead to passwords distanced enough in form from ordinary experience to achieve reasonable security. The transformations chosen are easy both to remember and to execute, i.e., the passwords are easily re-created from the expressions; if the sets of passwords are considered in isolation, however, only those of Example 1 exhibit *intrinsic* properties fostering their re-creation.

Adopting a second approach, the user initially chooses a set of character strings through an appeal to *episodic* memory. Thus, he chooses a set of character strings reflecting an idiographic view of experience, i.e., he appeals to private, personal experience. Representative topics of such strings include notable but private episodes in the remote past, personal fantasies, voting patterns, intimate personal habits, details of private living quarters, and unspoken opinions or impressions. The method is illustrated in Example 3:

Example 3. Table 3 relates passwords to a list of foods once distasteful to the user, in the aftermath of childhood overindulgences. The expressions are placed in chronological order of events to facilitate list reconstruction. Each password designedly incorporates the three initial letters of three key words, including both components of "eggplant" (but not of "peanuts", "pineapple" and "coconut"), hence contains nine characters. To foster recall, the user may exploit both the vivid images associated with these passwords and their relative "pronounceability". To heighten security, the passwords of Table 3 may serve as intermediate expressions that are themselves transformed, e.g., using methods described later.

The information imputed here to episodic memory differs greatly from that in semantic memory (and in our earlier examples): The former is ordinarily personal and private, the latter widely shared, even public. Of course, most information is shared in degree, and our examples only approach the two extremes.

In a third approach, password selection can be based on a judicious appeal to environmental cues; for this purpose, adjectival, adverbial and similar

Table 3
Relations among foods disliked during childhood and selected passwords.

Expression	Password
chocolate-covered peanuts	CHOCOVPEA
Pepsi-cola (and) pretzels	PEPCOLPRE
pineapple-coconut suckers	PINCOCSUC
fried (-) eggplant	FRIEGGPLA

expressions are generally preferable, from a security standpoint, to substantive expressions. Assume, for example, that a user in a public area is concerned about exposing password characters that require unusual reaches for keyboard entry. That user might base passwords on the expressions "reachable", "accessible", and "attainable", adjectives that both characterize and satisfy the requirement [14]. Similarly, a user who keeps her child's photograph in an open workstation area might choose the adverbial expressions "lovingly", "happily" and "playfully" rather than the obvious, i.e., the child's name. The keyboard and photograph serve as effective cues in the respective examples. Still, the adjectival and adverbial expressions are themselves somewhat removed from objective experience, and suitable passwords can be generated from them using transform techniques suggested earlier and developed further below.

4. Transform Techniques

All of the suggested approaches require transforms to generate passwords distanced from chosen expressions. A multitude of transforms are available; however, among inexpert computer users dealing with untranscribed information, not many transforms will generally be deemed easy both to remember and to execute. For example, lacking a transcription, some users cannot easily excerpt every third, or every fifth, character from an ex-

Table 4
Illustrative transforms yielding passwords from chosen expressions, with examples.

	Transform	Illustrative Expression	Resultant Password
1.	transliteration	photographic schizophrenic	FOTOGRAFIK SKITSOFRENIK
2.	interweaving of characters in successive words (or numbers)	duke,iron tent pole	DIURKOEN TEPONTLE
3.	translation	strangers	ETRANIERI
4.	replacement of letter by decimal digit (modulo-10 index of letter in natural order)	cabbage	3122175
5.	replacement of decimal number by letter (with corresponding position, in natural orders)	10/12/1492	JABADIB
6.	shift from "home" position on keyboard	zucchini	XIVVJOMO
7.	actuation of keyboard "shift"	6/6/1944	Λ? Λ? !($$
8.	substitution of synonyms	coffee break	JAVAREST
9.	substitution of antonyms	stoplight	STARTDARK
10.	substitution of abbreviations	relative humidity	RELHUM
11.	use of acronyms	Mothers Against Drunk Drivers, Nat'l. Orgn. of Women	MADDNOW
12.	repetition	pan	PANPAN
13.	imagistic manipulation (180° rotation of letters)	swimshow	SMIWSHOM

pression to form a password. On the other hand, most users can readily form a password by excerpting initial characters of words or numbers from familiar textual material, in the manner of Example 2. To form passwords of creditable length distanced from *short* expressions, a few transformations on a character-by-character basis will prove congenial to most users. For one such transformations, the decimal and alphabetic characters are each construed as forming a ring, that is, as occurring in their natural orders with the added provisos that "0" follows "9" and "A" follows "Z". An alphanumeric expression can then be transformed by replacing each character with an adjacent character in its ring. Thus, the password "UPNBUPFT" results from substitution of succeeding characters for those in the "tomatoes" item of, say, a list of favorite vegetables. Similarly, the password "3SNLZSNDR" results from substitution of *preceding* characters for those in, say, the "4 tomatoes" item from a favorite recipe. Additional sample transforms congenial for many users are summarized in Table 4. For heightened security, transforms can be applied *in sequence*; the number of convenient transforms available suffices to make the approach sound.

Earlier, we deferred discussions of both the choice of case for password letters and the use of characters other than alphanumerics. Despite the implications for password security, we suggest that user comfort govern in these matters. In particular, the pattern of case variation among password letters should be convenient and easily recalled. Similarly, we suggest a measured use of "printing" characters other than alphanumerics, when convenient and as allowed by the system. For example, in forming passwords from expressions, punctuation should be carried over when congenial. (In this spirit, the hyphens in the expressions of Table 3 might be carried over to the passwords.) Again, we commend the natural use of special characters such as percent and pound signs. Generally, the use of non-printing characters seems undesirable, even if allowed by the system, on the basis of potential difficulties with mental imagery.

5. Mnemonics and Other Multiple-Encoding Techniques

During the password-selection process, users should be aware that information available for password re-creation can be enhanced, in both scope and recallability, through conscious preparation. Specifically, recall of relevant information can be expanded and heightened through recourse to mnemonic aids and other multiple-encoding techniques [15]. In particular, one advantage in forming passwords from selected characters of congenial expressions is that the expressions themselves then serve as mnemonic aids. Moreover, *direct* recall of passwords can be fostered through judicious choices. Clearly, the choice of passwords comprised of words, or their transliterations – as in Transforms 1, 3, 8, 9 and 12 of Table 4 – facilitates their direct acoustical encoding. Such encoding involves rehearsal – a method recommended in literature on memory – that is, the occasional repetitive articulation of passwords either at sub-audible levels, or at audible levels in seclusion [16]. To achieve "pronounceability" of paswords formed through patterned selection or replacement of characters in expressions – as illustrated in Transforms 2 and 5 of Table 4 – care is required in the choices of both expression and transform procedure. That is, trial passwords formed through patterned selection or replacement of characters in expressions are not generally "pronounceable" [17]. (See Table 2.) However, prospects increase if latitude is allowed in the selection or replacement pattern, e.g., if characters may be treated in pairs as well as singly. (Compare the two examples for Transform 2, Table 4.)

Recall can also be fostered through deliberate structural analysis of passwords [18]. Thus, the user may advantageously note such properties as password length and patterns in the occurrence of numeric characters, or of vowels and consonants among alphabetic characters. Recall of these structural properties can facilitate discovery of errors in trial password re-creations. In particular, comparative analysis of passwords in concurrent use can lead to encoding of information useful in combatting interference effects during re-creation attempts. Recall can often be fostered, too, through supplemental imagistic encoding of information relevant to password re-creation, e.g., through associating the vision of a heroic goal-line stand in football with the expression "iron duke" in the example of Transformation 2, Table 4 [19]. For further imagistic encoding, in this example, a cast-iron ducal bust is imagined to sit atop the workstation.

Mnemonic aids are especially important for users who work with *prescribed* character strings. Included here are passwords provided by coworkers for joint accounts and system-generated strings, e.g., account identifiers or "random" passwords for systems requiring extraordinary security. In these circumstances, users can employ the "initial letter" technique – a proven mnemonic method for recalling lists [20]. Thus, associating congenial expressions with the prescribed strings, the user might devise the sentence "We four often go to the cinema Fridays" to help recall the prescribed password "w4Og2TCF." Users may seek either an expression that is rooted in commonplace reality, or one that is designedly "bizarre," e.g, "*w*atch *four* *O*rangutans *g*rabbing *two* *T*iny *C*at*F*ish." That is, since published opinion that bizarre expressions are more easily recalled is not generally confirmed by experiments, and since the mental casts of humans may differ in this respect, users are perhaps best advised to cater to personal preference [21]. Alternatively, a narrative can be contrived with elements linked to successive characters of the password, e.g., "*w*alk *four* blocks from the *O*ffice, then *go two* blocks toward *T*own for *C*lothes and *F*ood" [22].

6. System-based Support for Password Methods

To this point, we have focussed on the development of materials on "user-friendly" password methods. But the *development* of such materials does not suffice; equally important is the "user-friendly" *distribution* of the materials. Specifically, guidance should be available on the system, rather than avoided or relegated to voluminous user documentation [23]. Its availability should be noted at initial sign-on; moreover, it should be offered each time a change of password is initiated. Access to materials addressing issues of both memorability and security should be facilitated through menu offerings. For example, descriptions and illustrations of methods for generating memorable passwords should be offered to all users. Certainly, information on mnemonic aids should be offered users who must cope with prescribed passwords. Clearly, the system should also provide critical technical information, e.g., the character set, and range in number of characters, permitted for passwords, and describe procedures for recovery in case a password is forgotten [24]. Users should be apprised automatically of the need to change passwords both routinely at appropriate intervals and exceptionally in the face of apparent intrusion attempts. System imposition of standards for passwords must also be considered: For example, the rejection of passwords less than three characters long should probably be the norm, rather than the exception. Enforced changes of passwords, and more general system assessment of the suitability of proposed passwords, e.g., rejection of dictionary entries, may be appropriate either now or in the future.

7. Conclusion

Experience suggests that many computer users are violating published strictures on password methods. Moreover, there is no reason to believe the multitude of computer novices now going on "user-friendly" workstations will accommodate to strictures reflecting, as they do, a technocentric focus, a lack of due regard for the user's situation. We have chosen, rather, an approach based on a model broadly representative of cognitive processes involved in password selection and subsequent re-creation. We are thus led to propose two approaches to password selection rooted in cognitive psychology. These approaches exploit principles of recall, reflecting particularized and generalized treatments of user experience, in conjunction with memory aids and simple formal transforms to produce memorable passwords distanced in form from ordinary experience. A third approach, based on the judicious use of environmental cues and transforms, may serve users with recall problems, especially in favorable environments. Intermediate approaches enable tradeoffs between password security and memorability appropriate to the context and cognitive style of the user. Admittedly, the approaches will lead to the use of passwords that are typically more vulnerable to discovery than those envisioned in system-oriented theory. However, such passwords are operationally superior to many chosen in the face of strictures reflecting a system perspective. In effect, we recommend an approach that accommodates, hopefully even appeals, to the human creative impulse. Still, the viability of password methods hinges on providing the user timely, system-based, "user-friendly" guidance, that is, guidance addressing memorability as well as security.

References

[1] Testimony before the Subcommittee on Transportation, Aviation and Materials of the Committee on Science and Technology of the U.S. House of Representatives on Sept. 26, 1983.

[2] The current emphasis on *user* selection of passwords seems sound, in light of recent psychological studies confirming that self-generated information is better recalled than information supplied by others. See, for example: N. Slamecka and P. Graf, "The Generation Effect: Delineation of a Phenomenon", Journal of Experimental Psychology: Human Learning and Memory, vol. 4, no. 6 (Nov. 1978), pp. 592–604; C. McFarland, T. Frey and D. Rhodes, "Retrieval of Internally versus Externally Generated Words in Episodic Memory", Journal of Verbal Learning and Verbal Behavior, vol. 19, no. 2 (Apr. 1980), pp. 210–25. For confirming results in the case of command names for computer languages, see D. Scapin, "Computer Commands Labelled by Users Versus Imposed Commands and the Effect of Structuring Rules on Recall", Proceedings of the Conference on Human Factors in Computer Systems, Mar. 1982 (Gaithersburg, MD), pp. 17–19.

[3] D. Parker, Fighting Computer Crime (New York: Charles Scribner's Sons, 1983), pp. 60–62; H. Wood, The Use of Passwords for Controlling Access to Computer Resources, National Bureau of Standards Special Publication No. 500-9, May 1977, pp. 1–31; L. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1977), pp. 6–21; C. Wood, "Effective Information System Security with Password Controls", Computers and Security, vol. 2, no. 1 (Jan. 1983), pp. 5–10.

[4] Fighting Computer Crime, p. 60. His findings are supported by unpublished results of a recent study by us. Moreover, we have found that even seemingly innocuous requests for lists of passwords from years past can traumatize administrators of computer systems. Some deem most passwords in use so transparent, so seldom changed, that publication of general descriptions of list properties would risk systemwide chaos. In private conversations, numerous experts – including system-level programmers – have admitted not changing their passwords in years. Moreover, many experts show embarrassment, during a general discussion of password security, if the security of their own password becomes even a tangential issue.

[5] The carrying of recorded passwords has been sanctioned by proponents of "one-time" password schemes, e.g., under conditions described by J. Anderson, "Information Security in a Multi-user Computer Environment," Advances in Computers (New York: Academic Press, Inc., 1972), vol. 12, pp. 1–36. However, we dissent out of fear that loss or theft of passwords may even lead to prolonged intrusion, since intermittent system use is typical among novices. For other disadvantages of one-time passwords, see Modern Methods for Computer Security and Privacy, pp. 12–13.

[6] Though several alternatives to conventional password methods are either presently in use or technically feasible, the password method of controlling computer access will apparently remain in wide use for some time. Identification cards and other physical keys suffer, as computer-access controls, from risk of damage, loss, duplication, loan or theft. "Call-back" procedures are now used to restrict computer access from remote sites to specific telephone lines; however, it is often infeasible to restrict physical access to authorized users, at either central or remote sites. Facilities for controlling computer access based on either fingerprinting, or "voiceprinting", of users are well within the state of the art. However, beyond substantial economic hurdles, psychological and moral barriers to the use of such facilities may not soon be overcome. As a general method of controlling computer access, signature or retinal analysis remains in the research phase.

[7] W. Estes, "Learning, Memory, and Intelligence," Handbook of Human Intelligence, ed. R. Sternberg (Cambridge: Cambridge University Press, 1982), pp. 191–224.

[8] In one popular taxonomy, cognitive style reflects the relative importance of right- and left-hemisphere cerebral activities. The right cerebral hemisphere supports intuitive, associative, synthetic thought, whereas the left cerebral hemisphere supports rational, sequential, analytical cerebration. Episodic and semantic memories are presumably manifestations of mental activities associated with right and left cerebral hemispheres, respectively. See R. Sperry, "Cerebral Organization and Behavior," Science, vol. 133, no. 3466 (Jun. 2, 1961), pp. 1749–57.

[9] H. Bahrick, P. Bahrick and R. Wittlinger, "Fifty Years of Memory for Names: A Cross-sectional Approach", Journal of Experimental Psychology: General, vol. 104, no. 1 (Mar. 1975), pp. 54–75.

[10] The suppression, during password entry, of audible "clicks" generated solely for the comfort of the user is both technically feasible and worthy of consideration by system designers.

[11] S. Porter, in "A Password Extension for Improved Human Factors", Computers and Security, vol. 1, no. 1 (Jan. 1982), pp. 54–56, proposes the use of "passphrases" 30 to 80 characters long, the illustrations given qualifying as "bizarre." Upon provision by the user, the passphrase is immediately "hashed," producing a residual 64-bit string that stores in nominal space. At subsequent sign-ons, the input is processed identically and its residual is compared with the stored residual as a basis for authentication. In its provision for nominal storage requirements, even with long passphrases, this procedure is system-friendly. However, it seems generally user-hostile, especially for inexpert typists. The author notes, rightfully, that computer experts may object to the expenditure of time involved in entering long passwords. Intermittent users will object to the fractional increase of time required for sign-on during brief use. Inexpert computer users may well be discomfited by any increase in procedural demands, whatever the level of their typing skill. We see a need to shift demands from the user onto the system, rather than vice versa.

[12] The use of highly structured consensual knowledge, e.g., the ordered names of the months, risks recurrence of a successful penetration. Consider, for example, the use each month of a password composed of the initial letters of the names of the current month and its seven successors. Such a procedure risks that, whatever the manner of initial password acquisition, an undetected intruder will divine the password origins and thus possess the key to future undetected intrusions.

[13] Here, we borrow generally from an insightful linguistic treatment of speech characterizers in Social Markers in Speech, eds. K. Scherer and H. Giles (Cambridge: Cambridge University Press, 1979). Much of that discussion has direct implications for the password-selection process.

[14] This example was offered by Peter Barton.

[15] For a general review of encoding and retrieving processes, see P. Morris, "Encoding and Retrieval", Aspects of Memory, eds. M. Gruneberg and P. Morris (London: Methuen & Co., Ltd., 1978), pp. 61–83. Mnemonic theory and practice is reviewed in M. Gruneberg, "The Feeling of Knowing, Memory Blocks and Memory Aids", Aspects of Memory, pp. 186–209. Except in the classroom, mnemonic aids have largely fallen victim to "the greatest memory aid even invented, a pencil and paper". (p. 206) Though their usefulness to some people is unquestionable, the manner of their contribution remains debatable. Their contribution may derive mainly from increased effort, or even confidence, attending their use. Problems associated with password methods may kindle a new interest in mnemonics.

[16] E. McNeil and Z. Rubin, The Psychology of Being Human, 2nd, ed. (San Francisco: Canfield Press (Harper & Row Publishers, Inc.), 1977), pp. 166–74.

[17] In A Random Word Generator for Pronounceable Passwords, Report AD-A017-676 of the MITRE Corporation, Nov. 1975, M. Gasser estimates the fraction of pronounceable passwords among *random* strings of letters. For random eight-letter strings, in particular, the fraction is estimated at 0.02653. The fraction of pronounceable strings among those obtained through patterned selection of characters from English expressions – our case – is not estimated in the open literature. For strings formed from initial letters of words, or through sparse periodic sampling, the relative frequencies of occurrence of letters should approximate those for the same letters in the language as a whole. (However, values of correlation coefficients among letters of such strings are typically much less than among letters of English text.) The pronounceable fraction is, therefore, somewhat greater among strings obtained through patterned selection than among random strings.

[18] R. Crowder, Principles of Learning and Memory (Hillsdale NJ: Lawrence Erlbaum Associates, Publishers, 1976), pp. 411–78.

[19] A. Paivio, Imagery and Verbal Processes (New York: Holt, Rinehart & Winston, 1971).

[20] Aspects of Memory, pp. 193–201.

[21] Aspects of Memory, p. 203.

[22] G. Bower and M. Clark, "Narrative Stories as Mediators for Serial Learning," Psychonomic Science, vol. 14, no. 4 (Feb. 25, 1969), pp. 181–82. The method has typically been used to foster recall of an ordered series of words, rather than of characters.

[23] Minimal, and traditional, guidance on password methods appears perhaps yearly in, for example, newsletters of the Michigan Terminal System (MTS) of the University of Michigan. These newsletters are mailed to subscribers, typically faculty and staff, and available at the computing centers to others, including most student users. Nevertheless, the use of deficient passwords is widespread, while the monthly rate of replacement of MTS passwords lost or forgotten has reached one in 600.

[24] Of course, manuals and posted notices will still be needed, e.g., by a user denied system access for want of a password.