FIPS PUB 83

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1980 SEPTEMBER 29

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Philip M. Klutznick, *Secretary*
Jordan J. Baruch, *Assistant Secretary for Productivity, Technology and Innovation*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the National Bureau of Standards, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, DC 20234.

James H. Burrows, *Director*
Institute for Computer Sciences
and Technology

Abstract

This Guideline provides information and guidance to Federal agencies on techniques and practices which can be used to control access to computer resources via remote terminals and networks. A variety of methods are described for verifying the identity of persons using remote terminals, as a safeguard against unauthorized usage. This Guideline discusses the three basic ways which may serve as a basis for verifying a person's identity: something the person KNOWS, such as a password; something the person HAS, such as a key or access card; or something ABOUT the person, such as fingerprints, signature, voice, or other personal attribute. The ability to automatically verify a person's identity via a unique personal attribute offers the prospect of greater security, and equipment for accomplishing this is beginning to emerge. There are several promising laboratory developments, although such equipment has not yet been interfaced to computer terminals to any great extent. In view of the present dependence on authentication techniques other than personal attributes, this Guideline provides advice on the effective use of passwords. This Guideline also discusses a variety of cards and badges with various forms of machine-readable coding that may be used for access control. In order to protect information used for identity verification, encryption is recommended.

Key words: Access control; authentication; authorization; computer network; computer security; encryption; Federal Information Processing Standards Publication; identification token; identity verification; password; personal attribute; personal identification.

Nat. Bur. Stand. (U.S.) Fed. Info. Process. Stand. Publ. (FIPS PUB) 83, 38 pages
(1980)
CODEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161.

Federal Information
Processing Standards Publication 83

1980 September 29

ANNOUNCING THE

GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline: Guideline on User Authentication Techniques for Computer Network Access Control.

Category of Guideline: ADP Operations, Computer Security.

Explanation: This Guideline provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals to safeguard against unauthorized access to computers and computer networks.

Approving Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index:

a. Federal Information Processing Standards Publication (FIPS PUB) 46, Data Encryption Standard.

b. Federal Information Processing Standards Publication (FIPS PUB) 48, Guideline on Evaluation of Techniques for Automated Personal Identification.

c. Federal Information Processing Standards Publication (FIPS PUB) 65, Guidelines for Automatic Data Processing Risk Analysis.

Applicability: This Guideline describes three basic methods by which users of computer terminals may be authenticated and provides information about the capabilities and limitations of each method. It is recommended that Federal agencies consider the use of these methods for safeguarding computers and computer networks, based on a computer security and risk analysis to determine the level of protection required.

Implementation: This Guideline should be referenced by Federal agencies having requirements for controlling the access to computer systems and networks via terminals, where there is a need to verify the personal identity of terminal users.

Specifications: Federal Information Processing Standards 83 (FIPS 83), Guideline on User Authentication Techniques for Computer Network Access Control (affixed).

Qualifications: This Guideline is based on knowledge obtained by NBS staff members from various departments and agencies of the Federal Government, as well as research and manufacturing organizations outside the Government.

All comments and recommendations are welcomed and will be considered in any future revisions. These comments should be addressed to:

Director
Institute for Computer Sciences and Technology
ATTN: User Authentication Guideline
National Bureau of Standards
Washington, DC 20234

Where to Obtain Copies of this Guideline: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 83 (FIPS-PUB-83), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, purchase order, or deposit account.

Federal Information Processing Standards Publication 83

1980 September 29

Specifications for

GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL

CONTENTS

Page

EXECUTIVE SUMMARY

This Guideline provides information and guidance to Federal agencies on techniques and practices which can be used to control access to computer resources via remote terminals and networks. A variety of methods are described for verifying the identity of remote terminal users, as a safeguard against unauthorized usage. This Guideline is intended to acquaint Federal ADP managers and security personnel with various authentication techniques and the basic principles underlying their operation and use.

This Guideline discusses the three basic approaches to verifying a person's identity: something the person KNOWS, such as a password, something the person HAS, such as a key or access card, or something ABOUT the person, such as fingerprints, signature, voice, or other personal attribute. Something known to a person has the disadvantage that it may become known to another person who may then gain unauthorized access. Similarly, a key or card may be misappropriated and used in the same manner. The ability to automatically verify a person's identity via a unique personal attribute offers the prospect of greater security, and equipment for accomplishing this is beginning to emerge. There are several promising laboratory developments, although such equipment has not yet been interfaced to computer terminals to any great extent. Nevertheless, it is expected that such equipment will become available in the next few years.

In view of the present dependence on authentication techniques other than personal attributes, this Guideline provides advice on the effective use of passwords, including password generation, distribution, lifetime, storage, and updating. A variety of cards and badges are also available that may be used for access control; these have various forms of machine-readable coding such as optical coding, electric-circuit coding, magnetic coding, capacitance coding, and an active-electronic badge.

The use of personal attributes for identity verification may be expected, at least initially, to operate with somewhat less precision than might be desired. This is due to the difficulty of performing precise, repeatable measurements of various anatomical or physiological characteristics. In practice, it is generally necessary to adjust the equipment for a compromise between rejection of correct individuals (Type I errors) and false acceptance of imposters (Type II errors).

This Guideline includes published results of certain field tests that were run on selected identity verification devices. These results showed Type I error rates ranging from 1.1 percent for speech to 6.5 percent for fingerprints, and Type II error rates from 2.3 percent for fingerprints to 5.6 percent for signatures. The devices tested were limited production models or developmental prototypes, and it is highly probable that substantially better performance can be realized through further development.

Information used for identity verification should be protected in transmission between remote terminals and the central computer. This may be done through encryption.

Closely related to access control is authorization, which defines the resources available to the authorized user and the permissible uses of these resources. This topic is briefly discussed to acquaint readers with the subject, and references are provided for further study.

SUMMARY GUIDANCE

* Access controls should be used as part of a comprehensive program in computer security and risk management.

* Access controls should provide a degree of protection commensurate with the value of the resources being protected.

* Each user should be assigned a unique identifier or "user name."

* Useful bases for verifying a person's identity are as follows:

  something the person KNOWS (such as a password)
  something the person HAS (such as a card or key)
  something ABOUT the person (a unique personal attribute)

AUTHENTICATION VIA PASSWORDS

* Passwords should have a sufficient number of characters and sufficient diversity to provide a degree of protection commensurate with the value of the resources being protected.

* Passwords should be comprised of easily remembered combinations of letters, together with small quantities of easily grouped numerals or other characters.

* Users who select their own passwords should avoid easily guessed choices such as familiar names, initials, and account numbers.

* Centrally generated passwords protect against the selection of easily guessed passwords by the users themselves.

* Randomly generated pronounceable passwords may be used as an aid to memorization.

* Each user should be assigned an individual password to establish accountability and auditability.

* When transmitted in printed form, passwords should be distributed only to properly authorized individuals.

* Passwords should be distributed in sealed envelopes marked, "To be opened by addressee only," and the contents destroyed as soon as the passwords are memorized.

* Centrally stored password lists should be properly protected, e.g., by encryption.

* Passwords should be protected during entry, e.g., by masking.

* Users should be allowed a limited number of unsuccessful attempts to enter their passwords, to allow for entry errors: this limit should not exceed five.

* A minimum time interval should be enforced between password entry attempts: this limit should not be less than 1 second.

* Passwords should be changed at intervals not to exceed 1 year, and at any time they are known or suspected to have been compromised.

* Passwords should be invalidated whenever the associated user's access privileges are revoked.

AUTHENTICATION VIA ACCESS CARDS

* Access cards with machine-readable data permit the use of individual codes for each user, which is recommended for accountability and auditability.

* Coded information should be changed at intervals to guard against discovery.

* Cards used for access control should be durable, resistant to tampering, difficult to counterfeit, and convenient to use.

* Facilities for the assembly and lamination of access cards should be available within the using organization to expedite card preparation.

* Card readers for access control should be tamper-resistant and should use line supervision and/or encryption for the communication lines.

AUTHENTICATION VIA PERSONAL ATTRIBUTES

* Useful personal attributes for verifying a person's identity are fingerprints, hand patterns, signatures, and voices.

* Devices based on personal attributes should have a low probability of rejecting a valid user and a low probability of accepting an imposter; in practice, a compromise setting may be required.

* The user of a personal identification device should be allowed a limited number of attempts to achieve recognition, and careful consideration should be given to the conditions for accepting a user who requires multiple attempts.

GENERAL CONSIDERATIONS

* A duress alarm procedure should be available in the event that an authorized user is forced to gain access on behalf of an imposter.

* Terminals and other remote equipment should contain built-in circuitry to produce a unique code in response to an interrogation command.

* Where necessary, encryption should be employed to protect information used for verifying personal identity; the Data Encryption Standard, FIPS PUB 46, is recommended.

* Access to computer resources, such as processors, memory, files, and programs, should be in accordance with proper user authorization, once the user identity is verified.

1. INTRODUCTION

This Guideline presents information on personal identification techniques and practices which can be used to ***control access to computer resources via remote terminals and networks.*** This information has been developed as part of a comprehensive program in Computer Security and Risk Management by the NBS Institute for Computer Sciences and Technology. As such, it is intended to be used in conjunction with other safeguards to achieve security and integrity in computer system operation. Other publications on this subject are indicated in the Bibliography at the end of this Guideline. Literature references in the Bibliography are indicated in square brackets for the benefit of readers who wish to obtain additional information on specific subjects, e.g., [WARF 79].

1.1 Need for User Authentication

Computer usage is continuing to expand rapidly as computers become more versatile, more plentiful, and less expensive. As the number of applications increases, computers are being entrusted with ever more sensitive and valuable information, and this carries with it increasing opportunity and temptation for misuse through intentional, self-serving manipulation on the part of anyone with access to a terminal [BEQU 78, MART 73, ANDE 72]. Such misuse may be perpetrated by either an authorized user or an unauthorized user. However, the incorporation of the appropriate access controls can limit the opportunity for misuse by an unauthorized user, and can restrict the access of authorized users to those resources for which they are properly authorized. Furthermore, the use of an appropriate combination of access controls, accountability provisions, and an effective audit trail can serve as strong deterrents to the misuse of resources by authorized users.

The control of access to computer resources is comprised of two major aspects:

1. Identification and authentication of authorized users.
2. Authorization for the use of the designated resources in the intended manner.

This Guideline describes the ways which may presently be considered for verifying the identity of terminal users to restrict network access to authorized individuals. It also describes system considerations for use in conjunction with identity verification to safeguard against circumvention of the access control provisions. The establishment and enforcement of authorization is the reponsibility of the computer operating system and specialized security software, and is beyond the scope of this Guideline. A brief discussion of authorization is presented at the end of this Guideline to acquaint readers with the subject and to provide references for further study. Software and operating system security, as well as data encryption, are the subjects of other publications in the Computer Security and Risk Management series. See Bibliography for a listing of other security publications.

1.2 Verification of Personal Identity

A key element in access control is the establishment of a positive, unique identification for each person or entity to which access is to be granted. This generally involves a two-stage process [HOFF 77]:

1. Identification—The presentation of a claimed identity ("user name") by an individual.
2. Verification or authentication—The presentation of privately held information to verify the claimed identity.

Each individual should be assigned a unique user identifier or "user name" by which he or she is known to the system. This name will generally be public information and is unlikely to change. It will be used by the system in referencing the user's authorization tables and in keeping a log of his or her system usage.

The privately held information used to verify the individual's claimed identity may exist in one of the following forms [BEAR 72, WABL 77]:

(1) Something KNOWN to the individual.
(2) Something POSSESSED by the individual.
(3) Something ABOUT the individual.

Something KNOWN to an individual can be a password, the combination to a lock, or a set of facts from his or her individual background. Something POSSESSED by the individual can be an object such as an access card, a badge with machine-readable code, or the key to a lock. Something ABOUT an individual can be his or her fingerprint, voice, signature dynamics, or some other personal attribute, such as the shape of the hand (hand geometry).

Reliance upon information known to an individual suffers from the disadvantage that ***this information could become known to an imposter*** who could then use the information just as readily as its rightful owner. Therefore, this information needs to be carefully protected, and should also be changed at intervals, since the chance of its being discovered by a would-be penetrator increases with time. Reliance upon an object possessed by an individual suffers from the disadvantage that ***the object may fall into the hands of an imposter*** and can then be used as readily by the imposter as by its rightful owner.

Because of the disadvantages of the first two methods described above, much emphasis has been placed on the development of techniques for using personal attributes for identity verification [WARF 79]. At the present time, several techniques are under development, though very few devices are yet commercially available, and costs are such that these devices are not economical for many applications. The ideal method of verification would make use of a personal characteristic which was unique to an individual, could be measured with good repeatability, and could not be copied or mimicked by another individual, even through the use of special equipment, such as recording devices. Because of the urgency of this problem, and the rate at which measuring and computing equipment is advancing, it seems likely that cost-effective devices for use in conjunction with remote terminals will become available in the next few years. This Guideline discusses the techniques which are presently the most promising and the implications of using such techniques for controlling access to networks. Because devices of this type are not yet widely available, this Guideline also discusses techniques based on the use of password-type information and the use of cards and keys as alternative methods of identity verification.

2. PASSWORDS

Passwords are widely used as a means of controlling access to computer networks. The purpose of the password is to authenticate the user at a remote terminal or other resource. In practice, a user typically logs onto a system and then provides a nominal (claimed) identity, such as a user name and/or account number. The system then requests the password which, when entered correctly, serves to verify the user's identity. As with other methods of authentication, passwords do not protect against erroneous or illicit actions by authorized users, and should be used with other security measures appropriate to the resources being protected.

This section presents information on the generation and selection of passwords, password distribution, protection in storage, password use, changing of passwords, and password lifetime [WOOD 78].

2.1 Password Generation and Selection

Passwords may be any sequence of letters, numbers, or special symbols or control characters, printing or nonprinting, for use in controlling access to computer networks and computing resources, including data.

Fixed passwords are passwords which remain in use for a prescribed period of use. One-time passwords are valid only for a single use and are then discarded.

Passwords should be comprised of a sufficient number of characters and generated in such a manner as to assure a degree of protection commensurate with the value of the resources to which access is being controlled. The total number of potential allowable passwords capable of being generated should be large enough to reduce to an acceptable level the risk of a valid password being discovered, either inadvertently or through a systematic process. In assessing this risk, it should be assumed that a would-be penetrator may have knowledge of one or more other passwords, from which to gain information on the structure of the passwords, and which may aid in uncovering the generation scheme, if not sufficiently complex [ANDE 72, MOTH 79].

Passwords should be comprised of easily remembered combinations of letters, together with small quantities of easily grouped numerals or other characters. Some systems allow users to create their own passwords, while in other systems the generation and selection of passwords is under central control. Passwords generated by the user are generally easy to remember. However, they suffer from the tendency of people to select familiar words such as family names, locations and addresses, and words from simple background facts like schools attended. The use of a central password generation facility can assure that the passwords are derived from a sufficiently large universe, that they have no association with any particular user, and that they are generated in a highly randomized fashion. Centralized generation and selection of passwords therefore offers a higher degree of security, although the passwords are generally more difficult to remember. In the event that users are allowed to create their own passwords, they should be cautioned against the use of simple or obvious words of the type mentioned above.

Where passwords are generated by a computational procedure, the procedure should be such that it would be extremely difficult to predict new passwords based on a knowledge of previous ones. Much attention is being given to the development of suitable algorithms for password generation [ANDE 72, GASS 75, HOFF 77].

Using the 26 letters of the English alphabet in any arbitrary arrangement, the number of possible passwords that can be formed using N letters is 26 to the Nth power. The total number of passwords comprises the password space. Thus, using 5-letter passwords, there would be 26 to the 5th possible combinations, which is equal to 11,881,376. The password space can be further increased by making a few numerical substitutions in place of letters. For example, instead of using a word such as MKFGT, one might use M8FG4. The intermixing of letters and numerals is recommended. The password space can be still further enlarged by allowing the use of punctuation marks and other symbols. In many systems the keyboard permits the entry of various special codes which do not produce visible graphics on the associated display. If these can be added to the repertoire of password elements, the password space may be enlarged even further. However, these are often used for special control operations and may not be valid for use in passwords unless there is a provision to ignore their control meanings during password entry.

If arbitrary arrangements of letters are used to form passwords, the resulting passwords will be mostly nonsensical and may be difficult for the users to memorize. As an aid to memorization, the passwords may be restricted to arrangements of letters which are pronounceable, even though nonsensical. This reduces the password space, but the number of allowable passwords can still be very large. The English language is not ideal for this purpose, in that the relationship between spelling and pronunciation in English is by no means unique. English is highly irregular in this regard. In an orthophonetic language, there is a one-to-one correspondence between the spelling of a word and its pronunciation. Spanish is a language having this property. Nevertheless, computer programs have been devised for generating arbitrary passwords that are pronounceable [GASS 75]. Algorithms underlying the generation of passwords must be ones which would be very difficult to break by cryptanalysis. Otherwise, if a would-be penetrator could get hold of some previous passwords, he or she might be able to use them to discover the algorithm and initiate it at a point which would allow him or her to generate valid upcoming passwords.

When passwords are comprised of numerals and other symbols intermixed with letters, the concept of pronounceability no longer has much validity, and the users are left to their own devices as to how to memorize them.

2.2 Assignment of Unique Passwords to Each User

Wherever possible, unique passwords should be assigned to each authorized user, rather than sharing a common password among a group of users, even though they may be accessing the same resources or data. The assignment of unique passwords enhances security for the following reasons:

1. Establishes accountability on an individual basis, enabling a record to be kept of what resources were accessed under each password and for what purposes,
2. Makes it possible to hold users accountable for illicit use of passwords, whether intentional or through carelessness,
3. Aids in discovering where a security breach may have occurred, if illicit usage is discovered,
4. Avoids the need to inconvenience a group of users in the event that a member of the group is "delisted," that is, the member's authorization is revoked,
5. Permits an audit trail to be maintained of system accesses and resource usage by individual users.

2.3 Password Distribution

Passwords should be distributed only to individuals with a legitimate need to know them and authorization to access the resources controlled by them. In the case of passwords generated centrally, it is preferred that they be distributed by a very limited number of staff members reporting directly to the ADP resource manager or a designated security control officer. In the case of passwords which must be distributed remotely, registered mail is recommended.

Passwords may be distributed by means of sealed envelopes marked, "To be opened by addressee only," and personally delivered to the addressee, if adequate precautions are provided and clear instructions given to destroy the contents of the envelopes as soon as the passwords have been memorized.

If users are permitted to create and enter their own passwords, this is usually done by first providing the user with a system-specified password which allows initial access to the system. For this purpose, the user generally must apply in person and be properly identified in order to receive the initial password. The user then accesses the system under this password and a routine is invoked which enables him or her to enter the password which he or she has created. Thereafter, the user must access the system under his or her own password; the initial password is no longer

valid for this purpose. The user may be given the ability to change his or her password at will by reinvoking the password establishment routine.

2.4 Protection of Passwords in Storage

Passwords used for network access control are usually stored in the form of tables or lists which contain the current password for each authorized system user. ***This information must be carefully protected, since it is critical to system security.*** Protection may be provided by storing the passwords in a transformed state that would be very difficult or impossible to reverse. One method of achieving this is to encrypt the passwords before storing them. The Data Encryption Standard (DES) is recommended for this purpose [FPUB 46, SPUB 27, SPUB 54].

Various algorithms have been suggested for transforming the password tables for protection in storage [TURN 73, SPUB 9]. In practice, the passwords are transformed by the system as soon as they are received for storage, and then stored in the transformed state. Then, when a password is supplied during an access request, this password is transformed and compared with the corresponding transformed value in the table. If a match occurs, the password is accepted.

2.5 Password Use and Vulnerabilities

Passwords are vulnerable to several threats when being entered into a terminal and being transmitted. Potential threats include observation of the user during entry, heuristic search, wiretapping, electronic eavesdropping, and piggyback infiltration. ***Provisions should be made to prevent the password from being seen during entry.*** On many CRT or printing terminals, it is possible to suppress the printing in order to allow the password to be keyed in without a visible display. It is the responsibility of the user to assure that his or her keyboard actions are not being watched surreptitiously while keying in the password. In systems where it is not possible to suppress the display of the password, it may be possible to mask out the password by over-printing it with several sets of arbitrary characters, or under-printing the area where it is to appear before it is keyed in. With printing terminals, care must be taken to avoid the possibility of someone discovering a password on a discarded printout. Another scheme is to use passwords comprised of nonprinting characters, such as control characters. This is less attractive, however, since passwords of this type are more difficult to memorize, and only a limited number of characters are available.

In the heuristic search type of attack, a would-be penetrator might try to gain access to a system by repeatedly trying to guess a password, using such insights as might be available. Or, he or she might program a computer to systematically generate passwords with the appropriate characteristics and have the computer repeatedly try to gain access automatically. ***To guard against these threats, there should be provision for imposing a time delay between unsuccessful access attempts, and a limit on the number of such attempts, after which further attempts from that source are ignored and a security alarm is generated.*** The time delay should be comparable to the time required for a person to enter a password, in order to prevent an automated system from trying passwords at a high rate. A delay of at least one second is recommended. The number of unsuccessful attempts should be limited to a small number, such as three to five, in order to quickly cut off a heuristic search. (A few unsuccessful attempts should be allowed as an accommodation to authorized users to allow for occasional entry errors.)

In the passive wiretapping threat, an adversary taps the transmission line anywhere between the terminal and the central system, and records the characters making up the password. He or she could, of course, record any other information being exchanged, by this same method. Electronic eavesdropping is done by an adversary using sensitive electronic monitoring equipment to detect electronic emanations, from which the password (and other information) may be derived. ***The defense against both the wiretapping and eavesdropping threat is to use data encryption,*** so that the password character stream cannot be obtained in the clear [MELL 73, FPUB 46, SPUB 27]. However, the encryption process ***must cause the password to be encrypted differently each time it is sent.*** If this is not done, the adversary can record and transmit the encrypted form of the password and it will appear valid to the central system.

In piggyback infiltration, an adversary allows an authorized user to log in to a system in the normal manner, and then utilizes this valid connection by means of a wiretap connected to a terminal of his or her own [WABL 77]. Another type of threat is that an adversary might try to mimic the central system in order to get the user to enter his or her password so that it can be intercepted by the adversary's terminal. Again, encryption can be used to counter these threats.

It is recommended that, upon logging in, ***each user be shown a record of the most recent access under his or her password,*** together with any unsuccessful intervening access attempts [WABL 77]. This will aid in uncovering any unauthorized accesses or attempted accesses which may occur between legitimate sessions.

2.6 Password Lifetime and Changing of Passwords

The lifetime of a password is the length of time that it remains valid. ***Passwords should be changed periodically, since the likelihood of their being surreptitiously discovered increases with time.*** It is recommended that passwords be changed ***at least once a year.*** The frequency of change depends on the sensitivity of the resources to which access is being controlled. Therefore, the frequency of change should be determined on the basis of a formal computer security and risk analysis [FPUB 65].

If it is discovered that a password has been compromised, or is believed to have been compromised, then the password should be invalidated immediately and a new password issued.

When a user's authorization to access a system is revoked for any reason, such as a transfer or termination of employment, ***the user's password should be invalidated immediately.*** If the same password is used by a group of users, it will be necessary to issue a new password to the group. This is one of the reasons favoring separate passwords for each user.

Procedures should be established for implementing password changes in an orderly manner. These procedures should include notification of the time at which the new passwords are to become effective and the time after which the old passwords will no longer be valid. There should be appropriate provisions for propagating the password changes within the central system in order to update all access provisions in accordance with the changes.

A provision should be made for reissuing a password to a user who forgets the password. In the case of user-generated passwords which are stored in a transformed state, the system may have no record of a password in its untransformed state, and therefore the system cannot retrieve the password in order for it to be made available to the user. In such cases, it may be necessary to create a new password.

There should be provisions for transferring access authority from one individual to another, in the event that one individual becomes indisposed or unavailable for duty and another individual has to take over that individual's functions. This could be done simply by providing the one individual's password to the other, but this would not provide an indication as to which of the two individuals was accessing the system. It would be more secure for each individual to have his or her own unique password.

2.7 Duress Alarm

A would-be penetrator might attempt to gain access to a network by forcing an authorized user to log in and perform the authentication procedure, whereupon the penetrator would then either take over the terminal or instruct the user to carry out the penetrator's bidding. ***To protect against this threat, a duress alarm provision should be included.*** This should be an inconspicuous action taken by the user to signal the system that he or she was being held hostage. It might be necessary for the system to perform in a normal manner, following detection of this signal, in order not to place the user in jeopardy. However, the alarm signal could be used to invoke security measures intended to circumscribe the penetrator's actions.

3. IDENTIFICATION TOKENS

The possession of a token, such as a key or machine-readable card, is one of the basic ways of verifying a person's identity [WABL 77]. If the token provides machine-readable data, it may be used for providing the claimed identity; its possession by the user is taken to verify the user's identity (assuming that it has not fallen into other hands). Or, the user may enter a claimed identity by such means as a keyboard, numeric keypad, or combination dial, and then use the token to verify the claimed identity. Computer terminals can be fitted with key locks or with badge readers for use in this manner. Alternatively, the token-actuated device could be distinct from the terminal and could control the terminal's operation by some means such as controlling the power line or the communications line to the terminal. This might be more susceptible to circumvention, however, than incorporating the token-actuated mechanism as an integral part of the terminal, using tamper-resistant construction.

A penetrator who succeeds in obtaining a token can use it as readily as the authorized user. Therefore, it is ***advisable to include some type of password scheme*** to deter unauthorized use of the token.

3.1 Need for Updating

The longer a security safeguard is in place, the more opportunity there is for would-be penetrators to become familiar with it and to devise a penetration scheme (such as appropriating and duplicating a key or making a counterfeit card). Therefore, ***the coding should be updated at intervals*** (such as replacing lock cylinders or reissuing cards with new codes). In the case of a card reader which reads a code and transmits it (preferably encrypted) to a central computer for checking, the change is readily carried out by issuing new cards and updating the master control list. The rekeying of locks may be less convenient.

3.2 Distinguishing Among Users

If a particular terminal is to be used by more than one authorized person, then ***there should be ways to distinguish which person is using the terminal.*** This will enable the central facility to enforce the proper authorization for the particular user. If a lock and key are used, each user will have the same key, and there will be no way for the computer to determine whose key is being used to activate the terminal. The use of cards with a unique code for each user enables the computer to determine which of the various authorized users is using the terminal (or, at least, which user's card is being used to activate the terminal).

3.3 Machine-Readable Cards

A variety of machine-readable cards have been developed for access control purposes, and these may be conveniently described in terms of the method of encoding information on the card. With some of these cards, the coding can be altered rather readily in the field; with others, the coding is either permanently built-in or requires special factory equipment for alteration. The various types of cards or badges that are presently in use are described in appendix A. Many of these can also include printed material, photographs, and so forth, and can serve as identification badges as well [SAND 77, WARF 79].

3.4 Design Objectives of Coded Identification Tokens

3.4.1 Badge Size

Several badge sizes are in common use. Selection of a particular size is usually a compromise between a smaller, easily handled badge and a larger badge with more room for a photograph, color-code indicators, and necessary printed information. Further, in some installations, size may be affected by the need to attach a radiation dosimeter to the badge.

Most commercially available coded-credential systems utilize the standard credit card size, 54 by 86 mm (2-1/8 by 3-3/8 in). This size, however, is too small or, at best, marginally acceptable for a picture badge. A slightly larger common badge size is 60 by 83 mm (2-3/8 by 3-1/4 in). Although the latter badge is not much larger than the standard credit card, its slightly smaller aspect ratio provides significantly more usable badge area when the badge is worn with the longer dimension oriented vertically. The choice of commercial coded badges is severely restricted if the credit card is unacceptable. One alternative is to require each employee to wear a larger photo badge and carry a separate coded card to be used where electronic badge readers are installed.

3.4.2 Badge Preparation

It is preferable that assembly and lamination of the badge be done at the facility site. Intolerable delays, administrative overhead, and reduced security may result if this cannot be done.

Coded badges must be enrolled in the memory of the control processor after fabrication. For simple systems, enrollment is done on a keyboard located on the control console. Unless provision for maintenance of a backup copy of the control processor memory is provided, all badges must be manually re-enrolled after each power failure or equipment malfunction. This could be a serious problem for large installations.

3.4.3 Durability

A badge should be able to withstand daily use for a period of 5 years, with normal care. Some polyvinyl-chloride (PVC) plastic materials deteriorate rapidly when exposed to sunlight and become brittle when the temperature drops below 0 degrees C. Most common credit card materials exhibit these problems; however, some PVC formulations are available which eliminate most of these problems. Polyester-based plastics are more durable, but care must be taken in their selection to ensure that reliable, permanent lamination of the badge can be achieved.

3.4.4 Resistance to Decoding and Counterfeiting

Any type of coded badge can be decoded and duplicated if sufficient money and talent are devoted to the attempt. The following list ranks the coding techniques described in appendix A, from the easiest to the most difficult to duplicate:

1. Electric-circuit code
2. Magnetic-stripe code
3. Magnetic code
4. Metallic-strip code
5. Capacitance code
6. Optical code
7. Passive-electronic code
8. Active-electronic code

Note that the first two coded badges are easily duplicated, while the last six are significantly more difficult to duplicate.

In general, it is not necessary to decode a badge to duplicate it. The degree of difficulty in decoding the badges listed follows approximately the same rank order. Often the code data are cryptographically encoded or contain other internal checks. Counterfeiting a new badge would then require both decoding and understanding the internal check algorithm; this type of counterfeiting is much more difficult.

Resistance to decoding and counterfeiting is not as important if the badge is used in conjunction with a separate identity verification system based upon a personal attribute. In this type of system, the badge number simply indexes a file, called the reference file, where personnel identifier data are stored in a central computer. Access is allowed only if the personnel identifier algorithm is satisfied. In this case, counterfeiting a badge will not, in itself, guarantee access.

3.4.5 Badge Readers

Where badges are depended upon for identity verification, badge readers are a vulnerable point at which to attack an entry-control system. ***Badge readers should therefore be provided with tamper sensors.*** Further, communication lines between the badge reader and any central console or computer ***should be protected by line supervision and/or encryption.***

4. VERIFICATION BY MEANS OF PERSONAL ATTRIBUTES

Because of the inherent drawbacks in other forms of identity verification (something KNOWN by a person or something POSSESSED by a person), much attention is being given to authentication methods based on something ABOUT a person [WARF 79, FONS 77]. Among the ***personal attributes*** being considered are hand geometry, fingerprints, signatures, and speech. This section reviews several of these techniques and presents the general considerations involved in using this type of authentication. This is an actively developing field and it is premature to say that any particular technique is superior from the standpoint of security and economy at this time. For any given application, however, one of these techniques may be similar to current methods and have a natural operational advantage over the others.

The rapid growth in the population of remote computer users and the increasing sensitivity of computer applications have combined to intensify the need for methods of authentication that can positively establish the identity of users at remote terminals. At the same time, advances in instrumentation technology and compact low-cost processors, together with improved methods of signal processing and pattern recognition, have opened up new possibilities for automated identity verification based on unique aspects of personal attributes [WARF 79, BEPR 77].

4.1 Problems of Measurement

One of the chief problems in using personal attributes for identity verification is the difficulty of performing precise, repeatable measurements on the human body. This is true whether the attribute is a relatively static quantity such as the fingerprint or finger length, or whether the attribute is dynamic, such as handwriting or speech. Because of the curvilinear nature of body surfaces and the plasticity of body tissue, it is difficult to establish accurate reference points and good registration for taking measurements or pattern matching.

Fingerprints are highly deformable, depending upon pressure both normal and tangential to the surface of the finger and the contact medium. The topological features are preserved under such deformations, and a trained analyst can pick these out, but it is more difficult to perform machine matching under these conditions [STOC 75].

Lack of precise repeatability is characteristic of most personal attributes and processes, including handwriting and speaking. This must be taken into account when testing and evaluating candidate identity verification systems. ***In testing such systems, provision should be made to vary all factors considered to have an influence on the attribute(s) being utilized.***

4.2 Intrapersonal and Interpersonal Variability

The inability to achieve precise repeatability in the measurement of a personal attribute for a given individual is designated ***intrapersonal*** variability. The variation in parameters from one individual to another is designated ***interpersonal*** variability [RIGA 75]. It is this interpersonal variation which allows one individual to be distinguished from any other. In order to allow for statistical variations in the measured parameters resulting from intrapersonal variability, a certain amount of tolerance must be allowed. If the tolerance is made too great, the ability to distinguish between individuals is diminished.

Identity verification devices can have an adjustable threshold which can be used to tighten or loosen the tolerance. Tightening the tolerance improves the ability to discriminate between individuals, thereby lessening the chance of an imposter being accepted in place of an authorized user, but at the same time this raises the chance of incorrectly rejecting an authorized user [WARF 79].

4.3 Method of Operation

Devices for the verification of identity based on personal attributes generally operate in the following manner:

(1) This user enters his or her claimed identity. This may be done by entering a name or a personal ID number or other identifier. Or, the user may insert into a reader a token such as a magnetic stripe card bearing such information in machine-readable form.

(2) The device then prepares to verify the claimed identity. This will be done by comparing a reference profile of the attribute associated with the claimed identity with the measured profile of the attribute as derived from the individual by a measurement process. Depending upon the device and the application, the reference profile may be obtained from a central file, it may be obtained from a local file in the device, or it may be read from a machine-readable token supplied by the individual. An alternate method is to measure the attribute and send the measured profile to a central location for comparison with the reference profile. It may not be necessary to send the entire volume of measured data to the central location when this method is used. Instead, a local processor can preprocess the data and derive a set of parameters representing the measured profile. These features can be used for the comparison. Alternately, a sequential decision scheme can be used which transmits information until a decision is reached at a prespecified level of statistical confidence. This makes the entry process shorter for the normal authorized user and longer for the imposter.

(3) The measured profile is compared with the reference profile and a measure of similarity is obtained. This generally results in an output signal from a comparator having a value lying between some minimum and maximum.

(4) The resulting value is compared with a preset threshold which results in a binary decision to accept or reject the individual (or to request more data).

4.4 Classes of Recognition Error

Because of practical limitations and the need to accommodate ***intrapersonal variations,*** there are ***two types of errors*** that are encountered with practical identity verification devices:

Type I errors: Falsely rejecting a correct user.

Type II errors: Falsely accepting an imposter.

In statistical treatments, the probabilities associated with Type I and Type II errors are usually designated A and B, respectively [WOLF 62].

The Type I error rate (false rejection rate) is calculated by dividing the number of false rejections by the total number of verification attempts by authorized individuals.

The Type II error rate (false acceptance rate) is calculated by dividing the number of false acceptances by the total number of verification attempts by imposters.

In operation, an identity verification device carries out a measurement or series of measurements on the designated personal attribute, processes this data, and compares the results with a reference profile. If the results match within a specified tolerance, the identity is considered to be verified. Within the device (or the associated computer) a scoring process is performed, resulting in a value which falls within a range. Because of intrapersonal variation, the match will not generally be exact, but will fall within certain limits for the correct individual and outside for an imposter. In analyzing the operation of such a device, it is instructive to take the data collected from a large series of measurements for both correct individuals and imposters, and to plot the results as shown in figure 1. Here the data is plotted against the range of possible scores, produced as the output of a comparator in the device, indicating the degree of match or mismatch. Ideally, the scores for correct individuals would all be grouped at the right edge of the graph, while those for imposters would all be grouped at the left edge. This would indicate that the device was capable of unambiguously distinguishing correct individuals from the imposters. However, in practice, this ideal may not be realized; instead, the device may operate in the manner shown in figure 2 [WARF 79]. This shows that the scores are spread out considerably, even to the point of overlapping. In this case, there is no value which can be used as a threshold such that it will effectively separate correct users from imposters. ***In practice, a compromise setting must be used.*** If the threshold is set at the point where the two curves cross over, this is referred to as the "equal error" setting [WARF 79]. This is the point at which the Type I and Type II error rates are equal, and the percentage of correct individuals being falsely rejected will equal the percentage of imposters being accepted. The error rate at this point is a single number which is a convenient value to use in describing the performance of such a device, rather than trying to describe the relationship between the two error rates in more detail.

It is evident from figure 2 that ***the threshold can be varied in a manner which will favor one error rate at the expense of the other.*** By moving the threshold to the right, the probability of accepting an imposter can be made arbitrarily low, at the expense of greater user inconvenience due to false rejection of correct individuals. Conversely, the threshold can be moved to the left to avoid false rejection of correct individuals, while increasing the risk of allowing an imposter to be accepted. Data on the performance of various actual devices is presented in appendix C.

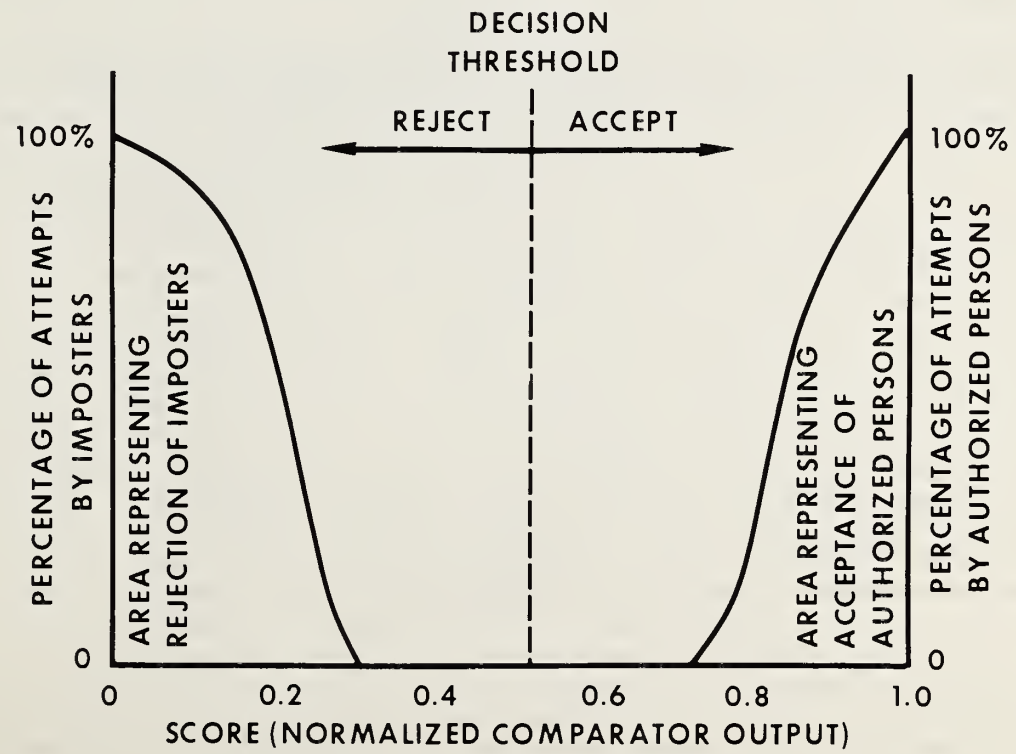

Figure 1. Preferred output of identity verification device.

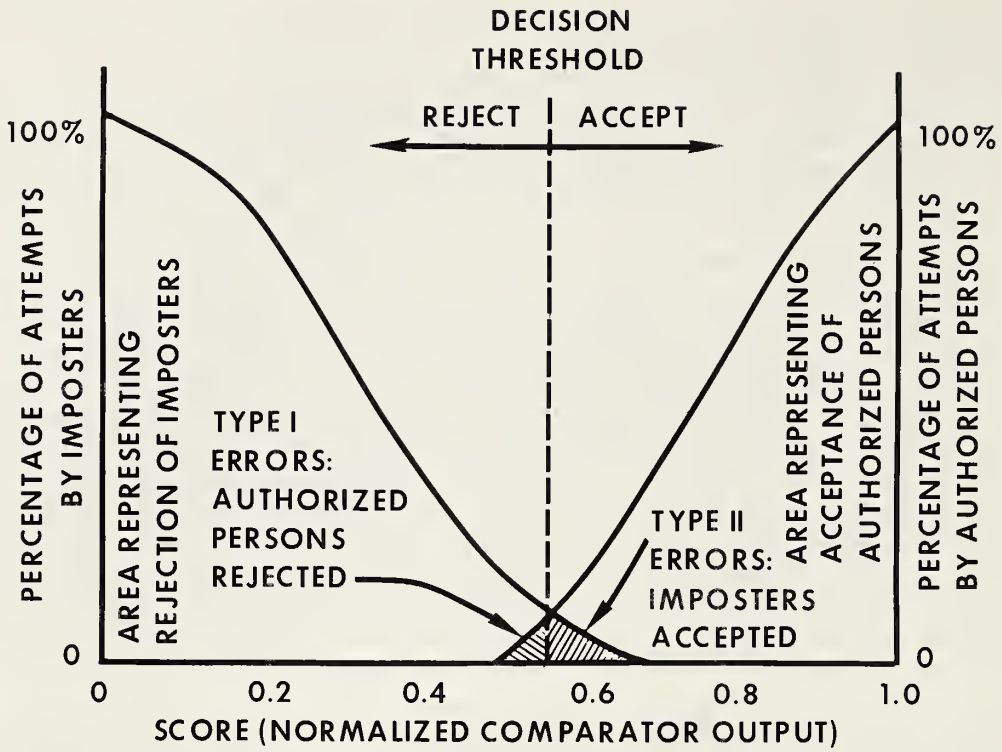

Figure 2. Typical output of identity verification device.

4.4.1 Variability of Attributes

The limitations encountered in actual devices arise from two sources, one being the imprecise nature of the attribute being utilized, and the other being the relative newness of the equipment and processing technology being used. The quality of the attribute places an inherent limit on the degree to which it is possible to distinguish one individual from another by means of that attribute [RIGA 75]. This is a function of the intra- and interpersonal variability of the attribute and its information "richness." To illustrate, consider a single system using only a person's height and weight. (These would obviously not be convenient attributes to measure for terminal users, but are selected merely for purposes of discussion.) It is possible to make scientific measurements of both of these quantities to several decimal places of accuracy, thereby having a large number of numerical values with which to label different individuals. It is intuitively evident that it would be very unlikely for two people's weights, for instance, to agree to within, say, a part in 10 to the 5th, when both are weighed on the same occasion. By resorting to height measurements as well, a further means of distinguishing them is obtained. With a moment's reflection, several drawbacks can be discerned in this scheme. First, we know that both a person's weight and height can vary measurably from one occasion to another. Depending on the time of day and the circumstances, a person's weight might vary by as much as 5 pounds from one day's reading to the next. For a person whose nominal weight is 150 pounds, this would be a variation of over 3 percent, so obviously a precise measurement to a very small fraction of a percent would be illusory as a means of verifying this person's identity over a period of time. It is easy to see that once the tolerance for this individual is opened up to a reasonable range (perhaps plus or minus 3 pounds), his or her weight becomes much too coarse a parameter to use in distinguishing him or her from others. In a group of any size, there would be many people whose weights were within a few pounds of each other. Height is also subject to significant variations. This is partly due to the fact that the spinal disks become compressed during the course of the day when the person is upright and become uncompressed when the weight is removed during sleep. Also, a precisely repeatable height measurement would be difficult to achieve because of the influence of a person's posture and the tilt of the head. A person who was 6 feet tall might show a variation of an inch, which is about 0.7 percent of his or her height. So again, a tolerance would have to be allowed, and the magnitude of the required tolerance would be such that the likelihood of accepting an imposter would be greatly increased.

4.4.2 Distribution of Values Within a Population

Another deficiency in the use of parameters such as weight and height as means of identity verification is the fact that the values for a typical population are not uniformly distributed over the full range of possible values. While the upper limit on height is 7 feet or so, the lower limit is certainly not zero, but is something closer to 4 feet for adults. Therefore, the available number range is not zero to 7 feet, but 4 to 7 feet. Furthermore, even within this range, the distribution is heavily clustered around the normal values for men and women. A similar clustering prevails for people's weights. The more the values are clustered, the greater the probability that the tolerance range on one person's parameter(s) will encompass the value(s) for another person, thereby making it easier for an imposter to gain acceptance.

4.4.3 Correlation Between Attributes

One further observation can be made with regard to the difficulty of using parameters such as weight and height for identity verification. This has to do with possible correlation between the parameters. If the parameters tend to vary in the same manner from one person to another, then the use of the two parameters does not provide as much distinct information about individuals as would two fully independent parameters. In the case of weight and height, two people of the same height can (and quite likely would) have different weights, and vice versa. Nevertheless, weight tends to increase with height, so there is a degree of correlation between these parameters. Therefore, the use of these two parameters would not be as useful in distinguishing one individual from another as would two independent parameters (given equal range, distribution, tolerances, etc.).

4.4.4 Measurement Limitations

The preceding discussion dealt with the quality of the attributes selected for identity verification and the suitability for this purpose. ***The quality of the attribute sets a fundamental limitation on its suitability as a discriminant among individuals.*** A further limitation arises in the ability to instrument the measurement of the selected attribute. Assuming that the attribute is a sufficiently rich source of information to distinguish a large number of individuals from one another and that it has an underlying stability and precision so that excessive tolerances are not required, can the attribute be measured with the requisite accuracy? Can an economical device be produced which will sense the attribute with the required precision and produce repeatable results? Will the device be stable over a long period? Will it have to be recalibrated periodially, and what kind of test inputs are needed for this purpose? What amount of data processing is required to match the measured data against a reference profile and is suitable software available for this process that can run on an economical computer in a reasonable length of time? These are questions which relate to the state-of-the-art in the field of identity verification devices. The answer is divided between how well the attribute can be sensed by the measurement process and how well the resulting information can be processed to achieve the necessary comparison.

The deformability of body surfaces and tissues and the lack of well-defined reference points present obstacles to the precise measurement of body features. This poses problems both in taking accurate physical measurements and in lining up images for matching patterns such as fingerprints. Fingerprints are a good example of an attribute which is known to be a very rich source of information, yet is difficult to sense and compare by machine [ELEC 73]. The information represented by fingerprint minutia, considering some 50-60 minutia per print, is such that it is possible to distinguish one individual from another in an extremely large population. However, due to distortions and the difficulty in obtaining consistent repeated impressions, this capability is drastically reduced. That is, the viewing and scanning process may cause some minutia to be overlooked and false ones to be sensed. Therefore, the information acquired is significantly limited, and the tolerances must be broadened to the point where the automated technique falls far short of the true capability of fingerprints to distinguish members of a large population. This is a case in which the equipment limitations (both in the sensing of fingerprints and the pattern matching algorithms) are the limiting factors, rather than a lack of sufficient detail (information richness) in the attribute itself. (Of course, if fingerprints were better behaved, in the sense of being easier to scan and not deformable, the equipment problem would be greatly eased, but that is a situation which may not be subject to control.)

4.5 Multiple Access Trials

As explained earlier, ***a practical identity verification device generally will not be able to distinguish between correct individuals and imposters 100 percent of the time.*** One way of dealing with this situation is to use a threshold setting which is a compromise between the Type I and Type II error rates.

Where security is the paramount consideration, the threshold will be set to hold the Type II error rate below the limit determined by a formal risk analysis [FPUB 65]. At this setting, the Type I error rate should not be so high as to unduly burden the correct users due to excessive false rejections. If it is, then this approach is not a solution to the problem. However, there will always be false rejections (as long as the Type I error rate remains non-zero). This produces the strategy of ***allowing would-be users more than one opportunity*** to try to verify their identity [DODD 75]. That is, if they are not accepted on the first try, they may apply again. Typically, the system will offer them the opportunity to try again. They then repeat the verification "ritual." The expectation is that this time the statistical variation will bring their measurements within the required tolerance range to match their reference profile. The general practice is to accept the user once a successful verification has been achieved.

It is important to note that ***allowing extra trials also presents an advantage to the imposter.*** Assuming that there is a statistical variability in the measurement process (which is the reason that false rejections occur) the imposter has another opportunity to be recognized with each succeeding trial. Therefore, if multiple trials are to be allowed, proper consideration should be given to the decision rules which are applied in granting access, and the Type I and Type II error rates must be measured with the maximum number of repeated trials which will be specified beforehand.

4.5.1 Example of the Compromise Between Type I and Type II Error Rates Associated with Repeated Trials

Consider a device with a Type I error rate of 2 percent and a Type II error rate of 1 percent. This means that a correct user will typically be rejected on 2 percent of his or her access attempts. A common assumption is that successive attempts are statistically independent. Then, the user's chance of being rejected on both of two successive attempts is only 2 percent of 2 percent, or 0.04 percent, which is low enough to present very little hindrance to the user. However, the assumption of statistical independence is certainly not valid for a properly functioning system, if there is a physical basis for the attribute having deviated somewhat on a particular day. Hence, the 0.04 percent number is lower than will be experienced. Nevertheless, the user will have a better chance to be accepted as extra trials are allowed. However, the imposter acceptance rate also becomes larger. Under the assumption of statistical independence between trials and the Type II error rate of 1 percent assumed here, the chance of being accepted with two trials is approximately 2 percent, three trials is 3 percent, and so forth. As before, the assumption of statistical independence is not strictly applicable. Nevertheless, the imposter's chances of being accepted are definitely increased as more trials are allowed.

As is shown in appendix B, the use of two trials can have the effect of either improving the Type I error rate at the expense of the Type II error rate, or vice versa; they cannot both be improved simultaneously. However, the use of three trials affords the possibility of a substantial improvement in both the Type I and the Type II error rates at the same time. By requiring success in two out of three attempts, the chance of falsely rejecting a correct user can be reduced to 0.12 percent, while the chance of falsely accepting an imposter can be reduced to 0.03 percent, for the assumptions stated previously. Furthermore, if the user succeeds on the first two trials, it is not necessary to require the third trial, thus saving time and effort.

4.5.2 Improvement Due to Multiple Trials

The above example shows that, ***if an identity verification process is fairly good to start with, then by applying it iteratively, its effectiveness in discriminating between correct individuals and imposters can be substantially improved, PROVIDED THAT THE TRIALS ARE STATISTICALLY INDEPENDENT.*** The degree of improvement can be worked out statistically for any number of iterations, using various decision rules to establish the required performance levels. Since this basic assumption is never precisely true, the degree of improvement can vary drastically. As a practical matter, ***repeated trials can make a good system's error performance better, but they cannot make poor performance good.***

4.6 Verification Based on Multiple Personal Attributes

Because of the imperfect operation of the various presently available identity verification devices based on personal attributes, the strategy has been suggested that more than one device be used, in order to more accurately discriminate between correct users and imposters [REVI 75]. In order to realize an improvement, the decision rules that are to be applied must be chosen to meet the system objectives. If two devices are used, it is not possible to simultaneously improve both the Type I and Type II error rates, as shown in table I.

Table I

Combining two identity verification devices

	Assumed Values	
	Device A	Device B
Type I error rate	3%	4%
Type II error rate	1%	2%

Performance of Device A and Device B assumed to be statistically independent.

Rule 1: Access granted if accepted by either device—
Probability of correct user being rejected: 3% × 4% = 0.12%
Probability of imposter being accepted: 1% + 2% = 3%*

Rule 2: Access granted only if accepted by both devices—
Probability of correct user being rejected: 3% + 4% = 7%*
Probability of imposter being accepted: 1% × 2% = 0.02%

*Simplified calculations are shown, based on approximations which apply when both error probabilities are small.

It will be observed that with two devices there are only two available decision rules. Rule 1 accepts the person if either device accepts the person and thus greatly reduces the chance of false rejection (0.12%) at the expense of an increased chance of accepting an imposter (3%). Rule 2 accepts the person only if both devices accept the person, thereby greatly decreasing the chance of accepting an imposter (.02%) at the expense of an increased chance of false rejection (7%). Of course, if each device has a variable threshold, then these may be varied to achieve an acceptable overall system.

A possible alternative, when two devices are used, is to establish the rule that a person will be granted access if accepted by both devices, and denied access if rejected by both devices. However, if the two devices are in disagreement, an alternative verification procedure will be invoked, such as calling upon the system security officer to confirm the identity. Following this procedure, the lower figures can be realized for both the Type I and Type II error rates.

4.7 Combining of Different Methods of Identity Verification

It is, of course, possible to combine the use of different methods of identity verification. The previous discussion referred to devices based on personal attributes. A system might use one device based on an attribute and one based on passwords, or a token, such as a plastic card. A commonly encountered system is the banking terminal which makes use of a magnetic stripe card and a PIN (Personal Identification Number). The PIN is a type of password. When identity verification based on personal attributes becomes established, a person could, upon logging in, be asked to verify his or her identity both via an attribute and via one of the other methods. In assessing the degree of security offered by these combined techniques, the procedure is similar to that described previously. The probabilities for the separate techniques are combined using the appropriate statistical techniques to obtain the resulting probabilities for the combined techniques. As before, the results are dependent on the decision rules that are applied. A major problem in quantifying the error rates in this approach is the difficulty of estimating the Type II error rate realistically. For example, it is dependent on the probability that a user will lose his or her card.

4.8 Examples of Attributes Used for Authentication

Several methods of identity verification based on personal attributes are discussed in appendix C, as examples of the present technology. This is quite an active field of development and other implementations may occur using the same or other attributes. In the test results which have been published to date, ***no one particular technique has emerged as being clearly superior in all aspects,*** considering effectiveness in distinguishing among individuals, length of time required for recognition, acceptance by users, cost, and other factors [BISS 77.1]. Some of

the equipment tested to date has been in the form of developmental models or laboratory prototypes, and this usually has implications with respect to performance.

5. IDENTIFICATION OF REMOTE DEVICES

Terminals and other remote devices can be equipped with circuitry which will respond to an interrogation command and transmit an identification code for the device. This code may be a simple identification scheme which merely identifies the type of device, or it may be a security code uniquely identifying that individual unit [MART 73, ANDE 72]. This can be a useful safeguard against an unauthorized terminal or device masquerading as an authorized one. There is more chance for this to occur on switched networks because of the ability to communicate between arbitrary points. However, even in a hard-wired network, an imposter terminal might be attached by some means such as a wiretap.

The use of a built-in code to identify a terminal or device does not provide much security if an eavesdropper can discern the code by prying into the terminal or by means of a wiretap, and then falsify the code using a device of his or her own. Therefore, the circuitry which generates the code in the device should be ***protected by a tamper-resistant housing,*** and the transmission should be ***protected by encryption.***

6. THE ROLE OF ENCRYPTION IN NETWORK ACCESS CONTROL

The use of encryption to protect information communicated between computer systems and remote terminals is currently receiving much attention [FPUB 46, SPUB 27, SPUB 54, DIHE 76, RISA 78].

Encryption may be used to preserve the confidentiality of information being transmitted and can aid in safeguarding against various threats such as ***wiretapping, electronic eavesdropping, misrouting, substitution, modification, and injection of messages.*** Data files can also be safeguarded by encryption techniques [SYKE 76].

Encryption is achieved either through a secret process (that is, the manner in which data is transposed and/or substituted) or through a commonly known process which depends on a secret parameter (called a "key") used by the process. In order to allow compatibility of encryption processes within the typical variety of network components, the latter method is strongly recommended. The encryption process is generally specified in an algorithm (a set of rules or steps for performing a task). Decryption is the inverse process. Even with encryption, it might still be possible for an imposter to ***imitate encrypted responses of a fixed nature if they were always the same.*** However, it is a relatively simple matter in a system to use numbering schemes in the dialogue that would cause ***identical information to be encrypted differently,*** in a manner that would be, in practice, impossible for an imposter to imitate.

The encryption algorithms used for communications security are not discussed in this Guideline. Information on this subject may be found in the references [FPUB 46, SPUB 27, SPUB 54, DIHE 76, RISA 78]. The use of encryption is often appropriate for controlling access to computer networks. One of the uses for encryption in this connection is to protect information which must be transmitted in order to verify the user's identity. Secret identification information (e.g., passwords) must be protected from disclosure, and nonsecret identification information (e.g., signature characteristics) must be protected from replacement and repetition. Encryption algorithms may be used as a means of achieving "digital signatures," which are, in effect, a means of verifying the identity of message senders and recipients. These two uses of encryption are discussed separately below.

6.1 Protection of Information Used for Identity Verification

When passwords or other information known to an authorized user are entered into a system to verify the user's identity, ***it is possible for a perpetrator to intercept that information*** by some means, such as a wiretap. The perpetrator can then use that information to ***impersonate the authorized user.*** To guard against this threat, the keyboard and/or terminal used to enter the secret information should be ***safeguarded against tampering,*** so that the information cannot be tapped while it is in the clear. ***Encryption can be used to protect the information*** from the point where it leaves the keyboard or terminal and is transmitted to its destination. In cases

where encryption is being used for protecting the working information being transmitted to and from the terminal, this same encryption capability may be suitable for protecting the verification information. The encryption process used for protecting the verification information must have provisions for causing the information to be ***coded differently with each transmission*** [SPUB 27]. Otherwise, a perpetrator might record the encrypted information from a point in the transmission path and spoof the system simply by injecting that same encrypted information, without ever having to decrypt it. Encryption systems generally have provisions for achieving the required variability.

When a personal attribute is used for identity verification, a set of measured values are obtained and digitized and used for comparison with a reference profile. This information, in clear form, can be used by a skillful perpetrator to ***simulate the data obtained from an authorized user***, thereby deceiving the verification process. To guard against this threat, the device which measures the attribute should be ***safeguarded against tampering***, so that the measured data cannot be tapped while it is in the clear. ***Encryption can be used to protect the information*** from the point where it leaves the device and is transmitted to its destination. Verification systems based on personal attributes are configured in a variety of ways. In one configuration, the measuring device sends the measured values to a central system where the reference profile is stored and where the comparison takes place. In this case, the measured values should be encrypted for transmission to the central system. In another configuration, the reference profile is sent to the measuring device with the comparison taking place in the device. In this case, the reference profile should be encrypted to prevent a perpetrator from being able to inject a reference profile of his or her own. Also, the device will produce a pass/fail signal, based upon the results of the comparison, and this will be transmitted elsewhere, such as back to the central system which controls network access. ***This pass/fail signal should also be encrypted***; otherwise, a perpetrator might be able to simulate this signal and produce a false pass response without ever having to deceive the measurement device.

Generally, the personal attribute sensing device will be either an integral part of a remote terminal or will be closely associated with such a terminal. Precautions should be taken to assure that the equipment ***enclosures are tamper-protected*** and that there are ***no exposed leads*** which would permit a perpetrator to tap sensitive information which could be used to deceive or circumvent the verification equipment.

6.2 Digital Signatures

One form of authentication is the "digital signature," in which the sender of a message attaches a coded identification to the message, enciphered in such a manner that only the intended recipient can decipher the signature, thereby verifying the identity of the sender to the intended recipient. A method for carrying this out using the Data Encryption Standard (DES) is described in NBS Special Publication 500-54, "A Key Notarization System for Computer Networks" [SPUB 54]. This method is based on making use of individual station identifiers in the process of encrypting keys which in turn are used for encrypting messages between the stations. Because of the hardware arrangements and operating procedures used with this system, it is possible for a sender to encipher a signature (or any other message) in such a way that only the prearranged recipient can correctly decipher it.

Digital signatures may also be achieved through the use of proposed public key cryptosystems. These have not yet undergone security review for certification. In these systems, the encryption key (procedure) differs from the decryption key (procedure), and knowledge of the encryption key does not result in knowledge of the decryption key [DIHE 76, RISA 78, DEND 79]. (In contrast, the DES uses the same key for both encryption and decryption.) In public key cryptosystems, users may freely publicize the keys for encrypting messages which are to be sent to them; however, they keep secret the corresponding decryption keys.

The encryption and decryption procedures for some public key cryptosystems are inverses of each other. In normal practice, a message would first be enciphered for transmission and then be deciphered upon receipt to recover the information. However, the procedures in these systems may be applied in the reverse order, first using the decryption procedure to conceal the information, and then using the encryption procedure to recover it.

A secure digital signature may be achieved as follows. Assume that user A wishes to send a secure digital signature to user B. User A first passes the signature through A's own private decryption procedure, which, in effect, leaves it in unintelligible form. User A then enciphers the signature in this form using B's public encryption procedure (for privacy) and sends it to B. User B first deciphers the signature using B's secret decryption procedure. B then applies A's public encryption procedure, thereby recovering the digital signature. At this point, user B knows that the signature must have come from user A, since only A could have passed it through A's secret decryption algorithm. In practice, it is preferable to apply this process to entire messages, rather than just the authenticating signature, in order to prevent a valid signature from being attached to a falsified message. It is entirely feasible to handle complete messages in this manner.

7. AUTHORIZATION

While a full description of authorization is not the subject of this Guideline, a brief introduction is presented below for the reader who is not familiar with this area, and bibliographic references are indicated for further reading. Once the identity of a user has been established and authenticated, he or she may be granted access to the network and may request the use of various resources available via the network. These resources consist of various entities such as host computers, areas of main memory, files, programs, auxiliary memory devices, and instructions, and are frequently referred to as objects. ***Users must have proper authorization in order to be granted access to these objects*** [HNKF 78, GRDE 78, HSKM 79, HSBA 76]. Each user has an associated set of access privileges to which he or she is entitled, which may be called his or her capability profile. Similarly, each object has associated with it a set of requirements for its use, which may be called an access requirement profile. An access request is authorized when the requestor's capability profile matches the objects' access requirements profile.

7.1 Range of Capabilities

An object may have many ways in which it is capable of being used, such as reading data from a file, writing data into a file, creating a file, carrying out a transaction, executing a program, compiling a program, and invoking various operating system routines. Thus, there is a range of capabilities associated with an object, ***not all of which may be authorized for use by every user*** [HNKF 78, GRDE 78]. It is possible to visualize this situation as a

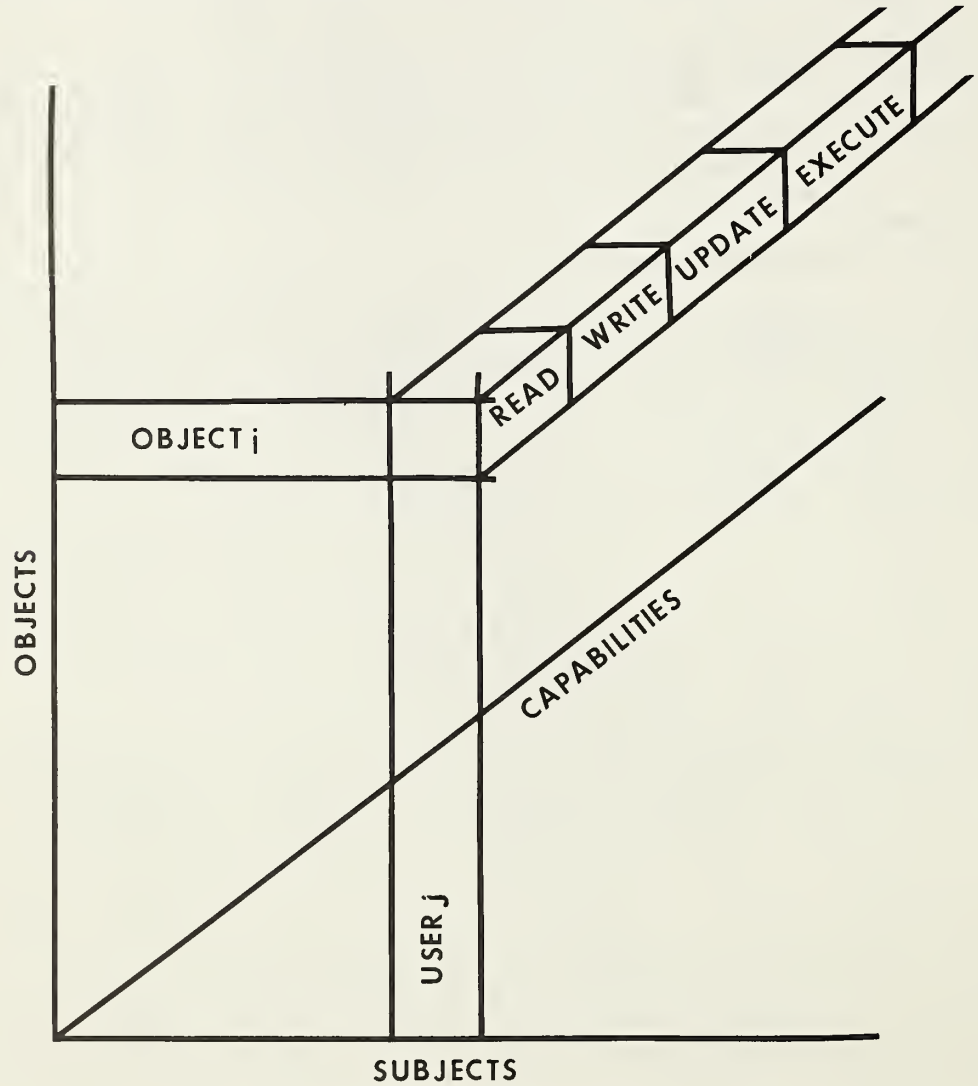

Figure 3. Access authorization matrix.

three-dimensional array, with users along one dimension, objects along another, and capabilities along the third, as shown in figure 3.

7.2 Levels of Access Control

It is useful to visualize access control and privacy protection in three levels, namely, 1) memory, 2) procedure, and 3) logical [HSBA 76].

1) ***Access control at the memory level*** regulates access to memory in terms of units of memory. Concern at this level is with defined regions of memory, rather than with the contents of memory. Consequently, everything within a defined region is subject to the same access control, as specified for that region. Furthermore, this protection applies to the contents only while they remain in the defined region. Protected regions of memory are typically defined by means of memory bounds registers or storage protections keys which control access to the bounded memory regions.

2) ***Access control at the procedure level*** regulates access to procedures, where a procedure is a set of programs and associated data. Access control at this level is concerned with the conditions under which programs can pass control from one to another. That is, the execution of programs must be monitored in terms of calls, returns, and the passing of parameters.

3) ***Access control at the logical level*** regulates access to structured data on the basis of logical entities such as fields, arrays, records, and files. These entities may have little resemblance to their physical or virtual storage images. The user is allowed to associate access control requirements and protection measures with logical units, thus the access control mechanism can facilitate direct control and protection of the information regardless of its location. A further advantage is that the user need not be familiar with the physical or virtual storage structure of the computer system.

Control mechanisms operating at the logical level must enable the user to specify shared and private data in terms of logical entities of the database. The user must be able to assign access rights and protection requirements to these entities, to specify the collections of these entities and access rights that other users may have, and to incorporate additional authentication and checking measures.

7.3 Access Authorization Principles

A set of access authorization principles which have been defined in [SPUB 21] are summarized here:

1. Least Privilege—No requestor shall have any access privileges which are ***not required to perform its function*** (need-to-know). As a corollary to this, access to resources shall be separated (compartmentalized) whenever such separation adds to security.

2. Least Common Mechanism—There shall be ***minimal shared (common) mechanisms,*** other than those that are expressly there for security purposes.

3. Reference Monitor Approach—Access control mechanisms must be such that they are: (1) ***always invoked,*** (2) ***isolated from unauthorized alteration,*** and (3) ***accredited as being trustworthy.***

4. Object Versus Path Protection—Protection can be provided to either the ***object itself*** and/or the ***path to the object.*** The network aspects are almost entirely path-oriented protection.

7.4 Composite Authorizations

Several entities are involved in almost every computer transaction, e.g., a person, a terminal, a HOST computer, and a process. Each of these entities must be authorized to either receive, process, or transport the information being handled. The logical intersection of these authorizations (in some situations, the authorizations may be other than the logical intersection, e.g., the use of statistical programs) will establish the level of information which can be sent via this sequence of entities, but a further step-by-step authorization check is also necessary to ensure that only the proper entity (or entities) are the ultimate recipients of the information, e.g., one entity may be authorized to process, but not to copy the information.

In some instances, a requestor will be connected to a HOST which will, in turn, need to access other resources on the requestor's behalf. This need can iteratively grow to the general Nth party authorization problem, which extends the previously discussed Nth party authorization problems [SPUB 21]. ***Authorization is a larger problem than authentication*** since the latter is strictly binary at each intermediate requestor. In contrast, the authorizations of each intermediate requestor may differ, as may the authorization needs when information is

processed at the different nodes along the chain. Two different approaches are possible: (1) continually subsetting the authorizations as necessary so that the final privileges are the intersection of those of the original requestor and all intermediate nodes, thereby ensuring that no intermediate node gets any information for which it is not authorized, and (2) handling the authorizations iteratively on a pair-wise basis, so that the Nth level will provide any requested information for which the N-1'st is authorized, and leave the burden of further controls on passing of data to the HOST. This approach allows the use of so-called "statistical programs" in which specific details are lost, e.g., "what is the average value of the class of xxx's," instead of "what is the value of a particular xxx" which might be sensitive. Of course, the latter may be the result of a cleverly devised statistical request, a well known problem that is outside the scope of this Guideline. For further discussion see reference [HOFF 77]. The possibility of such programs should be considered, in order that the network design be such that it can accommodate new advances if and when they become available.

7.5 Access to the Authorization Mechanism

The authorization mechanism is called upon whenever a user presents an access request for an object. The mechanism must therefore be readily accessible for frequent use. There will also be occasions when the mechanism must be modified to reflect changes in status for users and objects. It is evident that this mechanism has a ***critical security function,*** and it ***must be properly protected*** from unauthorized modifications [SPUB 21]. Detailed discussions of authorization mechanisms covering their design, use, and protection, are contained in NBS Special Publication 500-21, "Design Alternatives for Computer Network Security, Volume 1," by Gerald D. Cole [SPUB 21].

APPENDIX A

TYPES OF IDENTIFICATION TOKENS (CREDENTIALS)

A variety of machine-readable cards have been developed for access control purposes, and these may be conveniently described in terms of the method of encoding information on the card. With some of these cards, the coding can be altered rather readily in the field; with others, the coding is either built in or requires special factory equipment for alteration. The various types of cards or badges presently in use are described below. Many of these can also include printed material, photographs, and so forth, and can serve as identification badges as well. This information is from the "Entry-Control Systems Handbook," SAND77-1033, Sandia Laboratories, Revised September 1978.

A.1 Photo ID Badge

The most common credential is a color-coded badge with a facial photograph which can be checked visually by a guard. It is difficult to quantify the effectiveness of a photo ID badge system since inspection of the badge is very subjective and no known controlled tests have been made. It is commonly required that a laminated photo ID badge be used for access authorization in certain controlled areas. The laminated construction renders the badge resistant to tampering.

A badge exchange system minimizes the possibility of the badge being counterfeited, lost, or stolen. Under this procedure, duplicate badges are held at each entry-controlled point. When an employee requests entry, a guard matches the individual to the photograph on the corresponding exchange badge held at the entry-control point. If the comparison matches, the guard exchanges the badges and grants the employee access. The employee's badge is held at the entry-control point until the employee leaves the area, at which time the badges are again exchanged. In this way, the exchange badge worn within the controlled area is never allowed to leave the area. The badge exchange system does not, however, prevent someone from making up their face to match the image on a stolen badge in order to gain unauthorized access.

A.2 Optical-Coded Badge

The optical-coded badge contains a geometric array of spots printed on an insert laminated into the badge. Photodetectors in the badge reader detect the relative optical transmission of the spots and hence the code. To make this coded badge more tamper resistant, the pattern of spots can be concealed by making the badge opaque to visible light but transparent to infrared light. The spots are printed with ink which is opaque to infrared light. This technique offers good tamper protection and badges are reasonably difficult to counterfeit.

A.3 Electric-Circuit-Coded Badge

The electric-circuit-coded badge is a plastic laminated badge containing a printed circuit pattern that selectively closes electrical circuits when inserted into a badge reader. For this credential, the badge reader is simply a card-edge connector normally used for a printed circuit board. The badge can be decoded with a simple electrical continuity tester and, consequently, counterfeit badges can be easily fabricated.

A.4 Magnetic-Coded Badge

Several magnetic-coded badge systems are presently in wide use. This badge contains a sheet of flexible magnetic material on which an array of spots has been permanently magnetized. The code is determined by the polarity of the magnetized spots. The badge reader contains either magnetic sensors which are interrogated electrically or magnetic reed switches which are mechanically actuated when a magnetic spot with the proper polarity is located adjacent to the reed. The magnetic spots can be accidentally erased if the badge is placed in a sufficiently strong magnetic field. However, field experience has shown that this is not a significant problem. The amount of data which can be encoded on this type of badge is limited to approximately 60 bits of information. Since it is possible to build equipment to recode or duplicate the pattern of magnetic spots, fabrication of a false credential is possible. It is more difficult, however, to falsify this type of credential than to fabricate an electric-circuit-coded badge.

A.5 Magnetic-Stripe-Coded Badge

Magnetic-stripe encoding is widely used in commercial credit card systems, and numerous vendors manufacture equipment which is compatible with the American National Standard Institute (ANSI) standards for this technique. With the magnetic-stripe-coded badge, a stripe of magnetic material located along one edge of the badge is encoded with badge data. These data are then read as the magnetic stripe is moved past a magnetic read head. Credential forgery is relatively easy since data from the magnetic stripe can be decoded and duplicate badges encoded by the use of parts from a common magnetic tape recorder.

Three materials have been utilized as the magnetic-stripe medium. The most common material, a single-layer, 300-oersted magnetic stripe, has proven susceptible to accidental erasure. The second material, a dual-layer, 300/4000-oersted tape, provides erasure protection on the 4000-oersted layer; however, accidental writing on the 300-oersted layer may present a problem. The third material, a single-layer, 4000-oersted tape, is impervious to accidental erasure.

Two types of encoding are specified in the ANSI standard for magnetic-stripe encoding. These are described in the following standards:

> American National Standard Specifications for Credit Cards, X4.13-1971, American National Standards Institute, 1971
>
> American National Standard Magnetic-Stripe Encoding for Credit Cards, X4.16-1973, American National Standards Institute, August 1973

One type, the American Bankers Association (ABA) standard, allows up to 40 numeric characters. The other, the International Air Traffic Association (IATA) standard, has up to 90 alphanumeric characters. The use of alphanumeric IATA coding allows the badge holder's name to be included in addition to a badge number. One disadvantage of the 90-character data encoding, however, is that more accurate reader spacing and alignment are required.

A.6 Passive-Electronic-Coded Badge

The passive-electronic-coded badge is a badge into which electrically tuned circuits are laminated. In order for the code to be read, a swept-frequency, radio frequency (RF) field is generated and then the frequencies at which significant energy is absorbed are detected. These frequencies correspond to the resonant frequencies of the tuned circuits and are decoded to give a unique badge number or code. An important advantage of this technique is that the badge does not need to be inserted into a reader mechanism but can simply be placed near the antenna which serves as the read station. The disadvantages are (1) badges can be decoded with common RF test instruments, allowing counterfeit badges to be fabricated, and (2) the number of unique code combinations is limited to a few thousand.

A.7 Capacitance-Coded Badge

The capacitance-coded badge is a badge into which an array of small conducting plates is laminated. Selected plates are connected and the code is read from the badge by an electronic reader which measures the capacitance of the plates and distinguishes which plates are isolated and which are connected.

A.8 Metallic-Strip-Coded Badge

The metallic-strip-coded badge utilizes rows of copper strips which are laminated in the badge. The presence or absence of strips in the rows determines the code pattern, which is read from the badge as it passes through an eddy-current sensor. This technique was developed for use with the Controlled Access by Individual Number (CAIN) system. The badges are durable and can be read reliably. In addition, each badge can be encoded with approximately 40 data bits.

A.9 Active-Electronic Badge

The active-electronic badge system consists of a portable, electrically coded badge and a stationary interrogation unit. The interrogation unit supplies power to the badge by magnetic induction and receives and decodes the credential number transmitted from the badge.

When the interrogation unit is placed at strategic locations, such as corridors or doorways leading to the controlled areas, the system can automatically monitor, identify, and log the individual badge entering or leaving that particular area. The employee is not required to take any action whatsoever to accomplish the badge reading since the badge is read automatically when the employee passes through the RF field generated by the interrogation unit.

INFLUENCE OF MULTIPLE TRIALS ON ERROR RATES FOR AUTHENTICATION BASED ON PERSONAL ATTRIBUTES

Because of the limitations in identity verification devices based on personal attributes, it may be necessary to provide users additional opportunities for authentication, in the event they fail to be properly verified on the first attempt. However, it is important to recognize that this also provides an advantage to the imposter who is attempting to gain access by impersonating an authorized user. In this appendix, several illustrative examples are given to show the effect of applying various decision rules, where multiple trials are allowed.

B.1 Allowing Two Trials

For the case of two trials, several decision strategies are possible, as shown in table I.

Table I

Permit two trials to gain access

Illustrative Assumptions:
Type I error rate = 2%
Type II error rate = 1%
Statistical independence assumed among trials.
Rule 1: Access granted if either trial succeeds—
Probability of correct user being rejected: 2% × 2% = 0.04%
Probability of imposter being accepted: 1% + 1% = 2%*
Rule 2: Access granted only if both trials succeed—
Probability of correct user being rejected: 2% + 2% = 4%*
Probability of imposter being accepted: 1% × 1% = 0.01%

*Simplified calculations are shown, based on approximations which apply when both error probabilities are small.

It can be seen from the figures in table I that, by allowing two trials, it is possible either to greatly benefit the correct users, while at the same time easing the task of the imposters (Rule 1), or to greatly enhance the rejection of imposters at the expense of increased inconvenience to the correct users (Rule 2).

Rule 2 requires two trials, thereby increasing the time to carry out the verification process. With Rule 1, the process can be terminated after the first trial for correct users, if they pass the first trial. This is quite a savings in effort, since the likelihood of being rejected is small to start with, so only an occasional second trial will be required. To recapitulate, ***using two trials it is possible to improve the performance for one category of individual at the expense of the other,*** but not to improve the performance for both categories simultaneously.

B.2 Allowing More Than Two Trials

By increasing the number of trials, a greater variety of decision rules become available, and it becomes possible to improve the performance for both categories of individuals simultaneously, as described in the following discussion.

Consider the use of (up to) three trials. Now the decision rules can be to accept a person if he or she passes one trial, two trials, or all three trials. The effects of these various rules are tabulated in table II.

Table II

Permit (up to) three trials to gain access

Illustrative assumptions:
Type I error rate = 2%
Type II error rate = 1%
Statistical independence assumed among trials.

Rule 1: Access granted if a single trial succeeds—
Probability of correct person being rejected: 2% × 2% × 2% = 0.0008%
Probability of imposter being accepted: 1% + 1% + 1% = 3%*

Rule 2: Access granted if two trials succeed—
Probability of correct person being rejected: 0.12%
Probability of imposter being accepted: 0.03%

(The calculations for Rule 2 are a bit more difficult than for Rules 1 and 3, involving the tabulation of various possible outcomes.)

Rule 3: Access granted only if three trials succeed—
Probability of correct person being rejected: 2% + 2% + 2% = 6%*
Probability of imposter being accepted: 1% × 1% × 1% = 0.001%

*Simplified calculations are shown, based on approximations which apply when both error probabilities are small.

Observe, from the figures in table II, that for Rule 2, requiring at least two successful trials, the performance is greatly improved for both categories of individuals. Thus, the chance of false rejections for correct users is decreased from 2 percent to 0.12 percent, while the chance of accepting an imposter is decreased from 1 percent to 0.03 percent. These results are dependent on statistical independence among trials, and in actuality the improvements would probably be less dramatic, but nonetheless significant. Using Rule 2, it is only necessary to achieve two successful trials in order to determine acceptance. Thus, if the first two trials are successful, a third trial is not required, which expedites the process.

APPENDIX C

EXAMPLES OF PERSONAL ATTRIBUTES USED FOR AUTHENTICATION

Several methods of identity verification based on personal attributes are discussed in this appendix. This is quite an active field of development and various implementations using these or other attributes may be encountered. In the test results which have been published to date, ***no one particular technique has emerged as being clearly superior in all aspects***, considering effectiveness in distinguishing among individuals, length of time required for recognition, acceptance by users, cost, and other factors [BISS 77.1]. Some of the equipment tested to date has been in the form of developmental models or laboratory prototypes, and this usually has implications with respect to performance.

C.1 Fingerprints

Verifying identity by manual fingerprint comparisons is a well-known technique widely used in forensic work as well as routine checking of applications for certain types of employment. Inked fingerprint impressions on cards are generally used and the comparisons are made by skilled examiners. As a result of this experience, the uniqueness of fingerprints has been well established [ELEC 73]. Fingerprints are compared mainly on the basis of "minutiae," which are the various detailed features that can be discerned by an examiner, such as the ridge endings and bifurcations exhibited by the friction ridges.

A fingerprint may contain up to 150 minutiae, with a typical print having 40 to 60 minutiae. These may be described in an X-Y coordinate system in which the coordinates of the minutiae are indicated, as well as certain feature information, such as the angle at which the ridges lie at that point and the type of feature (ridge ending, bifurcation, trifurcation, island, dot, etc.). Fingerprint impressions are invariably distorted, and some minutiae may be obscured or false minutiae may arise due to variations in inking or obtaining impressions. A skilled examiner can often make allowances for these distortions and, given sufficient features, can make a positive decision as to whether two prints do or do not match. The number of minutiae available, together with the feature information, make fingerprints an extremely rich source of information, and they are intrinsically capable of being used to distinguish among the members of an indefinitely large population. From a practical standpoint, however, distortions produce a considerable amount of variation.

In the last 15 years, research and development efforts have addressed the automation of fingerprint matching for verifying personal identity. Equipment has been produced which permits an image of the fingerprint to be obtained without the use of ink, and then compares this image, or details extracted from it, with information in a reference file. Two basic viewpoints have been relied upon to perform this function. In the first, a direct comparison is made between the "live" print and a file print. This may be performed, for example, by means of optical correlation and a score obtained which indicates the degree of match. To allow for possible variation in the placement of the finger, the file print is rotated slightly during the comparison to obtain the best alignment. This approach has the disadvantage of requiring a file of actual print images, together with a mechanism for rapidly selecting and positioning the print images in the device. If this approach is implemented as a total comparison of the "live" print and the reference print, considerable distinguishing information is lost. If selected portions of the images are employed, the approach becomes susceptible to variations in position and distortion. It has the advantage of relative simplicity. Careful evaluation of devices based on this viewpoint is suggested.

The second viewpoint relies on signal processing (for example, signal processing on a digitized image) to extract information about the location and direction of the minutiae and then compares this information with a list of minutiae from a reference file. A typical minutia list employs one to three 8-bit bytes per minutia and consists of a few hundred bytes of data for a print. With redundancy extraction and small files this can be reduced by an order of magnitude for the finger, to a few hundred bits. Digital processing is used both for extracting the candidate minutiae (generally facilitated with special hardware) and for performing the matching process (generally carried out by computer algorithms) [ELEC 73, STOC 75].

A list of minutiae may be extracted at the individual terminal or at a central facility. The latter approach requires a high bandwidth to the central facility; extraction at the terminal is feasible both technically and economically. Once the minutia list has been extracted, there are three ways to proceed. First, the device may have stored in it the minutia files for all valid users, and can retrieve the designated file for comparison purposes. (The designated file is that corresponding to the user's claimed identity.) Second, the device could call for the designated

minutia file to be transmitted from a central computer located in a secure area, and then perform the comparison locally. Third, the device could transmit the minutia list to the central computer where the comparison would be carried out. Appropriate forms of transmission security should be employed for the data in transit [SPUB 27]. The third method has the advantage that it does not require file storage in the device and reference files may be stored in a secure location. For reasonable data transmission speeds, such as 1200 or 2400 baud, the time to transmit the minutia list can easily be less than one second.

It is feasible to scan a finger and carry out the comparison in about one second. To this must be added the time to key in a claimed identity (or insert a card bearing this information) and the time to position the finger on the measuring surface. In addition, if a match is not obtained the first time, it may be necessary to reposition the finger one or more times, and to switch to an alternate finger if a match is not achieved on the first finger. The number of retries adds significantly to the time, if this occurs very often.

The most extensive testing of an automatic fingerprint system reported to date is that performed under the BISS program [BISS 77.4]. In this program, during the field tests, the fingerprint equipment exhibited a Type I error rate of 6.5 percent, a Type II error rate (casual imposters) of 2.3 percent, and an average verification time (including retries where encountered) of 8.9 seconds. This device was designed and built by one manufacturer a number of years ago and at this time is no longer available. No other public test data are available with which to judge the representativeness of these error rates but the basic technology should be capable of significantly better performance.

C.2 Hand Geometry

The shape of a person's hand (hand geometry) has been found to exhibit sufficient interpersonal variability to serve as a basis for distinguishing one individual from another to a useful level of accuracy. Equipment has been developed which automatically measures one aspect of the hand, namely the lengths of the fingers, and uses this information as a means of verifying a person's identity. The measurement process employs certain subtleties, such as starting the measurement at a point determined by the rounding at the end of the finger and ending at a point determined by the translucency of the web between the fingers [BEPR 77]. A device of this type has been in production for several years and is in use in a number of installations for entry control purposes. In one form of the device, the user carries a magnetic stripe card on which an ID number and his or her finger length data have been recorded. The data on the card is scrambled so that it would be difficult for an unsophisticated person to devise a way to circumvent the device. In order to use the device, the user inserts his or her card in a slot in the device and then positions his or her hand on the measuring surface with each finger resting in a slight groove. The device then measures the finger lengths to obtain four 3-digit numbers which are compared with data deciphered from the card. The measurement and comparison process occurs in less than one second. An output signal from the device, indicating pass or fail, can be used for any desired purpose. The device can also be connected to a central computer which stores the reference data and does the comparison. In this case, the users could enter their claimed identification numbers either by means of a card or a numeric key pad. This information would be transmitted to the central computer along with the measured finger length data. If the device were used with a remote terminal, the users could first log onto the terminal, establishing their claimed identity via the terminal. They would then be presented with a message asking them to verify their identity, whereupon they would place their hand on the hand geometry device, causing a set of finger measurements to be sent to the central computer. Upon proper verification, they would be allowed to proceed with the use of their terminal; otherwise, they could be denied access to the network. Appropriate transmission security should be used to protect the data in transit.

The readout from the hand geometry device consists of four 3-digit numbers. In order to assess its ability to discriminate among the members of a population, it is necessary to determine the degree of repeatability for a given individual, and the degree to which people's finger lengths tend to cluster around normal values. Repeatability varies somewhat among individuals; that is, most individuals measure quite consistently (within a few parts per thousand), while a few individuals exhibit somewhat more variability (perhaps 10 or 15 parts per thousand). This seems to be characteristic of devices based on personal attributes: most of the failures to correctly recognize an individual are associated with a small percentage of the population. When a computer is used for maintaining the reference file and doing the comparisons, it is possible to establish different tolerance limits for different individuals. The tolerances may be tightened for those individuals who are very consistent and relaxed for those who are more erratic. While it is possible to do this, it must be recognized that a clever penetrator will make it a point to find out who has the broadest tolerances in order to make his or her task easier. Therefore, if any tolerances are relaxed, these are the ones that should be used in assessing the system security. The use of a computer makes it possible to track gradual changes in a person's measurements, if these should occur. Such procedures work well for systems which perform well, but can

cause degradation with a poor system, since noisy measurements quickly distort the reference file. A further degree of discrimination can be gained by measuring both hands, first one and then the other.

Other hand features have been studied for possible application as identity verifiers, such as the general contour of the hand, or the visible features, such as skin creases in the palm. The goal is to establish a set of features which have a high degree of information richness, are easily sensed by automatic means, are highly repeatable for the same individual, and differ significantly over the members of a population [FONS 77].

C.3 Signature Dynamics

In recent years there have been a number of brief examinations and several significant efforts to derive electrical signals during the process of writing a signature that could be analyzed by a computer as a means of verifying identity. These efforts have demonstrated that the physical motions which occur during the writing of a signature can be used to distinguish one individual from another with very reasonable Type I and Type II errors. The writing of a signature is a conditioned reflex and is done with little conscious attention to the formation of the string of characters comprising the signature [CRWO 77]. Signatures frequently become so stylized that it is difficult or impossible to separately recognize the individual characters forming the signature. Because of this, it is difficult for one person to mimic the dynamic motions associated with another person's signature. The act of mimicking requires conscious control, and conscious control has associated with it characteristics which differ from reflexive behavior.

The information in the dynamics of the signature is considerably more than that which is found in the static signature image. A device which scans the written signature and compares it against a reference copy can be easily deceived by a copy of the signature or a carefully drawn signature. The use of signature dynamics involves time-varying motions and forces which are difficult to perceive and to mimic.

There are various ways of obtaining signals which represent the dynamics of a signature. The quantities which may be measured during the writing process through suitable instrumentation are positions, forces, and accelerations. Instrumentation may be designed into the writing instrument (stylus) or writing surface (platen), or a combination may be used. The instrumentation may be applied to one, two, or three axes of motion [NRDC 75, STER 75, HELl 77, CRWO 77].

Time-varying position information may be derived by using an instrumented writing surface which can read out the coordinates of the stylus at a suitable sampling frequency. It is important to measure the time of these position measurements, rather than to use only the sequence of X-Y coordinates, since the dynamic information is important [NRDC 75].

Time-varying force information may be obtained either from an instrumented stylus or platen [CRWO 77, STER 75, LIHA 79]. The measured forces arise from two sources:

(1) the pressure supplied by the hand to the stylus which, in turn, presses on the writing surface, and
(2) the drag forces resulting from friction as the stylus is pushed along the surface.

It is not necessary to distinguish between these forces, though various implementations may utilize them in varying degrees. The important consideration is for the instrumentation to produce a consistent, repeatable output for a given input, and for the output signals to contain a sufficient quantity of information to enable the desired degree of discrimination to be obtained.

Handwriting exhibits rapid changes in velocity (acceleration), and rapid changes in acceleration (jerk). These can be measured with suitable transducers mounted in the stylus [LIHA 79].

One automatic signature verification system was tested under the BISS program [BISS 77.3]. In this program, during the field tests, the signature equipment exhibited a Type I error rate of 1.9 percent, a Type II error rate (casual imposters) of 5.6 percent, and an average verification time of 13.5 seconds. The equipment tested in this program used an instrumented platen which derived a single force measurement normal to the writing surface.

A stylus with more extensive instrumentation has been developed at the IBM Thomas J. Watson Research Center [LIHA 79]. This device measures two orthogonal components of acceleration, as well as the writing pressure on the pen cartridge. In a field test, this equipment exhibited a Type I error rate of 1.7 percent, and a Type II error rate of 0.02 percent for casual imposters. In deliberate forgery attempts, a Type II error rate of 0.4 percent was exhibited.

C.4 Speaker Verification

If all aspects of human speech are considered, the result is sufficiently complex and exhibits sufficient variation from one person to another to make it a candidate technique for distinguishing the members of a large population. The computer is an effective tool for analyzing the many subtle distinctions between one person's speech and

another's, and can therefore be used in a system to verify identity by means of the voice. Speech may be viewed as being made up of a series of transitions separated by regions of varying duration in which the sounds are relatively "steady" [WMMZ 75]. These regions are mainly due to vowels. The transitions have a "noisier" quality, coming from the various consonants. During the "steady" regions, the sound is influenced by the structure of the individual's vocal tract, throat, mouth, and nasal passages. This results in resonances and a harmonic structure which is partly controllable and partly inherent to the individual. In analyzing a person's speech for identity verification by a computer, the "steady" regions have often been employed. While the steady regions contain most of the speech energy, most of the information about what is being said is contained in the transitions, and the way in which individuals use their tongue, lips, and teeth is lost. This drastically reduces the size of the data base at any given level of reliability.

In order to establish references for comparison, a person to be enrolled first creates a reference file in the computer by repeating a "training set" of selected utterances a number of times. These utterances are spoken into a microphone and the resulting signal is digitized and sent to the computer. Various kinds of processing via special hardware may be done before or after digitizing. The computer builds a reference file for each of the utterances in the training set. Thereafter, when the person wishes to verify his or her identity, the computer requests that he or she repeat these utterances, whereupon it matches the new data against those in its reference file.

In order to prevent an imposter from simply recording a valid user's voice and playing it back to gain access, a specific strategy must be used [DODD 75]. For example, when the person enrolls, the training set is made up of utterances from each of four categories, such as adjectives, nouns, verbs, and adverbs. Then, when the person wishes to verify his or her identity, he or she is asked to repeat phrases made up by selecting a phrase at random from these categories. A sample phrase might be "Young Ben swam far." The words each have one syllable and have a prominent vowel sound. The computer can thus readily isolate the appropriate regions for making its comparisons. If another try is required, another random phrase is generated. Use of recordings is thus effectively thwarted for all but the most sophisticated penetrator. Unfortunately, this type of penetrator is of great interest from the point of view of system security.

The matching of features from speech by computer is done by processing algorithms which rely on a data base to characterize the desired response to an input. If a successful intrusion effort should be discovered, it would be possible, if a record had been kept of the original speech input, to analyze the successful deception, determine how it had been able to succeed, and refine the algorithms further to prevent a recurrence. It is also possible to track a person's voice in order to adapt to slow changes, such as might occur with aging or with growing familiarity with the system. Recognition by voice generally will present problems when a person has a health problem affecting the voice, such as a cold or laryngitis.

One approach to an automatic speaker verification system was tested under the BISS program [BISS 77.2]. In the field test, it exhibited a Type I error rate of 1.1 percent, a Type II rate of 3.3 percent, and an average verification time of 6.2 seconds. The four-word phrases took about 2 seconds to speak. The system pronounces the phrase first, and then the subject repeats it back. This consumes about 4 seconds (for verification with a single phrase). In the field test, an average of about 1.5 phrases were required for verification, accounting for the average verification time of 6.2 seconds. In this test 15.8 percent of the test subjects accounted for all of Type I errors. This is consistent with the expectation that the performance of the system is not uniform for a population, but that a minority of the population experiences all of the difficulty, presumably due to an unusual degree of variability for these individuals. Since the BISS tests were among the first to be conducted on this scale, considerable improvement is possible as these test results are analyzed and used to enhance the performance.

BIBLIOGRAPHY

[ANDE 72] Anderson, James P., "Information Security in a Multi-User Computer Environment," Advances in Computers, Vol. 12, Academic Press, Inc., New York, NY, 1972, pp. 1-36.

[BEAR 72] Beardsley, Charles W., Is Your Computer Insecure? IEEE Spectrum, IEEE, Inc., New York, NY, January 1972, pp. 67-78.

[BECK 78] Becker, Hal B., Security in the Distributed Environment, Computer Security and Privacy Symposium, Honeywell Corporation, Phoenix, AZ, April 1978.

[BEPR 77] Bean, Charles H., and James A. Prell, Personnel Access Control, Proceedings of the 1977 Carnahan Conference in Crime Countermeasures, UKY BU112, April 1977, ORES Publications, College of Engineering, University of Kentucky, Lexington, KY, pp. 7-17.

[BEQU 78] Bequai, August, Computer Crime, Lexington Books, D. C. Heath and Company, Lexington, MA, 1978.

[BISS 77.1] Fejfar, Adolph, Test Results—Advanced Development Models of BISS Identity Verification Equipment, Vol. I, Executive Summary, MTR-3442, Vol. I, The MITRE Corporation, Bedford, MA, September 1977.

[BISS 77.2] Foodman, Martin J., Test Results—Advanced Development Models of BISS Identity Verification Equipment, Vol. II, Automatic Speaker Verification, MTR-3442, Vol. II, The MITRE Corporation, Bedford, MA, September 1977.

[BISS 77.3] Fejfar, Adolph, Test Results—Advanced Development Models of BISS Identity Verification Equipment, Vol. III, Automatic Handwriting Verification, MTR-3442, Vol. III, The MITRE Corporation, Bedford, MA, September 1977.

[BISS 77.4] Benson, Peter, Test Results—Advanced Development Models of BISS Identity Verification Equipment, Vol. IV, Automatic Fingerprint Verification, MTR-3442, Vol. IV, The MITRE Corporation, Bedford, MA, September 1977.

[BISS 77.5] Fejfar, Adolph, and Peter Benson, Test Results—Advanced Development Models of BISS Identity Verification Equipment, Vol. V, Miscellaneous, MTR-3442, Vol. V, The MITRE Corporation, Bedford, MA, September 1977.

[CMSC 78] Development of Secure Systems—Introduction, The Information Technology Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 1-5.

[CRWO 77] Crane, Hewitt D., Daniel E. Wolf, and John S. Ostrem, "The SRI Pen System for Automatic Signature Verification," Proceedings of the Trends and Applications Symposium 1977: Computer Security and Integrity, IEEE Computer Society, New York, NY, May 19, 1977, pp. 32-39.

[DEND 79] Denning, Dorothy E., Secure Personal Computing in an Insecure Network, Communications of the ACM, Association for Computing Machinery, New York, NY, August 1979, pp. 476-482.

[DIHE 76] Diffie, Whitfield, and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, IEEE, Inc., New York, NY, November 1976, pp. 644-654.

[DIMA 79] Dixon, N. Rex, and Thomas B. Martin, Eds., Automatic Speech and Speaker Recognition, IEEE Press, New York, NY, 1979.

[DODD 75] Doddington, George R., Speaker Verification for Entry Control, Wescon Technical Papers, Los Angeles, CA, 1975.

[ELEC 73] Eleccion, Marce, Automatic Fingerprint Verification, IEEE Spectrum, IEEE, Inc., New York, NY, September 1973, pp. 36-45.

[FITZ 78] Fitzgerald, Jerry, Internal Controls for Computerized Systems, Jerry Fitzgerald and Associates, Redwood City, CA, 1978.

[FONS 77] Forsen, G. E., M. R. Nelson, and R. J. Staron, Jr., Personal Attributes Authentication Techniques, RADC-TR-77-333, Rome Air Development Center, Griffiss Air Force Base, New York, October 1977.

[FPUB 46] Data Encryption Standard, Federal Information Processing Standards Publication 46, U.S. Department of Commerce, National Bureau of Standards, January 1977.

[FPUB 48] Guidelines on Evaluation of Techniques for Automated Personal Identification, Federal Information Processing Standards Publication 48, U.S. Department of Commerce, National Bureau of Standards, April 1977.

[FPUB 65] Guidelines for Automatic Data Processing Risk Analysis, Federal Information Processing Standards Publication 65, U.S. Department of Commerce, National Bureau of Standards, August 1979.

[GASS 75] Gasser, M., A Random Word Generator for Pronounceable Passwords, The MITRE Corporation, AD/A-017 676, National Technical Information Service, Springfield, VA, November 1975.

[GRDE 78] Graham, G. Scott, and Peter J. Denning, Protection—Principles and Practice, The Information Technology Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 101-113.

[HELI 77] Herbst, N. M., and C. N. Liu, Automatic Signature Verification Based on Accelerometry, IBM Journal of Research and Development, Armonk, NY, May 1977, pp. 245-253.

[HNKF 78] Heinrich, Frank R., and David Kaufman, A Centralized Approach to Computer Network Security, The Information Technology Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 145-150.

[HOFF 77] Hoffman, Lance J., Modern Methods for Computer Security and Privacy, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

[HSBA 76] Hsiao, David K., and Richard I. Baum, Information Secure Systems, Advances in Computers, Vol. 14, Academic Press, Inc., New York, NY, 1976, pp. 231-272.

[HSKM 79] Hsiao, D. K., D. S. Kerr, and S. E. Madnick, Computer Security, Academic Press, Inc., New York, NY, 1979.

[LIHA 79] Liu, C. N., N. M. Herbst, and N. J. Anthony, Automatic Signature Verification: System Description and Field Test Results, IEEE Transactions on Systems, Man, and Cybernetics, IEEE, Inc., New York, NY, January 1979, pp. 35-38.

[MART 73] Martin, James, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1973.

[MELL 73] Mellen, G. E., Cryptology, Computers, and Common Sense, AFIPS Conference Proceedings, Vol. 42, National Computer Conference, 1973, AFIPS Press, Montvale, NJ, pp. 569-579.

[MEYE 73] Meyer, C. H., Design Considerations for Cryptography, AFIPS Conference Proceedings, Vol. 42, National Computer Conference, 1973, AFIPS Press, Montvale, NJ, pp. 603-606.

[MOLH 70] Molho, Lee M., Hardware Aspects of Secure Computing, AFIPS Conference Proceedings, Vol. 36, Spring Joint Computer Conference, 1970, AFIPS Press, Montvale, NJ, pp. 135-141.

[MOTH 79] Morris, Robert, and Ken Thompson, Password Security: A Case History, Communications of the ACM, Association for Computing Machinery, New York, NY, November 1979, pp. 594-597.

[NERB 78] Neilsen, Norman R., Brian Ruder, and David H. Brandin, The Information Technology Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 23-32.

[NRDC 75] VERISIGN—A System for Automatic Verification of Signatures, National Research Development Corporation, London, England, March 1975.

[PETE 78] Peters, Bernard, Security Considerations in a Multi-Programmed Computer System, The Information Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 77-80.

[PURD 74] Purdy, George B., A High Security Log-in Procedure, Communications of the ACM, Association for Computing Machinery, New York, NY, August, 1974, pp. 442-445.

[REVI 75] Rennick, R. S., and V. A. Vitols, MUFTI—A Multi-Function Identification System, Wescon Technical Papers, Los Angeles, CA, 1975.

[RIGA 75] Riganati, John P., An Overview of Electronic Identification Systems, Wescon Technical Papers, Los Angeles, CA, 1975.

[RISA 78] Rivest, R. L., A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, Association for Computing Machinery, New York, NY, February 1978, pp. 120-126.

[SAND 77] Entry-Control Systems Handbook, U.S. Department of Energy, Sandia Laboratories, Albuquerque, NM, SAND77-1033, September 1978.

[SPUB 9] Wood, Helen M., The Use of Passwords for Controlled Access to Computer Resources, NBS Special Publication 500-9, U.S. Department of Commerce, National Bureau of Standards, May 1977, GPO SN 003-003-01770-1.

[SPUB 21.1] Cole, Gerald D., Design Alternatives for Computer Network Security, NBS Special Publication 500-21, Vol. 1, U.S. Department of Commerce, National Bureau of Standards, January 1978, GPO SN 003-003-01881-3.

[SPUB 21.2] Heinrich, F., Design Alternatives for Computer Network Security, NBS Special Publication 500-21, Vol. 2, U.S. Department of Commerce, National Bureau of Standards, January 1978, GPO SN 003-003-01881-3.

[SPUB 25] Ruder, Brian, and J. D. Madden, An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse, NBS Special Publication 500-25, U.S. Department of Commerce, National Bureau of Standards, January 1978, GPO SN 003-003-01871-6.

[SPUB 27] Branstad, Dennis K., Ed., Computer Security and the Data Encryption Standard, NBS Special Publication 500-27, U.S. Department of Commerce, National Bureau of Standards, GPO SN 003-003-01891-1, February 1978.

[SPUB 33] Orceyre, M. J., and R. H. Courtney, Jr., Considerations in the Selection of Security Measures for Automatic Data Processing Systems, NBS Special Publication 500-33, U.S. Department of Commerce, National Bureau of Standards, GPO SN 003-003-01946-1, June 1978.

[SPUB 54] Smid, Miles E., A Key Notarization System for Computer Networks, NBS Special Publication 500-54, October 1979, U.S. Department of Commerce, National Bureau of Standards, GPO SN 003-003-02130-0.

[STER 75] Sternberg, Jacob, Automated Signature Verification Using Handwriting Pressure, Wescon Technical Papers, Los Angeles, CA, 1975.

[STOC 75] Stock, Robert M., Present and Future Identification Needs of Law Enforcement, Wescon Technical Papers, Los Angeles, CA, 1975.

[SYKE 76] Sykes, David J., Protecting Data by Encryption, Datamation, August 1976, pp. 81-84.

[TURN 73] Turn, Rein, Privacy Transformations for Databank Systems, AFIPS Conference Proceedings, Vol. 42, National Computer Conference, 1973, AFIPS Press, Montvale, NJ, pp. 589-601.

[WABL 77] Walker, Bruce J., and Ian F. Blake, Computer Security Protection Structures, Dowden, Hutchinson and Ross, Inc., 1977.

[WARF 79] Warfel, George H., Identification Technologies, Charles C. Thomas, Publisher, Springfield, IL, 1979.

[WMMZ 75] Weinstein, C. S., S. S. McCandless, L. F. Mondshein, and V. W. Zue, A System for Acoustic-Phonetic Analysis of Continuous Speech, Automatic Speech and Speaker Recognition, N. R. Dixon and Thomas B. Martin, Editors, IEEE Press, Piscataway, NJ, 1979, pp. 312-327.

[WOLF 62] Wolf, Frank L., Elements of Probability and Statistics, McGraw-Hill Book Company, Inc., New York, NY, 1962.

[WOOD 78] Wood, Helen M., The Use of Passwords for Controlling Access to Remote Computer Systems and Services, The Information Series, Vol. III, Computers and Security, C. T. Dinardo, Editor, AFIPS Press, Montvale, NJ, 1978, pp. 137-143.

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $13; foreign $16.25. Single copy, $3 domestic; $3.75 foreign.

NOTE: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS—This monthly magazine is published to inform scientists, engineers, business and industry leaders, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing. Annual subscription: domestic $11; foreign $13.75.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Services, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services, Springfield, VA 22161, in paper copy or microfiche form.

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

OFFICIAL BUSINESS

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-211

3rd Class Bulk Rate