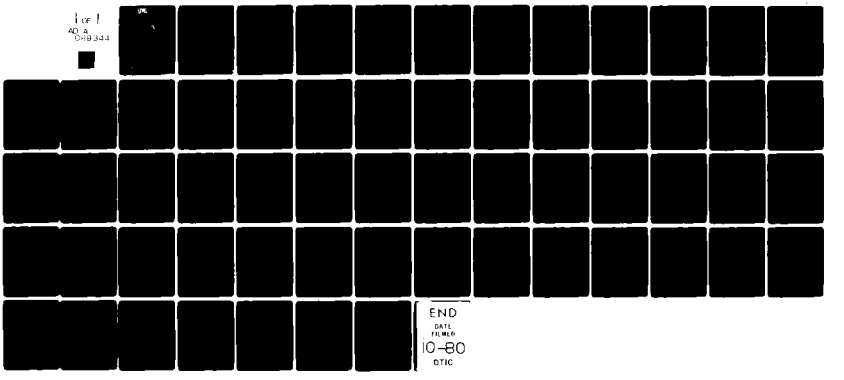
AD-A089 344 SYSTEM DEVELOPMENT CORP MCLEAN VA F/G 15/5
AUTHENTICATION DEVICES AND PROCEDURES.(U)
AUG 80 J M VASAK N00173-78-C-0455
UNCLASSIFIED SDC-TM-WD-7999/401/00 NL



LEVEL II

AD A089344

DTIC
ELECTE
SEP 22 1980
C

AUTHENTICATION DEVICES AND PROCEDURES

29 AUGUST 1980

TM-WD-7999/401/00

AUTHENTICATION DEVICES AND PROCEDURES

29 AUGUST 1980

TM-WD-7999/401/00

ABSTRACT

This paper contains summary descriptions and analysis of authentication devices, procedures, and technologies. Also included are performance comparisons, relative costs, and current areas of research and development. Special emphasis and study is placed on passwords, card systems, and identity verification devices since they are the primary instruments used to provide identification in access control schemes. Finally, recommendations are made for authentication procedures to be used in the Navy Supply System to help alleviate both current and potential problems related to user identification.

This report was prepared under contract N00173-78-C-0455, Task #10 for the Navy Ship Research and Development Center (NSRDC) for use in the Navy Supply environment.

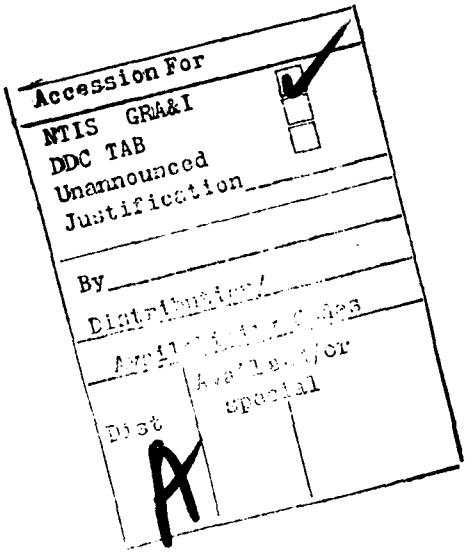


TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

The purpose of this task report is to provide summary information regarding currently available authentication devices and potential authentication techniques or procedures. This report is also to include a brief description and analysis of each device and technique as well as an evaluation of the overall effectiveness and potential use of authentication techniques and devices in the Navy Supply System.

1.1 BACKGROUND

Facilities with highly valuable equipment or computer centers with sensitive financial and personal data must be protected from threats that include theft, fraud, or vandalism, and unauthorized reading, modification, or destruction of data. But these installations must also provide entry to authorized users who need to perform legitimate tasks.

Access control procedures provide a method for determining who is allowed and who is refused access. Fundamental to the access decision process is the act of identifying or verifying the eligibility of the individual seeking access. This act of identification is known as authentication.

The Navy Supply System is responsible for billions of dollars of stored equipment whose management and control is based in part on the logistical and financial data stored in computerized files. Since a large number of personnel have daily access to both the stored inventory records and the supplies themselves, there is a great potential for costly abuse. One part in a solution to help eliminate this threat is the control of access to facilities and equipment. However, in order for access control to be most effective in this situation, individual identification of users must be performed so that authorization levels can be verified and accurate journals of user access can be maintained.

1.2 OVERVIEW OF REPORT

Through an extensive literature search and a survey of representative groups of vendors, information on available authentication devices, current research in the area, and potential identification techniques has been gathered.

The main body of the report begins by specifying the three main levels of identification found in the authentication process. These are:

- o Group identification
- o Claimed individual identification
- o Verified individual identification.

Descriptions, advantages, and disadvantages of each level are given in Section 2. The next three sections deal with the methods and devices that may be used to attain the various degrees of required identification. These techniques employ the use of passwords, coded badges, and automated identity verification devices which are detailed respectively in Sections 3, 4 and 5.

The useful application of this material to the Navy Supply System environment is highly dependent on accurate and complete descriptions of the needs, problems, current authentication processes, and resources of that system. Based on the information supplied, several recommendations for possible authentication schemes are presented in Section 6.

2. LEVELS OF IDENTIFICATION

In order to insure a high degree of access control to restricted areas and equipment, individual identification, as provided by authentication devices, is required. However, positive verification of a user's identity in all situations is not always desirable or necessary from either an economic or security standpoint. For example, controlling access to a small parking lot is often necessary but unique identification of the driver is hardly needed. In this case a token at an automatic gate or a parking permit displayed for a guard authenticates the user as belonging to a group that has been granted parking privileges. In other situations, such as requesting access to a password file in a computer, the above type of group identification is no longer sufficient and some means of individual identification is required for authentication.

Thus it is necessary to distinguish the various levels of identification that are possible in the authentication process, discuss their strengths and weaknesses, and examine which level is appropriate for the required setting. The levels of identification are as follows:

- Group identification
- Claimed individual identification
- Verified individual identification

In general security protection and economic costs increase with each successive level.

2.1 GROUP IDENTIFICATION

There are many circumstances when access must be restricted to an authorized group of users but the value of the items or the sensitivity of the data files being protected does not warrant the added expense and inconvenience

of requiring individual identification at time of access. Authentication in such a case consists of identifying a user not as an individual but as a member of a group with access rights. The devices used in the identification process can be pass badges, special uniforms, service rank, group passwords, duplicate keys, or decals and stickers. The systems may be automated, controlled by a guard, or be a combination of the two.

A common example of group identification is seen in the use of cipher locks on the doors to computer rooms. Here one code or combination is known to anyone in the group that has authorized access to the area. The cipher lock is a fairly easy, inexpensive method to control entry by automated means. The code can easily and quickly be changed as required by security and in the long run is much cheaper than changing traditional lock mechanisms and keys.

Another example of non-individual identification is found when a project team is working on a common task or with a common data file. In many cases a password is assigned to protect the data file. Then anyone who needs to access the file is given the common password. Thus a person who then uses the password is not individually identified but rather recognized as a member of the project group.

To properly determine the level of identification required as well as the amount of security needed, a cost-risk analysis should be conducted. Such a study is used to calculate potential threats, the probabilities of these threats occurring, and the expected losses resulting from successful penetration. These findings are then compared to the cost of providing protection to the system. While precise values are difficult to determine, some measurement of benefits can at least be indicated. If greater security than that provided by group identification is needed or if documentation of individual access is required, then one of the other two levels of identification must be used.

The advantages and disadvantages of group identification are summarized below:

Advantages

- o Relatively inexpensive
- o Easy to use
- o Little maintenance
- o Minimal guard judgement required in manual systems
- o Fast access time
- o Satisfies access control at a low security level

Disadvantages

- o Does not identify individuals
- o Easily compromised
- o Minimal deterent effect
- o Responsibility and accountability are diffused
- o No documentation or record of individual access

2.2 CLAIMED INDIVIDUAL IDENTIFICATION

When the value of the items to be protected increases, when security requirements grow, or when accountability must be assigned at a personal rather than group level, individual identification becomes necessary. One method to accomplish this is to have the user identified by means of a physical description, photograph, unique password, or individually coded badge. This system is relatively convenient to use and only moderately expensive while still satisfying more stringent requirements than group identification can usually satisfy.

Such a system does have some deficiencies; for even though an individual name or corresponding personal number is authenticated through the use of a password or badge, the actual user of these credentials does not necessarily have his true identity verified. It is possible for an unauthorized person to obtain a set of credentials through theft, bribery, duplication, or forgery and thereby defeat the system by posing as a legitimate user. Thus an imposter can use a claimed identity and be allowed access if he possesses the correct items or has memorized the right information.

Even with this drawback, this system of claimed individual identification is better than the group identification since at least an individual name is on the record as having been granted access. It should also be kept in mind that the theft, duplication, or forgery of credentials and the determination of secret passwords, codes, or procedures is difficult and expensive to accomplish. In fact one of the main strengths of a system is that, in many cases, the cost of circumventing it is greater than the expected value from a successful penetration. In most medium security level environments this system of individual identification is quite adequate.

The major advantages and disadvantages of a claimed individual identification system are summarized below:

Advantages

- o Allows documentation of individual access
- o Can be used to assign individual accountability
- o Only moderately expensive
- o Provides medium security
- o Has higher deterrent effect than group ID
- o Less likely to be compromised than group ID
- o Can be used in automated form at remote sites

Disadvantages

- o Counterfeit devices may be used
- o Does not verify identity of user
- o May rely on greater guard judgement in manual systems

2.3 VERIFIED INDIVIDUAL IDENTIFICATION

When highly sensitive data or extremely valuable facilities must be protected, then positive verified identification of individuals is required in order to allow access only to authorized users. As before, an identity is claimed and entered into the system with an encoded card or password, only now there must be some method to establish that the user is who he claims to be.

In order for identity verification to be successful, some physiological feature must be found that is unique to an individual, easy to measure, stable enough to allow repeated testing, and cannot be lost, stolen, or forged. The identity verification systems now under development are based on personal attributes such as hand geometry, fingerprints, speech characteristics, or handwriting dynamics. These systems are for the most part still experimental and fairly expensive. Research is continuing however, and some acceptable reliability results are starting to be produced.

Some of the advantages and disadvantages of verified individual identification are summarized below:

Advantages

- o Very difficult to bypass
- o Full automation allows remote access
- o High deterrent
- o Provides high level of security
- o User cannot transfer access capabilities even under duress

Disadvantages

- o High initial cost
- o Long access time
- o Equipment is still under development
- o Not yet reliable enough
- o High maintenance and repair cost
- o Rejection rate of valid users is still too high

3. PASSWORDS

As mentioned in Section 2, passwords can provide a basis for either group or individual identification schemes. When combined with other devices such as card readers or signature dynamics verifiers, they can be part of a total identity verification system. The use of passwords in an authentication scheme has several advantages which include the following:

- Well-known and well-understood properties
- Widely used and accepted by individual users
- Relatively easy to implement and maintain
- Relatively inexpensive
- Versatile

3.1 PASSWORD FEATURES

There are several features that are used to distinguish one password scheme from another. These factors are often used for a system description when security requirements are specified. The most common features are defined as follows:

- Password length is the number of characters (letters, numbers, or other symbols) constituting the password.

- Password composition specifies the type of characters contained in the password.

- Password lifetime is the time interval when passwords are valid. It is recommended that passwords be changed at least once a year and immediately if compromise is suspected.

- o Password source indicates if the password is generated by the individual user or by the system security facility.

- o Password ownership specifies whether the password is shared by a group of users or is unique for an individual user.

- o Password distribution is the manner in which passwords are sent from the source to the user or in the case of user-generated passwords, from the user to the system.

- o Password storage indicates whether passwords are stored in clear text or encrypted form to protect against unauthorized disclosures.

- o Password entry specifies the amount of concealment required when the user keys in a password.

- o Password transmission is concerned with the amount of protection to be provided while the password is being transmitted to the access control computer.

- o Password reverification indicates at which points or times in a transaction that the password must be resubmitted.

3.2 SECURITY CONSIDERATIONS

Password schemes should be resistant to attacks based on guessing or exhaustive testing. One of the ways to accomplish this is to make the number of possible passwords extremely large. This value is based on N, the number of possible characters used in the password composition, and L, the length of the password. The total number of passwords is then given by N**L where ** indicates exponentiation. For example, if the set of characters consists of the 26 letters of the

English alphabet and the password consists of three letters, then there are 26**3 = 17,576 different possibilities. Care must be taken in counting so that possible restrictions placed on password generation are considered. For example, if the password must contain a vowel or must be pronounceable, then the number of allowable passwords is severely restricted and thus security is lowered.

Other restrictions that will produce passwords with a high level of security include restricting the lifetime of the password to a one-time only use and having the password generated by a computer that produces near random passwords and whose algorithm is extremely difficult to deduce even if some passwords are known. Encrypting the password in storage and during transmission will further safeguard against unauthorized disclosure. Care must also be taken when entering the password at the terminal to avoid exposure. This can be accomplished by the use of a full duplex, non-echoing operation or by understriking the space where the password would appear before it is entered.

Besides limitations placed on the construction, storage, and transmission of passwords, security procedures can be applied to the use of passwords. For example a limit of five attempts to enter a valid password with at least a one second delay between each attempt would discourage system attacks based on guessing or exhaustive testing. This defense can be enhanced by having violations of these restrictions activate an alarm in the security center. It is also possible to activate an "entrapment" algorithm in which an intruder is lulled into a false sense of successful penetration while his attack is monitored and security is alerted.

User involvement can be solicited in the case of individual passwords by having a banner printed upon log-on that shows a record of the most recent log-on employing the user's password. Intervening unsuccessful access attempts can also be shown. If warranted by the environment, a hidden duress alarm can be installed so that an individual can secretly notify security if he is being forced to use his password.

3.3 FIPS DRAFT PROPOSAL

In Spring of 1980 there was a draft proposal for a Federal Information Processing Standard (FIPS) detailing a password use standard [1]. At this point the proposal is still under review and some modifications based on comments from an NBS workshop are envisioned. However, it is informative to see what some of the thinking is at this initial stage. The draft describes the procedures for the generation, distribution, use, storage, and modification of passwords. Also, five password security levels are proposed. They are labeled as minimum, low, medium, high, and maximum. For purposes of comparison, the minimum, medium, and maximum requirements as given in the proposal are listed below.

- o Minimum Pasword Security Level

  - Length: At least 3 characters
  - Composition: Letters or numbers
  - Lifetime: Up to one year unless compromised
  - Source: User generated
  - Ownership: Group organizational unit
  - Distribution: Via terminal
  - Storage: In the clear
  - Entry: Superimposed on understriking
  - Transmission: In the clear
  - Reverification: Enter only at log-in

- o Medium Password Security Level

  - Length: At least 6 characters
  - Composition: Real words with 2 or 3 numeric substitutions or all letters forming pronounceable non-words
  - Lifetime: Not to exceed 3 months

- Source: User or system generated
- Ownership: Group project or task, or individual
- Distribution: Via registered mail or orally
- Storage: Encrypted
- Entry: Non-printing
- Transmission: Encrypted
- Reverification: At least once per hour

o Maximum Password Security Level

- Length: At least 8 characters
- Composition: Random alphanumeric with special symbols
- Lifetime: Not to exceed one week or one-time passwords
- Source: System generated
- Ownership: Individual
- Distribution: Via registered mail with return of signed affadavit or orally with signed affadavit
- Storage: Encrypted
- Entry: Non-printing
- Transmission: Encrypted
- Reverification: Each transaction and each file opening; after 15 minutes of inactivity.

3.4 Individual Passwords

Unique, individual passwords, as opposed to those used by several people in a group, have a number of advantages beyond the obvious security ones. In certain applications these benefits may outweigh the added cost of their use. The main advantages are:

- o Establishes Accountability. A record of which files were accessed and when access occurred can be associated with an individual name based on the use of a unique password.

- o Increases Responsibility. An individual can be held responsible for the unauthorized use of his password, whether intentional or through carelessness. In doing this, a user will exercise more care in protecting his password.

- o Locates Security Lapse. In case of an unauthorized use, a security officer has a point where he can begin an investigation.

- o Minimizes Password Changes. Once a password compromise is suspected or when an individual has left a project, only one password needs to be altered. Thus other members working on the same task or with the same files do not need their passwords changed.

- o Audit Trail. An audit trail of system use can be clearly established and individually assigned.

There are, of course, some disadvantages with using unique individual passwords. These are found in added costs and more complicated procedures in distributing the passwords.

3.5 COST CONSIDERATIONS

While password schemes are certainly less expensive than most other viable authentication schemes, there are still some costs that must be considered.

These are:

- o Hardware Cost for Stand-alone Devices
- o Software Cost
- o Effect on System Performance
- o Storage Cost
- o Password Protection Cost including Encryption Cost
- o Generation Cost
- o Distribution Cost

3.6 PASSWORD DEFICIENCIES

For all the advantages in ease of use and minimal cost, there are some disadvantages in using only a password scheme for authentication. The problems are:

- o Memorization of difficult password
- o Detection of password theft
- o Verification of identity

If the password length is too short and not changed often enough, then exhaustive testing or guesswork may yield the password. On the other hand, if the password length is too long, then it is more difficult to memorize and may lead the user to write it down thus violating security. To help deal with the memorization problem, attempts have been made to associate images or pictures with two-digit numbers, for example, the number 37 would correspond to a picture of a telephone. A list of 100 images and their corresponding numbers would be posted at each terminal access point. The user would need only recall his two, three, or four images, look up the associated numbers, and enter his password. This procedure is currently being tested and may provide one answer to the problem of memorizing passwords [2].

Another serious problem can occur if a password is compromised. Since nothing physical has been lost, it is often hard to determine when or even if such an event has occurred. Printing access information banners at log-on or using one-time only passwords could help control this problem area.

Perhaps the most difficult problem area to deal with in a password scheme, and for that matter with most other authentication schemes, is that the object being recognized as legitimate is not the individual user but rather the artifact or password that is used. Hence if a password is valid, the system necessarily assumes that the user is also valid in a password-only authentication scheme. It is primarily for this reason that any situation calling for a reasonably high degree of security will require password use in conjunction with some other approved authentication procedure.

4. CARD SYSTEMS

Plastic cards that incorporate a unique personal identification number, whether this number is conveyed by means of a magnetic tape and a card reader or through raised letters as found on most common credit cards, have many of the same functions and properties as those found in password schemes. Indeed encoded cards or badges can be thought of as mechanical passwords. The main difference is that now a physical object is used to automatically enter a code that must be verified instead of the manual entering of a memorized code. Like passwords, cards can be used at all three levels of identification as mentioned in Section 2 and can be used in stand alone systems or in conjunction with other devices and authentication procedures.

4.1 TYPES OF CARDS OR BADGES

There are many types of card badges with different construction costs, encoding features, and levels of resistance to duplicating, decoding, and counterfeiting [3], [4]. A short description of each is given here for later reference.

- Embossed cards are widely used as credit cards and as pass badges. Their raised lettering containing name, identification number, and validation date offer almost no protection against misuse.

- Photo badges contain a facial photograph, sometimes against a color coded background, laminated between several layers of plastic. Care must be taken to obtain a good bond between the photo and the plastic in order to resist tampering efforts.

- Punched cards, or Hollerith encoded cards, have holes punched in the cards. The position of the holes, i.e., the code, is then read by light sensitive detectors. The code is plainly visible and hence is relatively easy to duplicate or alter.

- Electric circuit badges contain a printed circuit that activates selected electrical circuits in the badge reader. The badge reader is similar to a card-edge connector usually used with a printed circuit board. This type of card can be decoded with commercially available equipment.

- Magnetic stripe cards use a stripe of magnetic tape that is then encoded. The information is read when the stripe is moved past a magnetic read head similar to the kind found in common magnetic tape recorders. Consequently duplication of cards and data is possible.

- Differential optics cards are designed with a geometric array of dots printed on an insert that is laminated into the badge. Each dot offers up to 10 levels of optical density when scanned by infrared light beams in the card reader. This allows unique encoding of up to 65,000 different cards. To increase resistance to tampering, the badge is made opaque to visible light but transparent to infrared light. These cards are very hard to counterfeit.

- Magnetic-coded badges contain an array of ferromagnetic spots that are permanently magnetized. The code is then determined by the polarity of the spots. Unfortunately it is possible to obtain the equipment needed to decode or duplicate the pattern of magnetic spots.

- Metallic strip cards are encoded by imbedding rows of copper strips in the badge. The code pattern is read by means of an eddy-current sensor. This badge was developed for use with the Controlled Access by Individual Number (CAIN) system that is undergoing tests at the Lawrence Livermore Laboratory [3]. Each card can hold about 40 bits of code.

- Capacitance badges have an array of small conducting plates imbedded in the cards. The code is formed by connecting selected plates and then read by measuring the capacitance of the plates and distinguishing which plates are connected.

- Remote read cards have electrically tuned circuits, diodes, or transistors embedded into the badge. A microwave transmitter is aimed at the card and a receiver measures the different frequency harmonics that are determined by the number and relative position of the tuned circuits. In this way a code can be read remotely without the need to insert a card into a reader. Furthermore, such a system can automatically monitor, log, and identify individual badges. Unfortunately a relatively few number of unique codes are possible and counterfeiting by solid-state electronic devices is possible.

4.2 AVAILABLE FEATURES FOR CODED BADGES

Whether the card readers of encoded badges stand alone or are tied to a control processor, several useful features are possible.

- Automatic access logging in which the user's name, identification number, date, time of entry, and access location point are recorded or sent to another system for further processing.

- o Instant access changes that immediately cover all access points can made from a central control processor. Lost or stolen cards need not be recovered to be voided.

- o Multilevel access can be achieved in which encoded cards work only in those areas authorized from the control processor.

- o Time zone access in which certain cards are valid only during certain hours of the day is another feature easily programmed into the card readers.

- o Occupant lists stating who is present in which areas is possible if the use of encoded badges is required at the time of exiting a controlled area. In this way the access log will have a complete occupancy record.

- o Anti-passback control prevents two individuals from using the same card for either entry or exit. This is accomplished by checking the encoded card against the current occupant list.

- o Passwords can be used in conjunction with some card systems in which a keypad for password entry is located next to the card reader. Some systems have the password encoded on the card with access being granted if there is a match. However, such a system has very low security since, in many cases, it is easy to decode the information stored on a card. Other systems use the identification number encoded on a card to identify an individual name or record stored in the password file of a central processor. A memorized password is then entered into the system and compared to the correct password in the central file.

- o Central control processors that control access changes and levels as well as keep records of access can also be used to monitor smoke detectors, flood alarms, and emergency distress signals.

4.3 COMMERCIAL SYSTEMS

As already indicated in this report, there is an extensive array of available features and encoding schemes to be found in card-reading systems. This same variety is found in the commercial firms that market these products.

Almost any company can and will modify their system to fit particular customer needs. Hence prices and specifications of complete systems are difficult to obtain since these factors are determined on almost a case-by-case basis after customer requirements are made known. Some of the variables affecting the final design are number of users, number of access points to be controlled, type of access requested (e.g., entry to a storage area or access to a computer terminal), results of a cost-risk analysis, amount of required documentation of access attempts, physical environment, tamper alarms, and computer facilities available for use as a central control.

However, some indication of the relative features provided by commercial firms is possible. Table 4-1 which is taken from [4], gives a side-by-side comparison of some available products. It should be noted that these are catalog items and do not reflect the variations possible in custom designed systems. The maximum badge capacity refers to the maximum number of users that the system can accommodate and not the number of different card codes that are possible.

Table 4-1. Feature Comparison of Commercial Badge Systems

SYSTEM	BADGE TYPE	MAXIMUM BADGE CAPACITY	MAXIMUM NUMBER OF READERS	PASSWORD OPTION	COMPUTER INTERFACE	TAMPER ALARMS
Card Key Systems Model 880	Magnetic	62,000	128	Yes	Yes	Yes
Identi-Logic 6003	Electric Circuit	9,999	40	Yes	No	No
IBM Controlled Access Systems	Magnetic Stripe	4,096	63	No	Yes	Yes
Rusco Series 500	Magnetic	20,000	256	Yes	Yes	Yes
Schlage Electronics Model 414	Remote Read	1,500	8	No	No	No
Secom	Differential Optics	25,000 (est.)	765	Yes	Yes	Yes
Sentracon Series 670	Capacitance	65,500	255	Yes	Yes	Yes
Toye CRC-200	Differential Optics	8,000	100	No	No	No

4.4 SECURITY CONSIDERATIONS

If a card is lost or stolen, there is great potential for abuse. However, it is likely that the absence of such an important object as a badge will be noticed and promptly reported. At this point the central control processor can quickly notify all card readers not to accept the missing card. If a card is combined with a password scheme, then possession of only the card without the memorized code would not allow an intruder access. The security level would, of course, be reduced if group cards or group password codes were used.

Instead of possessing an actual card, an intruder may use a forged or duplicated badge. While it is true that any coded card can be duplicated or counterfeited if enough time and money is available, some cards are more resistant than others to this form of attack. The order in which coded badges may be duplicated, ranked from the easiest to the most difficult is as follows:

1. Embossed
2. Punched
3. Electric Circuit
4. Magnetic Stripe
5. Magnetic
6. Metalic Strip
7. Capacitance
8. Differential Optic
9. Remote Read

Counterfeiting a new badge requires not only decoding a badge but also decrypting the information since an encryption algorithm is often used to further protect encoded badges. For example, the optical coded card used by Secom of Los Angeles employs a code with 40 data bits and 24 check bits that is then encrypted [4]. Such a system makes successful counterfeiting prohibitively expensive.

Resistance to duplicating and counterfeiting is not as important if the card system is combined with a password scheme or, even better, a personal identification verifier. In these situations the coded number on the card is used only to index a central computer file which contains identification data such as passwords or physiological information.

In remote sites where card devices are used without guards, tamper alarms should be installed in the card reader. If the reader is not a stand-alone device, then protection must be granted to the communication link between the central processor and the reader. Data encryption and tamper alarms are two good safeguards.

Another area of security that must be considered whenever automated authentication devices are used is protection during system failure or power outage. Backup copies of access files should be maintained and a secure bypass procedure should be devised for use in case of extended system failure.

In the final analysis it is possible to defeat a card system whether or not an associated password scheme is used. The main reason for this is that the system does not verify the identity of the individual user but instead verifies the authenticity of the encoded card and the password. Hence an imposter with seemingly valid credentials can bypass the system. Greater security protection is possible through the use of identity verification devices which are discussed in Section 5. However, it must be noted that in many cases the cost of this increased protection can exceed the benefits to be derived. Careful analysis of total system requirements and costs must be considered.

4.5 COST CONSIDERATIONS

Precise cost determinations of a badge system depend on many factors such as size and special feature requirements. Also new technologies often drive prices down while inflation spirals them up. Even so some equipment price comparisons are useful in the sense of relating relative costs. Table 4-2, which is taken from [4], should be read with the understanding that the actual figures may be out of date. The items listed in the table cover only a small part of the total system cost.

The following factors will affect the total cost of a badge system of authentication.

- o Equipment
- o Software
- o Central Control Processor in Independent Systems
- o Repair and Maintenance
- o Installation and Testing
- o Tamper Alarms
- o Encryption Costs
- o Backup Files
- o Operating Costs
- o Card Replacement

Even with all of these cost considerations, there are many cases where an automated card system is less expensive than the cost of guards at each access point or the cost of changing locks and replacing keys each time one is lost or stolen. Also, several of the expenses are one-time costs in the life of the system.

Table 4-2. Comparison of Equipment Costs

SYSTEM	CODED PHOTO ID BADGE (LESS PHOTO)	BADGE READER FLUSH-MOUNTED	BADGE READER WITH PASSWORD CAPABILITIES
Coded Key Systems	$2.00	$873	$1969
Identi-Logic	$4.28	$342	$ 592
IBM	$1.42	$297	Not Applicable
Rusco Series 500	$1.95	$750	$1200
Schlage	$3.98	$112	Not Applicable
Sentracon	$2.70	$695	$1275
Toye CRC-200	$1.50	$665	Not Applicable

4.6 COMPARISON WITH PASSWORD SYSTEMS

Both badge systems and password schemes offer a fairly high level of secure access control even though neither method provides unique identity verification. When compared to passwords, some of the advantages of a badge system are:

- o Loss of badge is noticed
- o Access is faster with a card reader
- o There is less chance of error in use
- o There is no need for memorization
- o Some cards are hard to duplicate or counterfeit
- o Badge can contain added information such as photo

A few of the disadvantages are:

- o Badge is easier to steal
- o Card system is more expensive

5. IDENTITY VERIFICATION SYSTEMS

In order to provide maximum protection of resources, there must be positive identification of all individuals seeking access. Passwords or coded badges only provide a claimed identification for a person. This identity must be confirmed or verified if the highest level of security is required.

5.1 OVERVIEW OF VERIFICATION

A typical identity verification system works in the following manner. During an enrollment period, measurements of some individual physiological factor, such as fingerprints or speech characteristics, are taken and analyzed. The data derived from this is either encrypted on a card or stored in a computer file. When access is requested, the user enters a claimed identity into the system by means of a unique password or coded card. A measurement of the same physical element used in the earlier enrollment is taken. The extracted data is then compared with the information stored on the card or in the central file. If the two sets of data match within an acceptable tolerance, the identity of the user is considered to be verified. If in addition, the proper authorization conditions are satisfied, then the requested access is granted.

It is important to note that verification is not a true identification process. True identification is a process that in the end supplies either an individual identification or an "unable to identity at this time" response. This is similar to the process carried out by the police when they try to match the fingerprints of an individual against all of the prints on record. Identity verification on the other hand, is a much simpler process that supplies either a yes or no response. Here a claimed identity is presented along with collaborating identification such as a fingerprint. Now only two sets of data, the one taken from the person and the other from the information stored under the claimed identity, need to be compared to determine if there is a close enough match.

5.1.1 Verification Requirements

In order to verify a user's identity, information or features that are unique to that particular individual must be employed in the decision process. It is required that these features cannot be lost, stolen, transferred, or forged as is the case with passwords and badges. Furthermore, these factors must vary enough among individuals to provide unique identification characteristics yet be sufficiently stable to allow for repeated testing and measurement on a day-to-day basis.

Traditional systems have been based on the comparison of a user's facial features with photographs on stored badges or with video images called from a protected file in a computer. Human guards carry out the time consuming decision process. Unfortunately this allows for subjective judgment and human error when the number of users is large or possible collusion in other cases through bribes or threats.

To be objective, the matching or decision function should be automated. However, this adds another constraint on the selection of unique identifying features, namely that they must now be machine measurable and also amenable to an accurate matching algorithm.

5.1.2 Physiological Attributes

In order to satisfy the verification requirements for unique identification, physiological attributes are used. The most common ones in current use are:

- Facial features
- Hand geometry
- Speech characteristics
- Signature dynamics
- Fingerprints
- Modified electrocardiograms

The search for useful, reliable, and economically feasible sets of unique identification features still continues. Some factors that are under investigation include footprints, retina patterns of the eye, ear features, dental characteristics, enzymes, recognition of patterns and colors that are virtually impossible to describe or reproduce, brain waves, and muscular-skeletal responses. This last area involves applying a mechanical stimulus at one point on the body and observing the resulting signal at another. However, it should be kept in mind that user acceptance must be considered in any practical system of identity verification.

5.2 CRITERIA FOR SYSTEM EVALUATION

The major areas to consider in the evaluation of a system are the following:

- o Error rates
- o Resistance to circumvention
- o Verification time
- o User acceptance
- o Storage requirements
- o Hardware failure rate
- o Cost

5.2.1 Error Rates

Verification errors are commonly divided into Type I or Type II errors. The first type of error is the false rejection by the system of a claimed identity that is in fact valid while the Type II error is the false acceptance of a claimed identity that is in fact not valid. The Type I error rate is the ratio of the number of false rejections to the total number of verification attempts of all authorized users. A high Type I error rate will necessitate an authentication bypass system and will lead to more user complaints and higher operating costs.

The Type II error rate currently used may be thought of more as a random forgery rate rather than a deliberate forgery rate where forgery is considered as any action employing the verification technique that results in the false acceptance of claimed identity. As usually calculated, the Type II errors are found by comparing the data from a valid user's verification attempt with the data stored on all users and determining if there are any matches within the defined tolerance limits. In this way only coincidental or "random" false acceptances are measured. A more valid error rate, but also one that is more difficult, if not impossible, to calculate, would be the ratio of the number of false acceptances of deliberate forgeries to the total number of deliberate forgery attempts. Even though the Type II error rate is not intended to measure successful penetration of the system by deceit, a rate of more than 2% would be indicative of an unacceptable amount of laxity in the system.

Another point about Type I and Type II error rates is that they can be adjusted by changing the tolerance levels used in the decision or matching process. As the tolerance for deviation from the stored data decreases, that is, as the two data sets must be more alike to have a match, the Type II error rate will decrease. However, the Type I error rate measuring false rejection will increase due to the daily variations of physiological features. The opposite effect will occur if the tolerances are increased.

5.2.2 Resistance to Circumvention

Resistance to circumvention is a measurement of the ability of the system to resist attempts to deceive by counterfeited artifacts or created templates, or to bypass the entire authentication device. For example, speech characteristics and handwriting dynamics are most resistant to attempts at counterfeiting, with fingerprints and hand geometry next, and photo identification comparison being the least resistant. Bypassing the entire authentication scheme can be partially controlled with tamper alarms, line encryption, or communication line protection.

5.2.3 Verification Time

Verificatin time is the amount of delay experienced while a user is waiting for a decision to be made by the authentication device. It has been found that a delay of more than six seconds is unacceptable to most users of a system. Verification time also directly affects the number of persons that can be granted access over a period of time. This rate is known as the throughput rate.

5.2.4 User Acceptance

If users do not accept the system, there will not only be more complaints but also some authorized users may attempt to circumvent the system in order to avoid delay if the verification is too long or to avoid the whole authentication process if it is inconvenient or psychologically unacceptable. For example, some individuals complain about having fingerprints taken since this makes them feel like criminals yet they are perfectly willing to sign their names as a means of identification.

5.2.5 Storage Requirements

Each individual user has a file created in his name in a computer-controlled system. This file may contain the user's name, secret password, identity verification data, clearance level, areas of access, hours of access, or other information. The storage requirement refers to the number of data bits needed to store the required information in the user's file.

5.2.6 Hardware Failure Rate

The hardware failure rate can be used to indicate the reliability of a system and give some measure of the amount of down time and when it might occur.

5.2.7 Cost

The cost of a system is more than just the price of the hardware involved. Other cost considerations should include software development, repair and

maintenance, computer storage, backup systems in case of failure, and system installation and checkout. The total cost of the entire authentication system should be compared to the value of items being protected. This is usually done in a cost-benefit analysis when any system is considered.

5.3 SYSTEMS BASED ON FACIAL FEATURES

These systems all rely on a human guard verifying an individual's identity based on visual characteristics. The comparison is made using a photo badge or an image stored in a computer system. In general such systems can be slow, expensive, and subject to human error. These systems are more effective with a small number of users than with a large group.

5.3.1 Badge Exchange

In a manual photo identification badge exchange system, authorized individuals are issued color coded photo badges. Duplicate badges with different color codes are held at each entry point for which access is authorized. When a user requests access, the guard matches the photos on both colored badges to each other and to the individual user. If a match is made, the regular badge is exchanged at the control point for the new color coded badge and access is granted. A similar exchange takes place when the user leaves the controlled area. The photo badge may be coded with information that can be used with a card reader to document the person's name, time, and location of entry and exit.

Since the exchange badges do not leave the secure area, they cannot be lost, stolen, transferred, or forged. However, the system does rely on a matching being performed by a guard which entails the problems of accuracy, subjectivity, and reliability.

5.3.2 Video Comparator

A video comparator system also requires a guard to make an image comparison, as in the badge exchange, and decide if a close enough match exists. The difference here is that the stored image of the person requesting access is located in a secure area either on a video disk file or a microfiche video carousel. In addition the image comparison is made with a real-time closed circuit television (CCTV) picture of the user. Even though these systems can provide remote access with a CCTV and fast image retrieval with secure storage of a large number of images, the comparison and decision process still rests with a human guard. These systems are also much more expensive than the badge exchange. There are currently two commercial systems available [5].

The Ampex TVID system employs a coded badge that is used to call up the person's image from a video disk file which can hold 1,000 images. The stored picture is then compared with a real-time CCTV image by the guard and a decision is made. The file access time is less than two seconds. The cost of the system is approximately $35,000.

The TERA video comparator system can store up to 189,000 images on a microfiche video carousel. A coded card is used to call the user's image from the file in an average of three seconds. The comparison with a CCTV image of the user is made by a guard on a split-screen monitor. The controlling computer can be programmed with shift changes and thereby load a video buffer with up to 250 images. This reduces access time to 0.2 seconds. The images in this system have much higher resolution than a standard video system. The approximate procurement cost is $150,000.

5.4 HAND GEOMETRY

The shape of a person's hand provides enough data so that it may be used as the basis of an identity verification system [3], [5], [6], [7], [8]. In a device marketed by Stellar Systems under the product name IDentimat, a strong light source shines onto photo cells that are built into four permanent finger grooves used to position either hand. Measurements are then taken of the distance between the base and tip of the finger, the roundness of the fingertip, the skin translucency, width of finger, and distance from knuckle-to-knuckle for the four fingers. This information is stored as a 20 byte identifier either on a coded badge in encrypted form or in a secure computer file. The enrollment procedure which includes the initial hand measurement and the card encoding takes about two minutes.

When an individual user requests access and wishes to be identified, he enters his name or identifying number by means of a coded card or password and positions his hand over the sensing area. An algorithm compares the current measurement readings with those encoded on the card or stored in the computer. If there is a close enough match of the two sets of data, then the user's identity is considered to be verified. A threshold or tolerance level of acceptance must be predetermined since exact matches are almost impossible due to the day-to-day minor variations of finger size.

Early versions of this device showed a false reject or Type I error rate of almost 10%. Since then improvements in hardware, procedures, and the decision algorithm have reduced this error rate. In a two month test involving 1,178 transactions with 31 individuals in 1977, Sandia Laboratories recorded a Type I error rate of 0.89% and a false accept or Type II error rate of 2.97%. The average verification time was 5.95 seconds [5]. A maximum of two retries were allowed if initial verification was denied. It must be recalled here that the Type II error is for "random" false acceptance and does not measure concerted efforts at forgery, deception, or circumvention. It has been found that

artificial hand templates can fool the system. A system feature was added to randomly choose the right or left hand to be verified at time of entry in order to discourage the use of templates. The approximate cost of each hand scanner and built in card reader is $5,000.

Although not in use, devices could be added to a hand reader to further discourage the use of artificial hands. Besides an expensive CCTV video system, an infrared detector to detect the presence of radiation emitted by a "live" hand or a photo plethysmographic detector to detect the presence of time-varying reflections of light from surface blood blow of a live hand could be used [10].

5.5 SPEECH CHARACTERISTICS

There exist a variety of speech characteristics that may be used to provide unique identity verification. Two of the more commonly used factors are the relative amplitude of the different frequency components of speech and the vocal tract resonant frequencies determined by the anatomical construction of the throat, mouth, and nasal cavaties.

In a typical speech verification system an enrollment session is used to accustom the individual to the verification procedures and to obtain a voice recording of a list of preselected words. The various speech components are analyzed and the individual's reference speech pattern is determined. When access or identity verification is requested, a coded card or password is used to identify the user to the system and thus bring up the computer file containing the user's reference speech patterns. A sequence of words randomly chosen from the list used at enrollment are then repeated by the user in a microphone. The various speech components are automatically analyzed and compared with the stored patterns. If there is a close enough match as determined by the algorithm, then the user's identity is considered to be verified.

While tests of particular systems have shown speech verification to be relatively accurate, there are a number of general problems found in this type of system. The most common one is that certain speech characteristics are affected by illness, such as a common cold, and by emotional stress. If the thresholds governing the matching decision is set to accommodate these daily variations, then the number of false acceptance errors may be too high. But if the matching parameters are moved in the other direction, the number of false rejection errors may be unacceptable. Another problem is that the components of speech are dynamic. Thus the reference pattern of each user must be continually updated so that gradual changes will be reflected and hence reduce rejection of valid users. A final difficulty is that speech verification systems may be defeated by skilled impersonators familiar with the decision process or by tape recordings of the user's voice. Randomly choosing the words used at time of access tends to discourage the use of recordings and continually updating the reference patterns after each successful verification narrows the acceptance parameters and helps defeat impersonators.

5.5.1 Texas Instruments

Texas Instruments had developed an identity verification system that is based on the relative amplitude of different frequency components of speech [3], [5]. During the enrollment period the relative amplitude spectrum of 16 spoken words is recorded. The results for each user are stored using up to 9,408 bits of memory. The system does allow for update of this reference file after successful verifications.

When an individual desires access or identity verification, he enters a control booth and supplies a claimed identity to the system via a coded card or password. From the list of 16 reference words, four are chosen for the user to repeat. The relative amplitude spectrum is determined and compared with the reference file. In field tests the average verification time is 6.2 seconds.

This system, while not available commercially, has been extensively tested under a United States Air Force contract as part of the Base and Installation Security System (BISS) project. In field tests conducted by MITRE Corporation at Pease Air Force Base, the recorded Type I error rate measuring false rejections was 1.1% and the Type II error rate was 3.3% [9]. As part of the BISS project, MITRE tested not only the speech verification system from Texas Instruments, but also sysems based on signature dynamics and fingerprint verification. The field tests were conducted over a four month period from November 1976 to February 1977 and involved the same group of approximately 200 individuals. In this way direct comparisons of different verification schemes could be made outside of laboratory conditions. The above results for speech verification proved to be the overall best of the three systems tested. Since the MITRE test, there has been a report published in the 1979 Carnahan Conference on Crime Countermeasures from the Rome Air Development Center (RADC) that contains a claim that further development of this speech verification system has resulted in a 0.5% Type I error rate and a 1.8% Type II error rate with an average 6.2 second verification time [10].

5.5.2 Philips Laboratories

In a research paper presented at the 1980 Carnahan Conference on Crime Countermeasures [11], Philips Laboratories of Hamburg, West Germany reports the development of a low-cost, table model speaker verification device. The speech characteristics used as the basis of this system is the long term average spectral intensity which is determined essentially by the geometry of the vocal tract. One of the main advantages of using this factor is that it is a statistical feature which eliminates the need for non-linear time alignment of vectors due to varying rates of speaking. This allows the reference data to be stored using many fewer bits of memory. Eventually only 312 bits per person may be needed thus permitting encrypted cards to carry the necessary reference patterns. The system is still undergoing testing and refinements. Consequently, error rates under field conditions are not

available but laboratory tests are encouraging. The average verification time appears to be 8 seconds. It should be noted that this system would be vulnerable to Type I errors due to user illness that affects the configuration of the throat, mouth, or nasal cavaties.

5.6 SIGNATURE DYNAMICS

Signatures have traditionally been used as a means of identification since almost the beginning of access control. Most often they are used to provide a record of entry rather than a positive identification. The reason for this is that the graphic image of a signature is relatively easy for a skilled forger to duplicate. Also it is a fairly long and sometimes difficult process to manually verify the validity of a signature.

However, signatures can be used in automated identity verification systems if measurements are taken not of the finished signature but of the signature dynamics, that is, the acceleration, pressure, and velocity which occur during the signing process. These components are not discernable by studying a completed signature. Hence forgery in this case is very difficult.

In such a verification system, from one to seven signatures are written during an enrollment period so that various characteristics displayed in the process of signing can be measured, analyzed, and then used as a reference profile. For some systems, as little as 200 bits of information per person needs to be stored. A special pen, writing tablet, or a combination of the two that contain accelerometers or pressure sensing strain-gauges are used to obtain the raw data.

At time of access or during a verification attempt, an individual would enter a claimed identity by means of a coded card or password and then sign his name using the same type of pen or tablet as used during the enrollment

procedure. The claimed identity is used to provide the reference profile from storage to be compared with the dynamic factors measured when the user signed his name. If the comparison algorithm indicates a close enough match, then the identity is verified.

A signature verification system has several advantages. One of the main ones is that the process is psychologically acceptable to the user since signatures are a very traditional form of providing identification. The system as described would also allow access from remote sites as long as the sign-in equipment were available. Another feature is that in case of a forgery, there is a permanent record that may be analyzed during an investigation.

There are, however, a number of drawbacks to existing devices that employ this verification scheme. Since many of them are still in the developmental stage, equipment failures and variations in replacement parts have raised questions of overall reliability of apparently delicate hardware. In some cases error rates have not been computed in field tests outside of laboratory conditions. Also, the entire proces of picking up the pen, signing ones name, and awaiting verification is comparatively long resulting in some user complaints and a low throughput rate. Finally, some individuals have a high degree of variance between successive signatures. This necessitates a greater tolerance in order to validate a signature. Unfortunately this also allows forgers a much better chance to gain access. Even with these problems and a current relatively high cost factor, signature verification is probably the best hope for an acceptable identity verification system.

5.6.1 Signac System

Veripen Inc. of New York manufactures the Signac Signature Access Control System which is marketed by Sentracon Systems [5]. The special characteristic measured in this system is the level of pressure at pen tip. From three to five signatures are used during the enrollment period to provide a reference record of pressure levels recorded at certain time intervals. This system was one of the first to be commercially developed and costs approximately $75,000.

It was selected by the Air Force for the BISS project. In the comparative testing, a version of this system attained a 1.9% Type I error and a 5.6% Type II error in the field test. The average verification time was 13.5 seconds [9].

5.6.2 SRI System

The Stanford Research Institute (SRI) has developed a 3-axis pen in which a ballpoint tip, through an array of strain gauges, can measure three independent orthogonal components of force; that is, this system can measure downward pressure and motion in any direction on the two-dimensional plane of the paper [12]. A "parameter method" is then employed to extract features from the signature such as the total time for signing, the time the pen is on the paper, the maximum pressure, and the average pressure. It is possible to find some 50 features. Of these, some 10 to 20 features are selected for each individual and for each parameter the mean and standard deviation are computed. All of this information can be stored using about 200 bits which could be stored in a computer file or encoded on a card. A matching algorithm is used to compare data from a current signature with the stored data. Limited tests so far give a 2.5% Type I error and a 3.0% Type II error. During a test at Sandia Labs, the pen appeared to be fairly delicate and subject to failure [5]. Further work is being done on the development of a tablet to perform the measurements and on a correlation method to compare the original three waveform force signals with the waveforms in the writing sample.

5.6.3 IBM System

The signature verification system under development by IBM measures with a special pen two orthogonal components of acceleration and the downward pressure on a standard ballpoint pen tip [13]. This model is one that has been improved over a pen that measured only the acceleration rectors [14]. A correlation algorithm compares the three sets of waveforms in the current signature

and the stored reference. The segments of the waveforms are time-shifted to provide the best match. This also requires a lot of computing power which is provided by an IBM 370 with a System 7 front end. A test run by IBM with 248 subject over six months yielded a Type I error rate of 1.7% and a Type II error rate of 0.4% for deliberate forgeries. It should be noted that some test data was not used due to hardware failure. An independent field test has not been conducted.

5.6.4 Other Systems

There are several other companies that are actively working in this area [15], [16]. NCR Corporation is experimenting with a writing tablet that measures the pressure factor. It needs 110 bytes of signature storage and has an initial 1.5% Type I error rate and 1.2% Type II error rate [17].

National Physical Laboratory in the United Kingdom is working on a device similar to the Signac system [3].

Sandia Labs is developing a special pen and tablet combination that will measure pressure and forces on the pen tip in two areas [5].

5.7 FINGERPRINT VERIFICATION

Fingerprints have been used by law enforcement agencies for many years as a means of obtaining positive identification of individuals. However, taking the prints is usually messy and making a comparison is very time consuming. Fortunately, technological developments in optical scanners now allow fingerprints to be analyzed automatically without the need for inking a set of prints, and developments in algorithms for describing prints makes comparison testing much easier [6].

Some systems use optical scanners to send an image of a fingerprint to a central location where a human operator manually compares the print to one on a user's reference file. Such a system is very slow and for the purposes of this report impractical.

Fast, accurate methods of comparing data from a fresh print with a stored print have been developed. There are basically two methods. One is a metric approach in which distances between certain reference points in a print are measured. This method is susceptible to problems caused by distortion when a finger is placed against a scanner with varying pressure. The other approach relies on the topology of prints and encodes the relative positions of whirls and ridges that comprise a print.

Fingerprint verification under these automated conditions is very fast and does not rely on human judgement. However, there are a number of disadvantages to the system. Precisely because fingerprints have been used by the police for identification, the average user does not like the method since he feels that he is somehow being treated as a criminal. There are also problems with finger alignment, distortion, dirt, and cuts that cause a relatively high rejection of valid users. The system also requires a lot of computing power and at least 7,000 bits of storage per person. Due to the optical scanners as well as the computers, these systems are very expensive. Finally, artificial prints made of latex rubber can be used to defeat the system.

5.7.1 Calspan Corporation

Calspan Corporation markets a fingerprint verification system under the trade name Fingerscan [5]. An optical scanner is used to detect the "minutiae" of the fingerprints, that is, the tiny ridge endings and branches. Two attempts are allowed to match the print recorded in the reference file made during the enrollment period.

A variation of this system was tested in the BISS project for the Air Force by MITRE Corporation [9]. The field test results were a Type I error at 6.5% and a Type II error of 2.3%. The average verification time was 8.9 seconds. The price range of this system is from $50,000 to $80,000 plus $4,500 for each scanning terminal [7].

5.7.2 Rockwell International

An illumination and lens system is used to create an image of a fingerprint which is then scanned by a photoelectric device [5]. The original data of 60,000 bits is reduced by an algorithm to a more manageable 7,000 bits. Initial tests indicate error rates for both Type I and Type II errors at 1%.

5.7.3 Fingermatrix, Inc.

Up to 80,000 bits of information is collected when a finger is optically scanned using a dual-axis laser [5]. No formal tests have been performed yet on this system.

5.8 MODIFIED ELECTROCARDIOGRAM

The Rome Air Development Center (RADC) conducted a study in 1977 to search for new characteristics that would provide a basis for user identification [10]. One of the newest methods that was reported is based on a modified electrocardiogram called a C-trace. One of the components of a C-trace is an electrical signal generated by heartbeats that can be transduced by passive electrodes. An individual needs only touch one finger of each hand to an electrode in order to generate a C-trace waveform from which 10 features may be extracted to be used in a pattern recognition algorithm. A test using 57 people produced a Type I error of 1.2% and a Type II error of 1.1%. All of the hardware necessary to build this system is already available and only moderately expensive.

5.9 SUMMARY COMMENTS

The need for a fast, reliable, and accurate identity verification system continues to grow. The current state of the art, which is partially summarized in Table 5-1, does not yet meet all of the requirements of such a system. Further development of present systems and continued research is needed.

Table 5-1. Partial Summary of Verification Systems

System	Type I Error Rate	Type II Error Rate	Verification Time (Seconds)	Approximate Cost
Identimat (Hand Geometry)	0.9%	3.0%	6.0	$ 5,000
Texas Instruments (Speech)	1.1%	3.3%	6.2	N/A
Signac Veripen (Signature)	1.9%	5.6%	13.5	$75,000
Calspan Fingerscan (Fingerprint)	6.5%	2.3%	8.9	$75,000

As for now it must be realized that no known system is foolproof. Systems with lower error rates are continually being sought. Depending on security requirements, false reject and false accept error rates can be adjusted by combining some of the methods and devices presented in this section. Also, the thresholds determining the level of acceptance can be shifted to further affect the error rates.

The Air Force has selected speech verification as the primary system to pursue as a result of the BISS tests [9], [10]. However, signature verification also holds much promise with its new results. But before one of these expensive, high security systems can be considered for an installation, a cost-risk analysis must be performed to determine the benefits to be gained.

6. AUTHENTICATION DEVICES FOR THE NAVY SUPPLY SYSTEM

The Navy Supply System is highly dependent on accurate computer records for the management and control of its operation. Unreliable files whether created by intentional fraud or by innocent errors and omissions can have a devastating effect in terms of dollars lost due to excessive costs and in terms of possible short supply of critical parts for fleet operations. Part of the solution to this problem is to exercise close control over who has access to sensitive financial and inventory files. Also, since individual responsibility for both intentional and accidental data errors must be ascertained if there is to be prevention and correction of this problem, a reliable system of user authentication or identification must be established.

6.1 SELECTION GUIDELINES

Before any authentication system is considered, a cost-benefit analysis should be performed to determine the maximum predicted savings due to loss protection compared to the total cost of the protective system [18], [19], [20]. As part of this study, attempts should be made to determine a list of all potential risks or threats to data files, the probability of a risk occurring, and the expected loss expressed in dollars resulting from the occurrence of each risk possibility. This not only provides necessary information for the cost-benefit evaluation but also gives an indication of where resources should be allocated to provide maximum impact.

When considering the total cost of an authentication system, the following items must be included:

- Hardware
- Software
- Storage
- Installation and Testing

- o Maintenance and Repair
- o Computer Processing
- o Encryption Costs
- o Device Protection and Alarms

Other than cost benefits, there are several factors which will limit the choice of a prospective authentication system. These factors are given below.

- o Number of users
- o Number of access points
- o Number of access levels to be accommodated
- o Throughput rate
- o Level of identification
- o User acceptance
- o Ease of installation
- o Identification error rates
- o Hardware failure rates and reliability
- o Backup schemes
- o Environment
- o Future technology advances

6.2 NAVY SUPPLY REQUIREMENTS

In any large organization it is sometimes difficult to obtain a detailed description of the needs, problems, current procedures, and resources of the system. In the case of Navy Supply, when data on current authentication devices, procedures, and perceived problems was sought, the information in many cases was either unavailable or difficult to compile within the time frame of this report. Some facts and examples were obtained from the task statement and from discussions with the task monitor. Even so, the description of current problems and needs is limited to a few examples and is certainly incomplete.

Based on the information supplied by the Navy, it appears that there are primarily two areas of concern. The first is in the supply environment that includes equipment handling and storage areas. There have been recorded cases where terminals were logged on at the beginning of the day but left unprotected for a portion of the work shift. While documented loss has not been found as a result of this action, there is the potential problem of unauthorized access ranging from untrained personnel casually experimenting with a terminal to individuals trying to defraud the system. Apparently there is little incentive on the part of authorized users to carry out correct log-off procedures. Also, there is no reverification program or automatic log-off provided by the host computer following substantial line inactivity. The Navy wants better control of terminals and, in particular, authentication of each user of the system, especially following a lengthy period of line inactivity.

The second problem area focuses on the office environment. There users have access to receipt files and other financial data. The UNIX computer used in at least part of the office automation system does have a time-out feature to cover periods of inactivity at the terminals. The main concern here appears to be the verification of the identity of the actual user siting at the terminal.

6.3 RECOMMENDATIONS

The recommendations given here necessarily reflect the lack of complete background information concerning current problems and are therefore somewhat limited. After detailed loss figures due to terminal misuse resulting from inadequate authentication become clearer to Navy Supply, and especially after a determination of not only potential but actual causes of loss is completed, then the information, description, and analysis of authentication devices and techniques made in the body of this report may be usefully applied. However, at this point there are only a few general recommendations that can be made.

6.3.1 Utilize Existing Features

There is a need to clearly define security procedures as they apply to the use of terminals. In this way maximum use of currently existing computer system features could be obtained. For example, it should be standard operating procedure to log-off from a remote terminal after all transactions are completed or when leaving the terminal unattended. This action should be taken even though reinstituting the log-on procedure may be inconvenient or time consuming. With the terminal logged off, the existing password protection scheme of the host would then protect the data files. Periodic on site inspection or remote monitoring of line activity by security staff could enforce the log-off policy for those users who fail to comply with the required procedures. This method of control for the supply environment has the advantage of being inexpensive to implement without any computer system modifications. It does however rely on the forced willingness of some of the users to change their behavior.

6.3.2 Software Change

Another relatively inexpensive method to deal with the supply environment problem is a software program that requires a reverification procedure after a period of line inactivity. Such programs are fairly standard but can be modified to suit particular needs. For example, the program could issue a prompt which would request the user to press a certain control key in order to maintain access to the host. This permits the user time for thinking at the terminal without losing the connection to the main computer. If the prompt is not answered in a certain length of time, then the program can request the person at the terminal to reenter his password. This can be done without breaking the line and without imposing a time limit for a response. At this point if an invalid password is entered at the terminal, the terminal is automatically logged-off by the host.

Software changes depend on the capabilities and available support provided by the host which may be limited in the Navy Supply system. But even with a software implementation, such as the one described above, the user's identity would not have been verified. However, a log-on procedure that requires the user's name and a password, which may not be unique, may provide Navy Supply with a sufficient level of security at a price that can be afforded.

6.3.3 Coded Card System

While passwords provide good security if properly used, the group passwords often employed in the Navy Supply system lack features that provide for fairly reliable individual identification. This is great concern in the office environment as well as the supply area. A system, independent of the host, that can provide individual identification with reasonable security at a manageable price is a coded card system.

A system of card readers can be controlled by a central processor or minicomputer separate from the host. Instead of unlocking a door or gate as is often done by a card reader, a remote terminal would be unlocked when a valid card is read. The central processor could record the user's name, unique identification number, authorization levels, the terminal used, the date, and the time of day for future use in auditing studies, billing, or security investigations. Also, part of the reverification procedure could require reinserting the card into the reader thereby providing reidentification after prolonged line inactivity.

Using a combination of uniquely coded cards and passwords could provide a very good level of security, identification, and control. There are systems that could be custom designed for as little as $150,000 depending on the features desired. It should be realized that most of this price is a one-time cost and that with the life of the system spread over several years,

it is truly cost effective. Another advantage of the card system is that the central processor can also be used to monitor smoke detectors, flood detectors, and intruder alarms. In short, a total protection system is possible with this scheme.

For the sake of completeness, it should be noted that there are a number of terminals with built-in card readers. However, these systems require software support in the host.

6.3.4 Identity Verification Devices

Automated identity verification devices are not recommended for use in the Navy Supply System at this time. They are relatively expensive and still have unacceptably high false reject error rates. It is also possible to circumvent some of these devices with artificial templates. In almost every case the false accept error rate is only an approximation. New research and developing technology will lead to improvements in these devices and an eventual lowering of their cost. At that time it would be productive to reanalyze their cost-benefit values.

REFERENCES

[1] Workshop on Password Use, National Bureau of Standards, Gaithersburg, Maryland, June 1980.

[2] Wood, H., "The Use of Passwords for Controlled Access to Computer Resources," NBS Special Pub. 500-9, May 1977.

[3] Bean, C. H. and Prell, J. A., "Personnel Access Control," Proc. 1977 Carnahan Conf. on Crime Countermeasures, University of Kentucky, Lexington, April 1977.

[4] Austin, M. L., "Credentials," Entry Control Systems Handbook, Sandia Laboratory Report SAND 77-1033, 1977, revised September 1978.

[5] Broel, F. G. and Myers, R. D., "Personnel Identity Verification System," Entry Control Systems Handbook, Sandia Laboratory Report SAND 77-1033, 1977, revised September 1978.

[6] Sykes, D. J., "Positive Personal Identification," Datamation, November 1978.

[7] Meissner, P., "Personal Identification Devices Help to Keep Networks Safe," Data Communications, April 1977.

[8] Warfel, G. H., "Automated Identification Methods," Security Management, June 1978.

[9] Fejfar, A. "Test Results, Advanced Development of BISS Identity Verification Equipment," Mitre Corporation TR 3442, Bedford, MA, 1977.

REFERENCES (Cont'd)

[10] Woodard, J. P. and Maier, J. J., "Automatic Entry Control for Military Applications," Proc. 1979 Carnahan Conf. on Crime Countermeasures, University of Kentucky, Lexington, May 1979.

[11] Kuhn, M. H. and Geppert, R., "A Low Cost Speaker Verification Device," Proc. 1980 Carnahan Conf. on Crime Countermeasures, University of Kentucky, Lexington, May 1980.

[12] Crane, H. D., Wolf, D. E., and Ostrem, J. S., "The SRI Pen System for Automatic Signature Verification," Symposium Proc. Trends and Applications 1977: Computer Security and Integrity, Gaithersburg, MD, May 1977.

[13] Liu, C. N., Herbst, N. M., and Anthony, N. J., "Automatic Signature Verification: System Description and Field Test Results," IEEE Trans. on Systems, Man, and Cybernetics, January 1979.

[14] Herbst, N. M. and Liu, C. N., "Automatic Signature Verification Based on Accelerometry," IBM J. Res. and Devel., Vol. 21, May 1977.

[15] de Bruyne, P., "Developments in Signature Verification," Security Management, June 1978.

[16] Warfel, G. H., "Signature Dynamics for Access Control," Security Management, July 1980.

[17] Hale, W. J. and Paganini, "An Automatic Personal Verification System Based on Signature Writing Habits," Proc. 1980 Conf. on Crime Countermeasures, University of Kentucky, Lexington, May 1980.

REFERENCES (Cont'd)

[18] Bean, C. H. and Prell, J. A., "Personnel Access Control - Criteria and Testing," Security Management, June 1978.

[19] Meissner, P., "Guidelines on Evaluation of Techniques for Automated Personal Identification," NBS FIPS Publication 48, April 1977.

[20] Orceyre, M. J. and Cortney, Jr., R. H., "Considerations in the Selection of Security Measures for Automatic Data Processing Systems," NBS Special Pub. 500-33, June 1978.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

14

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: SDC-TM-WD-7999/401/00	2. GOVT ACCESSION NO.: AD-A089344
3. RECIPIENT'S CATALOG NUMBER:	
4. TITLE (and Subtitle): 6 AUTHENTICATION DEVICES AND PROCEDURES	5. TYPE OF REPORT & PERIOD COVERED: 9 FINAL rept.
	6. PERFORMING ORG. REPORT NUMBER: TM-WD-7999/401/00
7. AUTHOR(s): 10 John M. Vasak	8. CONTRACT OR GRANT NUMBER(s): 15 N00173-78-C-0455
9. PERFORMING ORGANIZATION NAME AND ADDRESS: System Development Corporation, 7929 Westpark Drive, McLean, VA 22102	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: Task #10
11. CONTROLLING OFFICE NAME AND ADDRESS: Naval Research Laboratory, Washington, DC 20375	12. REPORT DATE: 11 29 August 1980
	13. NUMBER OF PAGES: 58
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): 12 61	15. SECURITY CLASS. (of this report): Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Authentication; coded card; identification; identity verification; password; selection guidelines; test results

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document contains summary descriptions and analysis of authentication devices, procedures, and technologies. Also included are performance comparisons, relative costs, and current research and development areas. Special emphasis is placed on passwords, card systems, and identity verification devices. Selection guidelines are also given.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

339860

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)