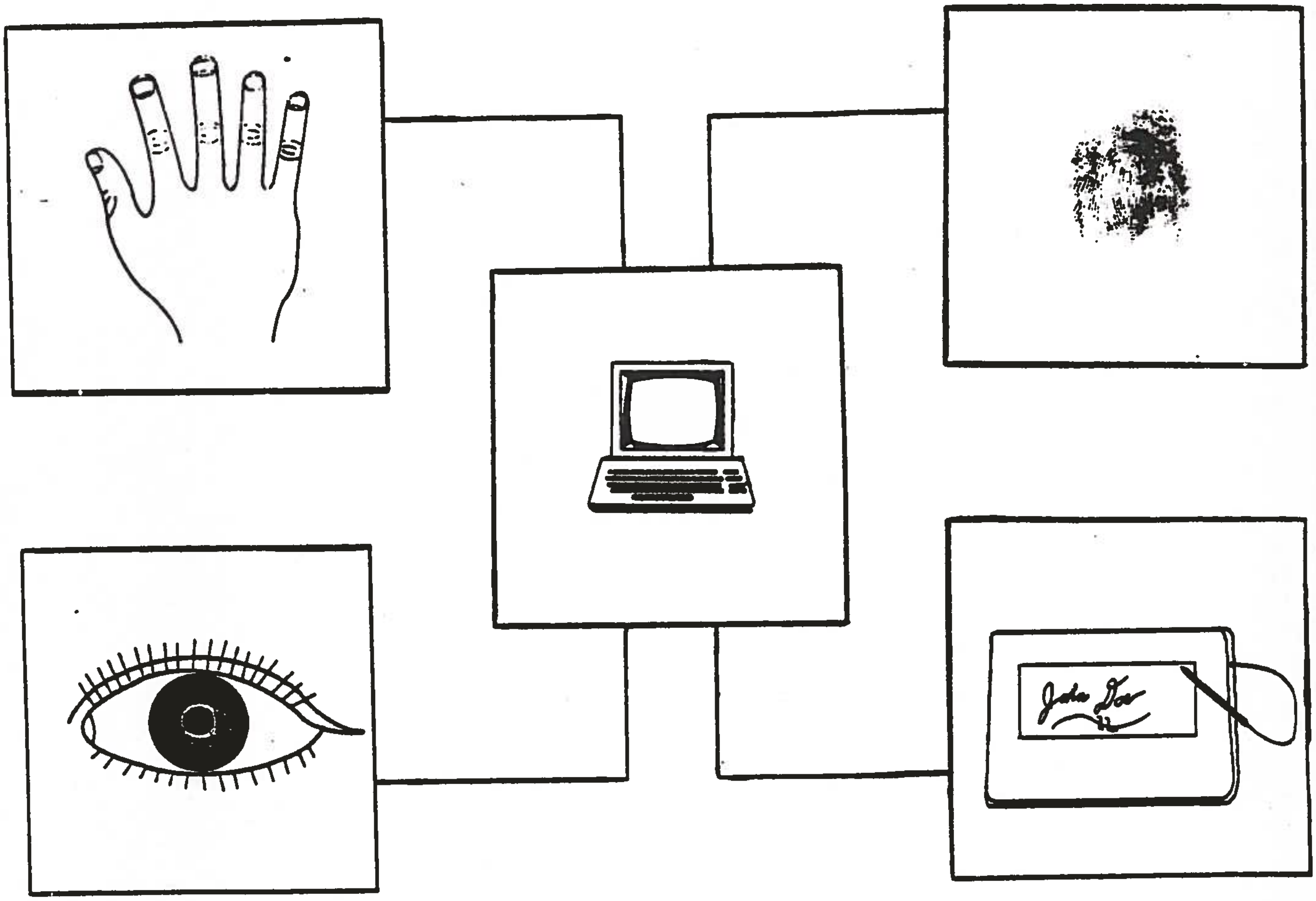
Computer Resource Management Technology Program (PE 64740F) Task #9 - Advanced User Authentication

DOT-TSC-RSPA-88-1
DOD-VA846-88-1

Final Report
March 1988



Prepared by

U.S. Department of Transportation
Research and Special Programs Administration
Transportation Systems Center
Cambrige, MA 02142

Prepared for

U.S. Air Force
Electronic Systems Division
ESD/XRSE
Hanscom, MA 01731-5000

Technical Report Documentation Page

1. Report No. DOT-TSC-RSPA-88-1	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle COMPUTER RESOURCE MANAGEMENT TECHNOLOGY PROGRAM (PE 64740F) Task #9 - Advanced User Authentication	5. Report Date March 1988 6. Performing Organization Code DTS-43
7. Author(s) L. Watson, W. Barron	8. Performing Organization Report No. DOD-VA846-88-1
9. Performing Organization Name and Address U.S. Department of Transportation Research and Special Programs Administration Transportation Systems Center Cambridge, MA 02142	10. Work Unit No. (TRAIS) VA846/D8050 11. Contract or Grant No. PE 64740F
12. Sponsoring Agency Name and Address U.S. Air Force Electronic Systems Division ESD/XRSE Hanscom, MA 01731-5000	13. Type of Report and Period Covered Final Report May 1987 - November 1987 14. Sponsoring Agency Code ESD/XRSE

15. Supplementary Notes

16. Abstract

This report examines the various technologies which can be used to perform user authentication, with an emphasis on biometric techniques. The methods by which each device performs the authentication of users are examined individually, and their suitability for a multi-level computer environment is assessed. The status and direction of computer user authentication devices and techniques, in general, are evaluated. Included in this report are independent testing results, government requirements, selection considerations, and a glossary of computer security and user authentication terminology.

17. Key Words User Authentication, Computer Security, Biometrics	18. Distribution Statement DOCUMENT IS AVAILABLE TO THE PUBLIC THROUGH THE NATIONAL TECHNICAL INFORMATION SERVICE, SPRINGFIELD, VIRGINIA 22161

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 138	22. Price

Reproduction of completed page authorized

EXECUTIVE SUMMARY

This report examines the various technologies which can be used to perform user authentication, with an emphasis on biometric techniques. The methods by which each device performs the authentication of users are examined individually, and their suitability for a multi-level computer environment is assessed. The status and direction of computer user authentication devices and techniques, in general, are evaluated. Included in this report are independent testing results, government requirements, selection considerations, and a glossary of computer security and user authentication terminology.

This document is intended to serve as a guide to user authentication devices, and is written at a level suitable for those at entry level engineer/computer scientist and above.

CONTENTS

CHAPTER ONE

Introduction

This report documents the Computer Security Advanced User Authentication study conducted by the U.S. DOT Transportation Systems Center (TSC) for the Computer Resource Management Technology (CRMT) Program Office of the Electronic Systems Division (ESD) of the U.S. Air Force. This is an engineering development program which focuses on problems associated with the acquisition, support, and development of computer resources in mission critical Air Force and other DoD systems.

Engineering development is termed "the final development and test of an item judged to be operationally, technically, and economically desirable and acceptable as a solution to a problem or to a technical objective". The CRMT Program is a primary vehicle for transferring to operational use, the products of advanced development efforts in computer resource technology, from work accomplished in Air Force laboratories, industry and academia; and is the only full-scale engineering development program that addresses computer security.

Findings and opinions within are in deference to the computer security and user authentication requirements set forth in the Department of Defense Trusted Computer System Evaluation Criteria[109], and the ADP Security Policy, Procedures and Responsibilities (Air Force Regulation 205-16)[119] documents. Both of these documents are a direct result of DoD Directive 5200.28, Security Requirements for ADP Systems[121] which support the DoD computer Security initiative as stated in the National Security Decision Directive 145, and address the processing, storing, using, producing or transmitting DoD confidential, secret, top secret classified information, or sensitive, critical unclassified information.

1.1 Background

During l985, ESD requested The MITRE Corporation perform a study of current technologies for personal identification of computer system users, in response to the Air Force's statement of need for security requirements of multi-level secure computer systems. The study produced a report which provided the framework for studying the use of expert system technology for automated user authentication. It included an inventory of current authentication technologies in both software and hardware, and an exploration of the advantages of expert system software over current technologies. This report was entitled Authentication Tools Study [27] and identified the following as the advantages of an expert system:

1. An Artificial Intelligence (AI) solution is basically a software solution that could be made portable among environments or incorporated within a hardware device.

2. Such a solution incorporates a series of sophisticated processes that evaluate the likelihood that the user is who s/he claims to be as opposed to using a single 'key.'

which data can be accessed without the recipient being identified and verified as an authorized user. The incorporation of a state-of-the-art identity verification device in an otherwise insecure system is analogous to installing a steel door on a safe with glass windows. The easy circumvention of any authentication mechanism renders it virtually ineffective. The scope of this report is only to detail the various characteristics of new and developing user authentication technologies; their integration into a system that is otherwise secure is assumed.

Although this report focuses primarily on biometric authentication technologies, some attention is given to other techniques, such as passwords and PINs, access keys and tokens, and password generators. The reason for this attention is that, while by themselves, these techniques offer only limited security, they can be combined with others to pose a much more formidable barrier to intruders. We will also focus briefly on government requirements and actions regarding computer user authentication, and on the factors to be considered when selecting a user authentication strategy.

program that attempts to login using different passwoıds repeatedly until it trips upon the correct one. To combat this, some systems lock out users after a certain number of unsuccessful attempts. Others create their own passwords or personal identification numbers (PINs), with some allowing the user to select from a randomly generated list. Also, the system may require that the password be changed periodically, or even within each session. The inherent problem with each of these methods is that the password becomes more difficult to remember. Users will be tempted to write down their passwords, and perhaps even tape them to the terminal screen. Obviously, this is not viewed favorably by those involved in system security!

Dynamic Passwords

There are some systems which employ a somewhat different procedure called dynamic or variable passwords. These are techniques which require the user to provide a different password with each login. The user keeps a list of active passwords arranged in a specific order, and he must keep track of the most recent password entered. Each time he decides to access the system, he simply enters the next password .on his list. The problem here is that unless he is capable of memorizing the list, and remembering consistently the last password entered, this method becomes more an issue of possession than knowledge. An intruder need only to obtain the list and examine the check marks to gain access to the system.

Interactive Pass-Phrases

Another method of knowledge based authentication is question and answer pass-phrases. This involves initially providing the computer with the answers to specific personal questions. Then each time the user logs in, he is asked one of the questions, to which he provides the appropriate answer. The effectiveness of this method is based primarily on the value of the question. Ideally, the answer to each question should be easy to remember, difficult to guess, universally applicable to all users, and word for word repeatable for each login. An example of a good question is "What is the name of my first girlfriend/boyfriend?" The response can be typed verbatim every time, is virtually impossible to guess, is known only by the user, and unlike many passwords, will likely never be forgotten.

The problem with this method is that not all questions are good ones, and .the registration process can be time consuming. However, if the computer is provided with good questions which obtain unique responses from each user, this method can be much more effective and no more inconvenient to the user than passwords.

Pass-Algorithms

Pass-algorithms is another recently developed knowledge based authentication methodology which is gaining increased popularity. Most often it is set up so that each user has a simple algorithm to remember, say, (Ax3) + 2. Each time the user logs in, the computer issues a value for A. The user computes the solution for his algorithm and enters that as his one-time password.

Pass algorithms have some undesirable characteristics, however. If the algorithm is too complex to solve mentally, or because numbers are more difficult to remember than meaningful character strings, the user may be tempted to write down his algorithm, thus sacrificing its secrecy to some extent.

2.2 - Possession-Based Authentication Methods

An identity verification device based on possession usually implies some kind of key. Today, the degree of sophistication of computer access keys is wide ranging. In this section, we will examine the different types of access keys currently available, and describe the virtues and drawbacks of each.

Metal Keys

Some personal computers come equipped with a simple metal key and lock. When locked, the computer will not operate. It is an inexpensive security method, one that is easy to operate and requires little maintenance. However, such keys are easy to duplicate, and the locks tend to be easily forced or jimmied. Metal keys simply do not provide a significant amount of security.

Magnetic Cards

Another type of access key which is becoming increasingly popular is the magnetic card. These are cards which contain information in a magnetic stripe that can be read by small stationary devices. They are being used to secure rooms in hotels and banks, and by credit card companies to store account information that can be easily read and transmitted. The cards are inexpensive and easy to carry. Weaknesses of such cards are that they are fairly easily scratched or erased, making the data unreadable, and they can be duplicated if the proper equipment is available. Some modifications in the layout of the tape have been made by some companies through a process called "watermarking" which makes the information more permanent, and the cards more durable.

Barcode Cards

Barcode cards are cards with thin lines printed on them which can be read by a light sensitive pen or infrared beam. They operate in a similar manner to the devices that scan products at supermarket checkout stands. These cards are slowly replacing library cards, and are being adopted by companies using time clocks. They are inexpensive and extremely durable, but are very easily duplicated. In fact, some are capable of being forged by simple photocopies.

Infrared Scanning

This technology involves the printing of a barcode inside the card, which can only be read using low-level infrared light. Unlike ordinary barcode cards, these are difficult to copy, but the systems supporting them are much more expensive.

Wiegand Cards

On a similar theme, Wiegand cards are cards which carry data internally, thus keeping it safe from scratching, yet can be read by being slid through a compact reading device. They contain processed short wires that react uniquely to changes in polarity and strength of magnetic fields which can be sensed by a Wiegand card reader. They are thicker and slightly more expensive than magnetic stripe cards, but they are becoming increasingly popular because they are more durable and much more difficult to counterfeit.

Barium Ferrite Cards

Sometimes called magnetic spot cards or magnetic sandwiches, barium ferrite cards are popular primarily because they are inexpensive. Barium ferrite, a magnetic substance, is arranged between two pieces of plastic to form specific codes. The drawbacks to this technology are that the cards are not particularly durable, and the codes can be erased.

In general„ card keys are especially useful in computer access control applications because the devices required to read them are compact and can be placed near, on, or in a workstation. They are also fairly inexpensive, especially in contrast to other means of user authentication. The problems they have are that they can be counterfeited by skilled people (some fairly easily), and can be lost or stolen. Also, they can be given away to unauthorized co-workers or friends, which makes auditing of system users meaningless.

Access Number Decryptors

There are other access control devices that need only be possessed in order to log into a computer system. One is an access number decryptor, or a password generator. When logging in, the system displays a random number or character string. The authorized user enters it into a calculator-like device which decrypts it using an algorithm and returns a different number or character string. The user then submits this string to the system, and access is granted if it is correct. Each device can contain a different algorithm, which indicates whose decryptor is being used.

Screen Reading Devices

Along the same lines, a screen reading device is one which interprets an undecipherable image displayed on the screen by the system. After being held against the CRT, it returns an access number which must be entered into the keyboard to obtain access to the system.

Both the decryptor and the screen reader have the advantage of being usable on remote terminals. This means a PC user can gain access to a mainframe through a modem, and the mainframe can, in turn, authenticate the user's identity. The problems with these devices are that they are fairly fragile in comparison to access cards, and like all other possession based methods, intruders need only to obtain the device to access the system.

Dial-Back Modems

Other ways of authenticating remote users are through special modems. With a dial-back modem, the user telephones the mainframe, enters his user ID, and hangs up. The mainframe then calls him back at a predetermined number, and the connection is made. The use of this device authenticates the user's location rather than his identity. However, if the user has possession of the predetermined system and modem, there is some evidence that he is the authorized user, the strength of which depends on the security of the remote site.

There are a few ways of circumventing this device other than breaking in and using the authorized workstation. Telephone lines are untrusted, and can be tapped, or even rewired so that the mainframe calls another location. Also, some outdated switching systems have an unusual quirk, where only the caller can terminate a conversation. If an intruder calls a mainframe through one such system, he simply remains on the line. If the dial-back device is not one which checks for a dial tone, it dials the number into the already active line, and the intruder initiates the connection. However, this specific combination of equipment is rare, and by itself is not considered a significant security threat.

Summary of Possession-based Methods

Like passwords, possession-based authentication methods tend to be fairly inexpensive to purchase and implement. Also, since cards, keys, and decryptors are

- dental information
- footprints
- lip prints
- dynamic actions (gait, golf stroke, etc.)
- head bumps (machine phrenology)
- responses to physical stimuli
- blood
- DNA and other chromosomal features
- saliva
- urine
- tongue prints
- eye geometry
- electrocardiograms
- electroencephalograms
- face shape (profiles)
- ear shape
- body part X-rays
- polygraph output using known questions
- scars and physical deformities
- wrist vein patterns
- ability to recognize objects in complex graphic figures
- characteristic performances during games or tests
- prose or authoring characteristics
- scent or odor
- interpupilary distance
- ability to dampen vibration

Devices which analyze these traits have not been extensively developed in industry due to the difficulties involved in acquiring accurate data and/or obtaining repeatable results, as well as the lack of acceptance by many system users. If, in order to log into a system, users were required to kiss a machine interface, have probes attached, or be subjected to a urinalysis, blood, or impact test, it is conceivable that they may resist using the system!

Biometric authentication represents the only means of potentially obtaining 100 percent certainty that a computer user is who he claims to be. Although biometric technology is only rarely employed at this time, increased usage is projected for the future(see Appendix D). Demand for such devices has been slow, due in part to the fact that current technology does not yield inarguable results. Because of this, two types of errors have become standard assessments of the accuracy of these devices. Type I errors occur when legitimate users are denied access, and Type II errors occur when intruders are granted access. We will refer to these error types when describing the effectiveness of specific devices, and we'll discuss them in greater detail in Section 2.5.

Unlike other methods of authentication, biometrics cannot be stolen, inferred, or given away. An excellent biometric authentication tool is one that is inexpensive and can accurately measure a physical trait that has high interpersonal variations and low intrapersonal variations. There are some devices which by themselves do not offer a great deal of security, but function effectively in combination with other techniques. The advantages and disadvantages of combining methods will be examined in the following section.

PIN. Most of those that do contain the PIN information in the card. Apparently, it is felt that three different layers of authentication provide more security than most systems require, and is asking for too much patience from legitimate system users.

While it is easy to understand why one would want high security, the need for protective measures to be unobtrusive may not be as obvious. If a mechanism inconveniences users a great deal, they will find ways of circumventing it. Users will be tempted to remain logged in after leaving the system to avoid dealing with the tedious authentication process. If the system has a periodic re-authentication process that is laborious, users may find some way to disable the clock mechanism or the authentication system altogether. These actions could leave the system virtually unprotected, and ironically would be caused by the very security measures designed to protect the system.

As is the case in other sensitive areas, security measures in the computer field require the cooperation of those who use the system in order to be effective. If users are made to understand the importance of computer security, they will realize that authentication devices are designed to protect them and the people they work for, and that it is therefore important not to undermine their operation, especially where highly confidential data is involved.

The amount of security required for a given system is not always easy to assess. Various methodologies exist for conducting risk assessments to determine how much should be spent on system security procedures and devices. Although this report does not encompass the details of risk assessment, it is enough to say that a system with highly sensitive information may require a rather exotic security system to ensure that data is not relinquished. Specific systems incorporating biometric technologies will be examined in detail in Chapter Three.

2.5 - Authentication Errors

Despite the wealth of technology and effort that has gone into developing techniques for the automatic identification of individuals, a flawless device is beyond today's state-of-the-art. Therefore, the effectiveness of a biometric device in performing this function is measured by the infrequency with which it makes a mistake. Basically, there are two types of errors which a fully operational authentication device can make:

- Type I Errors - Rejection of an authorized user (sometimes called False Rejection errors)
- Type II Errors - Acceptance of an imposter (sometimes called False Acceptance errors)

The rates with which Type I and Type II errors occur tend to be inversely related. That is, if the tolerance of a device is adjusted such that rejections occur less often, it then will be less likely that an authorized user will be rejected, but more likely that an imposter will be accepted.

In access control applications, it is usually considered desirable to encounter Type II errors less frequently than Type I errors. The theory here is that it is preferable to lock out an authorized user for the time being than to allow access to an intruder who could potentially damage the system or steal the data. Exactly how tight the tolerances should be set is a function of how sensitive the data is, independence is more relevant. If the machines carry different error rates, then rather than being doubled and squared, the error rates would instead be added and multiplied respectively.

Rarely is more than one biometric technology employed to secure a single device or facility. This is due primarily to the expense involved in purchasing each component, and the increase in work and patience required by system users when attempting access. In fact, we have found only two instances where two biometric devices are used in combination. They are both rumored to secure highly sensitive, defense-related facilities. They apparently work well together in their application, because the personnel understands the extreme importance of system security.

Although many devices come equipped with their own software drivers, it may be desirable to have software custom written for certain applications. Some variables which may have to be altered for certain applications include:

- The number of successful identification attempts required for access;
- The number of rejections allowed before an alarm is signaled;
- The action taken when an alarm is sounded (i.e. lock out user, notify system administrator, etc.);
- The types of devices or methodologies used for authentication;
- The requirements for accessing data of a higher security level;
- The type of information to be contained in a system-generated audit log.

Such software is an integral part of a computer security system; however, its highly customized nature makes it impossible for this report to cover the diverse software products currently available. The software available as part of a biometric device's security system will be described with the devices in Chapter Three.

and classification include North American Morpho Systems, Identicator Corporation, and NEC Information Systems. However, we are more concerned with investigating fingerprint devices aimed at access control. This is more commonly called a fingerprint authentication device, and is the type we will focus upon here.

The use of fingerprints for access control carries one advantage over other identification processes: An unauthorized person who fails to gain access via a fingerprint authentication device not only is unable to obtain stored data, but also leaves behind a highly detailed fingerprint, which greatly facilitates his capture. The possibility of entrapment is one of the best deterrents to crime of any type.

In October 1987, Russell Maxwell of Sandia National Laboratories pointed out that the accuracy of fingerprint verifying equipment is climate dependent. In a region of low humidity, fingerprints have a tendency to dry out and become chapped, making their images cracked and unclear. However, Maxwell found that this problem was correctable, largely through the regular use of skin moisturizer.

Fingerprint authentication devices have been commercially available for only a few years, but are one of the more popular types of identity verification. Two manufacturers, Fingermatrix and Identix, are among the few profitable firms in the biometric industry. While several companies are at work developing new fingerprint verifiers, those that are currently available are discussed below.

3.1.1 - Ridge Reader by Fingermatrix

Fingermatrix was founded in 1976, and in 1978 bought fingerprint analysis technology developed through Calspan Corporation's device called Fingerscan. Product development lasted six more years, resulting in the P100 Physical Access Control device. Several variations on this product have since been introduced. After typing in a PIN, the user places a preregistered finger on the scanning surface. The device builds a 400 byte template which describes the x, y, and theta components of the bifurcations (forks) for the ridges of each fingerprint. This data is compared to the historical, preregistered data for the claimed person, whereupon an accept/reject decision is made.

The Fingermatrix Ridge Reader

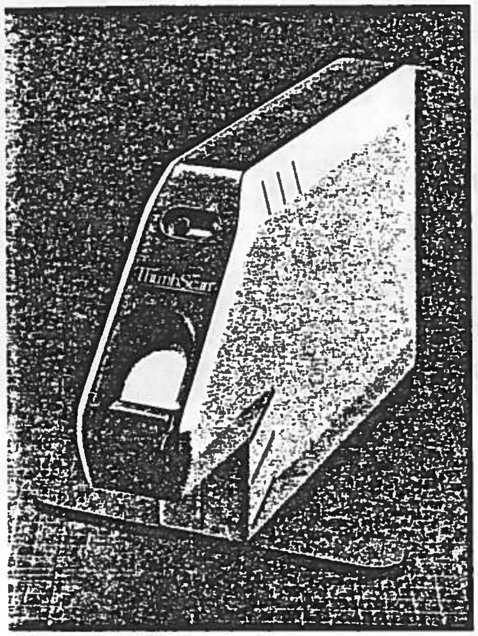
Each of the Identix products is aimed at physical access control applications, although data security may be achieved by providing the computer with software which integrates the Identix's decision responses with the host access control functions. Identix claims their tests indicate a Type I error rate of 2% and a Type II error rate of less than .0001%. It is assumed, although not stated directly, that to arrive at these rates, users registered using their highest graded fingerprint on the A to C scale. The price for each device has been $7500, but in September 1987, it was dropped to $5000.

3.1.3 - TSI Series by Thumbscan, Inc.

In June 1987, Thumbscan unveiled its thumbprint user authentication device after more than two years of development. Some have called it the first of the second generation biometric devices, because it is compact and inexpensive ($995, less than $500 in quantities > 100). It attaches to the side of a terminal, compares thumbprint images to those previously registered by the authorized user via a Xerographic technique, and makes an accept/reject decision.

There are currently three versions of the Thumbscan device. The TSI 101 is designed for use on asynchronous terminals, which includes most major minicomputer and UNIX-based environments. The TSI 201 attaches to bisynchronous terminals, such as the IBM 3270 series and compatible mainframes. The TSI 301 is intended for use on IBM PCs, XTs, ATs, and compatibles. The host program is available in either software or on expansion cards. The prices and accuracy of the three devices (and programs) is said to be the same. Design goals were to obtain Type I errors of about .5% and Type II errors of about .005%, but there has been insufficient field testing to determine if these goals have been met.

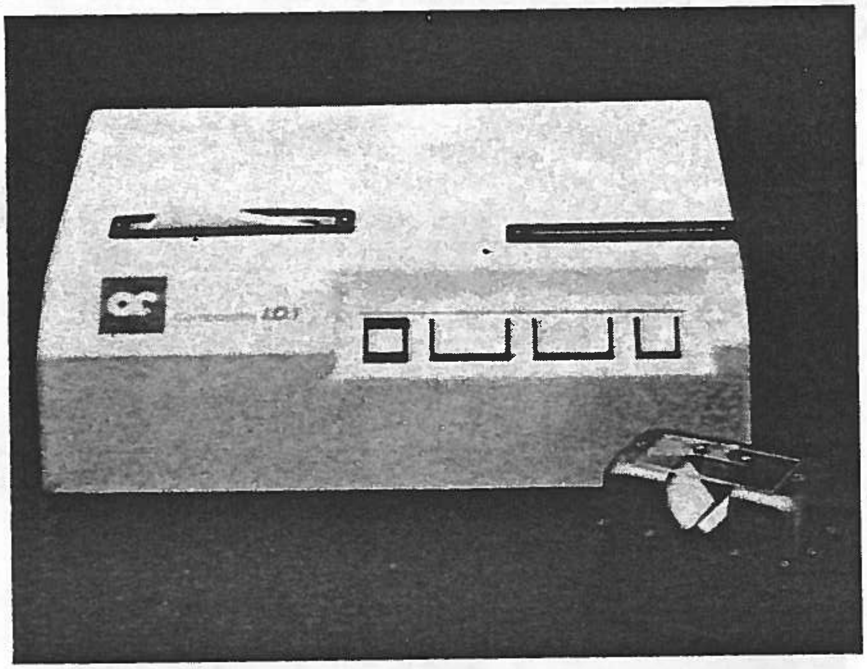
The Thumbscan TSI 201



3.1.5 - ID-1 by Comparator Systems

Comparator Systems was first organized in 1976, and introduced its first product in 1985. The ID-1 is a small desktop fingerprint authentication device. Upon enrollment, users record their fingerprints on a plastic card using a special ink. When access is attempted, the user leaves a fingerprint on another card, and both cards are fed into the machine, which compares them. The trouble with this device is that the reference print for the claimed person must be manually input by a security guard, so the system is only as secure as the reference cards and the guard who retrieves them. It is being used primarily in prisons and at border crossings. The ID-1 costs about $9250, but government and quantity discounts may apply.

The Comparator Systems ID-1



3.1.6 - Tenprinter by CFA Technologies

CFA is a privately owned company which developed a technology initially intended to identify people through the classification of their fingerprints. Tenprinter is a device designed to make comparisons using the FBI's 10-print cards, the standard forensic cards which shows the print of each finger on both hands. This product is primarily aimed at the law enforcement market. However, CFA has recently introduced several access control versions priced in the $1000-$1500 range. They can also be networked through a customized central processor costing between $20,000 and $40,000. There is no available information on operating procedures or accuracy.

3.1.8 - Fingerprint Authentication Product Summary

The table below contains information regarding the age, price, and accuracy of each fingerprint authentication device. The error rates given are those claimed by the manufacturer, and the prices are estimates for typical configurations.

PRODUCT	VENDOR	INTENDED APPLICATION	CLAIMED ERROR RATE	ESTIMATED PRICE	FIRST AVAILABLE
Ridge Reader D100	Fingermatrix	Computer security	Type I: .5% Type II:.001%	$3500	November 1984
Ridge Reader P100	Fingermatrix	Networked physical security	Type I: .5% Type II:.001%	$3500-$5500 per door	November 1984
Ridge Reader P200	Fingermatrix	Single door security	Type I: .5% Type II:.001%	$5500	November 1984
Ridge Reader P300	Fingermatrix	Smart card model of P200	Type I: .5% Type II:.001%	$5500	April 1987
IDX-10	Identix	Desktop unit for physical security	Type I: 2% Type II: .0001%	$5000	June 1986
IDX-10W	Identix	In-wall unit for physical security	Type I: 2% Type II: .0001%	$5000	June 1986
IDX-50	Identix	Smart card version of IDX-10	Type I: 2% Type II: .0001%	$5000	January 1986
TSI 101	Thumbscan	Asynchronous terminals	Type I: .5% Type II:.005%	$995	June 1987
TSI 201	Thumbscan	Bisynchronous terminals	Type I: .5% Type II:.005%	$995	June 1987
TSI 301	Thumbscan	PC Security	Type I: .5% Type II:.005%	$995	June 1987
Security Access System	De La Rue Printrak	Physical security	not stated	RFQ only	July 1987
ID-1	Comparator Systems	Guard assisted physical access	not stated	$9250	1985
Tenprinter	CFA Technologies	Physical access control	not stated	$1000 to $1500	August 1987
Fingerkey 2000	El-De	Stand alone with interface	not stated	$7000 to $8000	June 1987

3.3 - Speaker Recognition Systems

For many years, the efforts of several companies have gone into the development of voice technology. Aside from the synthesis of speech, most of the research in voice technology falls into two classes: Speaker recognition and speech recognition. The two differ in that a speaker recognition system determines who is speaking, rather than what is being said. Of the two, there is more research being conducted in the area of speech recognition, because of the efficiency and user friendliness of an effective system for voice input of data and text. However, our concern is with devices which identify people, which is what a speaker recognition system does.

Recognition of individuals by the sound of their voices is easier for a machine than recognizing what is said, because understanding the context of phrases and adjusting for accents are tasks which are not as easy to program. We as humans find speaker recognition more difficult, but not impossible. Those who are blind rely on voices as virtually their only means of differentiating between individuals, and some can do so with remarkable accuracy. They accomplish this by memorizing the tone and pitch of each person's voice as well as their typical remarks. Machines typically perform this task in a different way, by recording the waveforms produced when a person speaks a certain word.

Most speaker recognition systems, also called voice verifiers, employ a dynamic password system; that is, one where the system requests a different word be spoken with each login attempt. This is in an effort to discourage the use of tape recorders to circumvent the device, although each manufacturer claims that no tape recording it has produced has been capable of deceiving the system.

Human impersonation of an authorized user is not a very effective means of circumventing the device either. Although a person may be able to sound like another person, his or her electronic vocal representation, or glottal spectrum, is not as similar to the other person's voice as one would think. Therefore, a skilled impersonator would have no more success accessing classified data protected by the typical speaker recognition system than would anyone else.

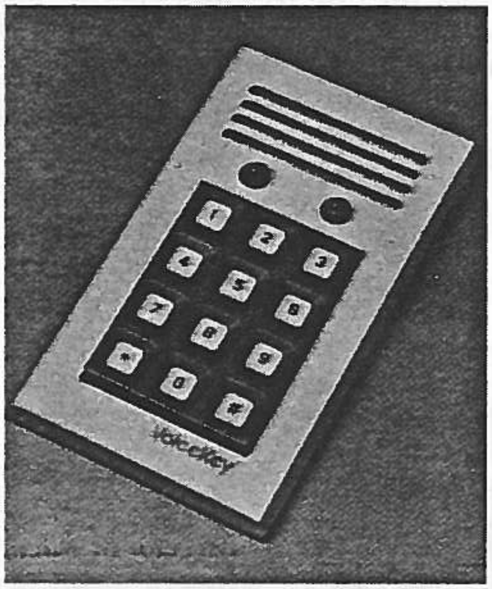
Below are the currently available speaker recognition devices. There are also two prototype systems developed by Los Alamos National Laboratories and by British Telecom Research Labs, but these devices are not available commercially. There are also systems by Voice Industries Corp., Interstate Voice Products, Texas Instruments, and Voice Identification, Inc., but they are aimed either at voice input of data, or at the identification of people for forensic purposes. While these devices have potential for use in access control applications, only those specifically designed for that purpose are listed here.

3.3.1 - Conversant 1 Voice System by AT&T

AT&T has been working on a speaker recognition system for several years. The Conversant 1 is a multi-purpose interactive system designed for remote access to data. As it was originally produced in September, 1985, it was only capable of accepting Touch Tone input, or clearly, preregistered code words which induced the system to perform a predetermined function, responding in synthesized speech. As technology improved, the system became able to translate text to speech, and will soon be capable of speaker independent speech recognition.

In the enrollment process, the system asks the user to select a PIN, and to repeat certain words which have unique audible characteristics. Such words include "Alabama", "evergreen", and other words that are typically multisyllabic and start with a vowel. The user is asked to repeat the words until the system has an accurate representation of the user's vocal pattern for each word. This process usually takes about two minutes. Each time the user logs in, he keys in his PIN and then is asked to repeat a randomly selected word for which his voice pattern has been recorded. The patterns are compared, and an accept/reject decision is made. The Voice Key incorporates one additional security feature; it requires the user to speak directly into the handset so that his vocal inflections can be picked up. A tape recording is said to be incapable of adequately reproducing these inflections, so even if a reproduction of the actual user's voice, speaking the appropriate word, is played back, the system will not allow access.

The ECCO Voice Key/VR [126]



During June 1987, ECCO found itself without direct competition, carrying the only speaker recognition device on the market[98]. This was due to the slow development of AT&T's product, the financial distresses of VoxTron, and the slow growth of the access control market which has been keeping firms possessing speech technology from wanting to enter it. Sales remained slow, nonetheless, because of sluggish demand and a price tag of about $8500 for its basic system. Since then, ECCO has made significant efforts to reduce the costs associated with voice access control by developing some simpler products. In September 1987, ECCO unveiled the Voice Key/VR, which sells for under $1000[126]. Although it is designed for single door applications, it contains computer interfaces for possible use as a data security system. In early 1988, ECCO expects to introduce Voice Pac, which is a speaker recognition module with no pre-programmed driver. It can be tied into a software program for data security, or a number of other applications. ECCO hopes to market the Voice Pac to OEM software houses, who will integrate it into their own security packages. Expected cost to the OEM for the speaker recognition module alone is expected to be only about $200.

Further down the road, VoxTron hopes to have packages available which allow system software developers to incorporate the Veritel into their secure operating systems. Accuracy of this system is indeterminate at this time, but is likely to be similar to the performance of the Veritron 1000. Error rates for the Veritron system are variable, both because the sensitivity is adjustable, and because each user's voice print template is updated with each successful login. This results in increased precision over time. According to Datapro Reports on Information Security, which obtains its data from the manufacturer, Type I errors decrease from 3% to .1% over several months, and Type II errors decrease from .01% to .0001%. Independent testing results on this and other products are included in Section 3.8. Since changing hands, VoxTron has increased the price of the Veritron 1000 to $31,000. The Veritel system costs roughly $45,000.

3.3.4 - Product Summary

At the present time, ECCO appears to be the most active in the development of less expensive speaker verification equipment. VoxTron has focused on the production of self-contained speaker recognition computer systems, and AT&T has emphasized it efforts on developing an elaborate, interactive computer, capable not only of speaker recognition, but of voice input and output as well. This leaves ECCO with a clear advantage in the security market, producing inexpensive speaker recognition devices with flexible uses.

The table below includes the age pricing and accuracy data regarding speaker verification devices. Prices for these devices are not particularly meaningful, as these systems vary considerably in configuration, which can have a drastic effect on the total cost of the system.

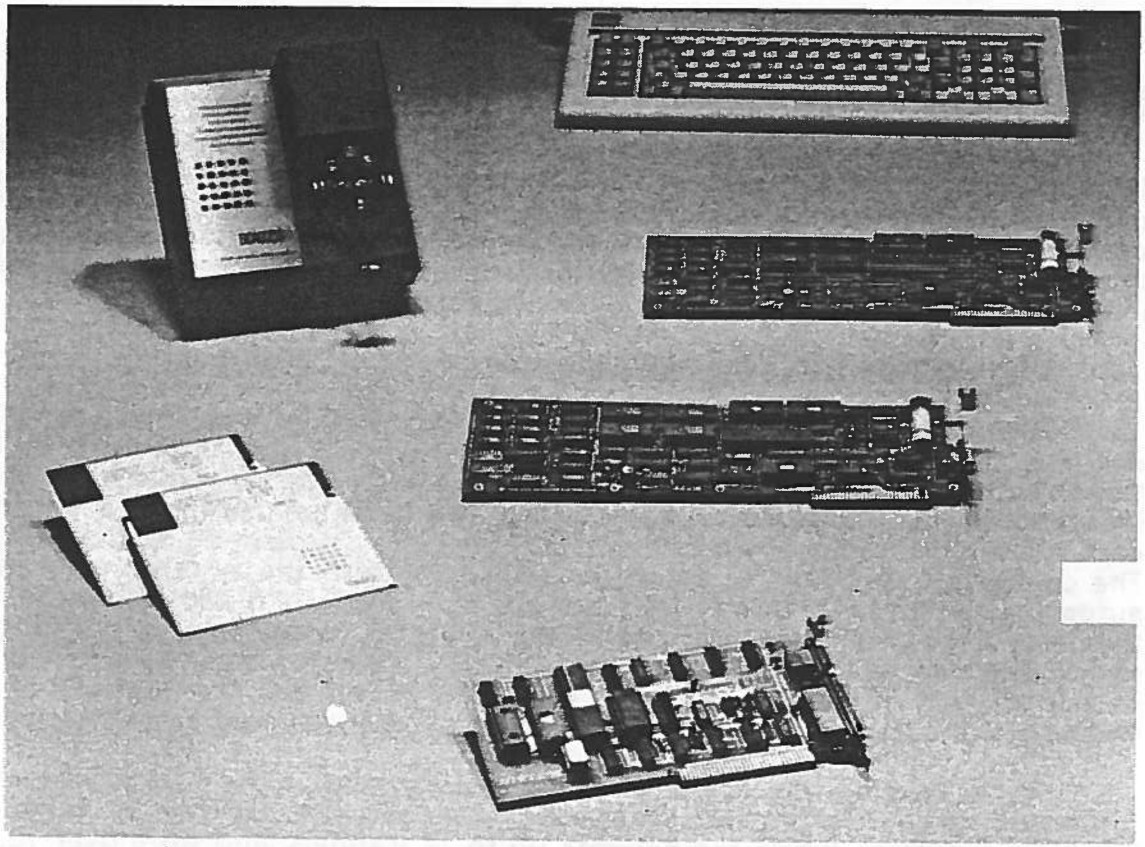
PRODUCT	VENDOR	INTENDED APPLICATION	CLAIMED ERROR RATE	ESTIMATED PRICE	FIRST AVAILABLE
Conversant 1	AT&T	Computer access control	not yet tested	RFQ basis only	July 1987
Voice Key	ECCO	Physical security	Type I: 1% Type II: .1%	$8500	March 1986
Voice Key/VR	ECCO	Single door security	Type I: 1% Type II: .1%	$1000	September 1987
Voice Pac	ECCO	Integration into OEM's software	not yet determined	$200	1988
Veritron 1000	VoxTron	Physical security	Type I: 1-3% Type II: .0001 to .01%	$31,000	September 1986
Veritel	VoxTron	Computer security	not yet tested	$45,000	January 1988

keystroke dynamics to analyze a login phrase and determine if the person at the workstation is the same as the person who enrolled under the given user name. The BioContinuous package also maintains constant auditing of keystroke actions to ensure that the person who logged in remains at the terminal throughout the session.

International Bioaccess Systems (IBS) was formed in 1981, and acquired keystroke dynamics technology from SRI International in 1984. The company's two products became commercially available in early 1987. The company does not claim to be able to determine psychological patterns through this technique, but they do claim to maintain a 98% accuracy rate. The products have adjustable sensitivity, which distributes the errors to the user's desired balance between Type I and Type II errors.

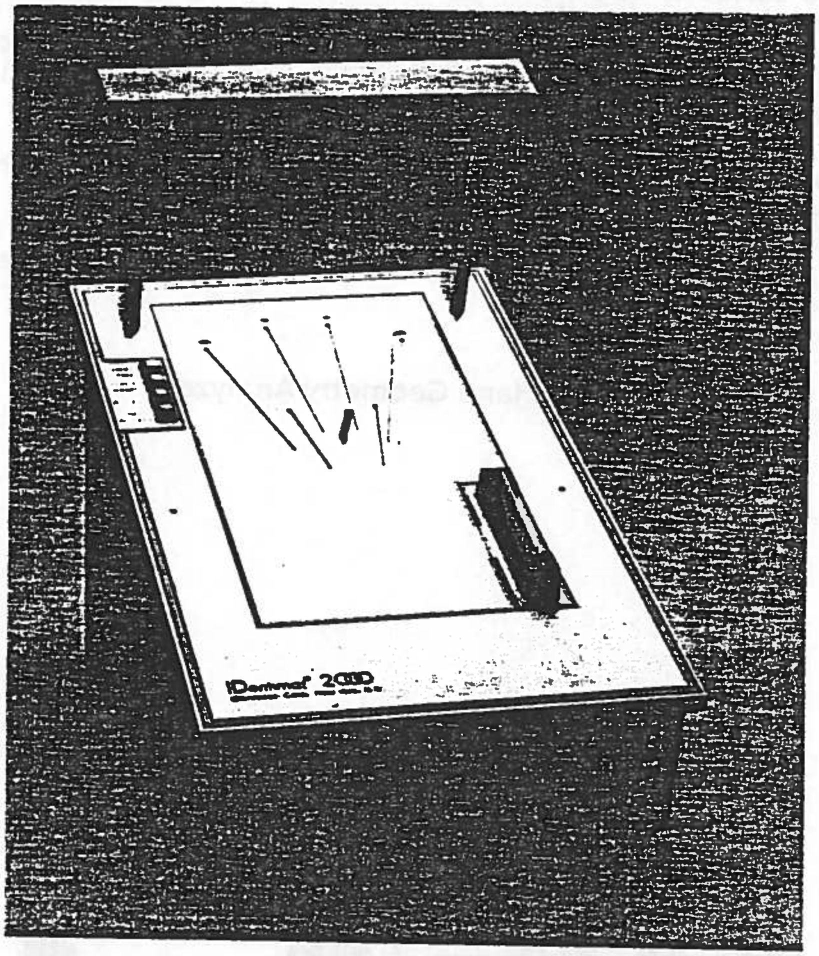
Although packages for larger systems are planned for release in the near future, only two products are currently available, designed for use on compatible versions of the IBM PC family. Because no hardware is required for operation, the packages are less expensive than most other biometric technologies. Current prices are $395 for BioPassword, and $835 for BioContinuous.

International Bioaccess's BioContinuous
Programs and Required Hardware



applications. The technology exists for integration of an infrared light source, as well as a transverse scan for increased accuracy, but these developments have not been aggressively pursued.

Stellar Systems Identimat



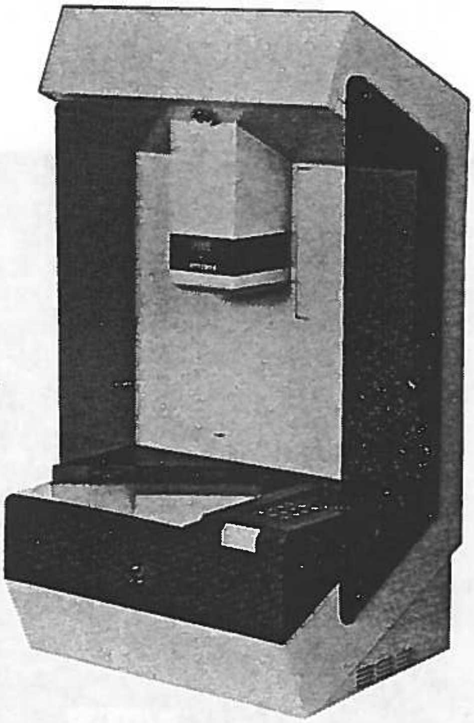
Stellar Systems is not vigorously marketing the Identimat, because they claim current demand for biometric devices is insufficient to warrant even moderate marketing costs. Also, as one Stellar Systems representative pointed out at an August 1987 security trade show, to actively develop and market this sort of product is not rational at this time, because there are too many competitive biometric devices available currently. This is especially true in the case of the Identimat, which for the most part is built using outdated technology, and costs roughly $8,000. In October 1987, it was announced that Stellar plans to discontinue production of the Identimat in December, 1987[128].

3.5.3 - Palm Recognition System by Mitsubishi

Mitsubishi Electric Sales America, a branch of a large multi-industrial Japanese firm, first introduced a prototype of the Palm Recognition System in 1984, but it was not ready for production until 1987. Like the Esselte device, it is a large, wall mounted unit designed for access.control to facilities. An illuminated plate records the outline of the palm with the fingers together. It is angled for use with the left hand so the device can be used by people in vehicles. It is a very quick recognition system with enrollment taking typically 20 to 30 seconds, and authentication is usually accomplished in less than 2 seconds.

Mitsubishi claims the Palm Recognition System is extremely accurate, with a Type I error rate of .0001% and a Type II error rate of .1%. The reader without the computer controller is priced at about $13,000. Since the device was just recently introduced, there is no track record of its effectiveness, and no independent testing has been completed on it. As it now stands, the device will not be easily adapted to computer access control applications.

The Mitsubishi Palm Recognition System



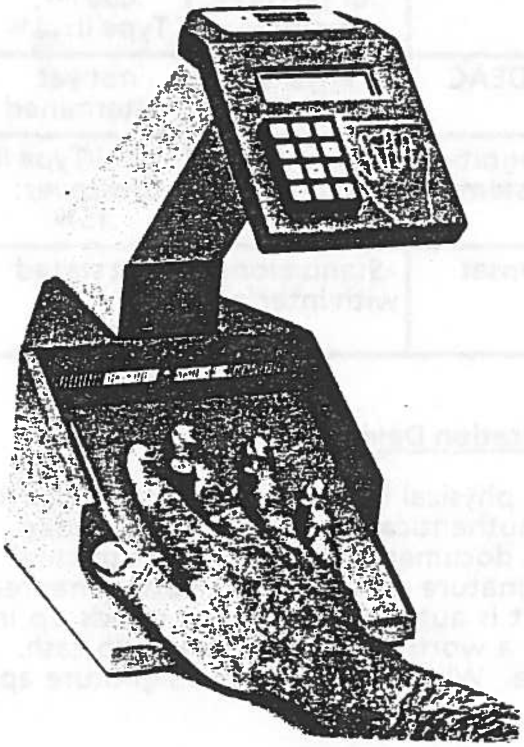
3.5.5 - ID-3D by Recognition Systems

The ID-3D was the first hand geometry device designed from the outset to be both accurate and inexpensive. It is the primary product of Recognition Systems, Inc. (formerly Productivity Products), and was invented by a former Stellar Systems Vice President who took a different approach to hand geometry measurement than did the Identimat. In addition to the length and width measurements of the outline of the hand, the ID-3D used a side mirror to determine the hand's height over its length. The device uses small pegs to assist the user in properly positioning the hand, and LEDs to confirm the position. These help to minimize the Type I errors.

The ID-3D has an RS-232 interface for easy integration into a computer system's security configuration. It is available in either a wall-mount design or as a desktop unit. Recognition Systems also offers a choice of a built in numeric keypad or a variety of card readers for stand alone applications. The ID-3D is said to be extremely accurate, with the Type I and Type II error crossover occurring at .15%. The results of independent testing on this product are given in Section 3.8.

The ID-3D is moderately priced, costing less than $5000, and $3300 per unit for quantities of six or more. The device also provides interface circuits for a magnetic stripe or Wiegand card reader instead of a keypad, but the cards are only capable of storing the user's PIN information; they lack the storage capacity to carry the biometric template. However, the reader is capable of storing 10,000 user templates. The device performed surprisingly well in Sandia Labs testing (see section 3.8), and as a result, the U.S. Department of Energy chose to purchase several units to be installed at the Savannah River Nuclear Power Plant[128].

The Recognition Systems ID-3D



of that person's conscious presence, and his awareness of the events or transactions that took place before him.

Strangely enough, however, the signature is the one form of authentication that does not remain constant over time. In fact, despite maintaining certain similarities, a signature can never be repeated exactly the same way twice. So why is it relied upon so heavily as positive identification in every day life? Here are a few reasons:

- Recording a signature requires no special equipment (besides a pen);
- Reading and comparing a signature requires no special equipment (only good eyesight);
- It is already socially accepted as a means of leaving a personal mark or stamp of approval;
- It is a virtually effortless act, doing little to inconvenience the person being identified.

Of course, there are some people who are quite adept at forging the signatures of others. The temptation to do so is great, as millions of dollars are debited and credited by signature each day. In fact, it is the threat of forgery that first prompted research in machine recognition of signatures, resulting in devices that carry potential for use not only in the prevention of forgery, but in access control applications as well. It is the public acceptance of signatures as a simple, standard means of authentication that establishes machine recognition of signatures as a desirable, user friendly approach to computer access control.

There are two basic ways of performing a quantitative assessment of a person's signature; through either static or dynamic signature analysis. Static analysis involves comparing the appearance of a finished signature with a preregistered signature of the claimed person. The height and shape of the letters, the embellishments, and other characteristic features are used in evaluating the similarities. Dynamic analysis, on the other hand, involves comparing the motions connected with the creation of the signature. Some signature dynamics devices measure parameters which include:

- Duration of contact between pen and pad
- Pressure used in writing certain letters
- Duration of rest between pen strokes
- Activities of pen while not in contact with paper

Signature dynamics devices are considered by many to be difficult to deceive, because while a skilled forger can create a signature that looks like the original, it is very difficult to create it using the same speed, rhythm, and pressure. Some devices use a combination of static and dynamic analysis to evaluate the authenticity of signatures. The comparative accuracy of these devices will be described below.

Although signature verification research was abandoned by some companies, such as IBM and Quest Micropad of Great Britain, there are many devices currently

The Confirma Tablet works along the same lines, by sensing the three components of the signature as it is signed. The pad, however, performs the sensing operation itself, allowing an ordinary pen or pencil to be used in creating signatures. Both the pen and the tablet have not undergone adequate testing to determine their accuracy, but internal analysis indicates the Type I and Type II errors crossover at 1.4% The devices are fairly inexpensive, and although Confirma's prices have not been made firm, their tentative cost schedule is as follows:

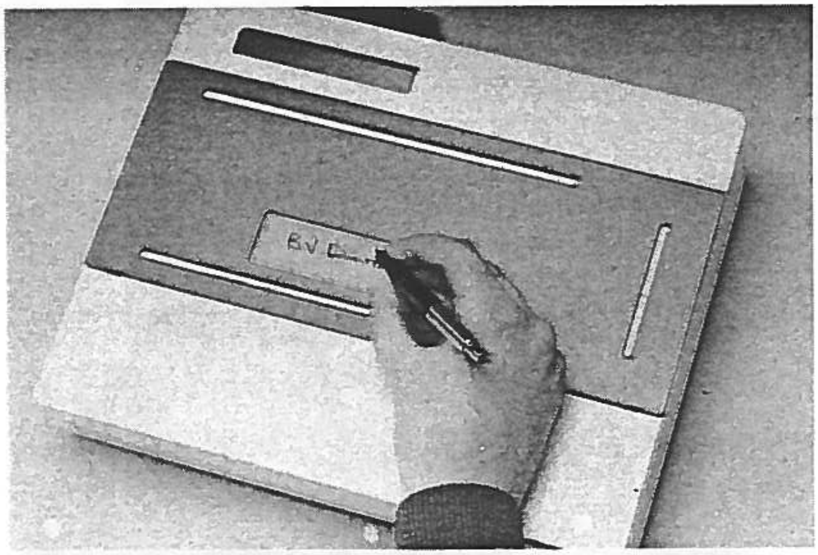
Confirma Pen	$500
Confirma Tablet	$600
Confirma Terminal Controller	$700
Confirma Interface Card	$550

It is anticipated that the applications software will be bundled as a package with the desired controller module. Quantitative price breaks may also apply.

3.6.2 - Signature Verification Unit by Thomas De La Rue Inc.

De La Rue is a major security printing company, printing much of the world's currency and travelers checks. It has many affiliates and subsidiaries, including De La Rue Printrak, with total corporate annual sales of more than $700 million. The Signature Verification Unit (SVU) was developed primarily in an effort to cut down on check forgeries. It is a sensitive tablet which generates a 40 byte template using both the dynamic and static characteristics of the handwritten signature. It has both an RS-232 and an RS-485 interface, which makes it easily adapted for networking or data access control applications with the proper software driver.

The De La Rue Signature Verification Unit

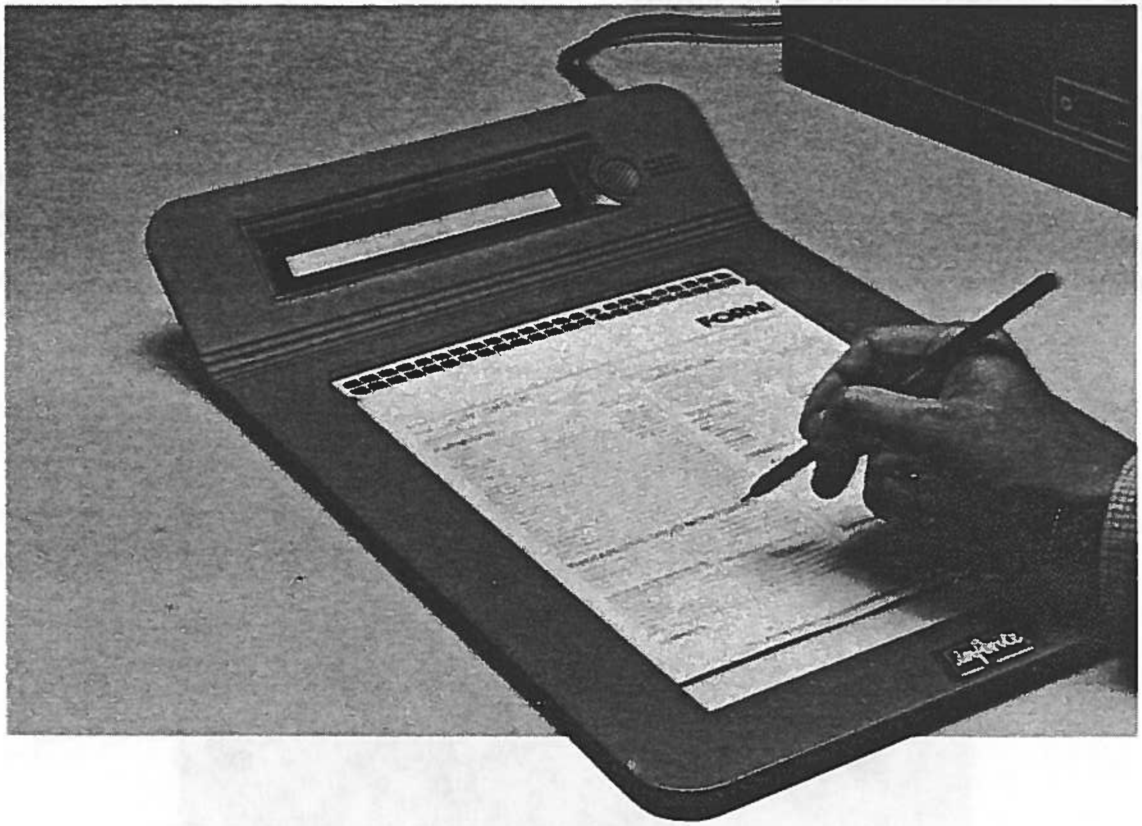


3.6.4 - Signature Verification System by Inforite

Inforite is the American affiliate of Toppan Moore of Japan, a computer products manufacturer. The Inforite system is a clipboard-like sensitive tablet which connects directly to an IBM compatible PC, which controls it. The system was originally developed to perform hand written character recognition, and this is still its primary function. There is optional software available which uses a signature dynamics algorithm to authenticate the writer's identity. Information is entered on a standard form, which has blocks for data input and for a signature. The location of the pen is recorded throughout the time it is in contact with the form, and the dynamics with which the signature was created is assessed.

Inforite claims its device carries a Type I error rate of less than 2%, and a Type II error rate of less than 4%. There is an internal algorithm which redefines the signature template after each successful login, so errors are less likely the more it is used. Inforite recommends that the enrollment process be comprised of at least ten signatures to minimize early inaccuracy. The basic character recognition system costs about $2000, with the optional signature dynamics software costing about $2000 more. Both modules are required for signature verification to be possible.

The Inforite Signature Verification System



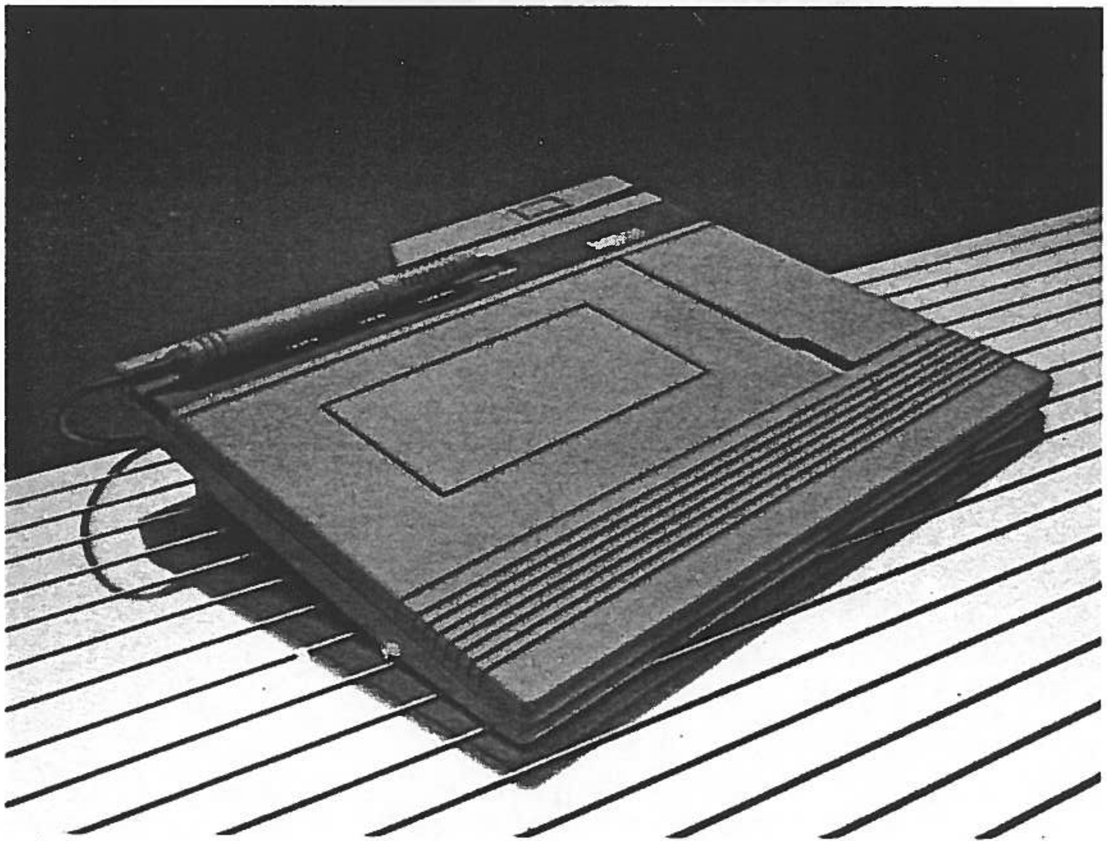
3.6.6 - Sign/On by Signify

Signify Inc., formed in 1965, is owned by another British security printing firm, McCorquodale Holdings Ltd. In September 1986, it released Sign/On, its first commercially available signature dynamics verifier. Sign/On is designed more for computer access control than for physical security, incorporating interface options for both IBM PC compatibles and the 3270.

Sign/On operates much like other signature dynamics devices. It has a wired pen attached to a sensitive tablet, and can operate as a stand alone unit. It has non-volatile storage capacity for 100 signature templates, each of which is 115 bytes in length. Registration requires about six signatures, and evaluation for each attempt takes about three seconds after signing. To enhance its position as a computer access control device, Signify has agreed to allow Sign/On to be supported by On-Line Software's host access control package. This package will require biometric signature verification in addition to passwords to obtain system access.

Threshold settings are adjusted by the factory, and is specified by the customer when the order is placed. The customer specifies a Type I error rate between .2% and 15%. The Type II error rates will vary accordingly. It is estimated that the Type I/Type II crossover occurs around 1.5%. The units are rather inexpensive in comparison to other signature verifiers, costing only $845 each.

The Signify Sign/On



3.6.8 - Signature Verification Product Summary

The age, claimed accuracy, and approximate prices of the signature verification devices is given in the table below. Only the price of the Ion track device could be quoted as configured for terminal security. Note also that some of the manufacturers have adjusted the threshold of their devices to reduce the number of false rejections, resulting in an unusually high percentage of Type II errors. However, the sensitivity of most of these devices can be increased, making them more appropriate for access control applications.

PRODUCT	VENDOR	INTENDED APPLICATION	CLAIMED ERROR RATE	ESTIMATED PRICE	FIRST AVAILABLE
Confirma Pen	Confirma	Stand alone PC driven system	Type I/Type II Crossover: 1.4%	$1200	June 1987
Confirma Tablet	Confirma	Stand alone PC driven system	Type I/Type II Crossover: 1.4%	$1300	June 1987
Signature Verification System	DigiScan	Stand alone with interface (static analysis)	Type I/Type II Crossover: <5%	$900	1987
Signature Verification System	Inforite	Stand alone PC driven system	Type I: 2% Type II: 4%	$3945	December 1984
Securisign	Ion-Track	Stand alone with interface & application software	Type I/Type II Crossover: 1.1%	$3645 (configured for terminal security)	1984
Sign/On	Signify	Stand alone with interface	Type I/Type II Crossover: 1.5%	$845	September 1986
Signature Dynamics Prototype	T.I.T.N.	Stand alone with interface	Type I/Type II Crossover: 3.5%	$1500	1988

3.7 - Retina Scanning Devices

It has been determined that, like fingerprints, no two people have the same retinal vasculature (the blood vessel pattern on the surface of the retina), and it remains virtually unchanged throughout life. Blood vessels branch out in an area around the fovea, formıng a unique, detailed pattern. This pattern can be safely traced with remarkable accuracy through the use of a low intensity infrared beam. Thus far, only Eyedentify Inc. has developed devices utilizing this technique.

Eyedentify's most recent modification is the Eyedentify Information Security (EIS) System. It was designed specifically for computer access control applications. This system employs the use of a small, hand-held camera (ICAM) to scan the retina. It plugs into a processor board which is fitted into the workstation. It can be used in a stand alone environment if an additional memory board containing the template data is installed in the system. For local area networks where one ICAM is shared, the processor board is external to the workstations and the host computer, while the templates are stored in the host's memory.

All of the Eyedentify systems have some common features; they all have an adjustable threshold, which is usually set at around 70% of an identical match. They are all capable of registering two eyes, such that both must be authenticated for access to be gained. They are most commonly installed in facilities requiring extremely high security, where their high accuracy is required and their high costs can be justified. The systems claim to have unheard of accuracy rates, with Type II error rates for just one eye of .0001%; however, this is nothing more than the mathematical probability of finding someone with the exact same template. It is suspected that far more than one in one million can pass a 70% threshold value. Type I errors occur roughly 5% of the time, more often due to improper eye positioning than being mistaken for an imposter. Independent test results for this product are given in section 3.8. Pricing for the Eyedentify systems ranges from $7000 to $11,000 per scanner, depending on model and configuration.

Despite being commonly accepted as having the most accurate biometric system currently available, Eyedentify has a significant sales obstacle in the area of user acceptance. Many people, quite understandably, have serious reservations about having their retina scanned by an infrared laser beam on a regular basis. Fears of permanent damage to their eyesight has kept users wary of retina scanners, and kept employers from purchasing them. As Brian O'Hare, Vice President of Bank of America, pointed out, "We spend large amounts of money making sure our employees are happy and feel safe in their workplace. We buy glare screens for every terminal, and quiet printers that won't annoy the people sitting next to them. For us to require employees to subject themselves to retina scans just seemed contrary to our policies regarding working conditions. That's why we opted for the fingerprint device."

Eyedentify emphasizes that its products are safe to use, even on a regular basis. They are happy to submit independent testing reports which state the method of scanning used is completely safe, and state in writing that they meet or exceed all FDA health regulations. Also, according to Smart Card Reports[130], Eyedentify products were met with resistance in 1985 by users who feared that AIDS could be spread through tears left on the scanning faceplate. Despite denials by Eyedentify that this was a reasonable possibility, the manufacturer elected to install headrests on each unit, which prevents the eye from comiing in contact with the scanner. Although most people's reservations about using the device disappear after trying it once, gaining user acceptance remains Eyedentify's top sales priority.

3.7.2 - Retina Scanning Product Summary

The product data for each of the Eyedentify products is presented in the table on the following page. Note that while the technology employed by each device is the same, their intended applications vary considerably.

capable of moving comfortably through the circulatory system of the human body, taking biological readings as they proceed. This device, acting as an invitro proximity card, would not only be able to positively identify the person whose body it inhabits, but would also be capable of perceiving the use of drugs or alcohol, or the development of infectious diseases. Unfortunately, this technology is still a long way down the road.

3.8.2 - Cost Comparisons

Comparing the prices of different biometric devices is a more difficult task than one might think. The devices tend to be modular in nature, with different components being used for different applications. Also, some devices are nestled in a larger, multi-purpose system, such as the AT&T Conversant 1. The price of this speaker verification unit alone bears little resemblance to the minimum configuration price of the entire Conversant 1 system, which controls it. Since applications vary so much regarding how much security is needed, what needs to be secured, and what existing equipment is capable of securing it, systems tend to be custom designed by the device manufacturer. It is for this reason that devices tend to fall into a certain price range rather than carry a specific price tag, and why many manufacturers are unwilling to provide any pricing information without a specific application in mind.

Software modifications are another source of grey areas in many quotations. An authentication device, by itself, does nothing unless it is driven by software. Off-the-shelf packages dedicated to specific applications are rare, because the configuration and requirements for each situation varies so greatly, and the volume of sales for biometric devices is low. From this, a vicious circle is formed: Sales are low because costs for devices are high; costs are high because systems need to be custom designed; custom designs are necessary because the sales for specific applications are low. Only an increase in demand brought on by greater security awareness can increase sales, resulting in less expensive devices designed to solve specific authentication problems.

3.8.3 - Accuracy Comparisons

Comparing the accuracy of the different devices is also difficult. It is unwise to rely strictly on figures provided by the manufacturers because they tend to perform tests in ways that bring about favorable results. Some perform simple Type I and Type II error rate tests using procedures that are inconsistent with common logic. For example, some give Type II error rates based on the odds of matching an authorized user's template, rather than on the likelihood of a random imposter being accepted at a given threshold value. Some even give Type I error rates at one threshold value and Type II errors at another.

The best way to obtain meaningful results is to have an independent organization test the devices using a consistent, scientific method. Such testing is currently being performed on several biometric devices at the National Computer Security Center in Fort Meade, Maryland, but the results have not yet been released (see Section 4.2). As of now, the only independent test results on biometric authentication devices that are publicly available were performed by Russell L. Maxwell of Sandia National Laboratories. In his July 1987 report "A Performance Evaluation of Personal Identity Verifiers"[118], Maxwell gives the details of performing error rate tests on five different biometric devices. The results are given in the table which follows.

CHAPTER FOUR

Selection and Implementation

Thus far, the various methods and associated devices used in access control, especially those that are biometric in nature, have been described. However, implementing any one or all of these methods doesn't assure protection beyond the initial access point. The computer system is only as secure as the many parts making up the whole, e.g., the PC and/or mainframe operating systems, the data bases, network, etc. The advances in security and the escalation of risk in certain environments represent a close race between those who are trying to protect the assets controlled by computers and those who are trying to compromise them.

In this chapter, we will briefly address other topics which either relate to building a trusted computer system or should be considered in the process of selecting and implementing a methodology to render a system less vulnerable.

4.1 - Government Requirements and Activities

4.1.1 - DoD Guidelines

The DoD Trusted Computer System Evaluation Criteria[109], commonly known as the "Orange Book", provides a basis for specifying security requirements and a metric with which to evaluate the degree of trust that can be placed in a computer operating system (Appendix E). A given operating system, when weighed against the criteria, is judged to be in a class ranging from D to A1. Guidance for applying the Criteria in specific environments is furnished in DoD Computer Security Center documents entitled "Computer Security Requirements"[110] and "Technical Rationale Behind Computer Security Requirements"[111]. An interpretation of the Orange Book criteria for computer networks is provided in the highly detailed "Red Book" entitled "Trusted Network Interpretations"[131].

The Computer Security Requirements document identifies the minimum class of system required for a given risk index. (The risk index is the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of the data processed by the system - Appendix F).[1] Determining the minimum class of system depends not only on the risk index, but also on the nature of the environment. (A system whose applications are adequately protected is said to be in a closed environment, otherwise it is considered to be in an open environment.)(Appendix I). Taking both the risk index and the environment into account, security index matrix tables reflecting the computer security requirement minimum evaluation class for both the open and closed environments have been constructed by the DoD National Computer Security Center (NCSC), and are presented in Appendices J and K, respectively.

[1] Appendix G describes the risk index calculation; Appendix H describes the levels of clearances and data sensitivities (e.g., classification) used in the calculations, and contains rating scale tables for each user clearance and data sensitivity level.

4.1.2 - National Computer Security Center Evaluated Products List (EPL)

Background

The DoD National Computer Security Center established at the National Security Agency (NSA) on January 2, 1981 in accordance with DoD Directive 5215.1, conducts a commercial Products Evaluation Program focused on the technical evaluation of off-the-shelf commercially produced systems. Products are evaluated against the detailed testing specifications in the Orange Book criteria, and from this, it is established whether the system employs sufficient hardware and software integrity measures for the simultaneous processing of a range of sensitive or classified information. This product evaluation culminates in the publication of an Evaluated Products List (EPL)[114], which is available to system developers, managers and users concerned with a system's relative suitability for use in processing sensitive information, from the National Technical Information Service (NTIS).

The products being evaluated range from central processors to add-on software packages. User authentication devices fall into a category called sub-systems. Currently, only four authentication products have qualified for addition to the list. They are:

- **The Access Key by Gordian Systems, a password generator;**
- **The CPP-300 Trusted Port Path Protector by Codercard, a smart card providing device authentication;**
- **The Watchdog by Fischer-Innis Systems, a file access control and audit program for PCs;**
- **The PFX Passport by Sytek, a password generator.**

The NCSC is currently evaluating a broader range of authentication products, including some biometric devices. The results of these tests are due in late 1987.

Definition of Evaluation

The Overall Evaluation Class (the level of trust rating) referred to in the EPL, is the highest class for which the product satisfies all the requirements in the Criteria. Appendix L presents the classes, along with the requirements and their associated elements which must be satisfied under each class.

In addition, the product may include some features and assurances from higher classes. In those cases where a product includes all the essential elements for a higher class, that class is included within the product's Range of Feasible Use.[1] Note that for these cases, the product does not have to meet all the requirements for the higher evaluation class, but the implemented mechanisms are sufficient to

[1] The "Range of Feasible Use" is intended to convey the overall system integrity level of the product as it is delivered by the vendor and indicates that this product could be used in an environment requiring an evaluation class within this range so long as the missing features are not essential to the operational capability.

with multilevel security features. Multiple security levels are necessary in systems that allow access to users of varying clearances to keep them from accessing information for which they are not authorized. Protecting information from unauthorized personnel by granting varying degrees of access privileges, rather than denying access entirely, can be a rather complex procedure. It involves the labeling of each user, device and piece of information not only with a security level, but also with need-to-know information covering certain periods of time. The implementation of such procedures has proven to severely limit the systems' processing capabilities and storage capacity.

It follows that the ultimate access control goal for an operating system is to make it impossible for an unauthorized person to read, change, add to, or delete the information that is stored within the computer system. This means that a multi-level secure operating system must be able to control the authorization of individuals and their programs to access equipment, data, and certain other programs. It should be made impossible to read data of a higher level, write to a lower level, or read anything without the need to know that information.

There are some operating systems that have been designed to do just that. Security features can include user access and password control, as well as the ability to prevent application programs from accessing data files or the operating system software, itself. File access controls allow the system manager to determine user/application access and execution privileges based on the security requirements of the system involved.

Users with different levels of security often need to share data or programs, but, as a rule, only one user may own the media on which the data resides. In these cases, some operating systems can allow other users to share media either temporarily or permanently, but grant read only capability.

It is an unfortunate fact of life, but even the best of systems are penetrable. While we are concentrating on the prevention of break-ins, some thought should be given to the detection of those that do occur. The old adage states that a chain is only as strong as its weakest link, and since detection is part of the security chain, lack of good detection measures weakens the chain. Improving audit trails, increasing the frequency with which the system users are monitored, building entrapment procedures, and controlling the users' awareness of selected system options on a need-to-know basis only, can assist in this end.

4.2.2. External Threats

Although the emphasis in terminal physical security has revolved around personnel identification, there are some other environmental considerations that, if ignored, will nullify all the efforts that have been invested in securing the system's data. Primarily the concern is with the physical security associated with the communications capability of computer systems. That is, systems involving terminals directly connected via cable to host computers or to controllers which are, in turn, connected to one another via telephone lines or coaxial cables. Combatting the threat of wire tapping to these lines can only be accomplished through effective data encryption or through the use of tempest technology.

Many government computers are accessible to the world via dial-up modems or connection to computer networks. It is this accessibility that is most difficult to control, and is the channel through which many computer crimes are knowledge and attitudes of the administrators and users of such systems. The community of users should be educated on the security hazards of the various operating systems and ways to protect against them. Not only would this lead to a level of protection that is stronger; but far more importantly, would represent a reasonable and thoughtful balance between security and ease of use of the system.

The minimization of risks is dependent on more than just the proper selection and implementation of a security device. It requires the security system be modified and maintained over time, and that management remain aware of the changing security needs of the computer system. This, coupled with government encouragement in the area of establishing and updating computer security standards, will result in more complete and less expensive system security techniques.

4.3 - Selecting a Security Method

Ideally, customers in the high security market would like an authentication procedure that poses no extra workload on the authorized user or employee. It must be inexpensive to buy and maintain, compatible with existing manual and other automated systems, socially acceptable, reliable and hard to compromise, and with a good audit trail to help catch and convict the imposter. Additionally, the impact to the on-line response time and run-time costs must not be excessive.

Certainly, there are many considerations that must be taken into account when selecting a security system for a computer. While many of these address particular environmental and system-specific factors, many others apply to virtually all computer security applications. Donn B. Parker, one of the more notable experts in computer security, outlined the more universal selection considerations in his article "Safeguard Selection Principles"[16]. Each principle is given, and described briefly, below.

- **Cost Effectiveness** - Security techniques range in cost from free to prohibitive. The amount of risk and the value of stored data help to determine how much should be spent on safeguards.

- **Minimum Reliance on Human Intervention** - The human element in a security system tends to be the most unreliable link in the chain. Completely automatic security systems are usually considered superior.

- **Override and Failsafe Defaults** - Alarm conditions should be able to be cleared quickly and economically by an authorized person.

- **Absence of Design Secrecy** - It should be assumed that an intruder is as familiar with the security system as are its designers; therefore the security provided should depend on the system's effectiveness, not on the secrecy of its design.

- **Least Privilege (Need to Know)** - It is best to provide only the information needed to perform the task at hand, rather than to provide all information.

In addition to the items in this list, there are other selection principles that apply specifically to user authentication devices. They are:

- **Accuracy** - Low Type I and Type II error rates.
- **Circumvention** - The device must be designed such that no person can access the system without undergoing an authentication test.
- **System Burdens** - The Authentication mechanism must not require excessive amounts of the system's memory or CPU time in order to operate.
- **Ease of Integration** - The device should be easily integrated into the specific environment in which it is required.

There are ways to further automate the selection process, such as assigning weights to each of the principles according to their importance for a particular situation, and then scoring each device on its ability to satisfy that principle's criteria. In any event, the selection process is a complex one, made so by the wide range of security devices available, and by various systems and environments that need to be secured. The best choice for a given situation may be the worst choice for another. The principles given here can only act as a guide to assist in the selection process.

<u>4.4 - Conclusions</u>

In reviewing computer security, we have determined that there are two basic approaches to limiting the resources of a computer system to authorized users:

1 **Physical Security** - operational measures taken to deny access of computer hardware, transmission lines, and storage media to unauthorized persons;

2 **Data Security** - measures taken to maintain the privacy of data through automated user identification and authorization for use of a shared computer resource.

Physical security can be considered a subset of data security, since one way of securing data is to allow no unauthorized persons near the computer system. However, data security offers much more flexibility, in that authentication mechanisms running on the system in which the data is stored enables the system to uniquely identify each individual. This means that many users can use the same equipment while accessing and processing data of different security levels, the number of which are only limited by the capabilities of the authentication software designers.

So which of the authentication methodologies described in Chapter Three is the best choice? As previously stated, this is impossible to determine without having a specific system and environment in mind. Each technology has its preferred market; i.e., an area which is more appropriate for its application. Speaker verification is the preferred biometric technology for remote user authentication or dial-up access to computers, since it can be performed using only a telephone. Fingerprint devices are well suited to identify those entering prisons a variety of costs. The problem is that the determination of an appropriate level of investment in techniques and practices which enhance security, through the performance of a risk analysis, is far from an exact science.

Hopefully the process of choosing the correct approach to the improvement of computer security will become clearer as identification technology improves. As devices become more capable of making positive identifications of users, and as the cost of their technology decreases, the decision as to which device to implement will become easier. The trends over the past few years indicate that while there may never be a single "right" choice for user authentication, technological improvements ensure that there will be far more good choices than bad ones.

4.5 - Recommendations

This report examined the various technologies available which can provide advanced user authentication. The techniques were based on knowledge, possession, and biometrics. The biometric technologies were focused upon because, when coupled with passwords and/or access cards, some can offer nearly complete protection to a computer system and its data.

The logical steps in the continued analysis of advanced user authentication technologies are:

- Select a computer which stores or processes sensitive data.
- Perform an analysis of the system's security needs, based on the value of the data and the likelihood of attempted intrusion.
- Select the safeguard mechanism, based on the selection principles stated in Section 4.3, which best satisfies these security needs.
- Install the security mechanism in the system.
- Test the effectiveness of the mechanism by assessing its actual accuracy and user acceptance, and make any necessary adjustments.

Experience can be gained by the actual installation of a device utilizing advanced user authentication technology. Such an installation can serve as a benchmark for future installation plans at other sites. Actual operations and unforseen problems can be documented over a period of time, and system-specific considerations can be developed to aid in the future selection of devices and the procedures of their installation.

APPENDIX A

BIOMETRIC DEVICE VENDORS

This table contains the names, addresses, product names (if any) and product descriptions for each vendor of biometric devices. The far right column indicates a bibliographic reference where more information can be found on each company's products. A "*" indicates product literature has been obtained on that product.

VENDOR	PRODUCT	DESCRIPTION	REF
AT&T Conversant Systems 6200 E. Broad St. Columbus, OH 43213 (614)860-4474	Conversant 1 Voice System	Interactive system with voice access control	* 30 100 130
British Telecom Research Lab Martlesham Heath Ipswich IP5 7RE, ENGLAND		Speaker Recognition Device (being tested)	101B
British Technology Group 101 Newington Causeway London SE1 6BU ENGLAND (44)-1-403.6666		Experimentation with devices using hand vein patterns, signature dynamics and voices	100 130
CFA Technologies 3356 Gorham Ave. St. Louis Park, MN 55426 (612)944-5878	Tenprinter	Fingerprint device aimed at identifying criminals. Plan to make an access control device	100
Comparator Systems Corp. 930 W 16th St, Suite E-2 Costa Mesa, CA 92627 (714)642-1349	ID-1	Compares fingerprints with those filed on cards. Must be manually operated	* 80A 100 130
Confirma Technology Corp. 333 Ravenswood Ave. Menlo Park, CA 94025 (415)326-6200	Confirma Pen or Tablet	Joint venture signature dynamics device with SRI Intl. and Visa USA	* 96 100 130
De La Rue, Thos. Inc. 13854 Park Center Rd. Herndon, VA 22071 (703)478-2840	Dynamic Signature Verification System	Signature dynamics access control device	* 80A 98 100
De La Rue Printrak 1250 N. Tustin Ave. Anaheim, CA 92807 (714)666-2700	Printrak, Orion, and Printrak Direct Reader	Fingerprint classifiers (previously developed by Rockwell) and direct comparator for access	100 130
Digiscan Corp. 30 Rockefeller Plaza, #4250 New York, NY 10112 (212)397-0717	Signature Verification System	Automatic static signature comparator (division of Cheque Alert, Inc.)	* 100

VENDOR	PRODUCT	DESCRIPTION	REF
Onset, Inc. 151 University Ave. Palo Alto, CA 94301 (415)327-5470		Super compact hand geometry device (has software bugs)	30 100 130
Palmguard, Inc. 10260 SW Nimbus Ave. Tigard, OR 97223 (503)692-6031	PG 2000	Palm reading device (no sales in first 5 years, president says their days are numbered)	65 80B 100 130
Pideac, Inc. 800 Livermore St. (rear) Yellow Springs, OH 45387 (513)767-7425	Mark I Scanner	Hand Geometry device (was awarded Air Force contract)	* 30 100
Recognition Systems 1589 Provincetown Rd. San Jose, CA 95129 (408)257-2477	ID-3D	Compact 3 dimensional hand geometry authenticator	* 83 100
Signify, Inc. 9005 Red Branch Rd. Columbia, MD 21045 (301)992-3035	Sign/On	Signature Dynamics device using wired pen	* 80A 100 130
Stellar Systems 231 Charcot Ave. San Jose, CA 95131 (408)946-6460	Identimat ID 2000	Hand geometry device using finger lengths. Identimation developed it but it will be dropped.	* 80A 100 128
T.I.T.N. 34 Avenue du Gen. de Gaulle 38100 Grenoble, France 33-76.22.41.95		prototype signature dynamics device	100 130
Thumbscan, Inc. 2 Mid-America Plaza,#800 Oak.Brook Terrace IL 60181 (312)954-2336	Thumbscan	Fingerprint verifier using thumbs (cheap at $995)	* 77 100 130
Veritec, Inc. 23801 Calabasas Rd. #2039 Calabasas Park, CA 91302 (818)716-0741	Vericode and Covert Chemical Signatures	Chemical countfeit protection. Research on Exvitro DNA testing, fast fingerprint verifier	*
Voxtron Systems, Inc. 9504 IH35 North, Suite 206 San Antonio, TX 78233 (512)653-7800	Veritron 1000 and Veritel	Speaker Verification device for computers and facilities(bought by Camarilla Corp.)	* 84 98 100

APPENDIX B

PASSWORD GENERATOR VENDORS

This table contains the names, addresses, product names and product descriptions for each vendor of password generating devices. The far right column indicates a bibliographic reference where more information can be found on each company's products. A "*" indicates product literature has been obtained on the described product.

VENDOR	PRODUCT	DESCRIPTION	REF
Atalla Corp. 2304 Zanker Rd. San Jose, CA 95131 (408)435-8850	Identikey and Confidante	Hand-held Key and keyboard unit giving dynamic passwords (acquired by Tandem)	* 2
Dallas Semiconductor 4350 Bellwood Pkwy. Dallas TX 75234 (214)450-0400	Key Ring	Password generating access key	2
Digital Pathways, Inc. 201 Ravendale Drive Mountain View, CA 94043 (415)964-0707	Defender II	Password key with encrypting modem	19
Enigma Logic, Inc. 2151 Salvio St, Suite 301 Concord, CA 94520 (415)964-0707	SafeWord and PC Safe 5.0	Hand-held Access key with PIN	* 7 10 19
Gordian Systems, Inc. 3512 West Bayshore Rd. Palo Alto, CA 94303 (415)494-8414	Gordian Access Key	Screen-reading access key and host software (bought by Thumbscan) (see also Optimum)	* 2 10 38A
Intellicard International 120 Plaza Del Sol, Suite 135 Denver, CO 80907 (303)528-6060	Unitary Card	Smart Card with 15 key pad, LCD display, and battery	100
LeeMAH Datacom Security 3948 Trust Way Hayward, CA 94545 (415)786-0790	Safetraq and Traqnet 2000	hand held card with decoder PIN and challenge code required for dial-ups	22 74
Microframe, Inc. 2551 Route 130 Cranbury, NJ 08512 (609)395-7800	RFG 100	Hand-held random password generator	* 20A 22
Optimum Electronics Inc. P.O. Box 250 North Haven, CT 06473 (203)239-6098	DL access key	Password generator for use with DL 2400 software (Same device as Gordian Key)	* 20A 22

APPENDIX C
ACCESS CARD OR KEY VENDORS

This table contains the names, addresses, product names and product descriptions for each vendor of access cards or keys and/or readers. The far right column indicates a bibliographic reference where more information can be found on each company's products. A "*" indicates product literature has been obtained on the described product.

VENDOR	PRODUCT	DESCRIPTION	REF
ADT 1 World Trade Center New York, NY 10048 (800)ADT-INFO	Card Guard	Card access control systems	115
Advanced Magnetic Products 21220 Devonshire, Suite 208 Chatsworth, CA 91311 (818)341-5232	Mag Card - 35 and MCR - 35	Barium Ferite card and reader	*
Allsafe Company, Inc. 1105 Broadway Buffalo, NY 14212 (800)828-7162	Allsafe Entry	Access control cards, readers and controlers	* 115
Amcard Systems, Inc. 2 Kane Industrial Dr. Hudson, MA 01749 (617)562-7111	Amcard	ID Card with magnetic stripe. Reader can manage up to 64000 card holders	
American Magnetics Corp. 740 Watsoncenter Rd. Carson, CA 90745 (213)775-8651	microMAX	Magnetic stripe access cards and microcomputer controller	
Amtel Security Systems, Inc. 365 N.W. 170th St. Miami, FL 33169 (305)652-7864	Voidex 2000	Easy-to-update card access control system	116
Analytics Communications 1820 Michael Faraday Dr. Reston, VA 22090 (703)471-0892	Sherlock System Authenti-Key	Smart Key with Encryption and Password protection	*
Anchor Pad Intl. 4483 McGrath St. Ventura, CA 93003 (805)658-2661	PC Sentry	Plastic card or Key access for PC's	19
Andover Controls Corp. York and Haverhill Sts. Andover, MA 01810 (617)470-0555	AC4 Plus 4	access control system using cards and card readers	*

VENDOR	PRODUCT	DESCRIPTION	REF
Casio, Inc. 3-2-1 Sakae-Cho, Hamura-Machi, Nishitama-Gun Tokyo, JAPAN 190-11		64 bit EEPROM cards, produced the Mastercard prototypes	100 130
Caulastics 5955 Mission St. Daly City, CA 93013 (415)585-9600		Photo IDs with magnetic stripes	
CelSat 219 Dauphin, Dollard-Des-Ormeaux, Quebec, CANADA H9G2K7 (514)630-0238		Smart token for access control. Interactive withCelsat controller	*
Codercard Inc. 16812 Redhill, Suite B Irvine, CA 92714 (714)662-7689	Codercard (Commercial)	Smart Card for Terminal Access (see Interstate Electronics)	* 388
Computer Applications, Inc. 552 NW 77th St. Boca Raton, FL 33431 (305)997-9660		Card acccess systems	115
Continental Instuments Corp. 70 Hopper St. Westbury, NY 11590 (516)334-0900	Proximity Pass	Access control systems using proximity cards and card readers	* 115 116
Control Module Inc. 680 Enfield St. Enfield, CT 06082 (203)745-2433	Controlled Access Systems	Bar code access controls	
Corby Industries, Inc. 1501 E. Pennsylvania St. Allentown, PA 18103 (800)OK-CORBY	Corby Card	Magnetic card access control systems, and IBM PC security systems	* 115
Cotag International, Inc. 685 Kromer Ave. Berwyn, PA 19312 (215)296-9160		Coded tags and tokens emitting radio frequencies, functioning like proximity cards	*
Cronos, c/o DOS Americas, Inc 2401-C Oak Hill Dr. Greensboro, NC 27408 (919)282-0004		Access control systems using magnetic cards	*
Cytrol Inc. 4620 W. 77th St. Edina, MN 55435 (612)835-4884	Cylock	Access key and file encryptor	19

VENDOR	PRODUCT	DESCRIPTION	REF
Elcom Industries, Inc. 10268 Bach Blvd. St. Louis, MO 63132 (314)429-3100	Inter Access	Terminal access control and auditing using plastic cards	* 115 116
El De (Israel) c/o Donura Corp New York, NY (212)307-5600	Reader 2000	Card reading device with keypad for access control	*
Falcon United Industries 7129 Gerald Ave Van Nuys, CA 91406 (800)432-5622	ProxCard and ProxTube	Proximity and plastic card access control systems	* 116
Faraday Corp. 266 Lindbergh Livermore, CA 94550 (415)449-5300		A De La Rue subsidiary. Smart cards usable either alone, or with their signature verifier	* 98
Federal APD Security Systems 24700 Crestview Court Farmington Hills, MI 48018 (800)521-9330		Magnetic card and digital access control	
Foster, L.B. Co. P.O. Box 2028 Cedar Rapids, IA 52406 (319)366-2771	LeFebure Unit	ATM cards (Proximity, Wiegand, Magnetic)	
Fujitsu Microelectronics, Inc. 3320 Scott Blvd. Santa Clara, CA 95054-3197 (408)562-1000	Memory Card	Variety of programable IC cards for various applications.	*
Galaxy Control Systems 3 North Main St. Walkersville, MD 21793 (800)445-5560		Infrared coded cards and controllers	*
GEC Card Corp. W. Hanningfield Rd. Great Baddow, Chelmsford, Essex, ENGLAND CM2 8HN	GEC iC Card	Contactless cards and readers, easily adapted to computer security	
Graphic Laminating, Inc. 5122 St. Clair Ave. Cleveland, OH 44103 (800)345-5300	Datacode Systems	Computer compatible ID cards	
Harco Industries, Inc. 10802 N. 21st Ave. Phoenix, AZ 85029 (602)944-1565		Machine readable ID cards and access systems	115

VENDOR	PRODUCT	DESCRIPTION	REF
Lan-Lok 12830 Hillcrest Rd., Suite 111 Dallas, TX 75230 (214)881-1366	Lan-Lok	A PC peripheral which requires a smart card be inserted for the system to operate.	*
Logicam Microcard, Inc. 21 E. 40th St., #2007 New York, NY 10016 (212)213-9521	Telecam	Smart card with reader for remote access	
Logicard Systems, Inc. 401 Columbus Ave. Valhalla, NY 10595 (914)769-1400	LSI-3	Typical plastic card with pre-assembled insert for a microprocessor and 16KB EEPROM memory	* 100
Mag-Tek, Inc. 20725 S. Annalee Ave. Carson, CA 90746 (213)631-8602		Magnetic stripe ID badges and activating terminals	115
Malco Systems 74 Gwynns Mill Ct. Owings Mills, MD 21117 (301)363-1600	Watermark Magnetics	Non-erasable magnetic stripe encoded cards for vestibule ATMs or for use on Pass Guard 2000	* 18 116 130
Mastiff Systems US, Inc. 2030 Power Ferry Rd. Atlanta, GA 30339 (404)984-0202	Mastiff Terminal Protection	Hand-held key and loop antenna at host	22
Matrix Electronics Inc. 1529 Lakeland Ave. Bohemia, NY 11716 (718)417-1880		Wiegand, magnetic, and proximity cards with keypad access	115
Maximum Security Centers 241 Elmwood Ave. Buffalo, NY 14201 (716)854-2324		Card systems for ATMs	
Micro Card Technologies, Inc. 14070 Proton Rd. Dallas, TX 75244 (214)788-4055	Micro Card	Smart cards integrating biometric information, used on Eyedentify and Identix, among others	* 83 98 100
Microframe, Inc. 2551 Route 130 Cranbury, NJ 08512 (609)395-7800	Magnakey and Cipherkey	Magnetic card terminal access device (can be used with Datalock 4000 encryption unit)	* 20A 22
Mitsubishi Electronics, Inc. 1050 E. Arques Ave. Sunnyvale, CA 94086 (408)730-5900	MF Series Cards	Variety of ROM cards, some as large as 512 KB	*

VENDOR	PRODUCT	DESCRIPTION	REF
PPI 2517 Wyandotte Rd. Willow Grove, PA 19090 (215)657-7500		Computerized card access systems either stand-alone or embedded	
PSI Corp. 1712 Springfield St. Dayton, OH 45043 (800)543-2510		Magnetic stripe cards with user photos	
Pyrotronics-Sentracon 51 Morgan Dr. Norwood, MA 02062 (617)769-4600		Plastic card readers for access control	
Radionics 1800 Abbott St. Salinas, CA 93901 (800)538-5807	Omega Pass and 8122A controller	Programmable Proximity card access system	97 116
Readak Corp. 28829 Chagrin Blvd Cleveland, OH 44122 (216)831-2070		Card access control systems	
Reader/Writer Inc. 6100 S. Maple Ave., Suite 112 Tempe, AZ (602)838-7613	RW250	Device which reads and writes all major IC cards	*
Recognition Equipment, Inc. 2900 Gateway Dr., Suite 600 Irving, TX 75063 (214)550-7900	Electronic Retina	Optical Readers for barcode data	20A
Rusco Electronic Systems, Inc. 1840 Victory Blvd. Glendale, CA 91201 (818)240-2540	Ruscard and Cardentry	Proximity access control card (7" limit) (Sister Co. of Interstate Voice and Codercard under Figgie)	* 84 97 116
Schlage Electronics Corp. 5457 Betsy Ross Drive Santa Clara, CA 95054 (408)727-5170		1024 bit RAM card and proximity card access control systems	100 115 116 130
Secom International, Inc. 9606 Bellanca Ave. Los Angeles, CA 90045 (213)641-1290	Secard	Permanent, non-erasable cards and controllers	*
Secura Key 19749 Bahama St. Northridge, CA 91324 (818)582-0020	Entracomp with Touch Card reader	Card and keyboard access control system	* 116

VENDOR	PRODUCT	DESCRIPTION	REF
Toshiba Corp. 2441 Michelle Dr. Tustin, CA 92680 (714)669-5255		Working on the VISA "super card" project	100
Triad Technologies, Inc. 6080 E. McDonough Dr. Norcross, GA 30093 (404)242-1922		Card Access Systems	
Veritec, Inc. 23801 Calabasas Rd. #2039 Calabasas Park, CA 91302 (818)716-0741	Vericode and Covert Chemical Signatures	Two dimensional barcode ("cubecode") and Chemical countfeit protection.	*
Wells-Fargo Alarm Services 780 5th Ave. King of Prussia, PA 19406 (215)337-3855	Pass Way 8	Uses choice or combination of proximity or Wiegand card readers, or keypads	87
XCP, Inc. 8 West Main St. Dryden, NY 13053 (607)844-9143		Card control devices for computers	

APPENDIX D

Personal Identification News
Reader Survey on Projected Use of Biometrics[98]

George Warfel, Sr. and Benjamin Miller, editors of Personal Identification News, conducted a survey of their readers to assess the future trends of identification technologies. The executive of the future will carry much more than just an access card, according to the readers. Nearly 50% answered that optical memory cards will be commonplace and another 65% said a photo ID would still be needed. PIN readers also think that some biometrics will be common by 2000. The percentage of respondents mentioning each biometric is listed below:

Signature	90%	Hand Geometry	26%
Voice	49%	Keystroke	16%
Fingerprint	46%	Retina Scan	13%

Readers were also asked to look at biometrics from the applications point of view and indicate which type of device is most likely to dominate in each of the eight application areas. A prediction of the year in which biometrics would become commonplace for that application was also requested. The results follow:

- PHYSICAL ACCESS - MILITARY — By 1990
  Fingerprint 35%, Eyescan 35%, Hand 20%
- PHYSICAL ACCESS - INDUSTRIAL — By 1991
  Hand 48%, Fingerprint 25%, Voice 20%
- PHYSICAL ACCESS - COMMERCIAL — By 1992
  Voice 40%, Hand 25%, Signature 25%
- PHYSICAL ACCESS - RESIDENTIAL — By 1994
  Voice 55%, Hand 20%
- COMPUTER ACCESS - MILITARY — By 1991
  Finger 30%, Eye 30%, Key Stroke 20%
- COMPUTER ACCESS - COMMERCIAL — By 1991
  Keystroke 45%, Signature 25%
- ATM — By 1994
  Fingerprint 50%, Signature 25%
- POINT OF SALE — By 1995
  Signature 80%, Hand 13%

The consistency of responses between this year and last was surprisingly strong on the biometric questions. The major notable change was an across the board addition of a year to the estimated date of strong market penetration. The preference for hand geometry in the industrial security field was also interesting because it came almost entirely from vendors. Two losers were noted as compared with last year. Eyescans were selected by 65% to dominate Military Physical Access last year, but this year, popularity was halfed. Also, voice dropped out of favor in the Commercial Computer Access segment, but stayed strong in Residential and Commercial Access Control.

APPENDIX E

SUMMARY OF CRITERIA [1]

The DoD Trusted Computer System Evaluation Criteria(4) provides a basis for specifying security requirements and a metric with which to evaluate the degree of trust that can be placed in a computer system. These criteria are hierarchically ordered into a series of evaluation classes where each class embodies an increasing amount of trust. A summary of each evaluation class is presented in this appendix. This summary should not be used in place of the Criteria.

The evaluation criteria are based on six fundamental security requirements that deal with controlling access to information. These requirements can be summarized as follows:

a. Security policy--There must be an explicit and well-defined security policy enforced by the system.

b. Marking--Access control labels must be associated with objects.

c. Identification--Individual subjects must be identified.

d. Accountability--Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

e. Assurance--The computer system must contain hardware and software mechanisms that can be evaluated independently to provide sufficient assurance that the system enforces the security policy.

f. Continuous protection--The trusted mechanisms that enforce the security policy must be protected continuously against tampering and unauthorized changes.

The evaluation criteria are divided into four divisions--D, C, B, and A; divisions C, B, and A are further subdivided into classes. Division D represents minimal protection, and class A1 is the most trustworthy and desirable from a computer security point of view.

The following overviews are excerpts from the Criteria:

Division D: Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Division C: Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection and accountability of subjects and the actions they initiate, through inclusion of audit capabilities.

[1] See [111] Appendix A and References

APPENDIX F

SECURITY RISK INDEX MATRIX [1]

		Maximum Data Sensitivity						
		U	N	C	S	TS	1C	MC
Minimum Clearance or Authorization of System Users	U	0	1	2	3	5	6	7
	N	0	0	1	2	4	5	6
	C	0	0	0	1	3	4	5
	S	0	0	0	0	2	3	4
	TS(BI)	0	0	0	0	0	2	3
	TS(SBI)	0	0	0	0	0	1	2
	1C	0	0	0	0	0	0	1
	MC	0	0	0	0	0	0	0

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

[1] See [111] Table 3.

APPENDIX G

RISK INDEX COMPUTATION See [110]

The initial step in determining the minimum evaluation class required for a system is to determine the system's risk index. The risk index for a system depends on the rating associated with the system's minimum user clearance (R_{min}) taken from Table 1 and the rating associated with the system's maximum data sensitivity (R_{max}) taken from Table 2. The risk index is computed as follows:

Case a. If R_{min} is less than R_{max}, then the risk index is determined by subtracting R_{min} from R_{max}.[1]

$$\text{Risk Index} = R_{max} - R_{min}$$

Case b. If R_{min} is greater than or equal to R_{max}, then

$$\text{Risk Index} = \begin{cases} 1, & \text{if there are categories on the system to which some users are not authorized access} \\ 0, & \text{otherwise} \end{cases}$$

[1] There is one anomalous value that results because there are two "types" of Top Secret clearance and only one "type" of Top Secret data. When the minimum user clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1, which would result from a straight application of the formula)

APPENDIX H

DETAILED DESCRIPTION OF CLEARANCES AND DATA SENSITIVITIES [1]

This appendix describes in detail the clearances and data sensitivities (e.g., classification) introduced in the body of the report.

B.1 Clearances

This section defines increasing levels of clearance or authorization of system users. System users include not only those users with direct connections to the system but also those users without direct connections who might receive output or generate input that is not reliably reviewed for classification by a responsible individual.

a. Uncleared (U)--Personnel with no clearance or authorization. Permitted access to any information for which there are no specified controls, such as openly published information.

b. Unclassified Information (N)--Personnel who are authorized access to sensitive unclassified (e.g., For Official Use Only (FOUO)) information, either by an explicit official authorization or by an implicit authorization derived from official assignments or responsibilities.(15)

c. Confidential Clearance (C)--Requires U.S. citizenship and typically some limited records checking.(19) In some cases, a National Agency Check (NAC) is required (e.g., for U.S. citizens employed by colleges or universities).(20)

d. Secret Clearance (S)--Typically requires a NAC, which consists of searching the Federal Bureau of Investigation fingerprint and investigative files and the Defense Central Index of Investigations.(19) In some cases, further investigation is required.

e. Top Secret Clearance based on a current Background Investigation (TS(BI))--Requires an investigation that consists of a NAC, personal contacts, record searches, and written inquiries. A BI typically includes an investigation extending back 5 years, often with a spot check investigation extending back 15 years.(19)

f. Top Secret Clearance based on a current Special Background Investigation (TS(SBI))--Requires an investigation that, in addition to the investigation for a BI, includes additional checks on the subject's immediate family (if foreign born) and spouse and neighborhood investigations to verify each of the subject's former residences in the United States where he resided six months or more. An SBI typically includes an investigation extending back15 years.(19)

[1] See [111] Appendix B and References

2. Examination questions and answers used in determination of the qualification of candidates for employment or promotion.

3. Data that a statute specifically exempts from disclosure, such as Patent Secrecy data.(23)

4. Data containing trade secrets or commercial or financial information.

5. Data containing internal advice or recommendations that reflect the decision-making process of an agency.(24)

6. Data in personnel, medical, or other files that, if disclosed, would result in an invasion of personal privacy.(25)

7. Investigative records.

DoD Directive 5400.7 prohibits any material other than that cited in FOI Act exemptions from being considered or marked FOUO.(15) One other form of unclassified sensitive data is that pertaining to unclassified technology with military application.(16) This refers primarily to documents that are controlled under the Scientific and Technical Information Program or acquired under the Defense Technical Data Management Program.(26,27) In addition to specific requirements for protection of particular forms of unclassified sensitive data, there are two general mandates. The first is Title 18, U.S. Code 1905, which makes it unlawful for any office or employee of the U.S. Government to disclose information of an official nature except as provided by law, including when such information is in the form of data handled by computer systems.(28) Official data is data that is owned by, produced by or for, or is under the control of the DoD. The second is Office of Managment and Budget (OMB) Circular A-71, Transmittal Memorandum Number 1, which establishes requirements for Federal agencies to protect sensitive data.(30)

c. Confidential (C)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.(3)

d. Secret (S)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.(3)

e. Top Secret (TS)--Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.(3)

RATING SCALE FOR MINIMUM USER CLEARANCE[1].

MINIMUM USER CLEARANCE	RATING (R_{min})
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)/Current Background Investigation (BI)	4
Top Secret (TS)/Current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

See [110] Table 1.

[1] The following clearances are as defined in DIS Manual 20-1(2): Confidential, Secret, Top Secret/Current Background Investigation, Top Secret/Current Special Background Investigation.

APPENDIX I

ENVIRONMENTAL TYPES

See [111] Appendix C

The amount of computer security required in a system depends not only on the risk index (Section 2) but also on the nature of the environment. The two environmental types of systems defined in this document are based on whether the applications that are processed by the TCB are adequately protected against the insertion of malicious logic. A system whose applications are not adequately protected is referred to as being in an open environment. If the applications are adequately protected, the system is in a closed environment. The presumption is that systems in open environments are more likely to have malicious application than systems in closed environments. Most systems are in open environments.

Before defining the two environmental categories in more detail, it is necessary to define several terms.

a. Environment. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system.

b. Application. Those portions of a system, including portions of the operating system, that are not responsible for enforcing the system's security policy.

c. Malicious Logic. Hardware, software, or firmware that is intentionally included for the purpose of causing loss or harm (e.g., Trojan horses).

d. Configuration Control. Management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

C.1 Open Security Environment

Based on these definitions, an open security environment includes those systems in which either of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance (or authorization) to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.

b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.

APPENDIX J

SECURITY INDEX MATRIX FOR OPEN SECURITY ENVIRONMENTS[1]

		Maximum Data Sensitivity						
		U	N	C	S	TS	1C	MC
Minimum Clearance or Authorization of System Users	U	C1	B1	B2	B3	*	*	*
	N	C1	C2	B2	B2	A1	*	*
	C	C1	C2	C2	B1	B3	A1	*
	S	C1	C2	C2	C2	B2	B3	A1
	TS(BI)	C1	C2	C2	C2	C2	B2	B3
	TS(SBI)	C1	C2	C2	C2	C2	B1	B2
	1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
	MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

See [110] Table 5.

[1] Environments for which either C1 or C2 is given are for systems that operate in system high mode. No minimum level of trust is prescribed for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

[2] It is assumed that all users are authorized access to all categories present in the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

[3] Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Category

APPENDIX K

SECURITY INDEX MATRIX FOR CLOSED SECURITY ENVIRONMENTS[1]

Maximum Data Sensitivity

		U	N	C	S	TS	1C	MC
Minimum Clearance or Authorization of System Users	U	C1	B1	B2	B2	A1	*	*
	N	C1	C2	B1	B2	B3	A1	*
	C	C1	C2	C2	B1	B2	B3	A1
	S	C1	C2	C2	C2	B2	B2	B3
	TS(BI)	C1	C2	C2	C2	C2	B2	B2
	TS(SBI)	C1	C2	C2	C2	C2	B1	B2
	1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
	MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

See [110] Table 7.

[1] Environments for which either C1 or C2 is given are for systems that operate in system high mode. There is no prescribed minimum level of trust for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

[2] It is assumed that all users are authorized access to all categories on the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

[3] Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS (SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

APPENDIX L

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA SUMMARY CHART [109]

	SECURITY POLICY										
	DISCRETIONARY ACCESS CONTROL	OBJECT REUSE	LABELS	LABEL INTEGRITY	EXPORTATION OF LABELED INFORMATION	EXPORTATION TO MULTILEVEL DEVICES	EXPORTATION TO SINGLE-LEVEL DEVICES	LABELING HUMAN-READABLE OUTPUT	MANDATORY ACCESS CONTROL	SUBJECT SENSITIVITY LABELS	DEVICE LABELS
A1	□	□	□	□	□	□	□	□	□	□	□
B3	▨	□	□	□	□	□	□	□	□	□	□
B2	□	□	▨	□	□	□	□	□	▨	▨	▨
B1	□	□	▨	▨	▨	▨	▨	▨	▨	■	■
C2	▨	▨	■	■	■	■	■	■	■	■	■
C1	▨	■	■	■	■	■	■	■	■	■	■

	ACCOUNTABILITY		
	IDENTIFICATION AND AUTHENTICATION	AUDIT	TRUSTED PATH
A1	□	□	□
B3	□	▨	▨
B2	□	▨	▨
B1	▨	▨	■
C2	▨	▨	■
C1	▨	■	■

	ASSURANCE								
	SYSTEM ARCHITECTURE	SYSTEM INTEGRITY	SECURITY TESTING	DESIGN SPECIFICATION AND VERIFICATION	COVERT CHANNEL ANALYSIS	TRUSTED FACILITY MANAGEMENT	CONFIGURATION MANAGEMENT	TRUSTED RECOVERY	TRUSTED DISTRIBUTION
A1	□	□	▨	▨	▨	□	▨	□	▨
B3	▨	□	▨	▨	▨	▨	□	▨	■
B2	▨	□	▨	▨	▨	▨	▨	■	■
B1	▨	□	▨	▨	■	■	■	■	■
C2	▨	□	▨	■	■	■	■	■	■
C1	▨	▨	▨	■	■	■	■	■	■

	DOCUMENTATION			
	SECURITY FEATURES USER'S GUIDE	TRUSTED FACILITY MANUAL	TEST DOCUMENTATION	DESIGN DOCUMENTATION
A1	□	□	▨	▨
B3	□	▨	□	▨
B2	□	▨	▨	▨
B1	□	▨	□	▨
C2	□	▨	□	□
C1	▨	▨	▨	▨

□ NO ADDITIONAL REQUIREMENTS FOR THIS CLASS

▨ NEW OR ENHANCED REQUIREMENTS FOR THIS CLASS

■ NO REQUIREMENTS FOR THIS CLASS

GLOSSARY

Access
To obtain, communicate with, or otherwise make use of any component, program, or information in a computer system.

Access Cards
A plastic card containing machine-readable information used as a form of automatic identity verification.

Access Control
A strategy for limiting the access of objects to authorized persons.

Algorithm
A mathematical procedure which solves a problem. Typically the left side of an equation.

Audit
To automatically record the activities of users.

Authentication
The act of verifying that a user, device, or piece of data is that which it appears to be.

Biometric
Associated with unique, measurable biological characteristics.

Compromise
To lose or disclose sensitive information to an unauthorized person.

Configuration
A specific selection and arrangement of a system's hardware and software, allowing it to perform certain functions.

Controller
A computer which runs programs to control the activities of another device or devices.

Covert Channel
A communications path through which data can be passed for unauthorized use.

Data Access Control
A strategy for limiting access of computer resources and data to authorized persons by verifying their identity through a pre-login procedure. Passwords, access tokens and biometric devices have all been used to implement this strategy.

Data Encryption Standard (DES)
A method approved by the U.S. Bureau of Standards for encoding unclassified sensitive digital information.

Host
A user computer in a network.

Imposter
A person who attempts unauthorized access by claiming to be an authorized person.

Interface
A communications access point, through which data can enter and exit a system or device.

Keystroke Dynamics
The measurement of the speed and rhythm of a person's typing pattern, which is said to be a measurable characteristic of that person.

Least Privilege
Providing users only what need be known in order to perform their assigned task.

Logon
The procedure by which a user begins a terminal session.

Modem
A device designed to alter data so that it can be sent and received over telephone lines.

Multilevel Secure System
A system capable of processing data of more than one security level simultaneously, without compromising the data.

Need-to-Know
A job related requirement for access to specific information which must be accompanied by the appropriate security clearances in order for access to be authorized.

Network
A communications medium, and all attached components, which may include computers, controllers, access control mechanisms, and other hardware and software elements.

Operating System
An integrated collection of service routines which supervise the allocation of resources, and the sequencing and processing of programs by a computer.

Orange Book
Common name for the Department of Defense Trusted Computer System Evaluation Criteria (DOD 5200.28-STD). A Defense Department standard for the evaluation of the security of a computer system.

Packet
A portion of a data transmission which is limited in size, such that it can be sent through a computer network.

Smart Card
An access card containing a small integrated circuit on which data can be stored or a simple process can be run.

Software
A computer program or programs dedicated to the performance of a specific function.

System High
The highest security level supported by a system in a particular environment.

TEMPEST Technology
A technology which aims to secure computer systems from the threat of electromagnetic emanation monitoring.

Template
A digital representation of a user's measurable biometric trait which is stored and later compared with during the authentication process.

Threshold
The cut-off point in an authentication comparison above which access is granted, and below which access is denied.

Trusted Computer System
A computer system which employs sufficient security measures to be permitted to process data of more than one security level simultaneously.

Type I Error
Rejection of an authorized user. Sometimes called a False Reject.

Type I Error Rate
(Type I Errors) ÷ (Authorized User Attempts)

Type II Errors
Acceptance of an imposter. Sometimes called a False Accept.

Type II Error Rate
(Type II Errors) ÷ (Imposter Attempts)

Type I / Type II Crossover
For devices with an adjustable acceptance threshold, the point at which the Type I and Type II error rates are the same.

User
A person who utilizes the resources of a computer system.

ANNOTATED BIBLIOGRAPHY

[1] Anderson, Howard M. "The Conflict: User Friendliness vs. Effective Security." Datamation, September 15, 1985, supplement between p. 84 and p. 85.
Identifies remote login communications as the greatest security threat. Systems not requiring remote access are much easier to secure.

[2] Williams, Tom. "Access Control Plus Data Encryption Adds Up To System Security. Computer Design, August 1, 1986, pp. 44-46.
Points out two biometric devices (Eyedentify's retina scanner and Identix's fingerprint verifier) and an access key (by Gordian Systems) as being especially effective in conjunction with encryption and secure data transmission.

[3] Botting, Richard. "Novel Security Techniques for on-line Systems." Communications of the ACM, May 1986, p. 416 + .
Suggests the idea of a "hacker trap", a section of useless database to which the hacker is baited, but cannot exit. Once in it, the systems operator is alerted. Botting calls this the "Negative Security Zone".

[4] Schatz, Willie. "Putting on the Cuffs." Datamation, July 15, 1986, p. 40.
Describes legislation designed to stiffen penalties for "hacking".

[5] Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Prentice-Hall, Englewood Cliffs New Jersey, 1977, Chapter 2, pp 6-22.
Focuses mostly on the weaknesses and mathematical probabilities of cracking passwords.

[6] Karger, Paul A. "Authentication and Discretionary Access Control in Computer Networks." Computers & Security, December, 1986, pp. 314-324.
Describes concepts such as Girling's authentication server, where Host A gives a one-time password to the user after logging in. When connecting to Host B, he is asked for the password, and it is checked through a central processor.

[7] "Technology Watch:" Computers & Security, March, 1986, pp. 4-6.
Features three access keys: Access Key by Gordian Systems, Privacy/Plus and Lazer Lock by United Software Security, and Safeword by Enigma Logic through Quire Industries. Each uses optical screen sensors and is machine independent.

[8] Wood, Charles Cresson and Zeidler, Howard M. "Security Modules: Potent Information Security System Components. Computers & Security, March, 1986, pp. 114-121.
Discusses PIN management and access keys but focuses on encryption, and the use of "modules", computers used especially for the purpose of processing and storing security-related information.

[18] Davies, D.W. and Price, W.L. Security for Computer Networks. John Wiley and Sons, New York, 1984, Chapter 7, pp. 179-218.
A thoroughly researched chapter on advanced user authentication methods and devices. Features biometric devices, and describes briefly how each operates.

[19] Colby, Wendelin. "The Security Vow". Infosystems, March, 1985, pp. 94-97.
Describes briefly some computer security devices for various applications, such as Fingermatrix, Multisentry, Cylock, Linemux, Autocrypt 1, and others. Some selection criteria are listed.

[20A] Larson, Harry T. "Who Goes There?" Hardcopy, March 1985, pp. 59 + .
Interesting, easy to read article on the technology aimed at authenticating user identities. Provides a list of computer security vendors.

[20B] Larson, Harry T. "Who Goes There?: Rifkin Remembered" Hardcopy, March 1985, pp. 62-63.
Story of how one man foiled a bank's dynamic password system to rob $10.2 million. He got caught by bragging about the heist to his lawyer, who turned him in.

[21] Brinkley, Donald, L. Data Security for Distributed Tactical C3 Systems.
A paper presented at MILCOM '86 in October 1986, in Monterey, California. Describes System Security methods for tactical systems based on Orange Book criteria.

[22] Juris, Robbin. "Smart Tokens Provide See-Through Security." Computer Decisions, November 4, 1986, p. 52.
Describes an access key which stores biometric information, saving on the system's internal memory. However, the article fails to mention that someone capable of programming his own chip may be capable of producing his own access key and circumventing the device. Article also contains a table of vendors of dial-up security devices.

[23] Wong, Raymond M., et. al. "Polonius: An Identity Authentication System". IEEE Computer Society, January, 1985, pp. 101-107.
Describes the "Polonius Passport", a Sytek device which stores one time passwords. This is coupled with an authentication server, which checks the password with the host. The passport has its own PIN, coupling possession with user knowledge requirements.

[24] Page, Marcus. "Passwords Are Still Best Security Method". Government Computer News, Vol. 4, No. 12.
States that based on cost, error rates and user acceptability, passwords are the most efficient means of authenticating user identities. Article does admit that some systems provide greater security, but says these methods should also incorporate passwords. Gives cost estimates of other methods.

[33] "Computer Security: Issues and Responsibilities". Datamation, October 1, 1986, Supplement between p. 68 and 69.
Contains several articles, including those listed below:

[33A] Burrows, James H. "Future Directions for Computer Security: The Role of Standards".
Establishes the importance of setting security standards.

[33B] Cangemi, Michael P. "The Internal Auditor's Role in Computer Security".
Describes effective system auditing, both of users and the security measures themselves.

[33C] Hammer, Carl. "Computer Security and the Human Interface".
Gives examples of how computer security failed due to human errors.

[33D] Lobel, Jerome. "The Manufacturers' Responsibility for Computer Security".
Describes the need for computer manufacturers to develop secure access control mechanisms for computer systems.

[34] Daly, Alan. "VIC Readies Voice Recognizer". Mass High Tech, May 25, 1987.
Describes how VIC rose from the ashes of Verbex/Exxon, unveiling a device designed more for speech recognition than speaker recognition, but it may have security applications.

[35] Dooley, Bill. "Card Access Systems -- Tighter Security, Low Cost". MIS Week, April 14, 1986, p. 14.
Describes the use of magnetic stripe cards as access keys to installations. Focuses on Synergistics, a leading manufacturer from Natick.

[36] Watt, Peggy. "Teenager Charged With Four Counts of Illegal Hacking". Computerworld, February 17, 1986, p. 10.
Tells how an 18 year old boy accessed corporate mainframes through modems.

[37] "Guidelines on User Authentication Techniques for Computer Network Access Control". Federal Information Processing Standards, Publication No. 83, September 29, 1980.
Similar to FIPS #48, but uses updated terminology and looks at some biometric devices that didn't exist in 1977. A thorough report which understands the value of effective biometric user authentication.

[38] Hart, Denis. "Security Options Can Be As Varied, Complex As Systems Are". Federal Computer Week, October 26,1987, p. 29.
Sites companies such as Gordian and Thumbscan as offering identification technology that is on the cutting edge.

[39] Brindza, Stephen. "Security with a Personal Touch". Modern Office Technology, May, 1987, pp. 80-82.
Describes the Identix IDX-10 fingerprint analyzer. Used in a bank as a physical access control device, it has not yet been applied to an ATM.

[49] Neugent, Bill. "Conan and the Jargonauts". SIGSAC Review, Winter 1987, pp. 13-18.
A humorous article poking fun at both the jargon used by computer security experts, and at the apathy taken by systems operators towards security.

[50] Martin, James. Security, Accuracy, and Privacy in Computer Systems. 1973, Prentice-Hall, Englewood Cliffs, NJ.
A surprisingly advanced analysis of user authentication techniques, using some outdated terminology. Extensive analysis of voice verification (Bell Labs) and hand geometry (Identimation), as well as many knowledge-based systems.

[51] Lipton, David L. "Logical Authentication Methods". SIGSAC Review, Spring, 1986, pp. 9-20.
Describes some unusual authentication methods, digital signatures (encrypted functions), analog signatures (unencrypted passwords), pattern recognition, and pass-algorithms.

[52] Kramer, Steven. "Linus IV - An Experiment in Computer Security". Proceedings of the 1984 Symposium on Security and Privacy, p. 27.
Describes a random pronounceable password generation technique, where the user can select one of the generated passwords.

[53] Bloombecker, Jay. "Computer Security - For the People". Computers and Society, W,S,S,F, 1985, pp. 12-15.
Tries to illustrate the value of secure computers for the public good. Claims society must do more than just assume that their bank accounts, tax dollars, and personal information is secure.

[54] Taft, Darryl K. "Time-Based System Promises Enhanced Security". Government Computer News, May 22, 1987, p. 91.
Describes a product by Security Dynamics, which is a hand-held dynamic password generator which can generate 60 second passwords, as does software in the host. It also has a duress code.

[55] Sharma, Ravi Shankar. "Data Communications and Security". SIGSAC Review, Winter 1986, pp. 28-36.
Provides definitions and descriptions of how computer crimes are carried out, and therefore, how they can be prevented. Focuses on host access through remote terminals.

[56] Athanasiou, Tom. "DES Revisited". Datamation, October 15, 1985, pp. 110-114.
Article on the controversy surrounding the Data Encryption Standard, and a discussion of the conflict between the need for standardization and the desire to leave room for improvement.

[57] Miles, J.B. "Electronic Signature: More Security in Less Time". Government Computer News, April 24, 1987.
In addition to a "Digital Signature", which authenticates the sender's identity, the article describes a "Digital Envelope", which can be decrypted only by the intended recipient.

[67] Isenor, D.K. and Zaky, S.G. "Fingerprint Identification Using Graph Matching". Pattern Recognition, Vol. 19, No. 2, 1986, pp. 113-122.
A technical description of how fingerprints are distinguished from one-another. A two-dimensional array of pixels is used and the sensitivity is adjusted until the Type I and Type II error rates match.

[68] Harmon, L.D., et. al. "Machine Identification of Human Faces". Pattern Recognition, Vol. 13, No. 22, 1981, pp. 97-110.
Describes a method for recognizing faces based on characteristics of profile features. Decent accuracy was obtained (96%). Future research was being aimed at algorithms using polynomial fits for noses, foreheads, and chins for increased accuracy. Also, they hope to incorporate ear shape.

[69] Haton, Jean-Paul. "Speech Recognition and Understanding". IEEE, 1982, pp. 570-581.
Gives details of how speech can be interpreted by a computer, primarily for the purpose of recognizing spoken words. The techniques described are applicable to the identification of the speaker.

[70] Proceedings, 1977 International Conference on Crime Countermeasures --Science and Engineering.
A collection of articles concerning various aspects of electronic security, including computer user authentication methods. Also contains abstracts on other papers.

[70A] Bunge, E. "Automatic Speaker Recognition System AUROS for Security Systems and Forensic Voice Identification". pp. 1-7.
Describes a system for recognizing voices through algorithmic analysis. It is not done by comparing the waveforms for one word, but rather by comparing the known vocal characteristics with those encountered for any spoken words.

[70B] Hollien, Harry. "Status Report of 'Voiceprint' Identification in the United States". pp. 9-20.
A very critical analysis of voice identification techniques. Terminology is in a "we" vs. "they" context, with "they" being the voiceprint proponents. Article claims that voiceprinting is inaccurate science, and should not be used as evidence in court. Author's tone sounds as if he was convicted of a crime through voiceprint evidence.

[70C] Vidalon, Mario, et. al. "Frequency Parameters for Speaker Recognition". pp. 43-47.
Describes a method for constructing a speaker recognition system. Subjects utter a specific phrase, and the waveform is compared to a reference of the same phrase by the claimed speaker. No statistical conclusions were made.

[70D] De Bruyne, P. "A New Method of Signature Verification". pp. 99-103.
In 1977, it was new. It is a method of signature dynamics, where the duration of pen/paper contact is measured. Initial tests had large false-reject numbers.

[75] Hurst, Rebecca. "Don't Get Locked Into Too Much Security". Computerworld, June 3, 1987, pp. 37-40.
Despite the title, this article does not belittle the need for effective computer security. It points out password shortcomings, and contrasts them with biometric costs. The main warning is that security technology is changing so quickly that buying now may be a mistake.

[76A] Vacca, John. "Tinker, Tailor, Network Spy". Computerworld, June 3, 1987, pp. 41-44.
Illustrates that the most dangerous intruder to a computer system is the authorized user, who can embezzle and abuse the system for his personal gain or even amusement.

[76B] Vacca, John. "A Smarter Smart Card". Computerworld, June 3, 1987, p. 43.
Describes the Challenger Card, a joint effort by Sytek and Open Computer Security (UK). To access a protected system, one must know both the system user's password, and the password of the card, plus have access to the card.

[77] Iversen, Wesley R. "Fingerprint Reader Restricts Access to Terminals and PCs". Electronics, June 11, 1987.
Describes "Thumbscan", a thumbprint verifier. It's cheap ($995, $500 for quantities ≥100). They're shooting for Type I errors of .5% and Type II errors of .005%, but these are just design goals.

[78] Lipton, David L. and Wong, Harry K.T. "Modern Trends in Authentication". SIGSAC Review, pp. 36-42.
Provides details of many different authentication methods, including object recognition in graphic figures, chromosomal tests, etc. Gives five classes of identity traits: Something someone is, has, knows, does, or recognizes.

[79] "Product Checklist". Computerworld, June 3, 1987, p. 43.
Gives descriptions of a few new computer security products, such as: Dial-Guard, Black Box, and Racal Vadic.

[80A] "All About Biometric Access Control Systems". Datapro Reports on Information Security, December 1986, pp. 001301-001316.
An in-depth report on several biometric devices, prepared, in part, by George Warfel. Included are descriptions, testing evaluations, and vendor lists.

[80B] "All About Biometric Access Control Systems". Datapro Reports on Information Security, July, 1985, pp. 001301-001309.
Similar to [80A], but contains some different devices and different vendors.

[81A] "Signature Verification: Write for You?". Datapro Reports on Information Security, January 1987, pp. 701011-701012.
An overview of signature dynamics devices and static signature comparators. Some commercial examples (such as De La Rue and Signify) are cited.

[91] "Audit System Tackles Insider Threats". Government Computer News, March 13, 1987.

Describes Clyde Digital Systems' "Sentry Gate" ("Audit" for Government sales). It records every keystroke an a VAX for playback or software analysis.

[92] Mercer, Lindsay. "Implementing a Computer Security Policy". The Accountant's Magazine, August 1986, pp. 50-53.

Starts by trying to apply quantitative methods to a qualitative risk analysis problem of a random system. Fortunately, he gets tired of his, and concentrates on the concepts.

[93] Cooper, James Arlin. Computer Security Technology. Lexington MA, D.C. Heath and Co., 1984, pp. 49-57.

Chapter which provides descriptions on various hardware access control devices. Particular attention is given to biometric devices and associated research.

[94] Norman, Adrian R.D. Computer Insecurity. London, Chapman and Hall, 1983, pp. 311-329.

Chapter on performing risk analyses on computer systems. Good details on how to go about measuring the amount of risk, and therefore, how much should be spent on security.

[95] Cunningham, John E. Security Electronics. Indianapolis, Howard W. Sams & Co., 1977, pp. 157-161.

Chapter on personnel identification, giving descriptions of fingerprint verification, hand geometry, and voice prints.

[96] Warfel, George H., Sr. "Identification Technology". Auerbach Data Security Management, 84-01-10.

An overview of password, access card and biometric technology. Very concise, but not too detailed.

[97] "Product Update". Security, July, 1987, p. 118 +.

Provides information on a variety of new security products, primarily access control cards. A number of advertisements are also included.

[98] Personal Identification News, Warfel & Miller, Inc., June, 1987.

Features Thumbscan purchase of Gordian Systems, Camarilla resurrection of Voxtron, De La Rue reorganization, and information on Recognition systems, Fingermatrix, Micro Card, Drexler, Faraday, etc.

[99] Edwards, Robert W. and Edwards, Lynda E. "Unauthorized Entry". ICP Interface, Winter, 1982, pp. 22-26.

Describes the widespread growth of computer crimes, but focuses different types of encryption as solutions.

[100] Miller, Benjamin L. and Warfel, George H. Sr. "1987 Biometric Industry Directory". Personal Identification News, Warfel & Miller, Inc., 1987.

Provides extensive corporate and technical information on manufacturers of biometric identification devices and IC cards. Some articles describing the progress of biometric technology are included.

[106] Proceedings of the Department of Defense Computer Security Center Invitational Workshop on Network Security. March 19-22, 1985, Section Three.
A collection of papers regarding data security, which include:

[106A] Lipner, Steven. "Report of the Access Controls Group".
A detailed description of the problem of discretionary and mandatory access control, especially as they relate to computer networks.

[106B] Bailey, David. "Trust in Computer Networks"
Points out that Access Control is a weak point in the Orange Book criteria. A1 systems only require individual passwords located in trusted databases.

[106C] Gleason, T.P. "Network Access Control".
Describes the requirements for access control in a multilevel network. Proper separation mechanisms and network models are used.

[106D] Shirey, Robert W. "Access Control and Other Issues in Computer Network Security Evaluation".
Argues that the development of a "Trusted Network Evaluation Criteria" should not be an Orange Book translation for networks, but should be based on a layered, abstract reference model of computer network communication services.

[107] Aiken, Dina. Secure User Authentication in a Distributed Computing Environment (DE86-002960). Livermore CA, Lawrence Livermore National Laboratory, October 1985.
Starts off by accurately describing authentication and the problems associated with it, but deals more with the securing of the database and encryption.

[108] Computer Security: Security in Mission Critical Computer Resource Acquisition. Air Force Computer Security Program Office, February 1, 1985.
Describes each stage in the selection, accreditation, and management of a mission critical system. However, the recommendations regarding access control only stipulate that only authorized users may enter the facility, which means the computer must operate at system high.

[109] Department of Defense Trusted Computer System Evaluation Criteria (5200.28-STD) (Orange Book) December, 1985.
Established by the DoD, this book has become the standard for determining the level of security provided by a computer system.

[110] Computer Security Requirements. (CSC-STD-004-85) June 25, 1985.
Also known by its more descriptive name: "Guidance for Applying the Department of Defense Trusted Computer System Evaluatior Criteria in Specific Environments".

[111] Technical Rationale Behind CSC-STD-03-85: Computer Security Requirements. (CSC-STD-004-85) June 25, 1985.
Provides more detail to the vague generalizations made in reference [110].

[121] Security Requirements for ADP Systems. (U.S. Dept. of Defense Directive 5200.28) revised April, 1978.

The DoD's version of AF 205-16, which establishes procedures regarding the security of classified information.

[122] Naudts, John. "Access Control: It's In the Cards. Security Management, September 1987, pp. 169-173.

Describes the various technologies employed by access card manufacturers, as well as the current and future applications of cards which possess data.

[123] "Technology Watch - Access Control to Mainframe". Computers and Security, August 1987, pp. 295-296.

Describes the Dial-Guard product, which requires an access key for dial-up access to a mainframe.

[124] Verma, M.R., Majumdar, A.K., and Chatterjee, B. "Edge Detection in Fingerprints". Pattern Recognition, Vol. 20, No. 5, pp. 513-523, 1987.

Describes a mathematical enhancement process for obtaining clear fingerprint data from fuzzy images.

[125] Dwyer, Patricia A., Jelatis, George D., and Thuraisingham, Bhavani M. "Multi-level Security in Database Management Systems". Computers and Security, June 1987, pp. 252-260.

Gives an example of how to structure a multi-level relational database such that it is secure without sacrificing sharability.

[126] Personal Identification News, Warfel & Miller, Inc., September 1987.

This issue includes: Ecco's Voice Key/VR, and Identix price cuts.

[127] Doddington, George. "Speaker Recognition - Identifying People by their Voices." Proceedings of the IEEE, November 1985, pp. 1651-1664.

A detailed paper on how automatic speaker recognition is achieved, and how different devices accomplish it.

[128] Personal Identification News, Warfel & Miller, Inc., October 1987.

This issue includes: The demise of the Identimat; DOE's purchase of ID-3D's; Notable events of the SCAT Conference.

[129] Bright, Daryl C. Examining the Reliability of a Hand Geometry Identity Verification Device For Use in Access Control. Thesis, Naval Postgraduate School, Monterey, CA, March 1987.

Describes extensive testing of the Recognition Systems ID-3D device, while noting several considerations for testing biometric devices. Report concludes the ID-3D has a Type I/Type II crossover of .62%

[130] Smart Card Opportunities in the U.S. - Volume IV: Biometrics in Personal Identification. Smart Card Reports, May 1986.

A highly detailed, 260 page report on the various biometric devices that currently exist. An emphasis is placed on their use in conjunction with smart cards.