

NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



THESIS

SURVEY OF USER AUTHENTICATION MECHANISMS

by

Marianna B. Magno

September 1996

Principal Advisor:

William J. Haga

Approved for public release; distribution is unlimited

19961210 067

DTIC QUALITY INSPECTED 4

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

| | | | |
|---|----------------------------------|--|--|
| 1. AGENCY USE ONLY <i>(Leave blank)</i> | 2. REPORT DATE September 1996 | 3. REPORT TYPE AND DATES COVERED Master's Thesis | |
| 4. TITLE AND SUBTITLE: SURVEY OF USER AUTHENTICATION MECHANISMS | | 5. FUNDING NUMBERS | |
| 6. AUTHOR(S) Magno, Marianna B. | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000 | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. | |
| 12a. DISTRIBUTION/AVAILABILITY STATEMENT: Approved for public release; distribution is unlimited. | | 12b. DISTRIBUTION CODE: | |
| 13. ABSTRACT <i>(maximum 200 words)</i> The use of a password as the only traditional user authentication mechanism has been criticized for its weakness in computer security. One problem is for the user to select short, easy to remember passwords. Another problem is the selection of a password that is too long which the user tends to forget. Long passwords tend to be written down carelessly somewhere in the work space. Such practices can create serious security loopholes. Consequently, this is a survey of alternative password mechanisms and other improved devices that are now available in the marketplace to enhance computer security. It taxonomizes the existing inventory of user authentication mechanisms such as biometrics, challenge/response, password, smart card and token. | | | |
| 14. SUBJECT TERMS | | 15. NUMBER OF PAGES 74 | |
| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | | 16. PRICE CODE | |
| 18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified | | 20. LIMITATION OF ABSTRACT UL | |
| 19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified | | 20. LIMITATION OF ABSTRACT UL | |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18 298-102

Approved for public release; distribution is unlimited

SURVEY OF USER AUTHENTICATION MECHANISMS

Marianna B. Magno
Lieutenant, United States Navy
B. S., California State Polytechnic University, Pomona, 1983
M.B.A., Mississippi State University, 1987


Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION
TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 1996**

Author:

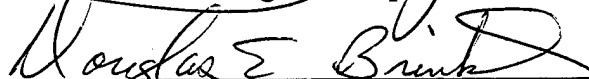


Marianna B. Magno

Approved by:



William J. Haga, Principal Advisor



Douglas Brinkley, Associate Advisor



Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The use of a password as the only traditional user authentication mechanism has been criticized for its weakness in computer security. One problem is for the user to select short, easy to remember passwords. Another problem is the selection of a password that is too long which the user tends to forget. Long passwords tend to be written down carelessly somewhere in the work space. Such practices can create serious security loopholes.

Consequently, this is a survey of alternative password mechanisms and other improved devices that are now available in the marketplace to enhance computer security. It taxonomizes the existing inventory of user authentication mechanisms such as biometrics, challenge/response, password, smart card and token.

TABLE OF CONTENTS

| | | |
|------|--|----|
| I. | INTRODUCTION..... | 1 |
| A. | COMPUTER SECURITY..... | 1 |
| B. | ISSUES | 2 |
| II. | USER IDENTIFICATION AND USER AUTHENTICATION..... | 5 |
| A. | THE PASSWORD (SOMETHING YOU KNOW)..... | 7 |
| B. | THE TOKEN, KEY, OR SMART CARD (SOMETHING YOU POSSESS)..... | 7 |
| C. | PERSONAL CHARACTERISTICS (SOMETHING YOU ARE).... | 7 |
| III. | TRADITIONAL PASSWORD METHOD..... | 9 |
| IV. | ADVANCED PASSWORD SCHEMES | 11 |
| A. | SYSTEM GENERATED PASSWORDS..... | 11 |
| B. | PASSPHRASES..... | 11 |
| C. | COGNITIVE PASSWORDS..... | 13 |
| D. | ASSOCIATIVE PASSWORDS..... | 15 |
| V. | ADVANCED AUTHENTICATION MECHANISMS | 17 |
| A. | TOKEN..... | 17 |
| B. | SMART CARD | 18 |
| C. | CHALLENGE-RESPONSE SYSTEMS | 19 |
| D. | BIOMETRIC TECHNOLOGY..... | 20 |
| 1. | Face | 21 |
| 2. | Fingerprints..... | 22 |
| 3. | Hand | 24 |
| 4. | Eye..... | 25 |
| 5. | Voice | 27 |
| 6. | Signature..... | 29 |
| 7. | Typing Rhythms | 31 |
| 8. | Summary | 31 |

VI. ORANGE BOOK EVALUATION (DoD 5200.28-STD)35

VII. CONCLUSION39

APPENDIX A. PRODUCT LIST41

APPENDIX B. SUPPLIER LIST55

LIST OF REFERENCES61

INITIAL DISTRIBUTION LIST65

I. INTRODUCTION

A. COMPUTER SECURITY

When one discusses computer security issues, there are four areas that are equally important in the computer security field: memory protection, file protection, general object access control, and user authentication. (Pfleeger, 1989)

Memory protection is important for multi-user environments today and increasingly important for the future. This is due to the increase in networking such as LAN and WAN. Advances in memory protection include mechanisms such as fences, base/bounds registers, tagged architecture, paging, and segmentation which are useful for machine addressing and protection. (Pfleeger, 1989)

File protection schemes include general-purpose operating systems which are often based on a three-or four-level format (for example: user-group-all). This format is reasonably straightforward to implement, but it restricts access control to fewer levels.

Access control is addressed by the access control matrix or access control lists organized on a per-object or per-user basis. It is flexible to use but the mechanism can be difficult to implement efficiently.

User authentication is an issue that becomes more important as unacquainted users seek to share facilities through networks.

This study surveys the known techniques, practices and mechanisms of user authentication. It orders these in a taxonomy of methods, including passwords and

authentication mechanisms such as token, smart cards and bio-technical devices (such as retina scans and finger prints). The resulting inventory, will be of value to computer security analysts, computer security managers and designers of operating systems. This paper will also attempt to tie in the NCSC Orange book and its demands for authentication mechanisms. Commercial packages to enhance user authentication will be reviewed as well.

B. ISSUES

With recent news coverage documenting the activities of hackers, the Department of Defense has impetus to strengthen authentication of the users of its information systems. (Littman, 1996; Schorow, 1996; Alexander, 1995; Baig, 1994; Borowsky, 1994; GAO testimony, 1991). For most computer systems, password protection represents the first line of defense against an intruder. Typically, each user must enter a user name and password to gain access to the system. But password protection is notoriously fallible due to such reasons as users tending to select not only easy to remember passwords but also writing them down where they can be seen. For these reasons, numerous technological refinements have been created to strengthen the authenticity of passwords. Just as security administration should be easy for administrators, so too should security be easy, simple and unobtrusive for end-users. That is an end-user shouldn't be aware that any extra security safeguards are in effect. If users perceive security as requiring additional effort on their part they may look for ways to get around it.

Unauthorized intrusions into Department Of Defense (DoD) computer systems was reported by the Government Accounting Office (GAO) during its testimony on computer security before the United States Senate. This testimony reported hacker intrusions into DoD unclassified sensitive computer systems during Operation Desert Storm/Shield. Between April 1990 and May 1991, computer hackers from the Netherlands penetrated 34 DOD sites. At many of the sites the hackers had access to unclassified, sensitive information on such subjects as military personnel (personnel performance reports, travel information, and personnel reductions), logistics (descriptions of the type and quantity of equipment being moved), and weapons systems development data. Among the reasons for this possible intrusion was poor password management. (Brock, 1996)

As unauthorized access to computer systems continues to mount, the need for protection of sensitive information is greater than ever before. The threat is definitely there. (Littman, 1996)

Government agencies, small businesses and medium-size corporations are vulnerable to penetration by illegal users. DOD sensitive information, data, sources, resources, mailing lists, corporate and trade secrets, expansion plans, marketing strategies, graphs, profit and loss statements, correspondence, and employee records are there for the taking. (Alexander, 1995; Littman, 1996)

II. USER IDENTIFICATION AND USER AUTHENTICATION

Controlling access to a computer system assists a computer security manager and system administrator in monitoring authorized users, monitoring and catching unauthorized users, and monitoring the various operations of the systems. (Russell and Gangemi Sr., 1992)

The two step process in computer security terms is called the identification step and the authentication step (Russell and Gangemi Sr., 1992). To ensure that only an appropriate user has access to a computer system, a user is required to identify himself with a user name and authenticate himself with a password.

Identification is not only a way to tell who the users of the system really are but serves as a check for each subject or object access request (National Semiconductor, 1996).

Authentication, on the other hand, is the verification of a user's identity. In just about any multi-user system, users must identify themselves and have the system authenticate their identity before they can use the system because accurate identification of users is the key to individual access right. (National Semiconductor, 1996) Most operating systems and computer system administrators have learned to apply reasonable but stringent security measures to lock out illegal users before they can gain to their systems. (Gips, 1995)

The analogy of the identification and authentication in computer systems happens in our daily life. Bank employee or staff often ask for identification of their customers such as driver's license before carrying on any financial transactions at the bank. The library staff require library card identification before allowing the library patron to check out any library materials. Military installations require military identification card before allowing military member to enter the commissary or the Navy Exchange.

People have developed systems of authentication using documents, voice recognition, and other trusted means of identification but in computer systems the situation is less secure (National Semiconductor, 1996). Anyone can attempt to log into a computing system. For example, unlike a professor who may recognize a student's voice and give out grades over the telephone line, the computer cannot recognize electrical signals from one person as being any different from those of anyone else. Thus, most authentication systems must be based on some knowledge shared only by the computer system and the user.

Methods of user authentication are numerous. Here are three most commonly cited in computer security literature:

- A. The password (Something You Know)
- B. The token, key, or smart card (Something You Possess)
- C. Personal characteristics (Something You Are). (Lawson, 1994; Russell and Gangemi Sr., 1992; Pfleeger, 1989)

A. THE PASSWORD (SOMETHING YOU KNOW)

The theory is that if you know the secret password for an account, you must be the owner of that account. The problem with this theory is that the password may be a stolen password, one that was written down near a computer terminal and was read by a passerby. The password was a simple word which can be easily arrived at. (Tuomy, 1995)

B. THE TOKEN, KEY, OR SMART CARD (SOMETHING YOU POSSESS)

The theory is that if a user has the key or equivalent, he or she must be the owner of it. The problem with this theory is that users might lose the key, it might be stolen from them, or someone might borrow and duplicate it. Electronic keys, badges, and smart cards are gaining acceptance as authentication devices for access to buildings and computer rooms (McCurley, 1995).

Another example is the use of automated teller machines (ATMs) cards. The ATM card is popular and people are increasingly familiar with this type of authentication.

C. PERSONAL CHARACTERISTICS (SOMETHING YOU ARE)

These signs are easily identifiable and differ from person to person. Using mechanisms called biometric techniques, the system will compare a user's particular trait, such as a fingerprint, handprint, retina pattern, voice, signature or keystroke pattern, with the one stored for the user and determine whether he or she is who they claim to be. Although the biometric system occasionally rejects valid users and accepts invalid ones, it

is generally quite accurate. The problem with these authentication systems is that some procedures are still not widely accepted. (Deane, et al., 1995)

The above mentioned methods of authenticating identifiable data will be elaborated upon in the following chapters on biometric recognition.

III. TRADITIONAL PASSWORD METHOD

Passwords are code words chosen by computer users or generated or assigned by the computer system. Passwords are used for authentication because they are easy to use and used properly they provide reasonable assurance. Password usage is assumed to be known only to the user and the system. As mentioned earlier, in some cases a user chooses passwords, while in other cases they are assigned by the system. The length and format of the password also vary from one system to another. (Fisher, 1984)

The use of passwords is fairly straightforward. Initially a user would enter some piece of identification, such as a name or an assigned user ID; this identification can be available to the public or easy to guess, because it does not provide the real security of the system. The system then requests a password from the user. If the password matches that on file for the user, he is authorized to use the system. If the password match fails - i.e., the user may have mistyped it - the system requests the password again. (Pfleeger, 1989)

There are many excellent suggestions for choosing appropriate passwords. These suggestions will prevent unauthorized entry into the computer system even if the intruder uses the "brute force attack" technique (which is a technique that uses automation to systematically try to guess passwords). (Russell and Gangemi Sr., 1992) A good password has the following characteristics:

1. Composed of letters, digits, and other characters, so that the base alphabet for an exhaustive attack is large. A mix of uppercase and lowercase letters is highly recommended.
2. Long passwords are better than short ones. Choose long passwords so that there are many more possibilities in case of an exhaustive attack. Most systems recommend passwords that are six to eight characters long. Some systems can take longer ones.
3. Using non-existing names or words. A password should not be a common word or name, that can be found easily in a dictionary, e.g., pet names, car names, reverse words or letters.
4. Passwords should not reveal a characteristic related to the possessor, such as a spouse's name or a street address.
5. Regularly change the passwords. Passwords should be frequently changed, so that even in the event of someone guessing it, the period of vulnerability is short.
6. Written records of passwords open the possibility of being found by outsiders.
7. Absolute secrecy of user's passwords. (Gordon, 1995; Bishop and Klein, 1995; Russell et. al., 1992)

The above is a cogent reminder of the essentials of password choice. These are true and tried parameters for determining a key function in the establishing of computer security.

IV. ADVANCED PASSWORD SCHEMES

Commonly, passwords are used as the sole authentication mechanism to a computer-based information system, controlling access to an entire set of computing resources through the operating system. (Ahituv, et al., 1987) These passwords are referred to as the primary passwords. Another category of password called the secondary password usually is used to further control access to various resources within the system. These various forms of password includes the system-generated passwords (Menkus, 1988, passphrases (Porter, 1982), cognitive passwords (Haga and Zviran, 1989), and associative passwords (Smith, 1987).

A. SYSTEM GENERATED PASSWORDS

With the system generated password, a password is automatically generated by the operating system and assigned to users. A common practice in this method is that a pseudo-random number generator arbitrarily creates a string of alphanumeric characters as the password. These passwords are more difficult to guess than the traditional passwords. But the disadvantage of this technique is that the composition of random alphanumerics makes them very difficult for users to remember. (Menkus, 1988)

B. PASSPHRASES

A variation of the traditional password system is an extended password, known as a passphrase. A passphrase consists of a meaningful sequence of words, e.g. "to be or not to be". (Zviran and Haga, 1993) A passphrase is designed to form a compromise

between ease of memorability and difficulty in figuring out. The longer extended password of 30-80 characters becomes difficult to guess. Passphrases are generated by a user, allowing a meaningful sequence of words to be selected. The longer the passphrases, the more security they provide.

The passphrase is one form of authentication that is secure and simpler compared to encryption. The passphrase is just a longer version of a password. Passphrases are equivalent to passwords in their ability to authenticate (Pfleeger, 1989). Research about password length indicates that there are relatively few long passwords that people can remember easily. Examples of passphrases are a line from a song or a list of countries, such as “roses are red violets are blue.” The disadvantage of a long password is that it takes more computer memory to store. The way to get around this problem is to condense passphrases for efficient storage. (Pfleeger, 1989)

The passphrase can also be used for a variable challenge-response system. This technique has been in use by financial institutions such as banks which use this technique to authenticate customers who want to make transactions by phone. A customer who opens an account with a bank reveals certain confidential information, such as name, employer, spouse's name, birth date, perhaps mother's maiden name, and so forth. The bank hopes that this information is not common knowledge (although this is not certain in every case). When someone tries to make a telephone transaction, the bank asks the caller to quote from this source of confidential information. Questions will vary each

time a call is made so that an impersonator will not be able to know all the confidential information in advance. (Pfleeger, 1989)

C. COGNITIVE PASSWORDS

In the cognitive passwords method, the user answers a set of very unique and personal questions known only to the user. This method is based on a question-and-answer mode, where, instead of a user entering just one password, he or she is required to enter several passwords, one at a time, when prompted by the computer. When the user answers correctly to randomly chosen questions and within the security parameter established then he or she will be allowed to have access to the system. Usually the system will give a second chance after which it will reject unauthorized users. This dialogue or question and answer technique between the user and the computer system is one of the alternatives available for user authentication.

In an earlier chapter, it was postulated that a password has to be long enough to make guessing by unauthorized users difficult. Unfortunately, from the user's standpoint a long password is also difficult to remember. A cognitive password therefore can replace the traditional password system where the user has to remember one or more long passwords.

Examples of cognitive password questions are: What is the first name of your best friend in high school? Who is your favorite actor or actress? What is your favorite vegetable? If you could change occupations, which new occupation would you choose?. These questions can be fact-based or opinion-based. (Zviran and Haga, 1990)

An empirical study to test the memorability of cognitive passwords and their susceptibility to guessing by people close to the users reveals that cognitive passwords are easier to remember by users than conventional passwords and more difficult to guess by others. The study reveals that only a few of the respondents remembered their conventional passwords, whether “self-created” or “computer-generated.” Only thirty-five percent of the subjects under study recalled their “self-created” conventional password and only twenty-three percent recalled their “assigned” passwords. The favored method of recall was either from memory or from writing down passwords. Table 4.1 below cites part of the results of the study to reveal the percentage of users versus “significant-others” to correctly answer a user’s cognitive password. As mentioned earlier, this study reaffirms the conclusion that cognitive passwords are difficult to guess, even by closely related people. (Zviran and Haga, 1990)

Implementing a cognitive password technique is quite simple: simple interactive software is needed to handle initial user enrollment and subsequent cue-response exchanges for system access (Zviran and Haga, 1990). As far as time and cost are concerned, organizations which are interested in implementing this method should perform requirement , cost and benefit analyses.

**Table 4.1. Percent of Accuracy in Using Cognitive Password Technique
(User Respondent vs. Significant-Other)**

| | User Respondent | Significant Other |
|---|----------------------------|------------------------------|
| What is the name of the elementary school from which you graduated? | 94 | 27 |
| What is the name of your favorite uncle? | 89 | 41 |
| What is the name of your best friend in high school? | 91 | 43 |
| What is your mother's maiden name? | 97 | 57 |
| What was the first name of your first boyfriend/girlfriend? | 95 | 19 |
| What is the occupation of your father? | 99 | 35 |

D. ASSOCIATIVE PASSWORDS

The associated password mechanism is another password mechanism requiring a series of passwords to verify user identity. (Smith, 1987) In this mechanism, a set of cues are constructed for each user and stored in the user profile. In this alternative, the user constructs a list of cues and responses that would be unique to the individual. A simple example would be the cue word "high" which would require the response "low." An initial list of approximately twenty cues could be installed under a one-user account which would allow flexibility in changing the cues presented to the user when log-on to

the system. Depending upon the security of the system, a user would be required to give from one to several correct responses. (Zviran and Haga, 1993)

To gain access into the system with cognitive passwords, every new user is assigned a user-ID and asked to create approximately twenty word associations for his or her user profile. Then a user desiring access enters his assigned user-ID which is matched against his profile. Having passed the user-ID validity test, a user is then presented with five randomly selected cues from the set of twenty word associations in his or her profile. The cues are presented one at a time and responded by the matching word association. Upon gathering all five responses, they are compared against the stored profile database of the user. If correct, access is granted. If one or more answers do not match, a user might be given a second chance and another set of five cues is randomly selected from the database. (Zviran and Haga, 1993)

Like the cognitive password, users find memorizing associative passwords easier than the traditional passwords.

V. ADVANCED AUTHENTICATION MECHANISMS

As mentioned in the previous chapters, a user authentication process can be based on three different methods: things the user knows such as passwords, things the user personally possesses such as tokens, and things the user is such as finger or handprints. (Russell and Gangemi Sr., 1992) This chapter will discuss the last two methods of the authentication process.

A. TOKEN

A token or smart card is “something the user possesses”, an object that users carry to authenticate their identities. In ancient times it was a common practice to carry the king’s ring to prove that a messenger was speaking on behalf of the king (Russell and Gangemi Sr., 1992). The use of a token is similar to an ID card as a means of authentication. We carry them to conduct our daily business, i.e., an ATM card (electronics means) to have access to our accounts at the banks, or a military ID card (manual means) to have access to military privileges etc.

A token usually requires a two-step authentication. In a typical application, access to a PC is as follows: 1) the user inserts an electronic key-shaped token for log-on and authentication; 2) once the system recognizes the token, it prompts the user to type their user ID and password. When the user passes all the authentication steps then he or she will be allowed to enter the system. If not, he or she may be given a few more chances.

When multiple failures occur, then the user will be locked out of the system and an alarm may be sounded. (McCurley, 1995)

In order to be effective, a token should be unique. In practice, ID cards can be forged but are still used for authentication.

The “magnetic stripe credit card” is another form of token for network communication. These cards are the size of regular credit cards with certain information recorded in magnetic form on the back. The magnetic stripe is read by a sensing machine. This is similar to the ATM card mentioned earlier. For example, an ATM machine permits a customer to perform certain banking transactions at any time, day or night. Since the possibility of loss or theft exists, these cards have to be in combination with an identifying word or number in order to use the card. (McCurley, 1995)

B. SMART CARD

A more advanced form of token card is the smart card or chip card - which is similar to a token card except it has a microprocessor embedded. Not only can the smart card retain information to identify the possessor, it can also hold information such as a bank or credit balance. Such a card is not merely a passive container of data. A smart card can actually perform computation, such as computing the response function of a challenge-response system, or performing link level encryption. An example of how this card is used is cited as follows:

Smith walks up to a terminal to initiate a log-on to a computing network. Smith enters his name on the terminal and receives the prompt for a password. Smith puts the

smart card in a slot and types his password. Instead of the password being transmitted in the clear, the password is encrypted by the smart card. The remainder of the transaction is decrypted at the receiving end. In this way, Smith can transact his business in the complete security of a computer network from any place in the world. (Pfleeger, 1989)

Several vendors offer smart card systems. The SecurID token from Security Dynamics is an example of access control security token which is used to positively identify users of computer systems and networks. Used in conjunction with Security Dynamics' hardware or software access control module (ACM), the SecurID token automatically generates a unique, unpredictable access code every 60 seconds. To properly identify and authenticate an authorized user, two factors are necessary. The first is something secret the user knows: a memorized Personal Identification Number (PIN). The second factor is something unique the user possesses: the SecurID token. The changing access code displayed on the SecurID token guarantees the user must have the token in his or her possession at the time it is used. (Security Dynamics, 1996)

C. CHALLENGE-RESPONSE SYSTEMS

There are two kinds of challenge response systems appearing in the market. The first type operates digitally; it functions much the same as a smart card, using a device like a pocket calculator. The user keys in the challenge, the device computes the response, the user reads the response in a display and enters it into the computer keyboard.

The second available challenge-response system uses a hand-held reader. The host computer generates a random pattern of dots that it displays on the user's screen. The user holds the device up to the screen, and the device senses the dot pattern and converts it to a number. The device then computes a numeric response for the challenge patterns. From a display screen in the device, the user reads the response and keys it into the keyboard. (Pfleeger, 1989)

D. BIOMETRIC TECHNOLOGY

Another kind of authentication technique is known as the biometric technique. Webster's dictionary (1978) defined biometrics as "that branch of biology which deals with its data statistically and by quantitative analysis".

Biometric authentication technology in computer security systems is the automatic authentication of an individual on the basis of a unique and measurable physical characteristic, such as a fingerprint (Kim, 1995). In biometric systems, a particular physical or behavioral characteristic is measured and later is compared to a library of characteristics belonging to many people. Biometrics is considered a newcomer by most in the access control industry, but the technology has been around for many years (Wilson, 1992). There are two types of biometric methods (Deane et al., 1995). The first type is based on physiological characteristics such as fingerprints, hand geometry, and retina patterns. The second type is the behavioral biometric method which is based on some aspect of behavior such as signature, voice, keystroke, and pointing patterns. A simple hand geometry measure to identify a person by finger length was developed in the

late 1960s and is called the Indentimat. This is the granddaddy of all biometrics. The other biometric technologies, fingerprint, voice recognition, retinal scan, keystroke dynamics and signature verification, were developed during the 1970s and 1980s. (Wilson, 1992). The different kinds of biometric methods will be briefly explained in the following paragraphs.

1. Face

One biometric method is the use of facial characteristics for identification. To cite one example, in the law enforcement business, this technology is used to recognize bank robbers, drug dealers, and terrorists in a crowd (Kim, 1995). For physical security officers, this method adds to the efficiency of their existing closed-circuit television systems. For computer security personnel, this technology could be incorporated by adding a small video camera into PCs that would monitor that the users sitting at the machine were authorized users.

The problems with this method is the inherent variances of facial features or expressions due to lighting conditions, camera angle, or changes of hair style. This will create substantial deviations with the stored "facial print" or template in the computer systems and can create errors. To remedy these problems, advance technologies have been introduced which include the use of neural network patterns exposed to infrared scans of hot spots to detect the most constant features on the face. (Kim, 1995)

2. Fingerprints

The other form of biometrics is the fingerprint-based personal identification system used to control access or verify an individual's identity. Historically, fingerprint identification has been used as a primary law enforcement tool, particularly in criminal justice organizations (Ellis, 1994). This technology is also very useful for such purposes as welfare identification, child-care screening, licensing, refugee identification, immigration, prison inmate control, gaining employee background checks, and high-security organizations such as defense plants, the military, and increasingly in banks. (Wilson, 1992; Russell and Gangemi Sr., 1992)

Every human being has unique set of fingerprints. Fingerprint verification systems examines the unique characteristics of your fingerprints and uses the information to determine whether you should be allowed access. The use of fingerprints to identify people dates from the late nineteenth century. In the past, manual methods were used to classify and cross-check fingerprints according to certain patterns of ridges and whorls - in particular, detailed features of the print called minutiae. A fingerprint may have up to 150 of these minutiae. In the late 1960s, the FBI automated its system for cross-checking fingerprints, and all fingerprint checking was converted to automated systems by 1983. (Russell and Gangemi Sr., 1992)

The application of this system usually starts with placing one finger on a glass plate. Then the optical scanner, image processing software and sophisticated algorithms

electronically read, analyze and compare a user's "live" fingerprint with a previously stored mathematical characterization or template of that fingerprint.

The fingerprint system digitizes the ridges and other characteristics of the fingerprint and compares these characteristics against the fingerprint templates stored in the system (or, in more primitive systems, against a print on a card that you carry). The system allows access only if your fingerprint sufficiently matches the template.

The more modern fingerprint verification systems also perform a three-dimensional analysis of the fingerprint including infrared mechanisms for ensuring that a pulse is present. This means that an intruder can't gain entry by presenting a mold of an authorized user's finger or, worse still, an authorized finger that's no longer attached to its owner. (Russell and Gangemi Sr., 1992)

Fingerprints have several advantages and disadvantages. The characteristics and stability of fingerprints are widely accepted, and they are unique in every human being. On the other hand, the process is slower than certain other types of biometric measurements. In addition, their ability to work properly depends on the condition of the fingers being presented. Burns or other physical problems can affect the system's ability to match fingerprints, as can any substance such as the presence on the fingers of such materials as dust, perspiration, grease or glue. (Russell and Gangemi Sr., 1992)

TouchSafe II is a fingerprint verification device from Identix Inc., Sunnyvale, CA. This device can be installed on a personal computer and is applicable for computer database and network systems. This fingerprint identity verification terminal is designed

for access control applications, preventing unauthorized personnel from accessing protected data, services or funds. (Indentix Incorporated, 1996)

3. Hand

Everybody has unique handprints. Handprint or hand geometry verification systems examine the unique measurements of your hand and use that information to determine whether you should be allowed access.

As mentioned earlier, the first version of hand geometry measured the finger length to identify a person. To get this measurement, the hand was placed on a flat platen and a 1,000 watt overhead lamp projected the shadows of the fingers through slots in the platen. Photoelectric cells scanned along the fingers to determine the position of the tips and webs, and thus the finger length. This device worked well but was too large, expensive and only average in performance. The production of this old version ceased in 1987. (Wilson, 1992)

Today, the total hand shape is identified rather than just the finger lengths. This technology was initiated by a study conducted by the Air Force in the early 1980's. Since then, the three-dimensional method of hand geometry has been available. A digital camera is used to capture a TV-like image of the hand both a top view, which gives length and width information, and a side view, which gives a thickness profile. To avoid variations of hand positions finger pins are used to properly position the hand on the platen. The image captured by the camera is converted into a digital electronic video signal that is transferred to the microprocessor memory. This data is represented in

memory in much the same way as a picture is printed in a newspaper, as a series of black and white dots. Each bit memorized is represented by one dot, or pixel. Approximately 32,000 pixels of information are analyzed to extract the identifying features of the hand. This will represent a template for each computer user. In verifying the identity of a user, the live hand picture is computed in the stored template. A small difference between the current hand reading and the template indicates a good match. Large differences are rejected by the electronic system. (Wilson, 1992)

Applications of this technology have expanded from the Department of Defense (DoD) to major universities, international airports, drug enforcement facilities, student dormitories, stock rooms, banks, insurance and financial institutions, manufacturing facilities, and hospitals. (Wilson, 1992)

One example of hand identity verifiers from the commercial market for physical access control is the ID3D HandKey from Recognition Systems, Inc. which can add "Who You Are" to the existing ID and security systems. This device can operate as a complete "stand alone" access control station. It can be used in a network setup or be integrated into third party access control systems, e.g. optional card reader. Enrollment is fast and with minimum data storage (small nine byte template). (Recognition Systems, Inc., 1996)

4. Eye

One kind of eye identification is retinal recognition technology. The proponents of this technology believe that the eye vascular pattern develops during embryonic

growth, stabilizes prior to birth and remains stable throughout life. One example in this category is the EyeDentification System 2001 from EyeDentify, Inc. As explained in their technical paper, the 2001 retinal recognition technology uses the natural reflective and absorption properties of the eye's retina. When an individual looks at the illuminated Green Dot Alignment target, an eye template is acquired from the light naturally reflected and absorbed by the retina. The retinal field has 192 data points identified that are used as the basis for creating a 96 byte digital template which is called an "eye signature." When a good template is acquired, it is then stored for future recognition or verification and is compared to other stored eye templates preventing duplication of data base files. (EyeDentify, Inc., 1996) The system will allow access only if your retina pattern sufficiently matches that of the one stored for you in the system.

Newer developments include the measurements of iris and pupil. Hand-held devices are being developed for workstation access.

This technology has been applied to many different fields such as access control, information security, research organization, government, banks, restaurants, etc.

The second kind of eye identification is the iris recognition technology. This technology is based on the patterns found in the iris of the human eye. The iris is the colored ring that surrounds the central black pupil, and the retina is the sensory membrane lining the eye. The difference in technology requires that retinal scanning use laser or infra-red beams and iris scanning use the camera lens to capture the iris prints.

Applications include:

- entry and access control
- computer and network security
- information access control
- financial transactions
- day-care center access control
- hospitals (IrisScan, 1996)

One example of commercial devices for iris scan technology is System 2000EAC from IriScan. To be identified, the subject simply looks toward the system's video lens from a reasonable distance. The system uses a standard video camera taking 30 frames per second with illumination provided by a 20-watt quartz-halogen bulb with a magenta filter at seven watts power. To acquire the iris image, the system software determines the inner and outer boundaries of the iris, and then identifies and encodes each feature of the iris as a multi-scale sequence coefficients, producing a 256-byte code. This code is stored in memory as the subject's template for comparing future recognition. For later identification, the user need only present his or her eye to the camera. (IriScan, 1996)

5. Voice

Characteristics of vocal and acoustic patterns are unique for each human being. Voice verification systems examine the unique characteristics of the human voice. Some systems also examine phonetic and linguistic patterns and use that information to determine whether one should be allowed access.

This speaker identification system requires the users to speak a particular phrase. The system converts the acoustic strength of a speaker's voice into component

frequencies and analyzes how they are distributed. The system compares the live voice to a stored voiceprint. This voiceprint is a “voice signature” constructed by sampling, digitizing, and storing several repetitions of a particular phrase. The speaker’s identity is verified by comparing stored voice prints of known origin against new samples of speech from the person claiming the identity. If the characteristics of the new samples match those of the stored prints within acceptable limits, the speaker’s claimed identity is accepted. Otherwise, it is rejected. (Russell and Gangemi Sr., 1991)

This technology is currently used for personal identification in banks, credit agencies, service companies, governmental services, telephone fraud prevention, etc.

One example of the devices available commercially is the Veritel Voice Verification system by Veritel corporation. The device is a Veritel board which is a half length, standard card that fits into any PC, plus the software to install it. Once the system is installed, the system administrator can begin the process of recording and verifying voiceprints for registered users. The system can act as the head-end for a wide variety of potential applications. Technical implementation of this method is as follows: the speaker is first enrolled in the system by capturing specific samples of speech and converting the audio to digital PCM (Pulse Code Modulation) using standard commercially available voice processing products. The PCM samples are saved on disk. When an access is attempted, the speaker is prompted to repeat the original phrase of speech and the audio sample is again converted to digital PCM. The two PCM samples are compared using a firmware algorithm that runs on the Veritel Voice Verifier Board.

The algorithm performs a series of transformations and comparisons such as: convert PCM to LPC, convert LPC to Cepstrum Coefficients, and time aligns the two Cepstrum representations using a Dynamic Time Warping function. It then compares the aligned patterns using a Distance Measure. If the Distance Measure between the two audio patterns is less than a selected threshold, access is granted. Otherwise, it is denied. (Veritel Corporation, 1996)

6. Signature

The use of the signature in our daily life is widely practiced and accepted. It is the norm of doing business. We put our signatures on checks issued to make payments, sign contracts and agreements. In biometric technology, there are two different methods of signature authentication. (Kim, 1995) One method is to compare the signature already written with the associated template. The weakness in this method is that the technology cannot detect a copied signature. The second method is to analyze signature dynamics. This signature verification examines the way a signature is written rather than what it looks like after being written. The focus in this second method is to look at the dynamic process of writing one's signature. It is the writing rhythm, contacts on the surface, total time, turning points, loops, slopes, velocity and acceleration and converting a signature into a set of electrical signals that stores the dynamics of the signing process mentioned above. The devices used in signature dynamics technology are wired pens and sensitive tablets. (Kim, 1995) The key in the recognition of a signature is to distinguish between the habitual parts from those that vary with almost every signing since everybody has a

unique signature and signature-writing pattern. Signature verification systems examine this unique characteristics of one signature, and the way in which one writes his or her signature. The system compares the signature to a signature template stored for users to determine whether one should be allowed access.

One commercial device from Cadix International Inc. is the ID-007 which placed no limitation on the styles or types of signatures. Any combination of languages, fonts, and handwriting systems is acceptable to the ID-007. This device will encrypt signatures to ensure that the individual's signature cannot be reproduced. Also to increase security, PIN numbers can be issued to users when making their signatures. ID-007 will compare the user's signature with signatures in the database as to shape and pen movement to determine whether the real person has signed the signature. This step is called "pattern matching." Users' signatures will change from time to time because of physical changes or the passage of time. ID-007 learns the slightly changed signature once ID-007 has recognized that it is the authorized user. One signature takes about 1.5 K bytes. For instance, 40M bytes hard disk on a personal computer can keep more than 20,000 signatures. Data size is independent of signature size, shape, or writing time. Several sampling are required to make the signature registration. Verification time is about 1 second. (Cadix Research & Development, 1996)

7. Typing Rhythms

Everybody has a unique pattern or rhythm of typing. Keystroke verification systems examine the unique characteristics of users keystrokes (users electronic signature) and use that information to determine whether you should be allowed access.

This technology is very similar to signature verification discussed earlier. Templates are being created and analyzed based on information such as the users' time that elapses between keystrokes, forming unique timing patterns. Users are required to generate a keyboard reference profile or template which will be used at a later date for verification and compare to the test profile. If large differences occur between these two profiles then the user involved is prevented from access. The goal is to determine whether you are, in fact, the person working at your workstation and under your account, or whether an intruder has gained access. This surveillance of work habits has raised right of privacy issues.

8. Summary

Biometrics technology can enhance and complement any organization's existing security system to provide a higher level of confidence by using physical characteristics that are unforgeable.

This technology offers solutions for user identification or authentication. Examples of such concerns are welfare recipients who sign up for benefits under six identities, a child is released to a stranger from a day care center, a hacker accesses sensitive databases or a counterfeiter makes copies of bank cards. Biometrics has become

the most foolproof method of automated personal identification in today's highly computer dependent world and continues to be in great demand. (Kim, 1995)

However, computer security managers should be aware that along with the strength of biometrics technology, proper assessments and applications are needed and should be the initial step prior to implementation.

Implications of the use of biometrics technology can include: user acceptance, performance, cost, speed, security loopholes, danger of misuse, legal aspects. (Kim, 1995).

To be broadly acceptable, biometric techniques must be legally safe to use, have regard for the user's privacy, and avoid those that are socially unacceptable. (Kim's, 1995) For example a fingerprinting scanner is associated with criminal overtones, while hand recognition is more associated with handshaking. Dynamic signature recognition is acceptable due to the already wide use of signatures as personal identification. When literacy rates are low, other methods such as voice, face or hand recognition may be more appropriate.

In terms of performance biometric applications are prone to two types of errors: rejection of an authorized user, or the incorrect acceptance of an unauthorized user. To produce optimum performance, adjustments of threshold settings for acceptance and rejection are necessary.

As in any investment, cost is one area to be considered. Does the benefit outweigh the cost? This question should consider operating costs, such as maintenance and training.

Verification time is another factor to be taken into account. Biometric verifications which involve several seconds are considered slow when compared to other methods such as password and ID verification.

Security loopholes are still the major concerns, especially during remote log-ons, where information is sent to the host computer for comparison with the stored template. Kim believes there are at least two potential weaknesses in this case. One is related to the database with the templates and the other to the transmission of the biometric reading. If stolen, the identity of authorized users cannot be changed as the password method could.

There is no questions that biometrics technology has been very popular around the world, for both the government and private sectors. This too has raised concerns over the legality of sharing private information from government or industry with third parties. It is important that individuals have ownership rights to their personal data. Hence they should be informed about data collection and have the right to decline the use of data by third parties. (Tuerkheimer, 1993) International conventions state that data should not be used for purposes other than the original purpose of collection, except with the authority of law or the consent of the individual (Clark, 1988).

In terms of cost, effectiveness, and human acceptance, the following table is presented as a guideline. (Rowe, 1996)

**Table 5.1. Comparison of Various Verification Methods
(Ratings on scale of 1 to 10: 10 is best)**

| Method | Cost | Effectiveness | Human Acceptance |
|---------------------|-------------|----------------------|-------------------------|
| Password | 1 | 2 | 8 |
| Smart card | 3 | 4 | 7 |
| Fingerprint | 7 | 8 | 6 |
| Handprint | 7 | 7 | 5 |
| Retinal scan | 8 | 10 | 4 |
| Iris scan | 8 | 9 | 6 |
| Face | 9 | 5 | 8 |
| Body form | 5 | 3 | 7 |
| Signature (written) | 8 | 2 | 9 |
| Signature (dynamic) | 8 | 8 | 7 |
| Keystrokes | 3 | 5 | 9 |
| Voice | 9 | 5 | 8 |

Like other matters in life, controversial results of research work exists in any field. One study intending to reveal the perceived acceptability of biometric security systems by a sample of banking and university staff was conducted by Deane et. al. (1995) The results from 76 respondents indicated that all biometric systems were perceived as less acceptable than the traditional password approach. Contrary to expectation, it was found that behaviorally based biometric systems were perceived as less acceptable than physiologically based systems. There is a positive relationship between acceptability and sensitivity of information. Conversely, the password method has negative relationship between the acceptability and sensitivity.

In closing this biometric discussion, success of implementation will still rely on proper assessment, planning, and training awareness programs.

VI. ORANGE BOOK EVALUATION (DoD 5200.28-STD)

The Orange Book Operating System Security Standard was published by the U.S. Department of Defense in 1985 (Melford, 1995). It came about as a consequence of increasing security consciousness on the part of the government and industry and the growing need for standards for the purchase and use of computers by the federal government. The need to quantify security or to measure trust was the primary motive behind development of this guidebook. It is useful for commercial vendors who develop secure systems to fulfill requirements stipulated by the government requisition office which has tied computer equipment purchases to Orange Book certification.

The objectives of Orange book are:

1. For measurement.
2. For guidance.
3. For acquisition. (Russell and Gangemi Sr. 1992)

Measurement: to provide users with a measurement with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information. For example, a user can rely on a B2 system to be "more secure" than a C2 system.

Guidance: to provide guidance to manufacturers as to what to build into their commercial products to satisfy trust requirements for sensitive applications.

Acquisition: to provide a basis for specifying security requirements in acquisition specifications. Rather than specifying a hodgepodge of security requirements, and having

vendors respond in piecemeal fashion, the Orange Book provides a clear way of specifying a coordinated set of security functions. A customer can be confident that the system he or she acquires has already been checked out for the needed degree of security. (Russell and Gangemi, Sr., 1992)

As the Orange Book puts it, the criteria “constitute a uniform set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into the various systems.”

The Orange book defines four broad hierarchical divisions of security protection.

In increasing order of trust, they are:

- D. Minimal security
- C. Discretionary protection
- B. Mandatory protection
- A. Verified protection

Each of these hierarchy levels define a set of evaluation criteria to ensure that an operating system completely carries out the controls (see Table 6.1).

Each class is defined by a specific set of criteria that a system must meet to be awarded a rating in that class. The criteria fall into four general categories: security policy, accountability, assurance, and documentation. (Rowe, 1996)

Table 6.1. The Orange Book Trusted-System Classes

| <i>Feature</i> | <i>C1</i> | <i>C2</i> | <i>B1</i> | <i>B2</i> | <i>B3</i> | <i>A1</i> |
|---------------------------------------|-----------|-----------|-----------|-----------|-----------|-----------|
| discretionary access control | X | X | S | S | X | S |
| object reuse | - | X | S | S | S | S |
| labels | - | - | X | X | S | S |
| label integrity | - | - | X | S | S | S |
| exporting information | - | - | X | S | S | S |
| labeling of output | - | - | X | S | S | S |
| mandatory access controls | - | - | X | X | S | S |
| subject sensitivity labels | - | - | - | X | S | S |
| device labels | - | - | - | X | S | S |
| identification and authentication | X | X | X | S | S | S |
| audit | - | X | X | X | X | S |
| trusted path | - | - | - | X | X | S |
| system architecture | X | X | X | X | X | S |
| system integrity | X | S | S | S | S | S |
| security testing | X | X | X | X | X | X |
| design specification and verification | - | - | X | X | X | X |
| covert channel analysis | - | - | - | X | X | X |
| trusted facility management | - | - | - | X | X | S |
| configuration management | - | - | - | X | S | X |
| trusted recovery | - | - | - | - | X | S |
| trusted distribution | - | - | - | - | - | X |
| user's guide to security | X | S | S | S | S | S |
| facility security manual | X | X | X | X | X | S |
| test documentation | X | S | S | X | S | X |
| design documentation | X | S | X | X | X | X |

(x = requirements for this class; s = same requirements as to left)

Each division consists of one or more numbered classes, with higher numbers indicating a greater degree of security. For example, division C contains two distinct classes (C2 offers more security than C1). The C2 level is today's de facto commercial IS security standard. It adds auditing facilities to the basic C1 requirements of a system security architecture, user authentication, and security documentation. Division B

contains three classes (B3 offers more security than B2, which offers more security than B1). B-level requirements add advanced privacy protection facilities; division A currently contains only one class. A1 levels reflect the government's most sensitive national security needs. Requirements include copious vendor documentation and costly and extensive testing beyond B3 demands by the National Computer Security Center.

Ongoing debates about the Orange Book are many and this guide will undergo revision in the future with the changing of technologies. But now it is still the standard for secure systems. Some of the debates have evolved in the following areas:

1. The model works only for government classified environment and is not appropriate for the protection of commercial data where data integrity is the chief concern.
2. It focuses on only one aspect of security, namely secrecy, while paying little attention to the principles of accuracy, availability and authenticity.
3. It emphasizes protection from unauthorized access from outside, while most security attacks actually involve insiders.
4. The guidelines do not address networking issues. (Another book called the Red book addresses this issue)
5. It contains only a small number of security ratings. (Russell and Gangemi, Sr., 1991)

Vendors can submit their operating system for free compliance testing for A and B level security to the NCSC. The center has discontinued evaluating C-level operating systems due to budgetary constraints. A few vendors choose to submit their commercial offerings because of the time involved- a new version is usually out before the evaluation is complete. Instead, most vendors design their operating systems "to meet" Orange Book requirements. (Melford, 1995)

VII. CONCLUSION

The future of access control techniques is now one of positive progress and development for the computer security industry. These advanced authentication mechanisms have become popular and widely used due to their high degree of accuracy and security.

As postulated in this survey, the traditional password is still the common means of authentication for the user. This paper concludes that passwords can be a strong component and basis of user authentication but that other advanced authentication mechanisms can be even more efficient and sophisticated such as tokens, smart cards, challenge response systems, and biometrics recognition techniques.

For the future, it appears that biometrics will become more popular as technology makes the cost of implementing these sophisticated verification methods more affordable.

APPENDIX A. PRODUCT LIST

- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, fingerprint identification
Product Name: TouchLan II
Product Features: Access control for network from a host computer
Supplier Name: Identix Incorporated
- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, fingerprint identification
Product Name: TouchSafe II
Product Features: Fingerprint identity verification for stand-alone or network configurations.
Supplier Name: Identix Incorporated
- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, hand geometry identification
Product Name: ID3D HandKey
Product Features: Add "Who You Are" to your ID and security systems.
Supplier Name: Recognition Systems, Inc.
- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, iris identification
Product Name: IriScan's System 2000EAC
Product Features: Biometric identification technology for entry and access control, computer and network security.
Supplier Name: IriScan
- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, retinal recognition
Product Name: System 2001 Retinal Recognition
Product Features: Applicable for access control and information security.
Supplier Name: EyeDentify inc.
- Authentication Method(s):** Biometrics
Device(s): Access-control hardware, signature identification
Product Name: ID-007
Product Features: Signature verification to identify a person.
Supplier Name: Cadix International, Inc.

Authentication Method(s): Biometrics
Device(s): Access-control hardware, voice/signature verification
Product Name: Veritel Voice Verification System
Product Features: Biometrics based access security method in which a speaker's identity is verified by comparing stored voice prints of known origin against new samples of speech from the person claiming the identity.
Supplier Name: Veritel Corporation

Authentication Method(s): Challenge-response
Device(s): Access-control hardware
Product Name: AccessKey II
Product Features: Challenge/response methodology for two-factor authorization security.
Supplier Name: Vasco Data Security Inc.

Authentication Method(s): Challenge-response
Device(s): Access-control hardware
Product Name: Multi-Platform Access Control System
Product Features: Offers both single-line (SLC) and multi-line (MLC) solutions for maximizing computer and network access control systems.
Supplier Name: CRYPTOCard, Inc.

Authentication Method(s): Challenge-response
Device(s): Access-control software
Product Name: Stoplight
Product Features: Security for PCs and LANs.
Supplier Name: Safetynet, Inc.

Authentication Method(s): Challenge-response, password
Device(s): Access-control software (token)
Product Name: LOCKout
Product Features: Solves organization's remote access security problems. Password protection is replaced with a unique, one-time challenge response technique using the LOCKout Data Encryption Standard (DES) solution. LOCKout Fortezza is a key component of the National Security Agency's MOSAIC program for secure Department of Defense messaging. It meets the needs of civilian and military government agencies who require the protection of sensitive but unclassified information.
Supplier Name: Secure Computing Corporation

Authentication Method(s): Password
Device(s): Access-control hardware
Product Name: DK1125
Product Features: Installed at the remote site between the user's PC and the modem for dial in remote user authentication to Security Systems.
Supplier Name: Optimum Electronics, Inc.

Authentication Method(s): Password
Device(s): Access-control hardware
Product Name: IDG-9102 Intelligent Data Guard
Product Features: Limiting access to dialup ports. Provides security for dialup modems in computer rooms, office environments, and telephone equipment rooms. The modem cannot be detected by hackers as carrier is not placed on the line nor is there any screen dialogue until the correct password has been received. The Intelligent Data Guard (IDG) will become the first line of defense because any unauthorized caller will never obtain carrier.
Supplier Name: Intelligent Supervisory Systems

Authentication Method(s): Password
Device(s): Access-control hardware
Product Name: SafeWord Token
Product Features: Password generators.
Supplier Name: Enigma Logic

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Access Manager
Product Features: Provides single sign-on user authentication and access control.
Supplier Name: Enterprise Systems ICL Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: ACSplus
Product Features: Stops unauthorized access to workstations.
Supplier Name: SecureNet Technologies Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: cypherPAD
Product Features: Drive locking, computer privacy system for Macintoshes.
Supplier Name: UsrEZ Software Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: D-View
Product Features: Provides password protection and Simple Network Management Protocol (SNMP) community name to prevent unauthorized access or manipulation of the devices on the network.
Supplier Name: D-Link

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Defender Security Server
Product Features: Runs on government-certified secure operating system.
Supplier Name: Digital Pathways, Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: E-NSI
Product Features: Operates in the MVS environment with all major security systems to permit seamless password authentication with multiple IBM AIX and AT&T UNIX systems. Interfaces with the AIX 3270 Host Connection Program, or TELNET and tn3270 on the server system to provide end-user authentication on the MVS host.
Supplier Name: Eberhard Klemens Company

Authentication Method(s): Password
Device(s): Access-control software
Product Name: EasySafe
Product Features: Security and encryption product designed specifically for notebook use.
Supplier Name: EliaShim-Safe Software

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Empower
Product Features: Security software for Macintosh, Power Macintosh, PowerBook, or Proforma computers.
Supplier Name: Magna

Authentication Method(s): Password
Device(s): Access-control software
Product Name: ETF/T
Product Features: For CA-Top Secret, allows controlled usage of special privileges during an emergency situation.
Supplier Name: Eberhard Klemens Company

Authentication Method(s): Password
Device(s): Access-control software
Product Name: FileGuard
Product Features: Access control security management for Macintosh systems.
Supplier Name: ASD Software, Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Guardian
Product Features: Access security for UNIX. Requires users to change passwords on a regular basis, generate easily remembered passwords.
Supplier Name: Datalynx

Authentication Method(s): Password
Device(s): Access-control software
Product Name: MasterSafe
Product Features: Access control and management system designed to protect DOS/Windows workstation from unauthorized access to programs or data in a stand-alone, networked, or client/server environment. C2 compliant.
Supplier Name: EliaShim-Safe Software

Authentication Method(s): Password
Device(s): Access-control software
Product Name: METZ Lock
Product Features: Protects against unwanted input from both keyboard and mouse.
Supplier Name: METZ Software

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Password Coach
Product Features: Provides consistent enforcement of policies which require users to create difficult-to-guess, yet easy-to-remember passwords.
Supplier Name: Baseline Software

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Password Genie
Product Features: Automatically generates passwords which have been screened with weak or easily-guessed password tests.
Supplier Name: Baseline Software

Authentication Method(s): Password
Device(s): Access-control software
Product Name: SafeWord Software
Product Features: Provides enhanced network authentication and ease of access to local and wide area networks via Dynamic Passwords that change with every log-on.
Supplier Name: Enigma Logic

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Security Administration Manager
Product Features: To help system administrator in keeping information security under control. Internal SAM security mechanisms guarantee consistent and controlled security definitions for all integrated target systems at all times.
Supplier Name: Schumann Security Software Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: SQL SECURE/Client Server Database Security
Product Features: For security and database administrator to manage all aspects of client/server database user authentication and security auditing.
Supplier Name: BrainTree Technology, Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Trusted Access
Product Features: Password management for automatic policy enforcement.
Supplier Name: Lassen Software, Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: ultraCOMMAND
Product Features: Network management and security administration system for the Macintosh.
Supplier Name: UstrEZ Software Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: ultraSHIELD
Product Features: Password managed computer access control for Macintosh.
Supplier Name: UstrEZ Software Inc.

Authentication Method(s): Password
Device(s): Access-control software
Product Name: Workstation Manager Plus
Product Features: A comprehensive workstation control and security product. Available for stand alone workstations and for Novell NetWare.
Supplier Name: PC Guardian

Authentication Method(s): Password, callback
Device(s): Access-control hardware
Product Name: Modem Security Enforcer
Product Features: Security for dial-up modems on in-house computer systems, LAN and WAN network nodes, PBX maintenance posts, station message detail recording devices.
Supplier Name: IC Engineering, Inc.

Authentication Method(s): Password, caller ID
Device(s): Access-control hardware
Product Name: IDG-9100 Intelligent Data Guard
Product Features: Uses Caller ID to deny access to unauthorized callers by preventing the ring signal from reaching the modem unless the telephone number of the calling party matches one of the numbers in the user-programmable directory.
Supplier Name: Intelligent Supervisory Systems

Authentication Method(s): Password, certificate-based
Device(s): Access-control software
Product Name: Secure Access System
Product Features: For remote users and tools for network administrators. Security features include: access control, authentication, integrity and privacy. Uses digital certificate authentication and access.
Supplier Name: Cylink

Authentication Method(s): Password, Challenge-response
Device(s): Access-control hardware
Product Name: Defender Series
Product Features: Controls user access by time-of-day or length of session.
Supplier Name: Digital Pathways, Inc.

Authentication Method(s): Password, Challenge-response
Device(s): Access-control hardware (token)
Product Name: RB-1 token
Product Features: Access control security, interoperable (Mainframe, midrange, LAN, PCs).
Supplier Name: CRYPTOCard, Inc.

Authentication Method(s): Password, Challenge-response
Device(s): Access-control hardware/smart disk
Product Name: SB-1
Product Features: Provides access control for IBM compatible PCs, protection of hard disk data, remote multi-platform hosts.
Supplier Name: CRYPTOCard, Inc.

Authentication Method(s): Password, Challenge-response
Device(s): Access-control software
Product Name: Software Secure Net Keys
Product Features: User authentication tools, employ Data Encryption Standard (DES) algorithm to generate unique, one time passwords.
Supplier Name: Digital Pathways, Inc.

Authentication Method(s): Password, dial back
Device(s): Access-control software
Product Name: CoSecure
Product Features: Modem security software with dial-back capability.
Supplier Name: CoSystems

Authentication Method(s): Password, encryption
Device(s): Access-control hardware
Product Name: PathKey Domain Series
Product Features: Delivers automatic and transparent remote access security services to larger, dynamically growing user environments.
Supplier Name: Paralon

Authentication Method(s): Password, encryption
Device(s): Access-control hardware
Product Name: PathKey Series
Product Features: Offers authentication and data encryption capabilities for small-to-medium sized workgroups (under 500 nodes), and operates in peer-to-peer or Client/Server configurations.
Supplier Name: Paralon

Authentication Method(s): Password, encryption
Device(s): Access-control software
Product Name: BoKs Access Control System
Product Features: Security for a Local Area Network or an Enterprise.
Supplier Name: Securix

Authentication Method(s): Password, encryption
Device(s): Access-control software
Product Name: LJK/Login
Product Features: Single authentication action will validate end-users for exchanging data with all the servers for which they are authorized access. Servers rely on public key signatures for proof of user identity.
Supplier Name: LJK Software

Authentication Method(s): Password, encryption
Device(s): Access-control software
Product Name: ProGuard
Product Features: For single PC protection and environments where multiple users share computers.
Supplier Name: Vasco Data Security Inc.

Authentication Method(s): Password, encryption
Device(s): Access-control software
Product Name: ultraSECURE
Product Features: Access management security software for Macintosh. Password controlled computer access control. Specialized versions available to authorized entities of the U.S. Government. Compliant Class C2, Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD).
Supplier Name: UsrEZ Software Inc.

Authentication Method(s): Password, ID
Device(s): Access-control software
Product Name: OmniGuard/Enterprise Access Control (EAC)
Product Features: Supplements existing security and access controls in UNIX clients, and provides complete security protection for PC and PC/LAN environments.
Supplier Name: Axent Technologies, Inc.

Authentication Method(s): Password, ID
Device(s): Access-control software
Product Name: OmniGuard/Enterprise SignOn (ESO)
Product Features: Network-wide user administration, identification, and authentication tool. Enables users to log on to the network and automatically gain secure access to heterogeneous platforms without multiple log-ins.
Supplier Name: Axent Technologies, Inc.

Authentication Method(s): Password, token
Device(s): Access-control software
Product Name: CA-TOP SECRET/PC
Product Features: Secures personal computers that are network-connected to a central IBM MVS mainframe. Also available CA-TOP SECRET for the VM environment.
Supplier Name: Computer Associates International

Authentication Method(s): Password, trusted systems technologies
Device(s): Access-control software
Product Name: The Argus B1/CMW, C2/TMW
Product Features: Advanced trusted UNIX operating system technology that provides Multilevel Security (MLS) for PCs, workstations, and servers.
Supplier Name: Argus Systems Group, Inc.

Authentication Method(s): Password, trusted systems technologies
Device(s): Access-control software
Product Name: DECAF (Version 1.1, for Solaris 2.x)
Product Features: Quarantine sensitive, personal, mission critical resources of all kinds. User installable, generic system security utility for creating secure execution environments for Java applets, and other network-borne applications or agents.
Supplier Name: Argus Systems Group, Inc.

Authentication Method(s): Password, two-levels
Device(s): Access-control software
Product Name: DiskGuard
Product Features: Security (hard-disk) protection for the Macintosh system which uses two password levels.
Supplier Name: ASD Software, Inc.

Authentication Method(s): Passwords, ID, and Pager combination
Device(s): Access-control software
Product Name: Pager Access Module
Product Features: Uses any standard digital display pager to provide direct dial authentication for secured remote network access. The logic is, if you KNOW the correct ID & Password combination, and you HAVE the right pager, it must be you.
Supplier Name: MicroFrame

Authentication Method(s): Smart Card
Device(s): Access-control hardware
Product Name: International SmartCard Reader
Product Features: Adaptable to a variety of popular international SmartCard standards and provides an alternative to AccessKey technology for user authentication.
Supplier Name: Vasco Data Security Inc.

Authentication Method(s): Smart Card
Device(s): Access-control hardware
Product Name: Model 10SM, 300, 350, 500
Product Features: Token-based information security product. Security services include: authentication, confidentiality, integrity, and non-repudiation. Can be used by organizational management, LAN administrators, system administrators, security officers, LAN users.
Supplier Name: Datakey

Authentication Method(s): Smart Card
Device(s): Access-control hardware
Product Name: PCSS Plus
Product Features: Personal Computer Security System that protects personal computer and network by positively identifying users before they gain access to the system. PCSS Plus identifies its users by way of smart cards and smart card reader/writer (desktop PCs).
Supplier Name: Personal Cipher Card Corporation

Authentication Method(s): Token
Device(s): Access-control hardware
Product Name: National Fortezza Crypto Card
Product Features: High performance data security token designed to meet the requirements of the U.S. Department of Defense's new Defense Message System (DMS). The DMS will handle "unclassified but sensitive" e-mail.
Supplier Name: National Semiconductor Corporation

Authentication Method(s): Token
Device(s): Access-control hardware
Product Name: PersonaCard 100 Series
Product Features: Security functions include: privacy, verification, digital signature and authentication.
Supplier Name: National Semiconductor Corporation

Authentication Method(s): Token
Device(s): Access-control software
Product Name: SOFTKEY
Product Features: For laptops, notebooks, or personal computers. Serves as the user's "have something".
Supplier Name: Optimum Electronics, Inc.

Authentication Method(s): Token (in-line token)
Device(s): Access-control software
Product Name: SofKEY
Product Features: A software security module that converts any MS-DOS based PC or Laptop into a "Direct Dial" positive user authentication token.
Supplier Name: MicroFrame

Authentication Method(s): Token (off-line token), password
Device(s): Access-control hardware
Product Name: PassKEY II
Product Features: A pocket sized positive user authentication token that generates a "one-time" password unique to each user & different for each use.
Supplier Name: MicroFrame

Authentication Method(s): Token based
Device(s): Access-control hardware
Product Name: Secure ID tokens
Product Features: Access-control tokens carried by authorized users.
Supplier Name: Security Dynamics

Authentication Method(s): Token based
Device(s): Access-control software
Product Name: ACE/Server
Product Features: Security software for client/server network
Supplier Name: Security Dynamics

Authentication Method(s): Token based
Device(s): Access-control software, hardware
Product Name: Access Control Module (ACM)
Product Features: Security software or hardware for host-based access control.
Supplier Name: Security Dynamics

Authentication Method(s): Token, Challenge-response
Device(s): Access-control hardware
Product Name: Access Key I & II
Product Features: Handheld token which can optically read a flashing pattern challenge.
Supplier Name: Optimum Electronics, Inc.

Authentication Method(s): Token, random password generator
Device(s): Access-control hardware
Product Name: PASCARD
Product Features: Random password generating token to authenticate users.
Supplier Name: Optimum Electronics, Inc.

APPENDIX B. SUPPLIER LIST

Supplier Name: Argus Systems Group, Inc.
Contact Name: Mary P. Sandone
Contact Title: Office Manager
Address: 1405A East Florida Avenue
Urbana, IL 61801
Phone Number: (217)384-6300
Fax Number: (217)384-6404
E-Mail:

Supplier Name: ASD Software
Contact Name:
Contact Title:
Address: 4650 Arrow Highway, Suite E6
Montclair, CA 91763
Phone Number: (909)624-2594
Fax Number: (909)624-9574
E-Mail: 102404.3630@compuserve.com

Supplier Name: Axent Technologies, Inc.
Contact Name: John C. McCurdy
Contact Title: Senior Account Manager
Address: 2155 N. Freedom Blvd.
Provo, UT 84604
Phone Number: (801)227-3718
Fax Number: (801)227-3781
E-Mail: johmcc@axent.com

Supplier Name: Baseline Software
Contact Name:
Contact Title:
Address: P. O. Box 1219
Sausalito, CA 94966
Phone Number: (415)332-7763
Fax Number: (415)332-8032
E-Mail: 3143490@mcimail.com

Supplier Name: BrainTree Technology, Inc.
Contact Name: Paul B. Currier
Contact Title: Sales Representative
Address: 62 Accord Park Drive
Norwell, MA 02061
Phone Number: (617)982-0200
Fax Number: (617)982-8076
E-Mail:

Supplier Name: Cadix International, Inc.
Contact Name:
Contact Title:
Address: 5000 Birch Street, East Tower,
Suite 210
Newport Beach, CA 92660
Phone Number: (714)476-3611
Fax Number: (714)476-3671
E-Mail:

Supplier Name: Computer Associates
International
Contact Name: Siki Giunta
Contact Title: Bus. Unit Executive
Address: One Computer Associates Plaza
Islandia, NY 11788
Phone Number: (516)342-2261
Fax Number: (516)342-5329
E-Mail:

Supplier Name: CoSystems
Contact Name: Sam Ng
Contact Title: Director of Business
Development
Address: 1263 Oakmead Parkway
Sunnyvale, CA 94086
Phone Number: (408)522-0507
Fax Number: (408)720-9114
E-Mail: samng@cosystems.com

Supplier Name: CRYPTOCard, Inc.
Contact Name: D. Wade Clark
Contact Title: VP, Sales & Marketing
Address: 1649 Barclay Blvd.
Buffalo Grove, IL 60089
Phone Number: (847)459-6500
Fax Number: (847)459-6599
E-Mail: token@cryptocard.com

Supplier Name: Cylink
Contact Name: Pat Confer
Contact Title: Area Manager
Address: 910 Hermosa Court
Sunnyvale, CA 94086
Phone Number: (408)735-5872
Fax Number: (408)735-6685
E-Mail: patc@cylink.com

Supplier Name: D-Link
Contact Name:
Contact Title:
Address: 5 Musick
Irvine, CA 92718
Phone Number: (714)455-1688
Fax Number: (714)455-2521
E-Mail:

Supplier Name: Datakey
Contact Name: Michael A. Locquegnies
Contact Title: Dir. Of Marketing & Sales,
Information Security Solutions
Address: 407 West Travelers Trail
Burnsville, MN 55337
Phone Number: (612)890-6850
Fax Number: (612)890-2726
E-Mail:

Supplier Name: Datalynx
Contact Name:
Contact Title:
Address: 6633 Convoy Court
San Diego, CA 92111
Phone Number: (619)560-8112
Fax Number: (619)560-8114
E-Mail: datalynx@netcom.com

Supplier Name: Digital Pathways, Inc.
Contact Name:
Contact Title:
Address: 201 Ravendale Drive
Mountain View, CA 94043
Phone Number: (415)964-0707
Fax Number: (415)961-7487
E-Mail:

Supplier Name: Eberhard Klemens Company
Contact Name: Susan J. Steiner
Contact Title: Administrative Assistant
Address: 10400 W. Higgins Road
Rosemont, IL 60018
Phone Number: (847)296-8010
Fax Number: (847)296-8016
E-Mail:

Supplier Name: EliaShim-Safe Software
Contact Name:
Contact Title:
Address: One South West 129 Avenue,
Suite 105
Pembroke Pines, FL 33027
Phone Number: (305)450-9611
Fax Number: (305)450-9612
E-Mail:

Supplier Name: Enigma Logic
Contact Name: Thomas J. Brady
Contact Title: VP Sales & Worldwide
Distribution
Address: 2151 Salvio Street, Suite 201
Concord, CA 94520
Phone Number: (510)827-5707
Fax Number: (510)827-2593
E-Mail: sales@safeword.com

Supplier Name: Enterprise Systems ICL Inc.
Contact Name: Richard A. Gill
Contact Title: Account Manager
Address: 11490 Commerce Park Drive
Reston, VA 22091
Phone Number: (703)648-3357
Fax Number: (703)648-3350
E-Mail: r.gill@reston.icl.com

Supplier Name: EyeDentify inc.
Contact Name: Buddy Boyett
Contact Title: VP, Business Development
Address: 10473 Old Hammond Hwy.
Baton Rouge, LA 70816
Phone Number:
Fax Number: (504)927-4290
E-Mail: (504)927-5385

Supplier Name: IC Engineering, Inc.
Contact Name:
Contact Title:
Address: P.O. Box 321
Owings Mill, MD 21117
Phone Number: (410)363-8748
Fax Number:
E-Mail:

Supplier Name: Identix Incorporated
Contact Name: Anna C. Stockel
Contact Title: Director, Fingerprint
Identification Products
Address: 510 N. Pastoria Avenue
Sunnyvale, CA 94086
Phone Number: (408)739-2000
Fax Number: (408)739-3308
E-Mail: anna@identix.usa.com

Supplier Name: Intelligent Supervisory Systems
Contact Name:
Contact Title:
Address: 6045 Augusta National Drive,
Suite 300
Orlando, FL 32822
Phone Number: (407)240-5543
Fax Number:
E-Mail: donniea@aol.com

Supplier Name: IriScan
Contact Name: Kelly L. Gates
Contact Title: Marketing Manager
Address: 133-Q Gaither Drive
Mt. Laurel, NJ 08054
Phone Number: (609)234-7977
Fax Number: (609)234-4768
E-Mail: iriscan@aol.com

Supplier Name: Lassen Software, Inc.
Contact Name: Gary Blackman
Contact Title: Sales Manager
Address: 1835-A South Center City
Parkway
Escondido, CA 92025
Phone Number: (619)737-3190
Fax Number: (619)737-0145
E-Mail: 76704,40@compuserve.com

Supplier Name: LJK Software
Contact Name:
Contact Title:
Address: One Kendall Square, Suite 2200
Cambridge, MA 02139
Phone Number: (617)558-3270
Fax Number: (617)558-3274
E-Mail: Sales@LJK.com

Supplier Name: Magna
Contact Name:
Contact Title:
Address: 1999 So. Bascom Ave., Suite 810
Campbell, CA 95008
Phone Number: (408)879-7900
Fax Number: (408)879-7979
E-Mail: magna@cup.portal.com

Supplier Name: METZ Software
Contact Name: Art Metz
Contact Title: Sales Representative
Address: P.O. Box 6699
Bellevue, WA 98008
Phone Number: (206)641-4525
Fax Number: (206)644-6026
E-Mail: CompuServe:75300,1627

Supplier Name: MicroFrame
Contact Name:
Contact Title:
Address: 21 Meridian Road
Edison, NJ 08820
Phone Number: (908)494-4440
Fax Number: (908)494-4570
E-Mail:

Supplier Name: National Semiconductor Corporation
Contact Name: Larry Van Valkenburgh
Contact Title: Dir., Channel Development, iPower Business Unit
Address: 1090 Kifer Road, Mail Stop 16-225
Sunnyvale, CA 94086
Phone Number: (408)721-5087
Fax Number: (408)245-7906
E-Mail: larry@ipower.nsc.com

Supplier Name: Optimum Electronics, Inc.
Contact Name: Charlotte Rebesch
Contact Title: Marketing Administration
Address: 425 Washington Avenue
North Haven, CT 06473
Phone Number: (203)239-6098
Fax Number: (203)234-9324
E-Mail:

Supplier Name: Paralon
Contact Name: Jacklen Evans
Contact Title: Account Representative
Address: 3650 131st Avenue SE, Suite 210
Bellevue, WA 98006
Phone Number: (206)641-8338
Fax Number: (206)641-1347
E-Mail:

Supplier Name: PC Guardian
Contact Name: Dan J. Gannett
Contact Title: Regional Sales Manager
Address: 1133 Francisco Blvd. E., Suite D
San Rafael, CA 94901
Phone Number: (415)459-0190
Fax Number: (415)459-1162
E-Mail: pcguard@ix.netcom.com

Supplier Name: Recognition Systems, Inc.
Contact Name:
Contact Title:
Address: 1520 Dell Avenue
Campbell, CA 95008
Phone Number: (408)364-6960
Fax Number: (408)370-3679
E-Mail:

Supplier Name: Safetynet, Inc.
Contact Name:
Contact Title:
Address: 140 Mountain Avenue
Springfield, NJ 07081
Phone Number: (800)672-7233
Fax Number:
E-Mail: safety@safe.net

Supplier Name: Schumann Security Software, Inc.
Contact Name: Amy Leith
Contact Title: Sales/Marketing Associate
Address: 312 Marshall Avenue, Suite 400
Laurel, MD 20707
Phone Number: (301)483-8807
Fax Number: (301)483-8349
E-Mail: 102214.2404@compuserve.com

Supplier Name: Secure Computing Corporation
Contact Name: Roy Lewis
Contact Title: Sales Representative
Address: 2675 Long Lake Road
Roseville, MN 55113
Phone Number: (612)628-6243
Fax Number: (612)628-2701
E-Mail: rlewis@sctc.com

Supplier Name: Personal Cipher Card Corporation
Contact Name:
Contact Title:
Address: 3211 Bonnybrook Dr. N.
Lakeland, FL 33811
Phone Number: (941)644-5026
Fax Number: (914)644-1933
E-Mail: CompuServe: 72130,3576

Supplier Name: SecureNet Technologies Inc.
Contact Name: Joshua M. Sklare
Contact Title: Sales Representative
Address: 2100 196th Street SW, Suite 124
Lynnwood, WA 98036
Phone Number: (206)776-2524
Fax Number: (206)776-2891
E-Mail:

Supplier Name: Security Dynamics
Contact Name: David A. Hammond
Contact Title: Manager, Marketing Communications
Address: One Alewife Center
Cambridge, MA 02140
Phone Number: (617)234-7402
Fax Number: (617)354-8836
E-Mail:

Supplier Name: Securix
Contact Name: Khris Loux
Contact Title: VP, Sales & Marketing
Address: 4104 24th Street, Suite 341
San Francisco, CA 94114
(415)695-9474
Phone Number: (415)695-0998
Fax Number: khris@securix.com
E-Mail:

Supplier Name: UsrEZ Software Inc.
Contact Name: Linda L. Cole
Contact Title: Communications Manager
Address: 18881 Von Karman Avenue
Tower 17, Suite 1270
Irvine, CA 92715
Phone Number: (714)756-5140
Fax Number: (714)756-8810
E-Mail:

Supplier Name: Vasco Data Security Inc.
Contact Name: Erling Smedvig
Contact Title: Sales Manager
Address: 1919 S. Highland Avenue,
Suite 118-C
Lombard, IL 60148
Phone Number: (708)932-8844
Fax Number: (708)495-0279
E-Mail: ess@vdsi.com

Supplier Name: Veritel Corporation
Contact Name: Robert Koretz
Contact Title: Sales Representative
Address: 640 North LaSalle Street,
Suite 552
Chicago, IL 60610
Phone Number: (312)751-1188
Fax Number: (312)751-1322
E-Mail:

LIST OF REFERENCES

Ahituv, N., Lapid, Y., Neumann, S., "Verifying the Authentication of an Information System User," Computers and Security, 6, pp. 152-157, 1987.

Alexander, M., "The Real Security Threat: The Enemy Within," Datamation, pp. 30-33, July 15, 1995.

Baig, E. C., "Shielding the Net from Cyber-Scoundrels," Business Week, p. 88, November 14, 1994.

Bishop, M., and Klein, D., "Improving System Security via Proactive Password Checking," Computers and Security, Vol. 14, No. 3, pp. 233-249, 1995.

Borowsky, M., "To Catch a Thief," U. S. Banker, pp. 75-78, November 1994.

Brock, J.L., <http://www.svpal.org/cgi-bin/gopher2html/govt/gao/full.text/GAO.IMTEC.92.5.Computer>, 1996.

Cadix International, Inc., 5000 Birch St., East Tower, Suite 210, Newport Beach, CA 92660.

Clark, R. A., "Information Technology and Dataveillance," Communications of the ACM, Vol. 31, No. 5, May 1988.

Deane, F., Barelle, K., Henderson, R., and Mahar, D., "Perceived Acceptability of Biometric Security Systems," Computers and Security, Vol. 14, No. 3, pp. 225-231, 1995.

Ellis, S., "Helping Captain Beenie Beat Fraud: Personal Finance," The Sunday Times, February 28, 1994.

EyeDentify Inc., 10473 Old Hammond Hwy., Baton Rouge, LA 70816.

Fisher, R. P., Information Systems Security, Prentice-Hall, Englewood Cliffs, NJ, 1984.

Gips, M., "PC Protection," Security Management, pp. 15-16, February 1995.

Gordon, S., "Internet 101," Computers and Security, Vol. 14, No. 7, pp. 599-604, 1995.

Haga, W. J., and Zviran, M., "Cognitive Passwords from Theory to Practice," Data Processing and Communications Security, 13(3), pp. 19-23, 1989.

Identix Incorporated, 510 N. Pastoria Avenue, Sunnyvale, CA 94086.

Infosecurity News, November/December 1995.

IriScan, 133-Q Gaither Drive, Mt. Laurel, NJ 08054-1701.

Kim, H. J., "Biometrics, Is It a Viable Proposition for Identity Authentication and Access Control?" Computers and Security, Vol. 14, No. 3, pp. 205-214, 1995.

Lawson, S., "Goodyear Navigates the Remote Obstacle Course," Infoworld, pp. 93-96, October 31, 1994.

Littman, J., "Mitnick Confesses: 'No One Is Secure!'," Datamation, pp. 6-11, January 15, 1996.

McCurley, K. S., <http://www.cs.sabduz.giv/~mccurley/health/node16.html>. March 11, 1995.

Melford, Robert J., "Secure UNIX for Enterprise Computing," Datamation, pp. 55-58, March 1, 1995.

Menkus, B., "Understanding the Use of Passwords," Computers and Security, 7, pp. 132-136, 1988.

National Semiconductor, 1090 Kifer Road, Mail Stop 16-225, Sunnyvale, CA 94086-3737.

Pfleeger, C.P., Security in Computing, pp. 196-241, Prentice Hall, Inc., Englewood Cliffs, NJ, 1989.

Porter, S. N., "A Password Extension for Human Factors," Computers and Security, 1, pp. 54-56, 1982.

Recognition Systems, Inc., 1520 Dell Avenue, Campbell, CA 95008.

Rowe, CS3600, Computer Security Lecture Notes, Spring 1996.

Russell, D., and Gangemi Sr., G.T., Computer Security Basics, pp. 55-78, O'Reilly & Associates, Inc., Sebastopol, CA, 1992.

Schorow, S., "Computer Hacker Tap Into Mischief," Boston Sunday Herald, <http://www.cdc.net/~x/1996/v4.asc>, March 10, 1996.

Schwartau, W., "New Keys to Network Security," Infoworld, pp. 51-52, May 15, 1995.

Smith, S. L., "Authenticating Users by Word Association," Computers and Security, 6, pp. 464-470, 1987.

Tuerkheimer, F. M., "The Underpinning of Privacy Protection," Communications of the ACM, Vol. 36, No. 8, August 1993.

Tuomy, J., "Addressing High-Risk Remote Access Applications with Challenge/Response User Authentication," Telecommunications, p. 58, 1995.

Veritel Corporation, 640 North LaSalle Street, Suite 552, Chicago, IL 60610.

Wilson, B., "Hand Geometry Boasts Simplicity, Convenience," Access Control, pp. 1-4, March 1992.

Zviran, M., and Haga, W.J., "Cognitive Passwords: The Key to Easy Access Control," Computers and Security, Vol. 9, No. 8, pp. 723-736, 1990.

Zviran, M., and Haga, W.J., "Passwords Security: An Exploratory Study," Naval Postgraduate School, pp. 1-24, May 1990.

Zviran, M., and Haga, W.J., "A Comparison of Password Techniques for Multilevel Authentication Mechanisms," The Computer Journal, Vol. 36, No. 3, pp. 227-237, 1993.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center2
8725 John J. Kingman Rd., STE 0944
Fort Belvoir, Virginia 22060-6218
2. Dudley Knox Library2
Naval Postgraduate School
411 Dyer Rd
Monterey, California 93943-5101
3. William J. Haga, Code SM/Hg1
Naval Postgraduate School
411 Dyer Rd
Monterey, California 93943-5101
4. LCDR Doug Brinkley, Code SM/Bi1
Naval Postgraduate School
411 Dyer Rd
Monterey, California 93943-5101
5. Moshe Zviran1
Faculty of Management
Tel Aviv University
University Campus - Ramat Aviv
Tel Aviv 69978
Israel
6. Lt. Marianna B. Magno2
c/o Commander
Space and Naval Warfare Systems Command
PMW 171, Building 600, Room 241
53560 Hull Street
San Diego, CA 92152