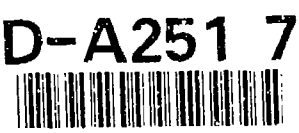

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

EVALUATION OF A BIOMETRIC KEYSTROKE TYPING DYNAMICS COMPUTER SECURITY SYSTEM

by

Kuan, Hung-i

March 1992

Thesis Advisor: Judith H. Lind
Co-Advisor: Gary K. Poock

Approved for public release; distribution is unlimited

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) AS	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
EVALUATION OF A BIOMETRIC KEYSTROKE TYPING DYNAMICS COMPUTER SECURITY STSTEM

12 PERSONAL AUTHOR(S) Kuan, Hung-i

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	1992, March	61

16 SUPPLEMENTARY NOTATION
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.

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	BioPassword Model 2100, Biometric technology, Keystroke Typing Dynamics, False Rejection Error Rate, False Acceptance Error Rate, Enrollment Time, Verification Time

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

This study evaluates an inexpensive personal computer access control system that relies on biometric keystroke typing dynamics technology, BioPassword Model 2100 (BioPassword). Enrollment time, verification time, false rejection error rate, false acceptance error rate, and user acceptance were evaluated for this system. The results show that BioPassword provides multilayer security through the inclusion of privilege control, audit functions, passwords, and verification of a personal behavioral characteristic, the rate and variation of typing a given password string. Enrollment and verification times were considered satisfactorily fast. Overall false rejection error rate was 22.5%, while false acceptance error rate was 3.4%. The false rejection error rate for acceptance as a function of trial number from one trial to five trials were 4.4%, 1.4%, 0.7%, 0.4%, and 0.3% respectively. These values were achieved under relatively uncontrolled conditions and should be improved on by using recommendations that are included. Users generally reported satisfaction with the system, which should be acceptable as part of an office automation system when used in conjunction with other standard security measures.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	UNCLASSIFIED	
22a NAME OF RESPONSIBLE INDIVIDUAL Judith H. Lind, Gray K. Poock	22b TELEPHONE (*Include Area code*) (408) 646-2543, (408) 676-2636	22c OFFICE SYMBOL OR/Li, OR/Pk

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution is unlimited

Evaluation of a Biometric Keystroke Typing Dynamics
Computer Security System

by

Kuan, Hung-i
Commander, Republic of China Navy
B.S., Chinese Naval Academy, 1977

Submitted in partial fulfiliment of the
requirements for the degree of

MASTER OF SCIENCE IN
TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1992

Auther: Kuan, Hung-i (管弘一)
Kuan, Hung-i

Approved by: Judith H. Lind
Judith H. Lind, Thesis Advisor

Gary K. Poock
Gary K. Poock, Co-Advisor

Dan C Boger
Dan C. Boger, Second Reader

David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This study evaluates an inexpensive personal computer access control device that relies on biometric keystroke typing dynamics technology, BioPassword Model 2100 (BioPassword). Enrollment time, verification time, false rejection error rate, false acceptance error rate, and user acceptance were evaluated for this system.

The results show that BioPassword provides multilayer security through the inclusion of privilege control, audit functions, passwords, and verification of a personal behavioral characteristic, the rate and variation of typing a given password string. Enrollment and verification times were considered satisfactorily fast. Overall false rejection error rate was 22.5%, while false acceptance error rate was 3.4%. The false rejection error rates for acceptance as a function of trial number from one trial to five trials were 4.4%, 1.4%, 0.7%, 0.4%, and 0.3% respectively. These values were achieved under relatively uncontrolled conditions and should be improved on by using recommendations that are included. Users generally reported satisfaction with the system, which should be acceptable as part of an office automation system when used in conjunction with other standard security measures.

TABLE OF CONTENTS

1. INTRODUCTION

A. THE NEED FOR COMPUTER SECURITY

Since the first computers were built in the 1940s, these systems have become a part of everyday life. The low-priced personal computer especially has made access easy for nearly everyone. In the U.S., for example, the total number of personal computers shipped to major metropolitan areas was expected to be 6.5 million in 1986. At the end of 1985, close to 1.5 million personal computers were linked to local area networks. Over 3 million systems operate in homes throughout the country. [Ref. 1:p. 1]

The computer has become an important tool for fields such as academic research, the military, education, banking, communications, etc. Its powerful capabilities have reduced the need for manpower, and have saved precious resources and much time. On the other hand, computers are vulnerable, and users have experienced numerous problems over time. A growing concern of computer users is how to make a vulnerable computer system secure from intrusion. This concern is especially widespread among professionals and managers.

Cronin defines computer security as follows:

> Security assumes the safe and continuous operation of your computer system performed by trained, authorized personnel. The computer

system itself must be protected, as well [as] the integrity of all programs and data. Finally, security means that any entered data can be retrieved at any future time, without alteration by accident or deliberate intent. [Ref. 1:p. 2]

Pfleeger asserts that computer security consists of maintaining three characteristics: secrecy, integrity, and availability.

- *Secrecy* means that the assets of a computing system are accessible only by authorized parties. The type of access is "read"-type access: reading, viewing, printing, or even just knowing the existence of an object.
- *Integrity* means that assets can be modified only by authorized parties. In this context, modification includes writing, changing, changing status, deleting, and creating.
- *Availability* means that assets *are* available to authorized parties. An authorized party should not be prevented from accessing those objects to which he or she or it has legitimate access. For example, a security system could preserve perfect secrecy by preventing everyone from reading a particular object. However, this system does not meet the requirement of availability for proper access. [Ref. 2:pp. 4-6]

The most serious computer security concerns in the past have related to computer software. Software is a critical component of the computing system. It includes the operating system, utility programs, and data. Software accidentally can be deleted or misplaced by novices or by unauthorized users, or it can be pirated or destroyed by malicious individuals or spies [Ref. 3]. The result can be a minor annoyance or interruption, or it can be a disaster.

In the U.S., computer crime in the nation's fastest growing industry. The average loss for each reported crime has exceeded $100,000. [Ref. 1:p. 1] In

the case of software theft, the Software Publishers Association estimated that nearly half of the software running on personal computers in the U.S. was pirated, a figure that rose to 80% in Germany and an incredible 98% in South Korea [Ref. 4:p. 4].

In the case of malicious intrusions, numerous computer systems have been threatened or destroyed by virus attacks. A recent example was the virus called "Michelangelo," which threatened to destroy all data on infected hard disks on the birthday of the artist Michelangelo, 6 March, in 1992. During the 1991 Persian Gulf War, the U.S. military raised concerns about the threat posed by computer viruses that could affect the ability to wage electronic warfare. Numerous computers at Army installations were found to be infected with viruses prior to Gulf operations. Fortunately the viruses were found and removed before the war started. Otherwise, havoc might have resulted if the viruses disabled computer systems during wartime. [Ref. 5:p. 97]

Computer hardware also can suffer from security problems, as systems continue to get smaller. It is very easy for a thief to walk off with a personal computer. According to the U.S. Federal Bureau of Investigation, more than 94 million dollars worth of office equipment was stolen in 1980. This figure is expected to increase steadily with time. [Ref. 1:p.15] Theft is not the only problem. Computer hardware also can be subjected to abuse by the users. It might be sabotaged by an angry employee who has been laid off, or damaged by an impatient user.

As awareness of security problems and needs have grown, many control systems and devices have been developed and are now available on the market. These security control systems and devices generally include such things as data encryption, software control systems, and hardware control systems. Generally they are designed to protect the three vulnerable points of a computer: data, software, and hardware.

B. COMPUTER SECURITY CLASSIFICATIONS

Weiss separates computer security systems into five classes. These classes are referred to as physical security, privilege control, encryption, audit control, and identification authentication systems. [Ref. 6:p. 4(1)]

1. Physical Security Systems

Physical security is applied to protect computer hardware. Physical security technologies are the earliest, most effective, and least expensive security methods [Ref. 2:p. 15]. Using locks on doors, a guard at the entrance, or chains to lock hardware to the tables can deter most thieves. Some advanced alarm systems use photoelectric, microwave, ultrasonic, or passive infrared technologies. Other sophisticated devices use new and innovative biometrics technologies for entrance control. These include retinal scan, fingerprint, and voice verification systems. Advanced techniques are catching the attention of computer supervisors, and are expected to play a important future role in computer security.

2. Privilege Control Systems

Privilege control is used to allow various individuals to have different levels of access for different kind of resources. Using internal program controls, a computer supervisor can enforce security restrictions, such as limiting access within a database management program used for military purposes. Using such systems, operators with different levels of security clearance can be allowed access to specific levels of classified information.

3. Encryption Systems

Encryption is the most powerful method that can be used for data security. Modern coding technologies are used to transform sensitive data so that the resulting information is unintelligible to persons without proper access. Decryption or decoding is necessary; otherwise the data are meaningless and useless. Encryption can be used for data stored in files or transmitted on networks.

4. Audit Control Systems

Audit control techniques are used to record access to a computer system in terms of who, what, when, and where. Some audit programs are transparent to users; only the supervisor can access these records. Others, such as those included in most operating systems, provide audit information to all users. Audit programs can record file names, the file transaction times, and file sizes. With this for reference, users can determine if there has been

any unauthorized change in files since the proper user last logged on to the system.

5. Identification Authentication Systems

Identification authentication is used to verify some characteristic of an individual who tries to access a computer system. Three basic methods are used for verification. The first method is to verify something he or she knows, such as a password, a number, a code, a fact, or historical information. The second method is to verify something he or she has, such as a card, a key, a uniform, or a badge. The third method is to verify something that is a unique characteristic of the individual, such as a fingerprint, eye retina, or keystroke typing dynamics. These last identification authentication methodologies are known as biometric identification technologies.

C. BIOMETRICS COMPUTER SECURITY TECHNOLOGY

1. Biometric Technologies

Biometrics is the field of science which measures physical characteristics of the human body to establish identity [Ref. 7:p. 2]. Biometric technologies are defined as automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic [Ref. 8:p. 9].

A biometric device that is used in the access control industry has three major components: (1) a mechanism to scan and capture a digital or

analog image of a personal characteristic; (2) compression, processing, and comparison of the image with stored data; and (3) an interface with application systems. Biometric devices use automated methods to verify or recognize an individual's identity. Thus they operate rapidly, usually requiring only a few seconds to permit or deny access. [Ref. 8:p. 9]

Biometric technologies can be divided into two categories. First are those that are based on physiological characteristics of an individual. Second are those that recognize and take advantage of a behavioral characteristic. [Ref. 8:p. 11]

A physiological characteristic is a relatively stable physical characteristic such as a fingerprint, the geometry of the hand, the eye retina or iris patterns, facial image, or the veins on the back of wrist. Measurement of such characteristics generally is accurate and is unalterable. However, the devices are sophisticated and expensive.

A behavioral characteristic is a unique habit or pattern of individual behavior. Characteristics that may be used for access control include signature dynamics, keystroke typing dynamics, and voice patterns. Systems based on behavioral characteristics are usually less accurate and the characteristics can change with time. They are less sophisticated and thus cheaper. Regular updating of the measured pattern is required to overcome shortcomings of these systems.

2. Keystroke Typing Dynamics for Computer Security

Keystroke typing dynamics, also called *typing rhythms*, is one of the biometric technologies used in computer security. This technology analyzes an individual's unique typing pattern on the computer keyboard, and uses that pattern for identification purposes. As with the signature and voice pattern, each individual's typing pattern is distinctive.

During enrollment in a typing dynamics security device, the typing inputs of the user are sampled 1,000 times per second, and stored in the memory of the device as an *electronic signature*. For access after enrollment, the user must successfully generate a logon electronic signature that matches the stored signature. Systems using keystroke typing dynamics have two advantages. First, the system is compatible with normal computer tasks; users use only the standard computer keyboard for enrollment and verification. Second, verification input is via the existing keyboard; the whole machine is uncomplicated and thus cheaper than many other systems. [Ref. 8:p. 15]

International Biometric Systems, Inc., was the first company that developed and marketed a keystroke dynamics identification device, called BioPassword Model 2100 (BioPassword). The company suffered setbacks in 1988 due to poor marketing and, in 1991, was taken over by Phoenix Software International. A new product called BioLock is expected to be made commercially available by Phoenix before the middle of 1992.

As the successor of BioPassword, BioLock is basically the same as its predecessor with two differences. First, BioLock is a software system, while BioPassword required a plug-in board. Second, BioLock will be less expensive than BioPassword. The company has not announced a price, but the new system is expected to sell for around $100, which is one-third of the price of the BioPassword system.

D. GOAL AND OBJECTIVES OF STUDY

The Republic of China Navy currently has an office automation program underway. Personal computers will be the most important equipment in the newly automated system. Success of the automation program will depend on the critical component of computer security. Only with the guarantee of a secure computer environment can the office automation program be fully and satisfactorily deployed.

The goal of this study is to evaluate the performance of BioPassword Model 2100 for possible use of keystroke typing dynamics technology by the Republic of China Navy. The BioPassword is the only product available that uses keystroke typing dynamics technology. The device has not previously been evaluated by any independent organization. The results of this evaluation may be used as a reference for the Republic of China Navy or other interested organizations as they compare this technology with that used by

other biometric devices. Potential users then should be able to make wise choices among devices, depending on specific security needs.

The objectives for the BioPassword evaluations are as follows.

- Determine ease of enrollment and anticipated verification time.
- Determine false rejection error rates that might be expected.
- Determine false acceptance error rates that might be expected.
- Evaluate the overall level of security that can be expected.
- Determine whether this kind of system should be acceptable to its proposed users, the Republic of China military officers.

E. SCOPE AND LIMITATIONS

The scope of this study is limited to biometric technologies used for computer security. Only one of these biometric technologies, keystroke typing dynamics, and the only product available using this technology, the BioPassword Model 2100, will be evaluated. Although some inferences have been drawn from published data about other systems, no attempt will be made in this study to compare the BioPassword system directly with other computer security technologies or devices, due to the differences in the technologies, designs, criteria, and applications.

Several limitations of this study should be noted.

- Only 24 study participants were used in the evaluations. No analysis was carried out to determine the significance level of the results for this sample size.

- The BioPassword system provides an adjustable verification threshold value from 0 to 10. Due to the available study time, only a very low threshold value of 2 was tested.

- Test results obtained here may differ from what might be found using another group of test participants. This is due to the distinctive characteristics of human physiology and behaviors on which biometric technologies are based. Since the test participants were all Republic of China military officers studying at the Naval Postgraduate School, the results should be applicable for use by the Republic of China military agencies. However, they may not generalize to the public in general.

II. BIOPASSWORD MODEL 2100

A. INTRODUCTION

The BioPassword Model 2100 (BioPassword) is a computer access-control device manufactured in 1989 by International BioMetric Systems, Inc. As with fingerprints and the retina of the eyes, no two signatures are exactly the same [Ref. 9:p. 1]. Similarly, each individual's typing dynamics are unique. For a given sequence of characters, each person will demonstrate slightly different pauses between the characters. Based on this knowledge, the BioPassword System uses the innovative technology of keystroke dynamics to provide access control to stand-alone personal computers. [Ref. 10:p. 1-E]

Using a proprietary technique, BioPassword generates a unique *electronic signature* which represents the keystroke typing dynamics or typing patterns of each user as he or she enters a character string which is used as a password. The electronic signature, stored in the BioPassword memory, is verified, along with the user's identification string and the password characters, before access is permitted to the computer on which the system is installed.

Two types of users are defined by BioPassword. These are referred to as normal users and superusers. Normal users are those users who are permitted access to a personal computer protected by BioPassword. A superuser is the

security administrator who oversees the use of BioPassword on a given computer. If desired, more then one individual can be given superuser status. However, due to the limited number of users who can enroll at any one time, it is impractical to designate more than one or two persons as superusers.

Once installed, BioPassword is automatically activated when the personal computer is turned on or reset. After that, BioPassword prompts the user for his or her identification and password, and verifies both of these along with the keystroke typing dynamics of the password, using the electronic signature recorded during the enrollment process. If the verification is positive, the user is allowed to use the computer. If the verification is negative, the user may repeat the entry sequence as many times as has been specified by the superuser. If the verification is still negative after these attempts, the personal computer is locked by BioPassword. That is, the keyboard will no longer accept inputs. Only the superuser can unlock the computer.

BioPassword is equipped with several sophisticated security management functions that increase BioPassword's security control ability. These functions are an integral part of the BioPassword system, along with the keystroke typing dynamic biometric algorithm. These security management functions include the following.

- Auditing and audit reporting
- Keyboard locking and privacy features

- Forcing users to change passwords periodically
- Counting sequential failures
- Setting of access threshold value
- Security timeouts
- Setting of permitted working hours
- Secure, unattended data processing

B. BIOPASSWORD FUNCTIONS

The BioPassword functions fall into two categories: superuser functions and normal user functions. Most of the functions are available only to the superuser.

1. Superuser Functions

The superuser is the key person for systems that use BioPassword. Using the management functions provided by BioPassword, superusers can configure a number of options that affect system performance, either on a computer-wide available to the superuser, or an individual user basis. The options available to the superuser, along with their functions, are discussed below. [Ref. 10]

a. Management of Users

One of the superuser's main functions is to enroll and to assist the individuals who will use the system that is secured via BioPassword. He or she uses nine functions to carry out this part of the job.

(1) Display a List of Users

This function provides a list of the current system users on the computer screen, along with their identification strings and user status as normal users or superusers. Passwords are not shown in this list or elsewhere, since they generally are known only to the user.

(2) Add User

This function allows addition of a new user or superuser to the system. As currently designed, a maximum of six users can be enrolled in the system at any one time. At least one of them must be a superuser. The superuser assigns an identification string (often the user's name) and a temporary password to a new user during enrollment, and specifies whether normal user or superuser status is enabled. The new user then can use the assigned identification and the temporary password to log on the system and continue with the enrollment procedure. During enrollment, the user will be requested to enter a new password and to type it approximately 15 times. During this process the unique electronic signature of the user is created and stored in the BioPassword memory.

(3) Remove User

This function allows removal of the electronic signatures from the BioPassword system. The superuser who is logged on the system cannot remove himself or herself from the system. This restriction prevents the superuser from accidently leaving the system in a no-superuser situation, which is a fatal failure of the system.

(4) Add Samples for User

This function allows a superuser to allow a user to update his or her electronic signature by adding more samples of password typing dynamics (about six samples) into BioPassword memory. Users tend to type their passwords faster and faster as they became more familiar with them. Consequently, after some time they may not be successful in logging on the system because the most recent typing pattern may not match the original pattern. The function of adding samples is used to solve this problem.

(5) Change User Status

This function allows the access privilege of any of the users to be changed from superuser to normal user or vice versa. As with the *remove user* function, the superuser who is using this function cannot change his or her own status. Without this safety factor, a superuser might accidently designate himself or herself to a normal user and leave the BioPassword system in the fatal status of being without a superuser.

(6) Set Working Hours

The superuser can specify a certain period of working hours each day of the week. The working hour period can be different for different users. The normal user can access the system only during the specified working hours. The superuser has no working hour limitations. This function is very effective in preventing system use by normal users during unauthorized times.

(7) Set Access Threshold Value

Access threshold values are the tolerance limits of the BioPassword when verifying the users' electronic signatures. The highest threshold value is 10, referred to as *lock*. This setting effectively locks all users out of the system. The lowest value is 0 or *bypass*, which disables the electronic signature verifying algorithm and allows access to all users. The superuser selects a threshold value according to current security needs. For new users, the value is usually relatively low (that is, between 1 and 3). Once the users become familiar with their passwords, the value can be set higher for increased security. A typical setting for experienced users is 5.

(8) Force Change of Passwords

This function allows the superuser to require that all users (including superusers) change their passwords, if a security breach is

suspected. Using one of the BioPassword functions, normal users also can change their passwords any time they desire without involving a superuser.

(9) Clear Sequential Failure Counter

Each individual user's unsuccessful logon attempts are recorded by a *failure counter* in the system. The failure counter is reset to zero if the user logs on successfully before the maximum value is reached. If the maximum value is reached, the system will lock the user out from making further attempts. Only the superuser can reset the sequential counter, by using the *clear* function to unlock the system.

b. System Parameters

The superuser also is responsible for general BioPassword system management. Several security management functions are provided specifically for this purpose. Using these functions, the security of the system can be set at the desired level.

(1) System Timeouts

Two parameters can be set that are related to how long a user can be inactive before the system will lock the keyboard.

- *Timeout if no activity for xx minutes.* After a user logs on the computer, he or she may leave the terminal, resulting in the possibility of intrusion. To prevent that from happening, the superuser can set this function for a value between 0 and 20 minutes (value of 0 will disable the function). If the user does not use the keyboard for the set time period, the computer will lock. The user must log on the computer again for continued use.

- *Warn user xx seconds before timeout.* A warning tone is given prior to the timeout. The length of the warning period may be set by the superuser with a range of 0 to 60 seconds (value of 0 will disable the function).

- *Timeout superuser in xx seconds.* This is similar to *timeout if no activity for xx minutes*, but applies to the superuser only. Since only the superuser can access the functions for managing the whole BioPassword system, it is very dangerous to leave the system unattended while the superuser is logged on. Using this function, the superuser can set a time ranging from 30 to 600 seconds after which the system will lock.

(2) System Lockout

The superuser can set the desired number of consecutive unsuccessful logon attempts that may be made before the system locks up, up to a maximum value of 20. If a user cannot log on the system within the permitted number of attempts, there is a *failure* in the logon procedure. The system will then initiate a *user lock* condition, keeping all users except the superuser from logging on. If additional attempts are made beyond this point, a *system lock* is initiated by this function, locking the system for a specific period of time ranging from 1 to 60 minutes, and preventing all users (including superusers) from accessing the computer.

(3) Working Hours

This function is different from the *Set Working Hours* in the superuser's User Management functions. It allows the superuser to define the default working hours that apply to all normal users. If a normal user

requires working hours different from the computer-wide default working hours, the superuser can use the *Set Working Hours* in the User Management functions to override the default. Again, the superuser is not bound by any working hour restrictions.

(4) Set BioPassword Clock

BioPassword provides its own secure clock which can function for the computer system as a whole. Only the superuser can set the BioPassword clock. Once set, the clock will be used to enforce the working hours restrictions and to record the times of logons and of attempted logons that result in failures. Each time a user logs on, the system displays his or her last logon date and time. By checking this message, the user can determine if an intrusion has occurred.

(5) Force Password Change After xxx Days

For system security, the superuser may require normal users to change their passwords periodically. The minimum time which one password can be used can be set between 1 and 120 days, depending on specific security needs. At the end of the period, each user is required by BioPassword to change his or her password. A shorter time period results in tighter security. However, it takes time for users to reenroll and, if they must do so too often, they may be forced to write down new passwords to remember them, increasing the risk of a security breach.

(6) Hot Keys Definition

Three sets of *hot key* keyboard combinations are defined by the superuser to protect the system when users must leave the system unattended, yet secure, for awhile. Each set includes three keys that are pressed simultaneously: two from among the Alt, Ctrl, and left shift keys and one number key (e.g., Alt-Ctrl-1). These may be selected as desired, so they will not conflict with an application's hot keys.

- *Hot Key One*. When pressed, the system is stopped, requiring the current user's reverification for restarting.
- *Hot Key Two*. When pressed, the keyboard is locked, but the system is still running. To restart, the current user must reverify.
- *Hot Key Three*. This is the same as the command to log off the system. When pressed, the running program stops and the system stands by for other users to logon.

c. Information Integrity Reports

BioPassword can generate auditing reports based on records of user actions in accessing the system. The reports include information such as the users' logon time, logon attempts and failures, causes of logon failures, superuser actions, etc. Superusers can request these reports whenever they are needed. The reports can be used to determine if intrusions have been attempted, so that necessary countermeasures can be taken.

d. Bypass of Biometric Verification

Superusers may bypass BioPassword's biometric verification algorithm. The system then will verify only the users' identifications and passwords, as some normal computer systems do. The maximum bypass time is 720 hours.

e. System Backup and Restore

The users' electronic signatures can be stored on a floppy disk and restored from the disk if the system loses its memory store. Backup is a very important procedure that the superuser should do every time a user is enrolled in the system account.

During this study, the system that was being tested failed several times. Using the backup, the system was restored to normal very quickly, without requiring that all users reenroll.

2. Functions for Normal Users

Normal users basically do not take an active role in BioPassword management. The superuser is responsible both for computer management and user access to the computer. However normal uses are allowed to utilize two functions. [Ref. 11:p. 3-5]

a. Changing Passwords

This function allows normal users to change their passwords any time they desire without involving a superuser. Once the normal users

execute this function, they only have to type in their new passwords for approximately six times to complete the process. It is very important for each user to change his or her password whenever there is a possibility that the password has been revealed to someone else.

b. Using Hot Keys

Three sets of *hot key* keyboard combinations can be defined by the normal users to protect the system when they must leave the system unattended, yet secure, for awhile. These functions are identical with the superuser's *hot keys* functions.

- *Hot Key One.* When pressed, the system is stopped, requiring the current user's reverification for restarting.
- *Hot Key Two.* When pressed, the keyboard is locked, but the system is still running. To restart, the current user must reverify.
- *Hot Key Three.* This is the same as the command to log off the system. When pressed, the running program stops and the system stands by for other users to log on.

III. BIOPASSWORD MODEL 2100 PERFORMANCE TEST

A. GENERAL TEST DESCRIPTION

1. Purpose

The purpose of this test was to evaluate the performance of the BioPassword Model 2100. Specifically, the *false rejection error rate* and the *false acceptance error rate* were determined through the test. Some of the BioPassword user functions also were evaluated. [Ref. 12:p. 2]

A false rejection error is the rejection of a validly enrolled user who performs a correct logon procedure. The false rejection error rate is the ratio of false rejects to total attempts at verification. A false rejection error is also called as a *false alarm error* or *type one error* [Ref. 6:p. 4(1)]. Data on false rejections were collected by test participants who attempted to enter the system using their own correct identification strings and passwords.

The false acceptance error is the acceptance of an imposter as a validly enrolled user. A false acceptance error rate is the ratio of false acceptances to total imposter attempts. A false acceptance error is also called as an *imposter pass error* or *type two error*. [Ref. 6:p. 4(1)] Data on false acceptances were collected as participants made "intruder attempts," trying to enter the system using someone else's identification and password.

2. Equipment and Environment

Two BioPassword Model 2100 systems were installed in two IBM personal computers, one PC model (referred to as PC No. 1) and one XT model (referred to as PC No. 2). The BioPassword system consists of a firmware board plugged into one of the computer's expansion slots. The computers were located in the Human Factors Laboratory at the Naval Postgraduate School, Monterey, California. The laboratory area used is an office-like space, comfortable and quiet. The computers sat on standard computer tables, each equipped with a suitable chair that could be adjusted as desired by the users.

3. Test Participants

A total of 24 male military officers participated in the test. All were officers from Taiwan, Republic of China, studying at the Naval Postgraduate School; they participated voluntarily, without monetary or other incentives. Since the results of the study are specifically intended for use by Republic of China military agencies, inclusion of only Chinese officers was considered appropriate. Since BioPassword is easy to use, no special training was provided to the participants other than a brief introduction before each individual enrolled in the test.

4. Test Procedure

The 24 participants were randomly divided into two groups; half were enrolled on each of the two IBM PCs equipped with BioPassword. Each

participant was assigned a word or name to serve as personal identification and a temporary password by the superuser. With the assistance of the superuser, participants enrolled in the BioPassword users account, using the assigned identifications, and then selected new passwords. Passwords could be any combination of letters, numbers, or keyboard symbols; six to ten characters were required. Each participant's identification and password were provided to all other participants. During intruder attempts, a participant would try to gain access to the system using another's identification and password. Participants were allowed to practice typing the passwords prior to making intruder attempts, up to the maximum allowed value of 20 unsuccessful attempts, before the system locked up.

After enrollment, the participants made five logon attempts and five intruder attempts each time they tested the system. This was defined as one set of trials. A total of 30 sets of trials were required to complete each participant's tests. Participants usually completed one or two sets of trials per day; continuous sets of trials without a break were discouraged to ensure that trials represent random samples of participant performance. The average time for a participant to complete the whole test was 35 days. In total, about three months were required to complete the BioPassword performance test.

5. Test Records

Two kinds of test records were maintained for data collection. The first was generated by BioPassword through its *Information Integrity Reports*,

as shown in Figure 3-1 and described in Chapter II. This report was printed out every other day for the participants' reference, so they could validate their own failed attempts at accessing the system. The superuser also used these records for monitoring test progress and for trouble shooting.

```
BioPassword - INTEGRITY REPORT              Fri Nov 22 19:39:55 1991

          ******************************************
          *              GROUP BY USER ID          *
          ******************************************

      DATE      TIME   COUNT      ACTION [ADDITIONAL INFORMATION]
-------------------------------------------------------------------
 ALL RECORDS FOR ID : kuanhi
    91/11/21 21:44:46   1            logon - passed.

 ALL RECORDS FOR ID : leemanyimg
    91/11/21 11:33:12   1            logon - wrong id.

 ALL RECORDS FOR ID : happyy
    91/11/22 15:13:10   1            logon - bad dynamics

 ALL RECORDS FOR ID : superuser
    91/11/22 19:39:04   2            audit viewed.
    91/11/22 19:38:48   2            user added.[chalie].
    91/11/21 08:36:42   1            user removed.[yinyin].
    91/11/21 08:34:30   2            logon - passed.
 ..................................................
 ..................................................
```

Figure 3-1. Example of BioPassword Information Integrity Report.

The second kind of report was kept by each participant on his own test record sheets, as shown in Figure 3-2. The participant marked an "S" on the sheet for each successful logon trial or intruder trial, and an "F" for each failed logon trial or intruder trial. Although data for 30 sets of trials were collected, only the first valid 25 of the 30 sets actually were included in the results. This permitted the discarding of suspect data that might be due to BioPassword malfunctions.

TEST PARTICIPANT RECORD

Test Participant No.:_____ Name:_____
Identification:_____ Password:_____

Please marks in the blanks "S" for "successful logon", and "F" for "failure logon"

1. Date/Time:_____ Logon Trial: 1___ 2___ 3___ 4___ 5___
Intruder Trial: 1___ 2___ 3___ 4___ 5___

2. Date/Time:_____ Logon Trial: 1___ 2___ 3___ 4___ 5___
Intruder Trial: 1___ 2___ 3___ 4___ 5___

3. Date/Time:_____ Logon Trial: 1___ 2___ 3___ 4___ 5___
Intruder Trial: 1___ 2___ 3___ 4___ 5___

. . . . . .
. . . . . .
. . . . . .

30. Date/Time:_____ Logon Trial: 1___ 2___ 3___ 4___ 5___
Intruder Trial: 1___ 2___ 3___ 4___ 5___

Figure 3-2. Test Participant Record Form.

6. Threshold Value

The threshold value (described in the Chapter II) was set at 2 for this test, on a range from 0 to 10. The low threshold value was selected to keep the false rejection error rate low in order to reduce user frustration. Even at this low value many of the volunteer participants were frustrated by frequent rejections.

B. SYSTEM PROBLEMS

The BioPassword evaluation tests were hampered by several system problems that interfered with the normal users' trials. The problems resulted in error messages that were displayed on the computer screen, and indicated

that some action must be taken by the superuser before the participants could continue with their trials.

First, an *SRAM/ROM incompatible. Consult your Superuser* error message indicated that the system's read-only memory (ROM) version was incompatible with the battery backed-up random access memory (RAM) data structure. This was the most troublesome problem encountered during the tests and occurred about six times. To fix the problem, the superuser had to open the PC's central processing unit cover and reset the six BioPassword board address switches. This process resulted in the clearing of all existing user's electronic signatures from system memory. Using a superuser identification sequence provided by the manufacturer, the superuser reenrolled himself, then restored the other users' electronic signatures from a backup file on a floppy disk. Without such a backup file, it would have been necessary for each user to be reenrolled in the system.

Second, a *System is locked. Superuser must log on* error message appeared in the upper right corner of the entry window when too many invalid logon trials had been made. During the tests, the System Lockout function was set at 20 (the maximum value, as described in Chapter II). Even so, this situation occurred often, usually due to participants making numerous intruder attempts. The superuser had to reset each participant's *Sequential Failure Counter* (as described in Chapter II) every day to prevent this situation from happening.

Third, the electronic signature of some users changed over time. Some users tended to type their passwords faster and faster as they became more familiar with them. The result was that the BioPassword system was not able to recognize these changed electronic signatures and rejected them as invalid logon attempts. This problem was fixed by using the BioPassword *Add Samples for Users* function to update users' electronic signatures in system memory when users reported logon difficulties.

IV. DATA ANALYSIS AND RESULTS

A. DATA COLLECTION

Data were compiled from two kinds of test records, described in Chapter III. The first kind was generated by BioPassword through its *Information Integrity Reports*. These reports were basically used for following test progress and to discard invalid data that resulted from BioPassword malfunctions. The second kind consisted of the test record sheets kept by the participants. These served as the primary source of acceptance and rejection results. As described in Chapter III, each participant completed 30 sets of trials. Each set included up to five logon attempts and up to five intruder attempts. The first 25 sets of valid data were used in the calculation of the results; the other five sets were discarded either because they were suspect or simply to keep all participants' numbers of trials constant.

In addition to the data collected during the trials, each participant was asked to complete a brief survey form. This survey was intended to collect information about how easy the system was to use, and how confident the users were about the level of security it provides.

In summary, eight kinds of data were collected and analyzed during this study, and the results are reported below.

- Average time to enroll in the system, and average time to complete the verification process.
- False rejection error rates for PC No. 1 (the PC model), both for the individual participants and for all participants who used that PC, as a group.
- False rejection error rates for PC No. 2 (the XT model), both for the individual participants and for all participants who used that PC, as a group.
- False rejection error rates as a function of the number of the trial (out of five attempts) on which the user was correctly verified.
- False acceptance error rates for PC No. 1 (the PC model), both for the individual participants and for all participants who used that PC, as a group.
- False acceptance error rates for PC No. 2 (the XT model), both for the individual participants and for all participants who used that PC, as a group.
- Comparison of results for the two PC systems.
- Participants' opinions on ease of use and the level of security provided by the BioPassword system.

B. ENROLLMENT TIME AND VERIFICATION TIME

The average enrollment time for both computers was approximately 2 minutes. Time was measured for a sample of test participants from when they started to key in their identifications and passwords until the *enrollment-completed* message was displayed on the terminal screen. This usually required typing the password about 15 times.

Verification time ranged approximately from 5 to 10 seconds for both computers, with an average verification time of 7.5 seconds. Time was measured from when a sample of test participants began to key in their identifications until BioPassword responded with a *valid logon* or *invalid logon* message on the terminal screen. Verification time varied as a function of the number of characters in the identifications and in the password strings, participants' typing skills, and their familiarity with the system.

C. FALSE REJECTION ERROR RATE

A false rejection error is the rejection of a validly enrolled user who performs a correct logon procedure. The false rejection error rate is the ratio of false rejections to total logon trials.

1. False Rejection Error Rates for PC No. 1

The individual false rejection error rates are the ratio of each test participant's false rejections to the total logon trials. As described in Chapter III, each individual made 150 logon trials; of these, 125 trials were used in the calculations. For the 12 test participants enrolled in PC No. 1, the highest false rejection error rate was 40% and the lowest was 7% (a difference of 33%). Table 4-1 and Figure 4-1 summarize these results.

For the group of 12 as a whole, there were 363 false rejections in 1500 logon trials. The overall group false rejection error rate for PC No. 1 was 24%, as shown in Table 4-1 and Figure 4-1.

TABLE 4-1. INDIVIDUAL AND GROUP FALSE REJECTION ERROR RATES FOR PC NO. 1

Partici-pants	Identifi-cations	Passwords	False Rejec-tions	False Rejection Error Rate (%)	Group False Rejection Error Rate (%)
1	tester1	liweiss	35	28	24
2	tester2	chiang	43	34	
3	tester3	leelee	49	39	
4	tester4	6550219	9	7	
5	tester5	137638	19	15	
6	kuanhi	happyy	20	16	
7	yangyang	yangyang	27	22	
8	leemanying	leemanying	50	40	
9	cccccc	4086555	33	26	
10	sherman	sherman	29	23	
11	kkkkkk	1234567890	19	15	
12	wwwwww	763980	30	24	

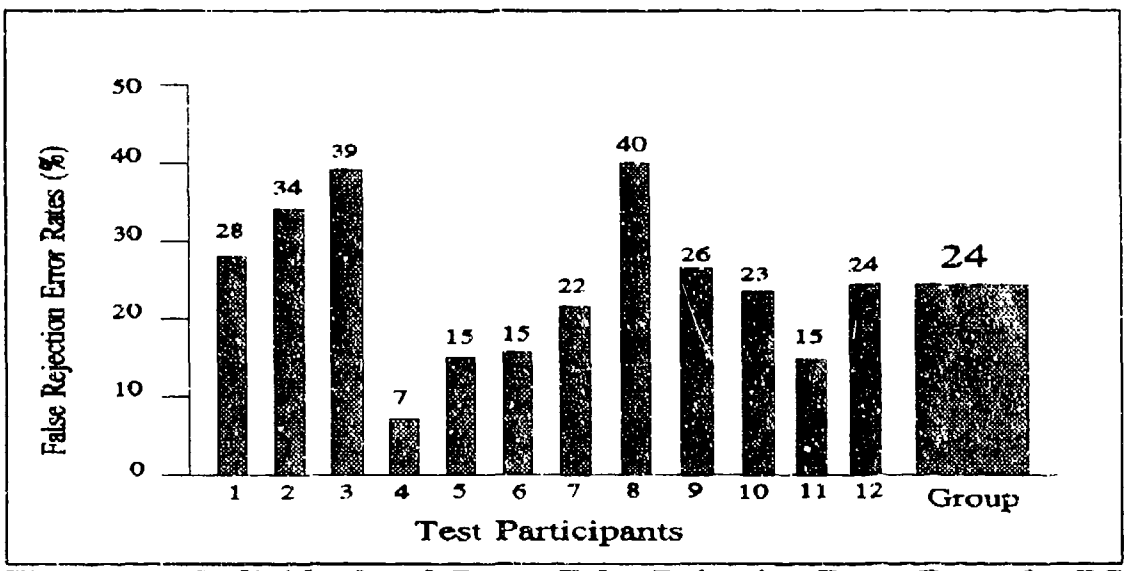

Figure 4-1. Individual and Group False Rejection Error Rates for PC No. 1. The Numbers Above Bars Indicate the Rates.

2. False Rejection Error Rates for PC No. 2

As With PC No. 1, PC No. 2 also h..d 12 test participants enrolled. For these individuals, false rejection error rate ranged from 39% to 9% (a difference of 30%). These results are provided in Table 4-2 and Figure 4-2.

There were 314 false rejections for the group as a whole in 1500 logon trials, resulting in a group false rejection error rate of 21%, as seen in the table and figure.

3. Acceptance as a Function of Trial Number

The number of times a valid user must attempt to enter a computer system before he is recognized will strongly affect how well users will accept the system. This parameter was measured for the BioPassword system using procedures proposed by Holmes and others for evaluating biometric security devices. This was done by measuring the false rejection error rate as a function of the number of the trial on which the user finally gained entry into the system. [Ref. 12]

For both computers combined, the average number of trials required for correct acceptance was calculated as follows. When the logon attempt was successful on the first trial, this was counted as five acceptances. If the logon procedure was accepted on the second trial, this was counted as one false rejection and four acceptances, etc. This approach simply calculated a

TABLE 4-2. INDIVIDUAL AND GROUP FALSE REJECTION ERROR RATES FOR PC NO. 2

Partici-pants	Identifi-cations	Pass-words	False Rejections	False Rejection Error Rate (%)	Group False Rejection Error Rate (%)
1	chieno	thailand	12	10	21
2	fffff	fuchen	23	18	
3	llllll	huifeng	21	17	
4	cccccc	rocchang	30	24	
5	yinyin	yinyin	17	14	
6	8178pp	wtli406	11	9	
7	tester5	hanhan	37	30	
8	tester8	87654321	22	18	
9	llllll	chalie	48	38	
10	wwwwww	wanglo	49	39	
11	bbbbbb	louisp	14	11	
12	ffffff	frand1725	30	24	

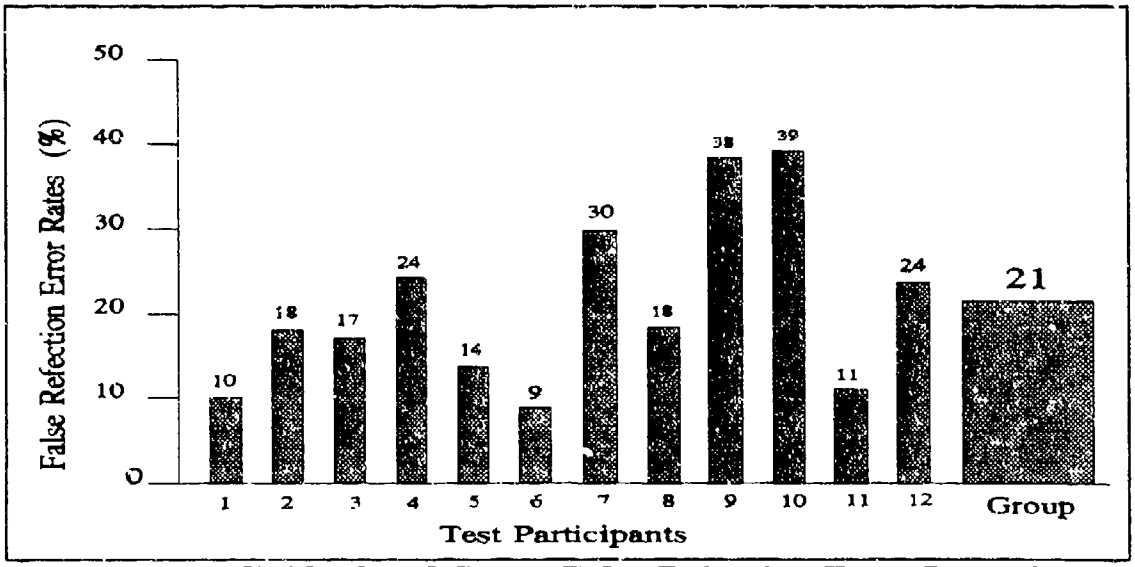

Figure 4-2. Individual and Group False Rejection Error Rates for PC No. 2. The Numbers Above the Bars Indicates the Rates.

weighted average number of trials until acceptance expressed as a percent of the total trials. Figure 4-3 provides the results.

As may be seen, false rejections were much more common (4.4%) on the first trial than on succeeding trials. Having failed to gain entrance on the first trial, the users experienced only a 1.4% false rejection rate on the second trial. False rejections dropped to 0.7%, 0.4%, and 0.3% on the remaining three trials in a five-trial set.

D. FALSE ACCEPTANCE ERROR RATE

A false acceptance error is the acceptance of an imposter as a validly enrolled user. The false acceptance error rate is the ratio of false acceptances to total imposter attempts.

1. False Acceptance Error Rates for PC No. 1

The individual false acceptance error rates are the ratio of each test participant's false acceptances to his total intruder trials. As described in Chapter III, each individual made 150 intruder trials; 125 of these were used in the calculations. For the 12 test participants enrolled in PC No. 2, the highest false acceptance error rate was 7% and the lowest was 0% (a difference of 7%). These results are illustrated in Table 4-3 and Figure 4-4.

For the group as a whole, there were 49 false acceptance errors in a total of 1500 intruder trials. The overall group false acceptance error rate for PC No. 1 was 3%, as shown in Table 4-3 and Figure 4-4.

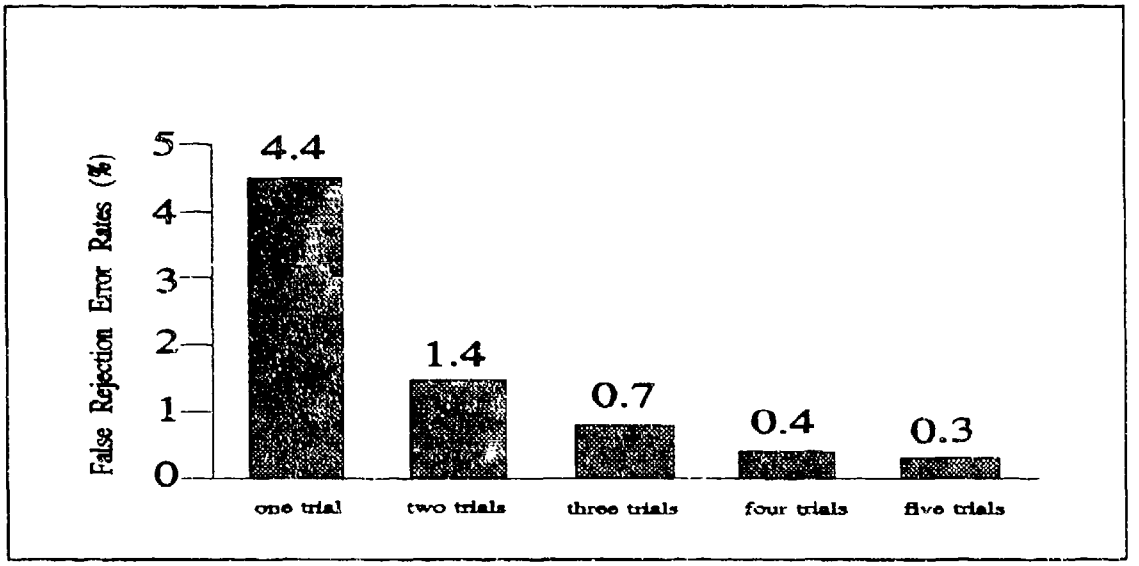

Figure 4-3. False Rejection Error Rates as a Function of the Number of the Trial on which the User Gained Entrance. The Numbers above the Bars Indicate the Rates.

2. False Acceptance Error Rates of PC No. 2

As with PC No. 1, PC No. 2 also had 12 test participants enrolled. Individual false acceptance error rates ranged from 13% to 0% (a difference of 13%). Table 4-4 and Figure 4-5 illustrate these results. For the group as a whole, there were 53 false acceptance errors in 1500 intruder attempts, for an overall false acceptance error rate of 4% (see Table 4-4 and Figure 4-5).

E. COMPARISON OF RESULTS FOR THE TWO COMPUTERS

As described in Chapter III, 24 test participants were randomly divided into two groups. Half were enrolled on each of the two IBM PCs equipped with BioPassword.

TABLE 4-3. INDIVIDUAL AND GROUP FALSE ACCEPTANCE ERROR RATES FOR PC NO. 1

Partici-pants	Identifi-cations	Passwords	False Accept-ances	False Accep-tance Error Rate (%)	Group False Acceptance Error Rate (%)
1	tester1	liweiss	0	0	
2	tester2	chiang	0	0	
3	tester3	leelee	4	3	
4	tester4	6550219	6	5	
5	tester5	137638	2	2	
6	kuanhi	happyy	8	6	3
7	yangyang	yangyang	3	2	
8	leemanying	leemanying	0	0	
9	cccccc	4086555	4	3	
10	sherman	sherman	5	4	
11	kkkkkk	1234567890	8	6	
12	wwwwww	763980	9	7	

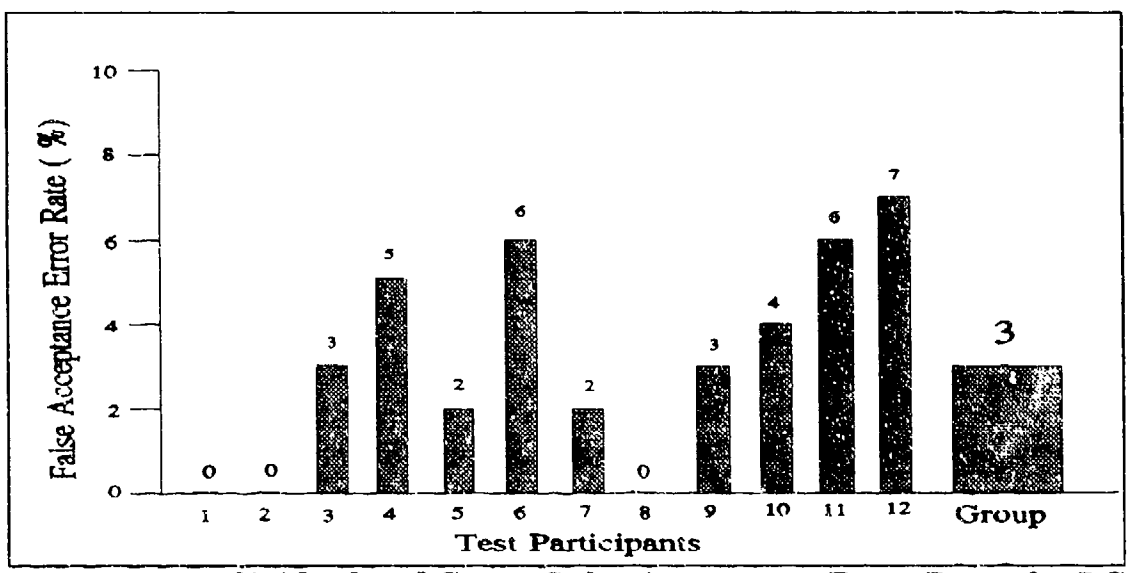

Figure 4-4. Individual and Group False Acceptance Error Rates for PC No. 1. The Numbers above the Bars Indicate the Rates.

TABLE 4-4. INDIVIDUAL AND GROUP FALSE ACCEPTANCE ERROR RATES FOR PC NO. 2

Participants	Identifications	Passwords	False Acceptances	False Acceptance Error Rate (%)	Group False Acceptance Error Rate (%)
1	chieno	thailand	1	1	4
2	fffff	fuchen	16	13	
3	llllll	huifeng	5	4	
4	cccccc	rocchang	1	1	
5	yinyin	yinyin	4	3	
6	8178pp	wtli406	1	1	
7	tester5	hanhan	2	2	
8	tester8	87654321	0	0	
9	llllll	chalie	11	9	
10	wwwwww	wangle	4	3	
11	bbbbbb	louisp	3	2	
12	fffff	frand1725	5	4	

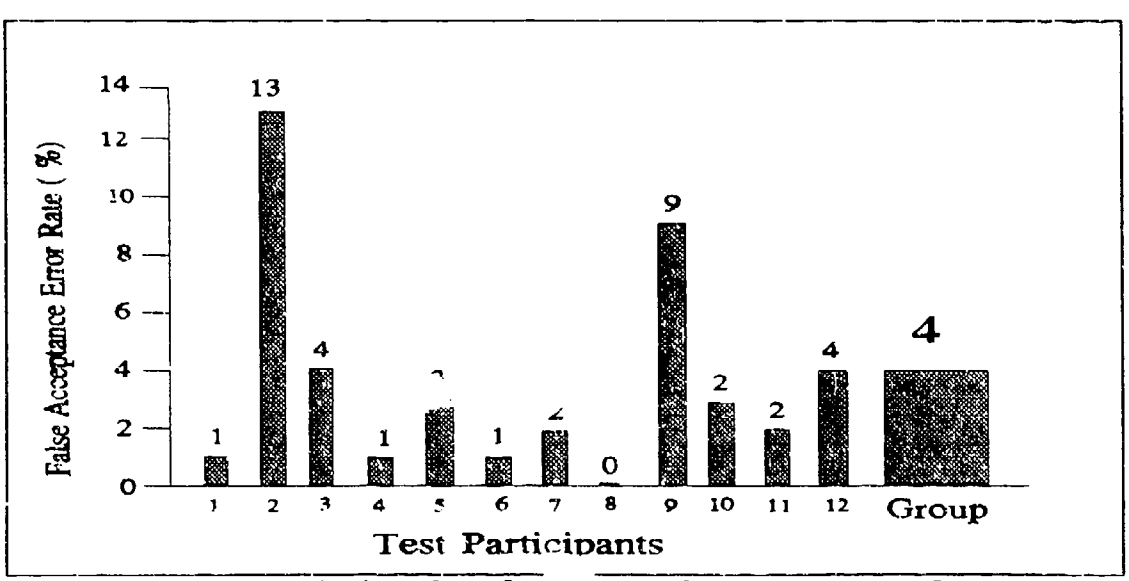

Figure 4-5. The Individual and Group False Acceptance Error Rates for PC No. 2. The Numbers above the Bars Indicate the Rates.

Overall false rejection error rates for PC No. 1 and PC No. 2 were 24% and 21%, a difference of 3%. Result of a t-test indicates that these results are not statistically different (df=11, t=-1.03, $p<0.05$). Similarly, false acceptance error rates were 3% for PC No. 1 and 4% for PC No. 2. This difference also was not significant (df=11, t=-0.08, $p<0.05$).

Since results for the two systems were not significantly different, they were combined to give a better picture of BioPassword performance. Figure 4-6 shows the combined BioPassword false rejection error rates for the two computers. Similar results for false acceptance error rates are provided in Figure 4-7. As may be seen, the combined false rejection error rate was 22.5%. The combined false acceptance error rate was 3.4%.

The variability of the individual false rejection error rates may be partly accounted for by the participants' widely-varying typing skills. The level of complexity of the passwords that were selected by the participants also was a factor. For example, one participant, who had a medium level of typing skill, adopted the longest password string, "leemanying." It was difficult to maintain constant keystroke typing dynamics using this string of characters, and he displayed the highest individual false rejection error rate, 40%. Another test participant, also with a medium level of typing skill, used his telephone number, "6550219," as his password, keying it using the numerical keypad on the keyboard. It was very easy for him to key in these numbers; consequently he had the lowest false rejection error rate, 7%.

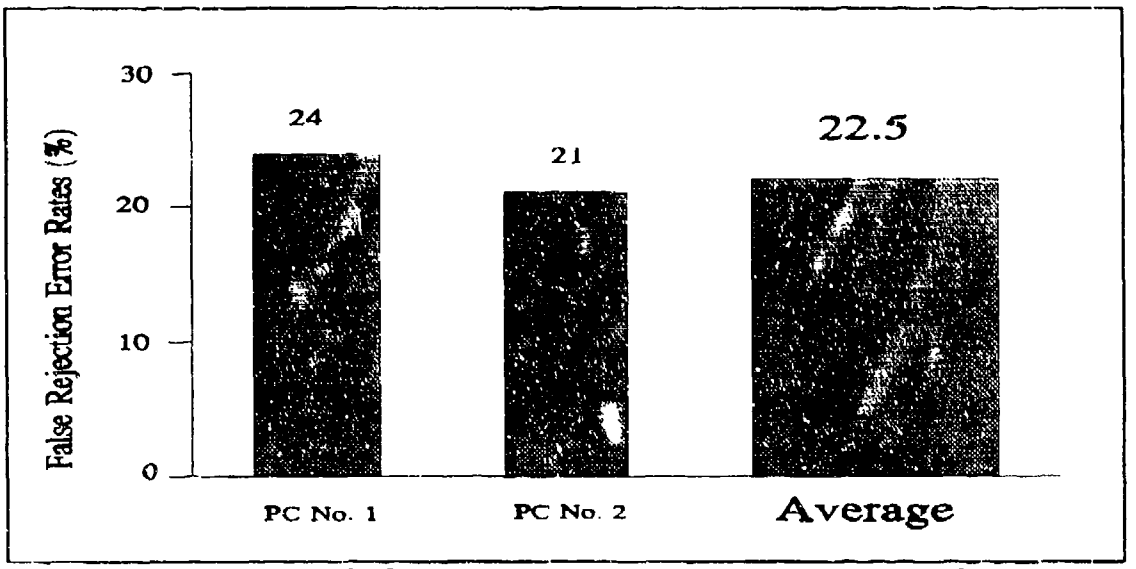

Figure 4-6. Average False Rejection Error Rates for Both Computers Combined. The Numbers above the Bars Indicate the Rates.

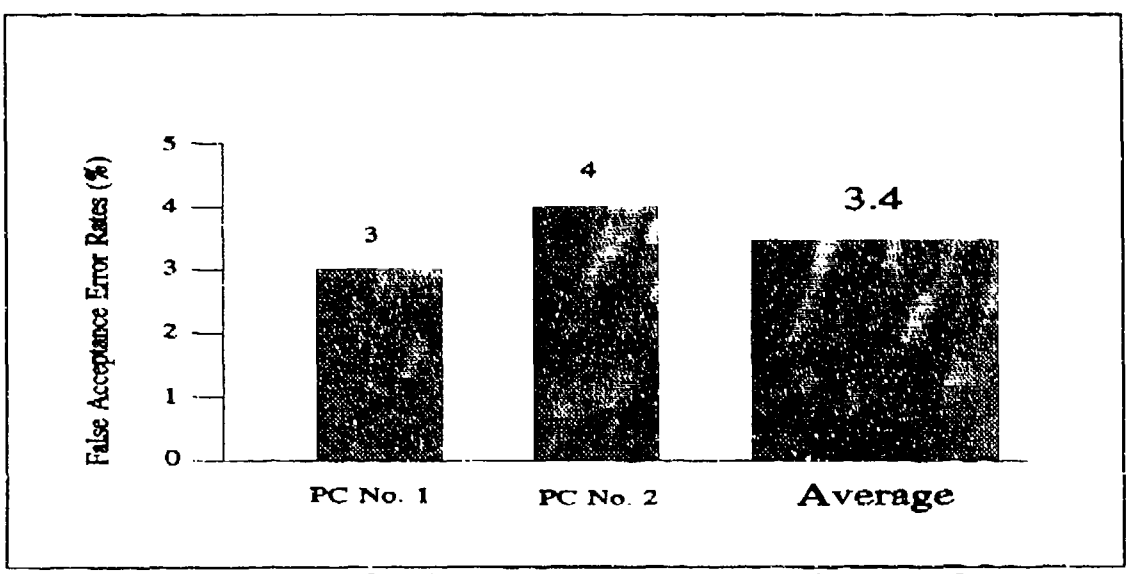

Figure 4-7. Average False Acceptance Error Rates for Both Computers Combined. The Numbers above the Bars Indicate the Rates.

False acceptance error rates displayed the opposite pattern. These rates depended on the number of practice attempts and on the complexity of the password. The passwords "1234567890," "87654321," and "yinyin" were easily typed using dynamics similar to those of the assigned user. As a result, intruder attempts with these accounts and passwords were commonly successful.

F. PARTICIPANT SURVEY

A questionnaire was distributed to the 24 test participants at the end of the test to obtain their opinions about the BioPassword system. All of the participants responded. Table 4-5 provides the results; both totals and percentages are shown. As may be noted, nearly all respondents found the concept of the system easy to understand (92%). A large majority also found enrollment easy, felt relaxed while using it, and considered the system "user friendly." However, 71% reported that logging on required concentration, and slightly over half found the system frustrating to use. A total of a 96% felt that it would not be easy for intruders to gain access if BioPassword were installed. The respondents were evenly split (50% each way) on whether they personally would buy the system.

TABLE 4-5. RESULTS OF PARTICIPANTS SURVEY

How do you feel about the BioPassword Model 2100?	Responses		
	Yes	No	Neutral
1. Is it easy to understand the *keystroke dynamics* used in it?	22 (92%)	1 (4%)	1 (4%)
2. Is it easy to enroll in?	21 (88%)	2 (8%)	1 (4%)
3. Is it user-friendly?	18 (75%)	4 (17%)	2 (8%)
4. Is it frustrating to use?	7 (29%)	13 (54%)	4 (17%)
5. Do you feel relaxed during logon procedure?	19 (79%)	5 (21%)	0
6. Does it require concentration while logging on?	17 (71%)	7 (29%)	0
7. Is it easy to intrude?	1 (4%)	23 (96%)	0
8. Would you buy it if you had a PC?	12 (50%)	12 (50%)	0

V. RESULTS, CONCLUSIONS, AND RECOMMENDATIONS

A. SUMMARY OF RESULTS

A summary of the results of the BioPassword Model 2100 performance evaluations is shown in Table 5-1.

TABLE 5-1. SUMMARY OF BIOPASSWORD EVALUATION RESULTS

Test Objectives	Results
Enrollment Time	2 mins
Verification Time	7.5 secs
False Rejection Error Rate of PC No. 1	24%
False Rejection Error Rate of PC No. 2	21%
False Acceptance Error Rate of PC No. 1	3%
False Acceptance Error Rate of PC No. 2	4%
Average False Rejection Error Rate for Both Computers Combined	22.5%
Average False Acceptance Error Rate for Both Computers Combined	3.4%
One Trial False Rejection Error Rate	4.4%
Two Trials False Rejection Error Rate	1.4%
Three Trials False Rejection Error Rate	0.7%
Four Trials False Rejection Error Rate	0.4%
Five Trials False Rejection Error Rate	0.3%
Acceptability of BioPassword to Proposed Users, Republic of China Military Officers.	Good

B. CONCLUSIONS

The results of the BioPassword Model 2100 user tests and survey of users show that the keystroke typing dynamics technology is easy to understand and is well accepted. It should be noted that BioPassword is not merely a device that uses keystroke typing dynamics technology for identification. The system also makes use of multilayer security control. The layers include (1) using an internal program for privilege control, i.e., restricting computer access to set time periods for different users as described in Chapter II, (2) providing audit functions to record computer access, (3) requiring a personal identification string and password for authentication, as is common for computers, and (4) using a biometrics technology, keystroke typing dynamics, to verify user identification via a behavioral characteristic. These sophisticated management functions greatly enhance the BioPassword security control capability, and were proven to be very effective.

As described in Chapter I, keystroke dynamics technology is based on human behavioral characteristics. Such systems are less accurate than systems based on physiological characteristics, since the characteristics can change with time. The extensive variability of individual false rejection error rates observed in this study have verified this problem. However, regular updating of the electronic signature pattern proved to be very helpful in lowering false rejection error rates.

The BioPassword system's performance was essentially the same when installed in two different personal computer systems. The difference in false rejection error rates and false acceptance error rates between the two systems was not significant. Although the average false rejection error rate, 22.5%, may seem high, the false rejection error rate for one trial is 4.4%, and drops to 1.4%, 0.7%, 0.4%, and 0.3% for the following four trials. That is, a BioPassword user has a 95.6% chance of logging on with the first attempt. If this fails, then there is a 98.6% chance of successful logon on the second attempt, and a 99.3% chance of logon on the third. This is very good performance for a device costing only $300.

The average false acceptance error rate, 3.4%, was observed under conditions where users had no limitations on practicing other users' passwords. If identifications and passwords were kept secret and practice attempts were limited, the false acceptance error rate is expected to drop to a very low value. BioPassword proved to be quite difficult to intrude, as 96% of the test participants noted.

Overall, BioPassword Model 2100 has demonstrated excellent performance at low cost for providing access control for stand-alone personal computers. The participants in the study generally found the system satisfactory for their use. The low cost of BioPassword and its successor, BioLock, is an important advantage in competing with other biometric devices. The system should be an appropriate one for the Republic of China Navy to

adopt and use for its office automation program, in conjunction with other standard security technologies and procedures.

C. RECOMMENDATIONS FOR FURTHER EVALUATIONS

The successor to BioPassword, Phoenix Software's BioLock, will be commercially available by the middle of 1992. These two device are similar, but results with BioLock still cannot be accurately predicted from BioPassword evaluations. Several recommendations for BioLock evaluations can be made, based on experience gained during this study.

- Use as large a sample size as possible.
- Classify test participants by their typing skill and use skill level to separate them into different test groups. Determine how results vary as a function of typing skills. [Ref. 3]
- Update each test participant's electronic signature regularly instead of only when this action is requested. This will make each individual's false rejection rate more accurate.
- Use a single identification and password for all intruder trials by all participants. Specify the number of allowed practicing attempts prior to each intruder trial. Change the intruder trial password once access has been falsely gained with it. Determine how many attempts it takes to gain false access with various kinds of passwords.
- Enforce an interval of at least a half a day between each set of trials. This will help ensure that trials represent random examples of typing dynamics.
- Test the system using all available threshold values if possible, to get a comprehensive picture of performance.

- Failures to log on due to typing the wrong password should be separated out by checking the *Information Integrity Report* (as described in Chapter II). The results can be used to improve the accuracy of the calculated false rejection error rate.

D. RECOMMENDATIONS FOR USE OF TYPING DYNAMICS DEVICES

Also based on this study, several recommendations can be made for any organization that intends to use keystroke typing dynamics devices for computer security.

- Include other security techniques along with typing dynamics, to provide multilayer security. Use of a variety of technologies can enhance security immensely.
- Keystroke typing dynamics are greatly influenced by human factors. These systems are not suitable for use in sites where computers must be used under emergency conditions, such as military combat units. Users cannot maintain normal typing patterns under stress.
- Choose passwords wisely; they are critical to computer security.

LIST OF REFERENCES

1. Cronin, D. J., *Microcomputer Data Security*, Prentice Hall, Inc., 1986.

2. Pfleeger, C. P., *Security in Computing*, Prentice Hall, Inc., 1989.

3. Interview between Judith Lind, Adjunct Professor, Naval Postgraduate School, Monterey, California, and the author, March 1992.

4. Daly, James, "SPA Fights Ignorance of Software Piracy Laws," *Computerworld*, 25 March 1991.

5. Alexander, Michael, "Military Sees Problems, Promise in Virus Strikes," *Computerworld*, 8 April 1991.

6. Weiss, Kenneth, "Security in a Network Computing Environment," *New Science Report on Strategic Computing*, v. 1, n. 4, April 1991.

7. Poock, Gary K., *Controlling Shipboard Access with Finger Print, Signature, and Dynamic Typing Biometrics*, draft, Naval Postgraduate School, Monterey, California, 1 October 1989.

8. Miller, B. L., *1989 Biometric Industry Directory*, Warfel & Miller, Inc., 1989.

9. Phoenix Software International, *BioLock: A Tutorial Guide*, 18 June 1991.

10. International BioMetric Systems, Incorporated, *BioPassword Model 2100 Superuser Manual*, 1990.

11. International BioMetric Systems, Incorporated, *BioPassword Model 2100 User Manual*, 1990.

12. Sandia National Laboratories, *A Performance Evaluation of Biometric Identification Devices*, by James P. Holmes, Russell L. Maxwell, and Larry J. Wright, July 1990.

INITIAL DISTRIBUTION LIST

		No. of Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5000	2
3.	Prof. Judith H. Lind, Code OR/Li Naval Postgraduate School Monterey, California 93943-5000	2
4.	Prof. Gary K. Poock, Code OR/Pk Naval Postgraduate School Monterey, California 93943-5000	1
5.	Prof. Dan C. Boger, Code AS/Bo Naval Postgraduate School Monterey, California 93940-5000	1
6.	Prof. Chyan Yang, Code EC/Ya Naval Postgraduate School Monterey, California 93943-5000	1
7.	Navy Headquarters Library Ta-chi, Taipei, Taiwan Republic of China	1
8.	Information Systems Center Bureau of Planning Navy Headquarters Ta-chi, Taipei, Taiwan Republic of China	2

9.	Naval Academy Library Tsoying, Kaoshiung, Taiwan Republic of China	1
10.	Commander Kuan, Hung-i 13th Floor, 157, Fu-sing South Road, Section 2 Taipei, Taiwan Republic of China	2