CSC-EPL-86/006

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF SYTEK PFX A2000 and PFX A2100

7 November 1986

Distribution Inside Cover

FOREWORD

This publication, Final Report of the Sytek PFX A2000 Evaluation, is being issued by the National Computer Security Center under authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center". The purpose of this report is to document the results of a sub-system evaluation of the Sytek PFX A2000 Identity Authentication System.

Approved:

Eliot Sohmer
Chief, Product Evaluations and Technical Guidelines
National Computer Security Center

FINAL REPORT
OF THE
SYTEK PFX A2000

TABLE OF CONTENTS

EVALUATION TEAM MEMBERS

Mary D. Schanken
John W. Taylor, Jr.

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

EXECUTIVE SUMMARY

The Sytek PFX A2000 product is intended to serve as a user-authentication mechanism for use with a wide range of host architectures. Since the Sytek PFX A2000 is a security sub-system rather than a complete computer system, it was not evaluated against an entire class in the Department of Defense Trusted Computer System Evaluation Criteria (August 1983), hereafter referred to as the "Criteria". Rather, it was assessed as to how well it performed User Authentication and Audit of the PFX A2000 system events.

The Sytek PFX A2000 system is a user-authentication mechanism intended for implementation with Automated Data Processing (ADP) systems which either lack a user-authentication capability or require additional authentication assurance. The PFX A2000 product is an IBM PC/AT resident, Challenge/Response device that acts as a back end server to a host machine. It supplies a host machine with a seven-digit "challenge" and one or two valid "responses", a seven-digit password that matches passwords generated by the hand-held PassPort.

The evaluation team has determined that the PFX A2000 system (requiring a PC/AT) and its counterpart, the PFX A2100 (requiring a PC or PC/XT - see Appendix), are useful and effective user-authentication mechanisms. The PFX A2000 system can provide user authentication for computer security designs lacking such a feature or, by using it in conjunction with an existing authentication mechanism, can enhance authentication assurance. Once operational, the product constitutes a reliable authentication device which satisfies vendor claims regarding its user-authentication capabilities (i.e., as described in the PFX A2000 Identity Authentication System Reference Manual, November 1985). Vendor claims, for the most part, refer to only two of the Criteria's requirements for User Authentication, the capability to identify each system user, and Audit, the capability to associate each user action with an auditable event. The PFX A2000 product is able to uniquely identify each user and audit PFX A2000 console events while providing protection for it's authentication data.

Since the PFX A2000 data base and associated software reside on the IBM PC/AT, only a knowledge of the host system application language and present security features is needed. The PFX A2000 Reference Manual provides adequate pseudocode for implementation on the host machine in order to pass communications to the PFX A2000 and receive the challenge and valid response(s). Because of this and the use of one-time challenges, the user-authentication data is protected. Even if the host machine does not protect this system code from use, a malicious user, by using the system calls to the PFX A2000, may only access a challenge

and response combination that immediately becomes invalid. For this password to be used, the malicious user would have to log-off and try to log-in to the user's account using the challenge/response combination he received earlier. However, the host machine would now ask the PFX A2000 to generate a new challenge and response which will not be the same as the one the malicious user has attained.

It is important to note that, like the host it serves, the PFX A2000 server (IBM PC/AT) is only as secure as the physical environment it is placed within. The PFX A2000 Reference Manual suggests that the same physical security be given to the PFX A2000 server as is given to the host machine. In addition, the IBM PC/AT should only be used as the PFX A2000 server and not as a multipurpose workstation. If the PFX A2000 server were to be routinely used as a workstation by someone other than the PFX A2000 system administrator, the user data base and PFX A2000 software might be open to corruption.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center (DoDCSC) was established at the National Security Agency. It's official charter is contained in DoD Directive 5215.1. In September of 1984, National Security Decision Directive 145 (NSDD-145) expanded these responsibilities to include all federal government agencies. At that time, the DoDCSC became known as the National Computer Security Center (NCSC).

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems, that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information, and assisting in the incorporation of computer security requirements into the systems acquisition process.

The NCSC Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multipurpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Sub-system Evaluation Program.

The goal of the NCSC's Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements in existing installations.

Sub-systems considered in the program are special-purpose products which can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of governmental departments and agencies. For the most part, the scope of a Sub-system Evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment or computer system on which the sub-system may be implemented. To promote consistency in evaluations, and where appropriate, an attempt is made to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. In addition, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be made available to the public by placing it on the Evaluated Products List (EPL).

The final evaluation report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT DESCRIPTION

PFX A2000 Overview

The Sytek A2000 system is a user-authentication mechanism intended for implementation on ADP systems which either lack a user-authentication capability or require additional authentication assurance. The A2000 product is a Challenge/Response device. It runs on a stand-alone IBM PC/AT and supplies the host machine with a seven-digit "challenge" and one or two valid "responses", a seven-digit password that matches passwords generated by the user's hand-held PFX PassPort.

The PFX A2000 System consists of:

- an IBM Personal Computer AT
- 512 Kb RAM minimum
- 20 Mb Winchester Drive
- 1.2 Mb Diskette Drive
- 1 (or optionally two) serial ports
- 1 parallel port (optional)
- Monitor and controller card
- Printer (optional)
- IBM Personal Computer XENIX Operating System
- the A2000 software package
- hand-held PassPorts (one per user, these remain in the possesion of the individual user)

The PFX PassPort is a portable, battery-powered, pocket-sized Personal Password Generator, similar to the calculators designed to be carried with a checkbook. It has a 24-key keypad (6x4) which performs basic calculator functions. The PassPort is designed to serve as a host hardware-independent, password-generating device which, in concert with host software and the PFX A2000, provides a mechanism for controlling access to a specific computer system, network, data unit, or program.

The IBM PC/AT (or compatible) running the XENIX operating system is needed to support the PFX A2000. It's serial port(s) is intended for use in communications with the host computer. The optional parallel port and printer are suggested requirements for reasons described later. It is also necessary to write approximately five one-page procedures on the host machine to communicate with the PFX A2000.

While the process for generating the challenge and responses is quite complex, the actual use of the A2000 system and PassPort device is quite simple. First, a typical host user must make the necessary connections to the host machine either by hard wiring or by dialing up via a modem. He must then enter his personal identification to the host system (in most systems a last name). The host machine passes this information to the PFX A2000 via an

RS-232 cable connecting the two machines. The PFX A2000 then does a table look-up in the data base for the personal identification name and retrieves the seed information associated with that name. Following this procedure, it retrieves a pseudo-random challenge, combines this with the seed information previously retrieved, and develops one or two responses. The PFX A2000 passes the challenge and valid responses to the host machine via the same RS-232 cable that it received the user personal identification on. After receiving the challenge and responses, the host machine displays the challenge information on the user's terminal. The user places his PassPort into identification mode by pushing the red button on the keypad. The passport then prompts the user for his PIN, a four- to eight-digit decimal string. The user enters his PIN, which is not echoed, to the PassPort. The ?assPort then prompts the user for the challenge displayed on the user's terminal and then combines this information with the key information stored within and generates a response. This response is then displayed on the PassPort's LCD display. The user types this response to the host machine's prompt. It is the responsibility of the host machine to compare this response with the one returned by the PFX A2000 and either allow or deny access to the user. This process and system configuration is depicted in Figure 1.

```
                                       Secure Environment
                                    +-----------------------+
                                    |                       |
 o      +-----+      +-----+        |   +-----+             |
/|\     | PIN |      |     |________|___|     | Host        |
/ \     | Key |      |xxxxx|        |   |     | Machine     |
        +-----+      +-----+        |   +-----+             |
user    PassPort     terminal       |      |                |
                                    |      |                |
                                    |   +-----+             |
                                    |   |     | PFX A2000   |
                                    |   |xxxxx|             |
                                    |   +-----+             |
                                    |                       |
                                    |                       |
                                    |   +-----+             |
                                    |   | PIN | PassPort    |
                                    |   | Key |             |
                                    |   +-----+             |
                                    |                       |
                                    |      o                |
                                    |     /|\               |
                          +---------+     / \               |
                          |                                 |
                          | PFX A2000 System Administrator  |
                          |                                 |
                          +---------------------------------+
```

Figure 1. PFX A2000 General System Interactions

PFX A2000 Features

First and foremost, the PFX A2000 system is a customized data base back-end processing machine that runs on the IBM PC/AT. It also acts as a server in that it accepts requests from the host resident, customer written software for valid challenges and responses. After this is understood, the application and use of this package can be easily comprehended. As a database machine, the PC/AT running the PFX A2000 system has various database management commands that it needs for basic maintenance such as "Add User", "Change User", and "Delete User". These database maintenance commands are only accessible by an authorized PFX A2000 System Administrator from the PFX A2000. For a user to be an authorized PFX A2000 System Administrator, a special software switch must be set when the user is added to the data base. As users are added to the data base, a secret key of 20 octal digits is randomly generated and associated with that user's personal identification. This secret key contributes to the uniqueness of each PassPort device. The key is entered into the PassPort by the system administrator and becomes the seed information by which each device generates responses from challenges.

The hand-held PassPort has it's own security features. Either the system administrator or the user may enter the PIN information (either one or two PINs) into the PassPort. Each PIN can range from four to eight digits in length and is treated as a string. For example, the PIN "9090" is not the same as the PIN "09090". Also, the PassPort functions even when an incorrect PIN is entered but generates an incorrect response. This eliminates the possibility of a malicious user randomly trying PINs until the PassPort allows him to proceed by entering a challenge. The PassPort, host, and PFX A2000 can work in conjunction to enable a stress response. By enabling the second response in the PFX A2000, it will return two responses rather than one to the host. The PassPort, by enabling the second PIN, will return the second response when this PIN is entered. When the host compares these two responses, it may determine that the user is under stress to perform this action and may take action as directed by the System Security Administrator, such as pretending it is not functional at the time.

The PFX A2000, because it is host-independent, maintains its own audit log for all its events. These audit entries contain the date, time, user, and action.

There are implementation peculiarities of this product which should be noted. Because the PFX A2000 system will be implemented in conjunction with host systems having different architectures, the specific subroutines located on the host system must be tailored to each customer's operating system and security design. As a result, the customer must write approximately five relatively short, about one page each, subroutines on the host system to be incorporated as part of the system's log-in procedure. These subroutines, written in detailed pseudocode, can be found in an appendix of the PFX A2000 Reference Manual. Source and executable code for the PFX A2000 system are provided with the installation diskettes.

An assumption of this authentication system is that each user will maintain possession of his own PassPort and will immediately report its loss. This will enable the system administrator to void the lost key on the data base and a new key and PassPort can be issued. This, however, is simply a security precaution since the malicious user has a better chance (by a ratio of better than 10:1) of randomly guessing the correct response than guessing the correct PIN (string of 4 to 8 digits) for a PassPort. The chances of guessing the correct PIN on the first attempt are one in 111,110,000 and steadily increase from there. On the other hand, the chances of guessing the correct response for a challenge are one in 9,999,986 (due to digit weighting) unless two responses are valid. Then the chances of guessing the correct response for a challenge are one in 4,999,993. One benefit of linking the authentication process to a physical device is that it becomes obvious to the user when his authentication capability may have been compromised (i.e., the PassPort has been lost). Another point of importance is that the PFX A2000 protects its data base from unauthorized access because it is a back-end data base machine and is separate and independent from the host system. For any user to access the data base to change or view the information stored within, he must log in on the PFX A2000.

DOCUMENTATION OVERVIEW

All of the technical information relating to the PFX A2000 system was obtained either through discussion with its designers, by review of the product documentation, or by testing. The PFX A2000 system documentation is primarily for those individuals responsible for installing the product on the host system. It assumes that these technicians have a sound understanding of what factors must be considered when interfacing feature-specific software within the host's operating system, data structures, and security design. A brief description of the documentation referenced by the evaluation team is provided below.

PFX A2000 Identity Authentication System Reference Manual

This document presents a thorough overview of the PFX A2000 system. It contains:

- a general overview of the system
- the installation manual for the A2000 software package
- a detailed account of each command associated with maintaining the data base
- a PassPort preparation guide for the system administrators
- the software requirements necessary for installation on the host system
- the interface specifications for communications between the two machines
- a PassPort operations manual
- the technicai specifications for the PFX A2000 and PassPort

It is intended for use by the system installers and administrators for installing and maintaining the data base and preparing the PassPorts for use.

PFX PassPort User's Manual

This document provides a detailed description of the operation of the PFX PassPort device. There is also a supplement to this document for detailed instructions in setting the PIN for the PassPort. Both documents are included with the PassPort device. The supplement may be removed if the system administrator wishes to set the PINs rather than allowing the user to set his own.

Polonius Pad Schematic

This document contains a schematic representation of a PassPort. Because of this, Sytek considers this document to be proprietary. Sytek therefore reserves the right to refuse requests for this document.

PFX Algorithms

This document contains the algorithms for challenge generation and response computation. Since the Center does not directly evaluate or comment upon the strengths or weaknesses of algorithms, this document was simply used to provide additional assurance in the uniqueness of each challenge/response combination. This document is considered proprietary by Sytek and they reserve the right to refuse requests for this document.

XENIX Installation and Operations Guides

These documents were used by the team to look for security-relevant flaws within the XENIX system that would affect the security performance of the PFX A2000 system. It must be noted that the team did not evaluate the XENIX operating system itself, but rather those aspects which could introduce problems in the operation of the PFX A2000.

PRODUCT FUNCTIONALITY

Test Procedures

As was stated in the Product Overview section of this report, the PFX A2000 system does not arrive at the customer's site fully operational. The customer must provide approximately five implementation-dependent software subroutines to complete the communication links between the host machine and the PFX A2000. The customer must also initialize the PassPort devices.

This brief review of the product's implementation process relates directly to the evaluation team's approach in testing the PFX A2000 system. Since the PFX A2000 also has a command which allows the console to act like the communication ports, the team chose to evaluate the product functionality in this way rather than evaluate code which the Center would have written.

The NCSC does not directly evaluate or comment upon the strengths or weaknesses of encryption algorithms. For this reason, testing of the product focused upon its ability to properly produce the correct challenge/response combination. There was no attempt on the part of the evaluation team to scrutinize or qualify the integrity of the PFX A2000 encryption algorithm.

Once the protection programs and security data base were installed on the IBM PC/AT, the evaluation team scanned the entire hard disk in search of visible user and key information. The team also tested the database maintenance commands it considered security relevant. The team's software testing of the product provided assurance as to the product functional correctness. Although the test suite was relatively small, the evaluation team did attempt, without success, to gain access by using incorrect passwords.

Test Results

The team unsuccessfully attempted to capture the key information stored within the PassPort device and therefore considers the hand-held device to be secure. The chip containing the key and PIN information inside the PassPort is a customized chip that only allows input from the keypad and output to the PassPort's LCD display. It is impossible, therefore, to retrieve the information without destroying the chip by stripping.

The team then attempted to capture key information from the PFX A2000. After all users were entered into the data base, the hard disk was unsuccessfully scanned for visual user and key information using the Norton Utilities. The team then entered XENIX, which is protected by a password mechanism. This password mechanism allows only valid XENIX users into the operating system. As suggested in the PFX A2000 Identity Authentication Reference Manual, all user and demonstration accounts should be removed by the system administrator at installation time for extra security measures. The protection bits, XENIX file protection mechanisms that allow read, write, and execute access to files, are not modifiable from the PFX account, but by setting the protection bits from the super user account, the team was able to access the database maintenance software from another user account by following the tree structure within XENIX.

To bring the PFX A2000 up for operation or maintenance, there are three layered checks which must be passed. This is independent from bringing the host up. First, the user must log into XENIX as "PFX" and know the proper XENIX password for that account. Second, the user must be able to produce a valid Master Key Diskette or have knowledge of the Master Key, which is a 28-digit hexidecimal number. The last check before entering the system is use of the PassPort device for a challenge generated by the system. This logging in procedure for bringing up the PFX A2000 is one considered by the team sufficient for identifying database managers.

Once someone has passed this procedure, there are a number of database maintenance commands, only a few of which the team considers security relevant. The first of these commands is the "Change User" command. The "Change User" command allows the database administrator to change the user's key information or biographic data in the data base. The team feels that this command is secure because the user's key information is not echoed to the console screen but rather suppressed. This is equivalent to a system administrator being able to change password information without being able to see the previous information in a password system. However, this command, along with the "Add User" command, has no assurance that the user's key information will not duplicate another user's key information.

The second command is the "Set Master Key" command. This command is used to change the Master Key on a valid Master Key Diskette. It then re-encrypts the data base using the new Master Key. However, when invoked using a write-protected diskette, this command will update the data base using the new master key without writing the key to the disk. After this, it is possible to continue to use the PFX A2000 system but the master key must be entered manually. Because of this flaw, there is no means to create a new valid Master Key Diskette and it becomes impossible to change the master key again.

The last security-relevant database maintenance command is the "View Log" command. This command enables the system administrator to view the audit log containing all events that have taken place at the console. It must be noted that this command will not print the entire audit log, but only the latest portion of about 50 previous entries. This is also the case when the audit log is spooled to the printer. This can be remedied by entering XENIX as the super user and printing the file from there. Another problem the team found with the audit mechanism is that it does not warn the system administrators as it becomes full. When the primary audit log becomes full, it is moved to a second file. When the primary audit log becomes full again, it rotates the new file to the old one and overwrites the oldest information in the oldest file. Although both files combined will hold 10 Mb of audit information, the team has found this way of dealing with audit overflow unacceptable. These problems can be circumvented by the use of the real time audit trail available on the system. The real time audit mechanism for the PFX A2000 system is a background process which captures each entry as it is written to the audit log and writes it to the printer. This can be enabled from the system maintenance mode. Because of these audit difficulties, the team strongly recommends the addition of a printer to the PFX A2000 system.

The team also finds the need for minimal protection of the host communication software. Although a user will not gain any useful information by using the system calls to access challenge and response combinations, the host software must protect a user from directing the requests for challenge/response combinations to himself. For example, a user may redirect the requests for challenges and responses to his terminal. He may then log in to the host machine using another user's personal identification and enter the challenge and response combination he wishes to use. The team therefore feels that write protection must be enforced on the host machine software to eliminate this possibility.

In summation, the PFX A2000 system does provide a useful and effective user-authentication capability to host systems lacking such a feature or to computer security systems requiring additional user authentication. The product is able to uniquely identify each system user. However, there are minor security flaws in the database management system software which can be easily mended using conventional mechanisms available to the customer.

As mentioned earlier in the report, the functional integrity of the protection software and security data base are minimally dependent upon the degree of protection provided to them by the host's security system. It is for this reason that the PFX A2000 system is well suited for integration with any host system having or lacking any type of security protection.

APPENDIX

PFX A2100

The Sytek PFX A2000 has a sister system, the Sytek PFX A2100, designed to run on an IBM PC or compatible. Since both are functionally equivalent, the team decided to add this appendix to cover the differences between the two systems rather than issue two separate reports.

The first and most prominent difference is in the hardware configuration. The Sytek PFX A2100 system software is able to be run on an IBM PC or compatible using DOS 3.0, whereas the Sytek PFX A2000 is restricted to use on an IBM PC/AT or compatible using XENIX. This configuration, along with the difference in the Operating System, introduced a number of software changes the team investigated.

The first of these changes is the protection of the user's seed information. The information is stored on a floppy disk and was easily accessed by the team. Unlike the Sytek PFX A2000 system, the Sytek PFX A2100 does not encrypt the user's seed information. The second of these changes is in the boot procedure of the PFX A2100. This system does not require the PFX A2100 System Administrator to use a PassPort or Master Key, eliminating the three-level check used by the PFX A2000. Therefore, the security of the user's seed information is dependent upon the physical security of this one floppy. Sytek suggests that this disk be treated with the utmost protection and be locked away when not in use.

The PFX A2100 system must load the entire data base into the PC before attempting to accept identification requests. This information would be vulnerable to capture from the PC's memory, except that the PFX A2100 disables the "escape to DOS" sequences and performs a warm boot upon exit. This clears the PC's memory and the team finds this protection adequate.

Unlike the PFX A2000, the Audit Trail is not kept on a disk. It is, however, spooled to the printer and is similar to the real time Audit Log available on the PFX A2000. The team feels that a printer is necessary with the PFX A2100 system since no Audit Log is kept without it.

The last difference is in the "Change User" command. This command now echoes the user's seed information. This also requires the physical security of the system during use.

The Sytek PFX A2100 system, like the Sytek PFX A2000 system, does provide a useful and effective user authentication to host systems lacking such a feature or enhance computer security systems that require additional user-authentication assurance.

The product is able to uniquely identify each system user despite minor security flaws in the database management system software, which can be easily mended using conventional mechanisms available to the customer and basic physical security measures.

As with the A2000, the functional integrity of the protection software and security data base are minimally dependent upon the degree of protection provided to them by the hosts security system. It is for this reason that the PFX A2100 system is well suited for integration with any host system having or lacking any type of security protection.

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION
Unclassified

1b RESTRICTIVE MARKINGS

2a SECURITY CLASSIFICATION AUTHORITY

2b DECLASSIFICATION/DOWNGRADING SCHEDULE

3 DISTRIBUTION/AVAILABILITY OF REPORT
public release
distribution unlimited

4 PERFORMING ORGANIZATION REPORT NUMBER(S)
CSC-EPL-86/006

5. MONITORING ORGANIZATION REPORT NUMBER(S)
S 228,382

6a NAME OF PERFORMING ORGANIZATION
National Computer
Security Center

6b OFFICE SYMBOL (If applicable)
C1

7a NAME OF MONITORING ORGANIZATION

6c ADDRESS (City, State and ZIP Code)
9800 Savage Road
Ft. George G. Meade, MD 20755

7b. ADDRESS (City, State and ZIP Code)

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 NOS.

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT NO

11 TITLE (Include Security Classification)
Final Report Sytek PFX A2000/2100

12 PERSONAL AUTHOR(S)
Schanken, Mary D.; Taylor, John W.

13a. TYPE OF REPORT
FINAL

13b TIME COVERED
FROM ________ TO ________

14 DATE OF REPORT (Yr., Mo., Day)
861107

15 PAGE COUNT
19

16 SUPPLEMENTARY NOTATION

17 COSATI CODES

FIELD	GROUP	SUB GR

18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
NCSC, TCSEC, sub-systems, Sytek, PFX A2000, PFX A2100, Identification, Authentication (KT)

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

The Sytek PFX A200 and A2100 systems were evaluated against the authentication, identification, and audit requirements specified by the DoD Trusted Computer System Evaluation Criteria, dated 15 August 1983. It is a user-authentication mechanism for use with computer system which either lack user-authentication capability or require additional assurance. The PFX A2000 system is a "challenge/response" device. A hand-held PassPort device is used to combine the challenge with seed information to generate a seven-digit response which allows the user to gain access to the host computer system. This report documents the evaluation of this product. Keywords: computer programs, computer security, Test and evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. □ DTIC USERS □

21 ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a NAME OF RESPONSIBLE INDIVIDUAL
LTC L. Dain Gary, USA

22b TELEPHONE NUMBER (Include Area Code)
(301)859-4458

22c OFFICE SYMBOL
C12

EDITION OF 1 JAN 73 IS OBSOLETE

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

☆U.S. Government Printing Office : 1987 -1302/1348