CSC-EPL-91/001

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

SECURITY MICROSYSTEMS, INC.

LOCKIT PROFESSIONAL

27 March 1991

FINAL EVALUATION REPORT

Security Microsystems, Inc.

Lockit Professional 2.10

NATIONAL
COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

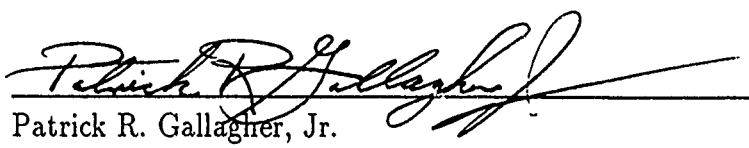
27 March 1991

CSC-EPL-91/001
Library No. S236,003

FOREWORD

This publication, the Final Evaluation Report of Security Microsystems, Inc.Lockit Professional 2.10 is being issued by the National Computer Security Center under the 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 the Security Microsystems, Inc. evaluation. The requirements stated in this report are taken from the *Computer Security Subsystem Interpretation* of the *Department of Defense Trusted Computer System Evaluation Criteria* dated 16 September 1988.

Approved:



Patrick R. Gallagher, Jr.
National Security Agency /
National Computer Security Center

27 March 1991

ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals, who were provided by the following organizations:

Paul A. Bicknell
Christine M. Chiles
Hilary H. Hosmer
Harold J. Wolfe

The MITRE Corporation
Bedford, MA

Trusted Product and Network Security Evaluations Division
National Security Agency
Fort George G. Meade, Maryland 20755-6000

Contents

EXECUTIVE SUMMARY

The National Security Agency (NSA) / National Computer Security Center (NCSC) examined the security protection mechanisms provided by Security Microsystems, Inc.'s Lockit Professional 2.10. Lockit Professional 2.10 is a subsystem, not a complete trusted computer system. It was therefore evaluated against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC).

The computer security features evaluated were Discretionary Access Control (DAC), Identification and Authentication (I&A), Object Reuse (OR), and Audit (AUD).

The evaluation team determined that the highest rating at which Lockit Professional 2.10 satisfies the DAC, I&A, Audit, and Object Reuse requirements of the CSSI is class D.

To obtain the level of trust described in this report, Lockit Professional 2.10 must be configured in accordance with the Trusted Facility Manual and properly administered. The security features above are rated only when Lockit Professional 2.10 is attempting to protect information on the hard disk drive of an IBM PC system or a system of compatible architecture. This generally implies all systems based on the Intel 8086, 8088, 80286, 80386 and 80486 architecture running the MS/PC-DOS operating system, versions 2.0 or greater.

LOCKIT Professional is a personal computer (PC) subsystem security product produced and marketed by Security Microsystems, Inc. (SMI) of Staten Island, New York. It consists of

- an electronic circuit card (that fits into a PC-type expansion bus slot) which authenticates users before they can boot up the system
- a set of software programs which limit the user to executing programs on a menu as configured by a System Administrator.
- supporting utilities.

The evaluation team has determined that the LOCKIT Professional subsystem provides some security protection but at the cost of putting a substantial burden on the System Administrator and limits the environment an experienced MS-DOS user might expect.

LOCKIT Professional can maintain user identification and authentication by requiring each user to enter a proper user ID and password prior to gaining access to LOCKIT Professional protected resources and LOCKIT Professional facilities.

The subsystem also provides both a hardware and software encryption capability but the evaluation team made no attempt to evaluate the strength of the data encryption algorithms used for password or file data encryption. The team only established that the data used in the functional testing was successfully transformed (encrypted/decrypted).

The evaluation team considered the inclusion of LOCKIT I Extended as part of the overall product to evaluate. After examining the functionality of LOCKIT Professional when combined with LOCKIT I Extended, it was determined that the two products are incompatible and that they should not be evaluated as a single computer security subsystem.

Subsystems are intended to add a level of assurance to an automatic data processing (ADP) system that has limited or ineffective security mechanisms. Subsystems are not intended to protect information on an ADP system which processes classified information because subsystems may not be capable of maintaining the integrity of classified information. Subsystems should not be added to a automatic data processing system for the sole purpose of processing classified or sensitive information.

Introduction

In June of 1990, the evaluation team began a subsystem product evaluation of Lockit Professional 2.10, a product of Security Microsystems, Inc.. The objective of this evaluation was to rate LOCKIT Professional against the *Computer Security Subsystem Interpretation* of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a final rating for each of LOCKIT Professional's features. This report documents the results of the evaluation. This evaluation applies to Lockit Professional 2.10 available from Security Microsystems, Inc. in June 1990.

Material for this report was gathered by the LOCKIT evaluation team through documentation and interaction with system developers.

Evaluation Process Background

The National Computer Security Center (NCSC), located within the National Security Agency (NSA), was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of trust technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program (TPEP), the Center works with the manufacturers of hardware and software products to implement and make available to the public technically sound computer security solutions. Under this program, the Trusted Product and Network Security Evaluation Division evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.

Subsystem Evaluation Program

The NCSC has recognized a 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 of the TCSEC. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations.

Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may be used as justification for processing classified material.

Subsystems considered in the subsystem evaluation program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria.* Additionally, 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, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog.*

Document Organization

This report consists of four major chapters and six appendices. Chapter 1 is an introduction. Chapter 2 provides an overview of the system hardware and software architecture. Chapter

3 provides a mapping between the requirements specified in the Criteria and the LOCKIT Professional features that fulfill those requirements. Chapter 4 provides comments from the evaluation team on the subsystem being evaluated. The appendices include a Bibliography, identification of specific hardware and software components to which the evaluation applies, acronyms used in this report, and a list of system calls available on a typical personal computer executing MS/PC-DOS.

System Overview

Security Relevant Portion (SRP)

The protection critical mechanism or the Security Relevant Portion (SRP) of Lockit Professional 2.10 consists of its hardware and software capabilities. A description of these mechanisms and their security relevant roles are described in the following two subsections.

Hardware Architecture

The LOCKIT Professional subsystem includes a separate circuit board which has the following features:

- 8 kilobytes of RAM
- a 3-volt lithium battery
- a time of day clock
- a set of dipswitches, and
- an optional DES encryption chip for hardware encryption.

The eight kilobytes of RAM are used to hold the login executable code for LOCKIT Professional, other information used in the identification and authentication of users, and various flag words used by LOCKIT. Using the dipswitches, the LOCKIT Professional's RAM can be memory mapped to become part of the extended ROM BIOS area.

The lithium battery provides backup power for the RAM (providing non-volatile RAM or NVRAM) and drives the clock even when the computer's power is off. The dipswitches establish the ROM BIOS extension location for the LOCKIT Professional board RAM chip(s). The DES encryption chip encrypts 64 bits at a time using a 56 bit key.

Hardware Access Protocol

The LOCKIT Professional board has control logic that enables the NVRAM, the clock chip and the DES encryption/decryption chip. This control logic is memory mapped and has certain locations that must be loaded with certain values, in a certain sequence to enable and disable the different portions of the LOCKIT board. Every time a LOCKIT function or utility accesses the LOCKIT board, it disables the board's RAM/ROM when it has finished using it.

An attempt to tamper with the board through this protocol, by providing invalid information in the protocol sequence, invokes a code path which will erase the contents of NVRAM.

Software Architecture

This section describes the software portion of the LOCKIT Professional subsystem. This software includes the executable code which normally resides on the LOCKIT hardware board (firmware), and the rest of the software programs and utilities which are executed in the MS/PC-DOS enviroment by the System Administrator and/or users.

The LOCKIT Professional Firmware

The following describes the software which is normally resident on the LOCKIT Professional board. The functionality of this executable code concerns itself mostly with Identification and Authentication of users prior to booting from the PC's disk.

The LOCKIT Professional firmware is installed using the HINSTALL.EXE program provided with Lockit Professional 2.10. This program is executed once prior to physically installing the LOCKIT Professional hardware board. HINSTALL.EXE first searches for any existing BIOS ROM extensions and calculates their length to determine the first available starting location for itself. This will tell the System Administrator how to set the dipswitches on the hardware board. The board is then installed in the system and HINSTALL.EXE is executed again to download certain LOCKIT Professional software to the LOCKIT board, including the initial user ID and encrypted password.

The setting of dipswitches memory maps the LOCKIT Professional NVRAM so that it becomes a ROM BIOS extension, and code within it will be executed during a power up sequence. The dipswitches on the LOCKIT Professional board allow the starting address to be set from segment C800 to EC00 in 16K word increments. This prevents the LOCKIT board from interfering with other expansion boards and ROMs.

The Boot Sequence

The following series of steps occur during a boot-up sequence on an IBM PC or system of compatible architecture.

- the power is turned on,
- a jump to location 0FFFF0H occurs which begins execution of ROM BIOS code,
- the power-on self tests (POST) are executed.
- a search is made for ROM BIOS extensions,
- since the LOCKIT board NVRAM has been memory mapped and is seen as a ROM BIOS extension, a checksum of the contents is verified to be zero, and control is passed to it,
  - the code in the LOCKIT board NVRAM moves itself to an unused area of system RAM,
  - this code in system RAM is now executed, prompting the user to login
  - a request to login is made
    * if the login fails, it is noted in the LOCKIT NVRAM and control is passed to code which sounds the alarm and enters an infinite loop with interrupts turned off (this forces a power recycle). The System Administrator sets a variable that determines the number of login attempts allowed before the failure sequence is invoked.
    * if the login succeeds, the user number is noted in the LOCKIT board NVRAM. Depending on the user, the default boot disk(ette) drive is set The If it is the System Administrator LOCKIT Professional will allow a boot from any drive. If it is not the System Administrator, only a designated drive can be used for booting.
    * control is passed back to the BIOS ROM which then continues the booting sequence.
- the ROM BIOS executes the bootstrap loader system call which reads the boot block from the disk(ette) to begin loading MS/PC-DOS.

The Logon Sequence

The details of the login sequence are as follows: The LOCKIT program displays the LOCKIT Professional screen and waits three seconds (or for any keypress) before displaying the request to enter a user ID. The user enters a user ID and is prompted for a password. The password provided by the user is not echoed on the screen and is immediately encrypted. The ASCII representation of the password in memory is cleared at this point. The user ID is encrypted and then compared to all of the stored encrypted user IDs (logon names). If a match is found, the user number corresponding to that user ID is stored in a location in the LOCKIT board NVRAM area. The corresponding encrypted password is then compared to the encrypted form of the password that was entered.

If the user ID and password are both correct, the user ID and the time according to the LOCKIT Professional clock is noted and saved in the LOCKIT board NVRAM and a determination is made as to which disk drive can be used as a boot device. LOCKIT Professional intercepts the "Get Default Disk Drive" system call and issues the "Set Default Disk Drive" system call for the correct disk drive, depending on whether the user is the System Administrator or a low level user. Only the administrator can use drive A. The information for the default is held in memory. Control then returns to the PC's BIOS ROM which begins a disk drive boot sequence.

If the user ID or password is incorrect, then the number of invalid attempts counter is incremented and the LOCKIT board clock is read and the time, date and encrypted invalid logon and password is stored in the LOCKIT board NVRAM area. If the maximum number of attempts (set by the System Administrator) is exceeded, the system enters an infinite loop, forcing a new power cycle. For more information on I&A please see page 18 (Identification and Authentication).

During the entire logon procedure, except when keyboard input is required from the user, the LOCKIT ROM software steals the keyboard interrupts to control the keyboard and prevent a CTRL-BREAK or CTRL-ALT-DEL sequence.

Miscellaneous Software/Hardware Interface

The following describes miscellaneous LOCKIT software which directly interfaces with the various components of the LOCKIT hardware.

The LOCKIT Clock

The LOCKIT clock circuit is not available to a DOS user in any way except through the use of the LOCKIT functions SMC_DATE.EXE, SMC_TIME.EXE, and SMC_CLK.EXE. The LOCKIT function SMC_CLK.EXE sets the PC's time of day clock using the LOCKIT clock. The LOCKIT clock and calendar can only be set using SMC_DATE.EXE amd SMC_TIME.EXE.

The DES Encryption Chip

The optional DES encryption circuit is a standard Western Digital, NSA approved DES implementation that encrypts 64 bits at the time using a 56 bit key. The LOCKIT program PCOPY.EXE will determine if the DES chip is present in the LOCKIT board and use it as the default encryption/decryption mechanism unless the -s option is used to tell PCOPY.EXE to use its proprietary software encryption algorithm instead of the DES chip.

The Lithium Battery Power Check

The LOCKIT board comes standard with a 3 volt lithium battery. The battery is used to maintain the data in the LOCKIT NVRAM chip and to keep the LOCKIT clock going even when the computer is powered off. No circuitry is provided to determine if the battery is low or beginning to go bad. However special routines in the KEYON.COM program test the LOCKIT NVRAM for an exact match with an encrypted copy of the LOCKIT ROM information that is stored in a file called "GOOD_ROM.BIN". If the decrypted information in GOOD_ROM.BIN is different from the contents of the LOCKIT ROM, then it is assumed that the battery is starting to fail, and a warning is put on the screen and the LOCKIT ROM is reloaded from the GOOD_ROM.BIN file.

LOCKIT Professional Subsystem Software

The following describes the components of the software which are loaded on the hard disk and are partly accessible to users. This software is itemized in Appendix B.

The primary security feature requirement behind LOCKIT Professional is that a user be confined within a shell and only be able to execute programs as offered by the user's menu hierarchy.

Menus

Menus are provided by the software or are set up by the System Administrator to control the set of programs to which users have access. Each user can have a unique menu or common menus from which to choose programs to execute. A menu has room for 45 items, but sub-menus make access to additional items possible.

Users should not be able to break out of the menu enviroment. The System Administrator must include the line:

SET COMSPEC=COMMAND.COM /C

in the file AUTOEXEC.BAT to ensure that any program invoked will return to the menu shell when it terminates. Each program that is allowed to be executed by a user must be tested to make sure that this feature of MS/PC-DOS works correctly.

The LOCKIT Professional subsystem comes with two menus included. The System Menu, which is both a default menu for users and an example template menu for the System Administrator, offers the user a list of common applications such as Lotus 123 and Wordperfect to choose from. The selection is done by moving a highlighted cursor bar to the application of choice. Unfortunately, the System Menu also includes three items which should *NOT* be on a default menu:

- Norton Utilities,
- PC Tools, and
- System Administrator Menu.

A knowledgeable user could use any of these to circumvent LOCKIT's security. The System Administrator's Manual and TFM warns of the danger of these entries and suggests that they not be provided to untrusted users. The menu entry in itself is harmless if the menu item does not really exist on the subsystem.

The System Administrator's Menu provides all of LOCKIT Professional's utility programs as menu items. There also is an exit to DOS, which makes it possible to circumvent all of LOCKIT's security features. The System Administrator's Manual recommends that in security-critical situations, this menu be kept off-line on a floppy disk stored in a safe place until needed.

All other menus must be defined by the System Administrator, either by editing existing menus or by building a menu from scratch. Building a menu is accomplished through the

menu building utility MENU.EXE. Menus may contain up to 45 items, including programs, other menus, an exit to DOS, or non-executable titles.

Each user is assigned an initial menu which appears after a proper login sequence. Once the user is assigned a menu, the items on the menu or sub-menus are the only programs the user may execute.

Each menu must be given a name and is stored as a separate file with extension . MNU in the \SMC subdirectory.

The menu builder utility MENU.EXE is a LOCKIT Professional *function.* This means that it can only be executed from a LOCKIT menu. It is called by the 'CREATE OR EDIT ANY MENU' item on the System Administrator's menu. A LOCKIT function cannot be executed from a normal MS/PC-DOS command level. LOCKIT Professional functions can be invoked with a /V argument which will calculate a checksum on the executable file and compare it to checksum value stored internally in the executable file to determine whether the function's executable code has been modified. The System Administrator can set up the functions so that they always called with a /V argument.

The following are the only types of descriptors a menu item may possess:

P Executable Programs, . EXE or . COM files not requesting redirected I/O.

D DOS internal or external programs or batch files. The "D" option is used for all . BAT files or external DOS commands that request redirected I/O.

M This option may be used to call another menu from within the current menu. Menus may be nested up to eight levels deep.

T This is for non-executable title blocks on the screen. These are used to group menu items into categories and to make the screen more readable and intelligible.

F This is used only for LOCKIT Professional functions. These are special LOCKIT Professional . EXE files which will execute only from within a LOCKIT menu. These include ACCTS.EXE, AUDREP.EXE, BROWSE.EXE, INSTDATA.EXE, SMC_DATE.EXE, SMC_TIME.EXE, and MENU.EXE.

Automatic Encryption/Decryption

The menu builder program also allows an entry for each menu item which permits the automatic encryption and decryption of target files used by that menu item. The encryption/decryption is accomplished using the PCOPY.EXE function.

Confining A User Within A Directory

The WHO.COM utility retrieves information from the LOCKIT Professional board on which user is logging in and sets the value of ERRORLEVEL to the appropriate value (between one and six) depending on who has successfully logged in. This value can be examined by the AUTOEXEC.BAT file and used to place a user in a specified directory. If there is no menu item available to a user to change the working directory, the user may be confined to their own working directory.

Since LOCKIT Professional provides the capability to identify a user before transfering control to that user, batch files can be written to do whatever is necessary to protect the system before relinguishing control to that user.

Access Levels

Access levels range from 1 to 99. Each non-titled menu item in a menu is assigned an access level through the menu builder program MENU.EXE. Each user is assigned an access level through the user accounts generator function ACCTS.EXE.

The user's access level must be equal to or greater than the level of a particular menu item for the user to be able to execute that particular menu item.

Only the items on a menu which have an access level less than or equal to the user's access level appear on the user's screen. A blank line replaces non-accessible items. An astute user may infer (correctly or incorrectly) that an empty item on the menu may represent a non-accessible item.

The access level of the System Administrator's Menu is set to 99, the highest possible level, to prevent anyone who is not the System Administrator from getting into the menu.

The File Check Program

Lockit Professional 2.10 comes with a utility FILECHK.EXE which uses checksums to verify whether files have changed. A file called FILECHK.DAT containing a list of pathnames of files to verify is provided as input. A file FILECHK.CHK containing checksums is generated as output. A subsequent run of FILECHK.EXE will generate new checksums and compare the results with the previous checksums. The value ERRORLEVEL will be be set accordingly.

SRP Protected Resources

The purpose of the Security Relevant Portion of LOCKIT Professional is to mediate the data flow between, and to provide protection of, subjects and objects in the computing system.

The CSSI only identifies one category of subject. However, it does identify two different categories of objects; named objects and storage objects.

Named objects can be referred to from outside the SRP by some form of name. These objects must have an acceptable discretionary access control (DAC) mechanism between named users and named objects. *Storage objects* contain data but may not necessarily be accessible from outside the SRP. However, the SRP must provide object reuse mechanisms for storage objects.

The following sections enumerate the subjects and objects of LOCKIT Professional.

Subjects

LOCKIT Professional has two types of subjects which can act as an active entity and can access or manipulate objects, a user and a terminate and stay resident (TSR) program.

A user is an individual who executes a program from their LOCKIT menu selection.

A TSR is a program which has been terminated but is still resident in physical memory until such time that it is re-activated.

Named Objects

Named objects as noted above must have a DAC mechanism. The following is a list of these objects.

- Files
- Directories
- Disk or diskette drives

Storage Objects

Storage objects on the other hand need no DAC mechanism. They must however integrate some type of an object reuse mechanism. The following is a list of storage objects on LOCKIT Professional:

- Main Memory
- Hard Disk Storage

SRP Protection Mechanisms

This section describes Lockit Professional 2.10's DAC, I&A, Audit, and Object Reuse mechanisms.

Discretionary Access Control

The Discretionary Access Control requirements in the TCSEC are related to the need to control the accessing of system resources by users. A subsystem which provides access control capabilities is required to include the functionality for restricting access to objects as well as the means for instantiating the authorizations for objects. DAC features include the mechanisms for the distribution, review, and revocation of privileges in the operations of the subsystem, particularly during object creation and deletion. In essence, the subsystem must mediate all access attempts to protected resources on the system.

The TCSEC defines discretionary access control as:

"A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject."

A *Guide to Understanding Discretionary Access Control in Trusted Systems* [6] goes on to say that:

"DAC controls are used to restrict a user's access to protected objects on the system. . . . DAC mechanisms control access based entirely upon the identities of users and objects."

Access control is typically accomplished in computer systems by constructing representations of an *Access Control Matrix* where defined users and protected resources form matrix rows

and columns. The access that any user has to any protected resource is defined at the intersection of the user row with the resource column and is usually implemented with some combination (or singly) of *Capabilities, Profiles, Access Control Lists (ACLs), Protection Bits, or Passwords.* Capabilities and profiles represent access control matrix information by row (i.e. are defined for users). ACLs and protection bits represent the matrix by column (i.e. are defined for protected resources). Passwords are singular and represent each point of row/column intersection in the access control matrix.

LOCKIT Professional's DAC facilities focus on preventing various kinds of user access to files and directories rather than in providing users with fine-grained control of access privileges to their files.

The LOCKIT Professional DAC mechanisms are based on a combination of access profiles established for each valid user and password based encryption. The access profiles take the form of individual user specific operations screen menus and have precedence over the use of passwords (i.e. a user must have an access profile granted privilege before a password can be used). The access profiles are static and cannot change while they are managing resource access for a valid user.

The screen menus used to implement the profiles define all the operations to which a user has access, and all the protected resources on which the user can perform the operations. All profile based access control decisions are made before a user attempts any non-password related access attempt. Access control is *proactive.* All access control checks are made when a user logs in and the inclusion of an operation in a user menu implies that the user has the necessary privileges to perform that operation.

Operations defined in menus can include execution of programs such as editors, compilers, utility programs, etc. Menu operations can also include DOS operations which can be specified uniquely to identify specific objects. Menu operations which don't identify specific objects can be performed on multiple objects, nullifying any access controls over those objects. For example, if a menu operation allows an editor program to be used, but does not specify a particular file, then the user may be able to edit all file objects on the system which are known to the user.

The System Administrator is responsible for establishing user's menus and has the use of various access controlled tools to do so. A system wide default menu exists and is the initial menu displayed to users regardless of any user's privileges. However, not all operations defined in this menu will be displayed to all users. Blank lines will occur for lesser privileged users where operations are displayed for more privileged users. The System Administrator can also create unique menus for users, containing privileged operations exclusive to privileged users. The opening of these special menus will be offered as a permitted operation on the default menu, but only to privileged users. Non-privileged users will simply see a blank

line on the default menu. The System Administrator's system maintenance menu is a special menu displayed only on the System Administrator's default menu.

Access Control Decisions

Access control decisions in LOCKIT Professional are made on the basis of access levels which the System Administrator assigns to each available menu item. LOCKIT Professional does not deal specifically with named objects, rather it deals with operations which can be performed on objects by users. These operations can be configured such that groups of privileged users perform only certain permitted operations on specific objects. All operations defined in menus are assigned access levels and users' access profiles are based on the access levels assigned to each user. A user's menus will only display those operations whose access levels are dominated by the user's access level. These are the only operations and objects which the user is permitted to access. The LOCKIT Professional software will prohibit a user from attempting any other operations. The System Administrator can set access control levels ranging from 0 (low) to 99 (high) for both programs and users. For a full description of access levels, please see page 11 (Access Levels).

The System Administrator creates user accounts using the ACCTS.EXE operation from the system maintenance menu. The new user's name, password, access level, and other information, is stored in an ACCTS.DBF file in the SMC directory in the root of the protected hard disk. This data is stored in encrypted form and can be accessed only by LOCKIT Professional.

The System Administrator also creates and configures menus using the MENU.EXE operation from the system maintenance menu. The configuration of each menu is stored in a *.MNU file also contained in the SMC directory. Each menu consists of defined operations and submenus, and the access level given by the System Administrator to each. The *.MNU data files are utilized by the LOCKIT Professional software when displaying each menu.

In addition to the operations menus LOCKIT Professional provides two other categories of Discretionary Access Control (DAC):

- File protection features including:
  - File hiding, preventing files being located by users,
  - Read-only files, preventing files being written/deleted by users,
  - File encryption with a user or system-provided key; and
- Device access control features including:

- Diskette boot protection, preventing LOCKIT Professional from being suppressed by booting a private copy of DOS,
- Hard disk lock, protecting the hard disk from being reformatted or otherwise accessed if LOCKIT Professional is not running,
- Keyboard locking, preventing LOCKIT Professional being interrupted during system boot.
- Diskette read/write lock, preventing the copying of data from the hard disk to floppys.

File Access Control

LOCKIT Professional file access control mechanisms are intended to provide some control over file objects not protected specifically by menus and access levels. As mentioned before, if a user has access to an editor program via his menu and the command for the editor does not identify a specific file then the user may be able use this editor on any file object since there is no access control otherwise available for files. In an attempt to limit this global capability LOCKIT Professional instituted file hiding and the making of files read-only. This is accomplished via a *PFILE.EXE* menu command used to toggle the normal DOS hidden and read-only attributes. Hiding files will simply prevent them from being displayed by the regular DOS directory listing command. Making files read-only will prevent them from being deleted or overwritten. Both of these protection mechanisms can be overcome if a user has access to the DOS *ATTRIB* command, or can invoke the DOS "set attribute" system call.

Likewise, encryption can be used to limit other users ability to read a user's private files. Files can be encrypted and decrypted via a *PCOPY.EXE* menu command with a non DES algorithm. The PCOPY.EXE command will prompt a user for a file to encrypt/decrypt and a key. No access control exists for the files, so there is no way to limit which files a user can encrypt. Users can also request the System Administrator to automatically encrypt/decrypt files when files are accessed via menu operations or utilities. The System Administrator does this at menu configuration time.

While encryption/decryption is not considered a conventional DAC mechanism, it serves as a limited DAC mechanism in the LOCKIT Professional system. Users can specify which files are to be encrypted, and the user provides the key which becomes the password to the file. The original user who provided the encryption key to the file can share it with anyone he wants, who in turn can share it with whomever he wants.

There is a major weakness in the LOCKIT Professional encryption/decryption scheme. Anyone can request that an encrypted file be decrypted and can specify a password. The file will be put through the decryption algorithm with the provided password, whether or not it is

the correct one. Once the file is processed with the invalid password, it cannot be accessed by a legitimate user who knows the valid password. The file must be reencrypted with the invalid password before it can be decrypted with the correct password. This is a denial of service problem, at least for the file(s) that were decrypted with an invalid password. It poses serious risk to a user who might accidentally decrypt a file with the wrong password and is not able to reconstruct the mistaken password.

Device Access Control

These features were described in the hardware/software interface section, so will be only summarized here.

When LOCKIT Professional is correctly installed and the LOCKIT PC board is plugged into the system chassis the installation procedure will cause the hardware configuration of the system to be altered such that any floppy disk drives can not be used as a boot device. The protected hard drive becomes the default and exclusive boot device, preventing a user booting a private copy of the DOS operating system and circumventing the security subsystem. This floppy disk boot protection assures that the system can only be booted with LOCKIT Professional functioning normally and with all access controls in place.

Also, when LOCKIT Professional is correctly installed the installation procedure will redefine various system dependent sectors at the beginning of the protected hard disk. These sectors contribute to the hard disk being recognized by DOS as a valid partition and by altering the structure of the sectors the hard disk will only be accessible to LOCKIT Professional. This hard disk lock prevents the protection mechanisms from being defeated by removing the add on PC board and booting DOS from a floppy. If the PC board is removed the system will only boot from the floppy drive and DOS, from the floppy, will not recognize that the system has a hard disk so no data or files on the hard disk can be accessed.

Keyboard locking is provided by a special LOCKIT Professional device driver which is added to the system CONFIG.SYS file. This device driver turns off the keyboard while *AUTOEXEC.BAT* is running and there by prevents users from being able to "break out" during system boot. This device driver also provides a screen blanking and keyboard locking capability which can allow users to leave the system unattended while running non-interactive procedures. The system is unlocked by the user or the System Administrator by typing in the password.

The keyboard lock can also be set to automatically become enabled if the system is left unattended for a specific amount of time. This time limit can be set to anything between 3 and 60 minutes and is configured by modifying the keyboard lock device driver. This automatic screen blanking and keyboard locking can be selectively disabled by other LOCKIT

Professional commands.

Floppy disk read/write locks are accomplished by placing sufficient access levels on all menu operations which access any floppy drives. In this way the ability to copy files to or from floppy disks can be permitted only to privileged users.

Principle of Least Privilege

The LOCKIT Professional subsystem does not adhere to the principle of least privilege for DAC. That is, users are not given the minimal set of privileges necessary to perform their job. Since access to privileged operations are granted on an access level basis granting a user the privilege to access a special, powerful, operation will also grant that user the ability to access any and all other operations and objects at that and all lower access levels. This means that privileges are not granted individually one by one, but are given out wholesale whenever a user is granted a higher access level. User privileges are not kept small in number and tend to grow quickly as higher access levels are granted.

LOCKIT Professional's Philosophy of Access Control

LOCKIT Professional, like many PC subsystems, places most of the responsibility for DAC on the System Administrator. The System Administrator is responsible for defining what functions each user needs to perform and specifying them to the LOCKIT Professional subsystem. Whether menus or access control levels or encryption/decryption levels are used, the System Administrator is responsible for all access control on the system. This responsibility, plus checking every application program to be sure it can't break out of the LOCKIT Professional menu shell, places a considerable burden on the System Administrator.

Identification and Authentication

LOCKIT Professional's strongest feature is the identification and authentication (I&A) mechanism which validates users before the PC can be booted up.

LOCKIT Professional provides facilities for establishing, maintaining, protecting, and specifying the characteristics of the I&A information. These include:

- Encrypted user database
- Audit of login/logout events

- Non-echoing passwords
- Control of password length
- Control of valid login times
- Control of the number of permitted login attempts
- System lockup

This section begins by describing the functions and interfaces of the LOCKIT I&A subsystem, then describes its architecture including files, programs, and hardware. Finally, it evaluates the effectiveness of the I&A mechanisms.

Identification

The user cannot boot up the PC until properly identifying himself to the LOCKIT I&A subsystem via an 8 character or less user ID. At the discretion of the System Administrator, a NULL user ID is provided to permit starting up the PC by hitting the ENTER key. A second exception is provided for VISITOR and GUEST user IDs that can be used by anyone. The System Administrator is responsible for restricting the functions users with general purpose user IDs can perform via menus.

Authentication

After providing a user ID, the user must authenticate himself with a password. Initially, passwords are specified by the System Administrator and must be 8 characters in length. The System Administrator can change the minimum required length of passwords and may permit users to change their own passwords. Users may be allowed to login only on certain days of the week or certain times of day. Passwords expire after a period of time determined by the System Administrator. The System Administrator can select whether to permit a user with an expired password to change the expired password at login time and can also set parameters which will warn a user that their password is about to expire, and how much advance warning should be provided.

User Interface

The user I&A interface is menu-driven and easy to use. The basic steps in the login procedure from the user's perspective are:

- When the PC's power is turned on, the PC goes through a number of self-tests, during which the user finds that the keyboard is locked.
- A screen appears prompting for the user's ID and password and the PC's keyboard is unlocked.
- As the user types in the user ID, it is echoed on the screen. After the user enters a carriage return, the cursor prompt moves to the password field.
- As the user enters the correct password, the cursor stays in place and nothing is echoed.
- After the password is entered, the results of the authentication check are given to the user. The options are as follows:
  - If the logon name is valid and the password is correct, the user is reminded of his last logon date and time, and a user menu appears defining the user's available options.
  - If the password is correct but expired, the user may be permitted to change it and proceed.
  - If the user name and password are not correct, or if the user is logging on at a time which is not permitted, then a large warning message flashes on the screen, and the user is given a chance to reenter the name and password correctly. The number of reentry tries is preset by the System Administrator. Once exceeded, the alarm sounds, the screen flashes a large warning message, and the system locks up.

    Only the System Administrator can unlock a locked system. To do so, the System Administrator must power down the computer, then turn it on and login under the System Administrator account.
- If the logon is invalid, an entry is made in NVRAM which includes the user's ID, attempted password, and a date/time stamp. Although this entry is never transfered to the real audit log file, the audit record is stored in NVRAM and is can be reviewed by the system administrator.
- If the logon is valid a record is written to the audit log showing the event, the date and time, and the user ID.

Changing Passwords

One of the user's options (if permitted by the System Administrator) is to change their own password. The user who selects the Change Your Own Password option by moving the cursor

to highlight the appropriate line on the menu is asked to enter the new password twice. The second time is for confirmation, since passwords are not echoed to the screen.

The System Administrator Interface

The System Administrator logon interface is identical to the regular user logon interface. The only difference is that a menu with many more options appears on the screen upon successful login.

Other I&A Functions

Once logged in, the System Administrator has a number of options relating to I&A which can be accessed only from the System Administrator's menu or from a sub-administrator's menu. The System Administrator can add, delete or edit user information such as logon name, password, access level, initial menu, user name, phonenumber, mail stop and time of day. The System Administrator can assign logon names and passwords, designate days of the week and times of day that logon is permitted, change the rate of password aging. In addition, the System Administrator can set the number of incorrect logon attempts permitted before lockout. All of these functions are invoked by highlighting the name of the function on the System Administrator's menu and then following the instructions on the submenus that are called up in response.

I&A Architecture

LOCKIT Professional's I&A depends upon several components including files, programs, and hardware. These were all described above in the hardware, software, and hardware/software interface sections, so are only briefly reiterated here.

Files

All of the I&A information about users is stored in the user accounts file (C:\SMC\ACCTS.DBF). User names and passwords are also stored in the LOCKIT board NVRAM memory. ACCTS.DBF data is entered by and maintained by the System Administrator using the ACCTS.EXE function, and is encrypted. The System Administrator is responsible for securely backing up this file.

Invalid login entries: When an unsuccessful login attempt occurs, a record of the event including the "bad" user ID, date and time of day, and password used is stored on the LOCKITboard in its NVRAM. These invalid login entries are never placed in the audit log file C:\SMC\AUDIT.LOG.

Accepted login entries: When a successful login occurs, the event is recorded in the audit log file C:\SMC\AUDIT.LOG.

Programs

SMCLOGON.EXE is the main shell program in the LOCKIT Professional system which confines a user within a menu enviroment. This program is called by the AUTOEXEC.BAT file after a user logs in and brings up the first level menu.

ACCTS.EXE allows the System Administrator to build the user accounts file, ACCTS.DBF.

AUDREP.EXE allows the System Administrator to report the contents of the audit trail.

CPW.EXE permits users to change their own passwords. Users are prompted for their old password, and a new password which will be in effect on the next login attempt. No password is echoed on the screen.

Hardware

The LOCKIT Professional board. Please see page 4 (Hardware Architecture).

Auditing

The auditing report utility AUDREP.EXE function provides reports sorted by user IDs, time, and date. The results can either be output to the screen, printed, or written to a specified file.

The log file created by AUDREP.EXE is located on the hard drive C:\SMC\AUDIT.LOG and is encrypted. The log file can only be examined by the System Administrator by selecting the menu item AUDREP FUNCTIONS from the System Administrator's menu. In the TFM, it is noted that this menu item should be assigned a very high access level so that a normal user cannot get access to this menu item.

Audit Configuration

In order to activate auditing the System Administrator must select the "yes" option when installing the software. This will enable the auditing features for LOCKIT Professional. If the *Audit* option is not selected then the auditing features will not be available.

Auditable Events

The types of events that are audited are:

- valid logons,
- invalid logons, and
- invocation of a menu item.

Audit Weaknesses

Most security-relevant events are not audited by LOCKIT Professional.

- All activities of all users which do not occur within LOCKIT Professional's menu environment. If any users escapes to a DOS shell (i.e. a COMMAND.COM enviroment, the system call level, or any program which provides a variety of commands which use system calls), no activities at this level are audited.
- Once a user invokes a program from a menu item, any activities performed by that program are not audited.
- Changing the System Administrator's password is not audited.
- Changing a user's password is not audited.
- Shutting off the PC's system clock is not audited.

If an untrusted user can somehow escape to the DOS enviroment at the COMMAND.COM level or lower, it is possible that the System Administrator might not find out about this security violation for an extended period since so no system call auditing is done by LOCKIT Professional.

While failed logins are audited, their audit records are kept in the LOCKIT board's NVRAM. At no time, are they placed in the actual audit file. They may be examined and or deleted using the LOCKIT Professional VIOLS.EXE function.

Hardware LOCKIT Clock

The LOCKIT Professional software reads the LOCKIT board clock to set the time/date stamps for the AUDIT.LOG entries. It does not rely on the PC clock which may be set by a user at the program level. If a user wants to change the LOCKIT Professional clock, the user must follow the protocol set up by LOCKIT Professional board. For more detail on this protocol please see page 5 (Hardware Access Protocol).

Object Reuse

Object Reuse in trusted computer systems is related to the need to totally remove no longer needed storage objects from the computer system. This is to prevent the scavenging of data by erasing any information remaining in a released storage object. In addition, it is also necessary to revoke any authorizations to released storage objects so that users who were able to reference an object before it was released will not be able to reference it after it is reassigned to another user. Object Reuse applies to objects with storage capability. In the case of LOCKIT Professional this includes RAM memory and disk(ette) blocks.

Physical Memory

The IBM PC computer running MS/PC-DOS does not provide any object reuse functionality on its own.

Small blocks of physical memory in the IBM PC are allocated by DOS in units of paragraphs (16 bytes) via the "allocate memory block" system call from the transient program area of memory. The segment base address of the assigned memory is returned by the call. This allocated memory area will not have been cleared since its last use and may contain data originating from previous allocations. DOS operations can be used to examine this memory and recover the data.

Memory is deallocated via the "release memory block" system call. The contents of the memory block is preserved during the de-allocation sequence.

The "Execute Program" system call allocates larger sections of physical memory without clearing residual information in it, as does the program termination system call.

LOCKIT Professional uses the SMCLOGON.EXE program which calls the LOCKIT function WBOOT.EXE. WBOOT.EXE causes a CTRL-ALT-DEL type warm boot to restart the LOCKIT Professional boot-up procedure. If the CBOOT.EXE program supplied with LOCKIT Professional is renamed WBOOT.EXE the computer will perform a *COLD* boot

(i.e. initialize all RAM, prior to re-starting LOCKIT Professional on behalf of another user). A cold boot sequence will also eliminate any residual TSRs.

Disk(ette) Storage

Hard disk space is allocated and deallocated indirectly by users via DOS file operations (i.e. create, open read, write, close, delete, create subdirectory, etc.). These operations reference the physical file structure anchored on the disk. Normal MS/PC-DOS operations (DEL or ERASE) do not clear any blocks on the disk which have been released for reuse by another program or user. The blocks can be easily accessed with any of the available disk utility programs (ex. Norton Utilities, PC tools, etc.).

LOCKIT Professional has the ability to clear the blocks on a disk(ette) formerly occupied by a file through the PURGE.EXE utility. The PURGE utility can be invoked to perform a standard DOS type delete, run a single pattern of zeroes on the space occupied by the file, or run that pattern seven times.

This satisfies the Object Reuse requirement for disk resident files if it is the only mechanism which users have for deleting files. This mechanism can be set up via LOCKIT Professional's menu system.

CPU Registers

Normally, registers are not cleared between program invocations, but if CBOOT.EXE is used, a cold boot will erase the contents of the PC's registers between users.

Evaluation as a Subsystem

This chapter presents the CSSI requirements (and interpretations) for the features that were evaluated. The computer security features that were evaluated for the Lockit Professional 2.10 product are Discretionary Access Control (DAC), Object Reuse (OR), Identification and Authentication (I&A) and Audit (AUD). For each feature, this chapter states the requirements, describes Lockit Professional 2.10's efforts to meet those requirements, and concludes with a statement as to the level of requirements that have been satisfied. This pattern is continued for each of the CSSI requirements for assurance and documentation. Finally, a rating assignment section (see page 47 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

Features

Discretionary Access Control

Requirement

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Interpretation

- D1:

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

2.1.3.1.1 Identified users and objects

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/D1, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to: access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

2.1.3.1.2 User-specified object sharing

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).

2.1.3.1.3 Mediation

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows access.

- D2:

The following interpretations, in addition to the interpretations for the DAC/D1 Class, shall be satisfied at the DAC/D2 Class.

2.1.3.2.1 Single-user access granularity

The DAC/D2 class requires individual access control; therefore, the granularity of user identification must enable the capability to discern an individual user. That is, access control based upon group identity alone is insufficient. To comply with the requirement, the DAC subsystem must either provide unique user identities through its own I&A mechanism or interface with an I&A mechanism that provides unique user identities. The DAC subsystem must be able to interface to an auditing mechanism that records data about access mediation events. The evaluation shall show that audit data is created and is available to the auditing mechanism.

2.1.3.2.2 Authorized user-specified object sharing

The ability to propagate access rights to objects must be limited to authorized users. This additional feature is incorporated to limit access rights propagation. This distribution of privileges encompasses granting, reviewing, and revoking of access. The ability to grant the right to grant propagation of access will itself be limited to authorized users.

2.1.3.2.3 Default protection

The DAC mechanism must deny all users access to objects when no explicit action has been taken by the authorized user to allow access.

Applicable Features

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempt. At the D1 level, this mechanism must control access by groups of users. The DAC subsystem must also provide the capability for users to specify how other users or groups may access the objects they control.

In order to qualify for the Class D1 rating for DAC, LOCKIT Professional must satisfy these criteria. To do this LOCKIT Professional provides three basic mechanisms:

- Menus for users which determine what programs they may run and how much access they have to system resources
- File protection including:

- file hiding
- read-only files
- encryption with user or system-provided key

- Device access control including:
  - Software based hard disk lock
  - Software based diskette read/write lock
  - Software based diskette boot lock protection
  - Software based keyboard locking

LOCKIT Professional utilizes user profiles and the accessing of objects by defined groups to implement DAC. User profiles consist of the operations menus displayed for each user. When completely configured, and in a secure state, all named objects will be defined in the menus. Groups of users are established for each defined operation on a named object. Groups are identified by assigned access level and consist of all users whose access levels are equal to or dominate the identifying group access level. The subsystem determines whether users are authorized for each access by comparing the user's assigned access level with the group level of each defined operation on each named object. If the user's level dominates the level of the operation the operation is permitted and is displayed on the user's operations menu. In this way all access control decisions are done and authorizations made when a user logs into the system, before any object accesses are attempted.

In LOCKIT Professional, named objects do not have owners. All objects must be identified prior to their accessing by users, by the System Administrator. All operations allowed to be performed on the objects (from creation to deletion) must also be established by the System Administrator and entered in system operations menus with corresponding access levels assigned. With the exception of encryption, the System Administrator is the only user who can make changes to access rights. Control permission (i.e. the ability to propagate access rights) is centralized and held exclusively by the System Administrator.

Encryption provides users other than the System Administrator the ability to deny object read access to users who are otherwise in the access group and have read permission. Encryption renders the contents of a file meaningless to those users who do not possess the encryption key. Other users may still have write access to the file and be able to corrupt or delete it. Further, users who do not have the encryption key are still able to decrypt the file with an incorrect password, thereby scrambling the file and denying access to the user who originally encrypted the file.

File hiding and the making files read-only is another control capability of LOCKIT Professional. This capability makes use of DOS file attributes and is not considered particularly secure due to the number of ways available to set and clear attribute bits.

LOCKIT Professional is always invoked and seems reasonably tamperproof (See page 41, Security Testing). The subsystem gains control of the system at system boot during which the keyboard is locked out preventing users from interrupting the boot. After this LOCKIT Professional is always in operation with users having to perform I&A (thereby establishing their identity) before being allowed to access system resources. LOCKIT Professional can be circumvented or even disabled, if users are able to enter the DOS command line, either through an operations menu permitted action or by escaping from some application program. The overall security of LOCKIT Professional depends on the System Administrator disallowing DOS access from operations menus and by not allowing applications which can be escaped from being included in menus. The subsystem also utilizes a plug in PC board to protect the hard disk and prevent floppy drive DOS boots. In the event that the PC board is removed the hard disk will not be referenceable due to reformatting recognizable only to software running on the PC board.

LOCKIT Professional fails to satisfy the D2 requirements for Discretionary Access Control because single user granularity is not supported for object access and because of insufficient audit capability.

Conclusion

Lockit Professional 2.10 satisfies the D1 requirement for Discretionary Access Control.

Object Reuse

Requirement

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Interpretation

- D2:

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

Applicable Features

LOCKIT Professional comes with two different programs which perform certain levels of object reuse on memory and CPU registers; WBOOT.EXE and CBOOT.EXE. One of the two will always be invoked whenever a user logs on or the system is rebooted. The use of WBOOT.EXE does not clear all of memory or the registers but the use of CBOOT.EXE does.

The program SMCLOGON.EXE is always invoked whenever a user logs on or the system is rebooted. SMCLOGON.EXE always calls the program WBOOT.EXE. The use of CBOOT.EXE can (and should) be enforced by renaming it WBOOT.EXE.

The enforced use of the PURGE.EXE utility as the only menu item allowed to a user to delete files, will clear disk space on deallocation only. The TFM states out that the System Administrator must ensure that all users (including the System Administrator) are forced to use this utility to delete files.

LOCKIT Professional does no object reuse after the default setup of the system. With manual intervention from the System Administrator, it can be set up correctly to satisfy the object reuse requirement.

Conclusion

Lockit Professional 2.10 satisfies the D2 requirement for Object Reuse.

Identification and Authentication

Requirement

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Interpretation

- D1:

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

- D2:

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user

ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

Applicable Features

The requirement is to be able to accurately authenticate the claimed identity of a user. I&A must be at least a two-step process. The I&A subsystem must be tamperproof and always invoked. The I&A must interface with the protected system in such a way that it can reliably pass authenticated user identities to the protected system. At the D1 level, group identification is sufficient but at D2, individual identification is required. At the D2 level, the I&A subsystem shall provide for the audit logging of security-relevent I&A events.

LOCKIT Professional provides a two-step Identification and Authentication mechanism which requires users to identify themselves with a logon id, then authenticate themselves by providing a password. The user's password is not echoed and there is no indication whether a rejection is due to invalid logon name or invalid password. If the limit on the number of invalid attempts is exceeded, the keyboard is disabled and the PC enters an infinite loop which can be terminated only by turning off the PC's power followed by a login by the System Administrator.

The identification and authentication data kept encrypted in NVRAM on the LOCKIT board cannot be accessed by any unauthorized user. Any attempt to access the information on the board without knowing the hardware access protocol causes the NVRAM contents to be erased. The identification and authentication data kept on disk in the ACCTS.DBF file is encrypted and accessible only to users who have a sufficiently high access level.

LOCKIT Professional's I&A subsystem provides the ability to uniquely identify each individual ADP user.

LOCKIT Professional's I&A subsystem provides for the audit logging of some security-relevant I&A events. For example, invalid logons are logged to a RAM-based file, and valid logons are logged in the audit log file on disk.

LOCKIT Professional fails to satisfy the D2 audit requirements because other security-relevant I&A events are not logged. Examples of such events are the addition/deletion of users and changing of passwords, either by the user or the system administrator.

Conclusion

Lockit Professional 2.10 satisfies the D1 requirement for Identification and Authentication.

Audit

Requirement

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Interpretation

- D2:

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied by auditing subsystems at AUD/D2.

2.4.3.1.1 Creation and management of audit trail

The auditing subsystem shall create and manage the audit trail of security-relevant events in the system. If the other portions of the system are unable to capture data about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store data about

events if the other portions of the system are capable of creating such data and passing them on.

2.4.3.1.2 Protection of audit data

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

2.4.3.1.3 Access control to audit

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

2.4.3.1.4 Specific types of events

Data about all security relevant events must be recorded. The other portion of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

2.4.3.1.5 Specific information per event

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

2.4.3.1.6 Ability to selectively audit individuals

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

Applicable Features

The auditing features provided by LOCKIT Professional meet only a small subset of the D2 requirement.

Access to auditing data generated by LOCKIT Professional is available only through the AUDREP.EXE program which should only be accessible through the System Administrator's menu. The AUDIT.LOG file is always kept in an encrypted state.

LOCKIT Professional audits only the valid and invalid login attempts, and invocation of menu items. The audit reduction facility allows for the viewing of audit data of one or more users on a selective basis. Events which are audited do not include a success or failure indicator (except for logins). In essence, if the event is audited, the event succeeded.

LOCKIT Professional cannot detect (and hence cannot audit) an escape to DOS other than such an escape performed through a menu item. There is no capability to audit any of the activities of users who are operating outside of the menu shell environment. This implies that any security relevant actions performed by programs which are invoked by menu items are not audited. This includes all actions performed by LOCKIT Professional functions themselves.

LOCKIT Professional does not audit the following security relevant events:

- creation and deletion of files,
- opening of files,
- changes made to passwords,
- addition and deletion of users,
- setting and changing user access levels,
- setting and changing of menu item access levels,
- changes to menu files,
- to auditing characteristics,
- changes to I&A information such as allowable login times,
- introduction of programs into the user's address space (if not invoked from a menu item),
- and changes made to the system clock.

The audit data is protected from access through the DAC mechanisns including access to AUDREP.EXE (via user/menu item access levels) and encryption.

Conclusion

Lockit Professional 2.10 fails to satisfy the D2 requirement for Auditing.

Assurances

System Architecture

Requirement

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

Applicable Features

Any personal computer based on the Intel 8086 or 8088 CPU only has one domain for both the operating system and user programs. Any personal computer based on the Intel 80286, 80386, or 80486 has more than one hardware domain, but only one is used by the MS-DOS or PC-DOS operating system. Therefore, all systems under which LOCKIT Professional executes operate with only one domain for the operating system, LOCKIT Professional software, and user programs.

A system for which there is only one hardware domain (memory domain) is a more vulnerable system. Any software executing on such a system can potentially access any other part (memory area) of the system. Such a system can establish a logically separate domain using the security features of a subsystem. This is effect becomes a software based architectural boundary. Software based security boundaries tend to be weaker than hardware based mechanisms.

Security Microsystems, Inc. attempts to set up a software based architectural boundary through some anti-tampering checks as described below:

- LOCKIT Professional functions will check that they have not been modified prior to their execution. This is accomplished through the use of checksums.
- The protocol to access the LOCKIT Professional board will invoke a procedure to erase the contents of NVRAM if the handshaking procedure is not provided in a correct order. This will prevent users from accessing the code. The code which is downloaded at installation time is otherwise kept in an encrypted file. The encryption is based on a proprietary software algorithm.
- The enforced use of the FILECHK.EXE during a login sequence could help to verify that a user's files have not been tampered with, if and only if the checksums are tamperproof or encrypted. There is no documentation to indicate this.

While LOCKIT provides FILECHK.EXE to detect modifications made to files, the team found no evidence that it uses that feature to check the integrity of its menu files or other important MS/PC-DOS system files.

LOCKIT Professional 2.10 makes no attempt to protect the static memory address space occupied by MS/PC-DOS or various LOCKIT Professional programs via the use of periodic checksums to determine if any of these have been tampered with while they are in memory. A user who "escapes to DOS" can modify anything in memory or on disk without being detected.

Conclusion

Lockit Professional 2.10 fails to satisfy the D1 requirements for System Architecture.

System Integrity

Requirement

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Interpretation

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

- D1:

This requirements applies to all subsystems evaluated at any class, regardless of the functions they perform.

- D2:

There are no additional requirements for System Integrity at D2.

Applicable Features

The LOCKIT Professional board executes a self-test on a power-up sequence. LOCKIT Professional does not provide any software to test the integrity of the base system hardware or firmware. This software is provided by the supplier of the PC on which LOCKIT Professional executes. Almost all PC suppliers usually provide some diagnostics software which tests all aspects of the hardware which was purchased. LOCKIT Professional users should have this diagnostic software.

Lockit Professional 2.10 does provide a batch file (TESTSYS.BAT) which can be executed to verify the system software provided to a site or user has not been modified.

LOCKIT Professional functions can be checked for any tampering on each invocation at the cosrt of system performance.

Conclusion

Lockit Professional 2.10 satisfies the D2 requirement for System Integrity.

Security Testing

Requirement

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected

system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

Applicable Features

LOCKIT Professional software and hardware features were tested to determine that they work as documented by the vendor. Generally, all features worked as documented. There are some major weaknesses in the product which are discussed in the documentation and are pointed out in this report. System testing consisted of setting up various users with certain parameters, creating menus with various constraints to determine whether a user could be confined given the limitations of the product as advertised. Overall, the team was satisfied that the product was sufficiently tested.

The first big feature which was tested was the ability for a user to return to the DOS COMMAND.COM level even with the *SET COMPSPEC=COMMAND.COM /C* line in the AUTOEXEC.BAT file. We chose to test this with PC TOOLS which allowed the tester to return to the DOS COMMAND.COM level. (The TFM warns the System Administrator to test each program placed on the system for this weakness.) Various other programs did not display the capability to escape to DOS as did PC TOOLS, and these programs returned the user to the menu environment.

The user level versus menu item level feature was tested and seemed to work properly as did the visibility of menu items. Attempting to execute LOCKIT Professional functions from the COMMAND.COM level failed as it was supposed to. These functions did work as advertised when executing them from the menu enviroment.

Password lengths, password aging, and automatic logout features worked properly. Access to audit data was not available to the non-privileged user.

Overall, the team concluded that the product was secure if the System Administrator was willing and able to carefully set all parameters correctly, set up all user menus correctly, and enforce a site policy for security, which included a process to carefully screen programs which are to be installed and used, to ensure that users cannot use them to circumvent security under LOCKIT Professional. This requires more care than usual from most site administrators. In addition, there is no carefully documented procedure to guide an administrator through the process.

Conclusion

LOCKIT Professional satisfies the D2 requirement for Security Testing.

Documentation

Security Features User's Guide

Requirement

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Interpretation

- D1

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

Applicable Features

The LOCKIT Professional subsystem comes with a user's manual which is considered the SFUG. It is well written, guides users step by step, is easy to use, but is somewhat incomplete.

The LOCKIT Professional User's Guide introduces LOCKIT and explains how to log on, log off, use a menu, automatic logoff, and how to encrypt and decrypt files.

It omits some details which may not pertain to all users, such as the ability to change one's password, or possible restrictions on log in to certain days of the week or certain times of day. It also omits user-oriented security information which appears in the System Administrator's Manual, such as storing sensitive data on diskettes that can be locked up. There is no reference in the SFUG to the PFILE.EXE utility which gives users the ability to hide files and make them read-only. There is also no reference to the FILECHK.EXE utility used in verifying the contents of files. Overall, the team felt that the SFUG was

inadequate in providing the user with all the necessary information which they must have in order to establish a secure environment for themselves. The descriptions of many SRP protection mechanisms were not described in the SFUG, although they could be located in other documentation not normally available to end users (ie. System Administrator's Manual; Trusted Facility Manual)

The warning on encryption contains a clue on how to deny service to users with encrypted files by decrypting the file with the wrong key.

If users are allowed access to the System Administrator's Manual and the TFM, they would have a much better sense of what should be done to run in a secure environment.

Conclusion

Lockit Professional 2.10 fails to satisfy the D1 requirement for the Security Features User's Guide.

Trusted Facility Manual

Requirement

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

Interpretation

- D1:

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

Applicable Features

LOCKIT Professional comes with a System Administrator's Manual and a Trusted Facility Manual. The combination of these two documents combined form the TFM for the purpose

of this evaluation.

The LOCKIT Professional System Administrator's Manual covers installation, and all of the features offered by LOCKIT Professional. The System Administrator's Manual covers system menus, the logon accounts database and utilities, the menu-builder, the audit-report utility, the encrypt/decrypt utility, file hiding and unhiding, exiting to DOS, and preventing exits to DOS. It describes how to de-install LOCKIT Professional as well. Finally, the System Administrator's guide gives hints and tips on protecting critical files and on protecting the System Administrator's account from compromise.

The LOCKIT Professional Trusted Facility Manual covers security matters in greater detail. Topics covered are: logon procedures, password aging, minimum password length, timed access control, invalid logon attempts, access levels on menus and users, and preventing escape from the menu shell enviroment. Other topics covered are: setting file attributes, file encryption/decryption, dangerous programs which can circumvent LOCKIT Professional security, using the WHO.COM utility in batch files to enhance security, object reuse considerations, and auditing.

All of the security documentation omits the importance of physical security to prevent physical removal of the LOCKIT Professional subsystem hardware.

All necessary features used in maintaining security are available but there is no comprehensive guide to correctly set up the system in a secure manner and maintain it. The team felt that this was important given the inherent weaknesses of the system which could be overcome by better documentation. The team reasoned that most administrators could not correctly set up LOCKIT Professional in a secure manner without a great deal of experience with system security and MS/PC-DOS. In addition, a secure system requires a considerable amount of time to set up and test.

Conclusion

Lockit Professional 2.10 fails to satisfiy the D1 requirement for the Trusted Facility Manual.

Test Documentation

Requirement

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the

security mechanisms' functional testing.

Interpretation

- D1:

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

- D2:

There are no additional requirements at the D2 class.

Applicable Features

The test plan entitled *LOCKIT Professional Software System Integration and Test Plan*, received from Security Microsystems, Inc. provides an good insight on the testing done on LOCKIT Professional.

There are ten functional areas tested including installation parameters, accounts management, menu generation, audit, logon, file protection, file encryption, file browser, file erase, and file change detection.

The document provides detailed procedures for testing the major components of LOCKIT Professional. Most procedures are manual since the interface to LOCKIT Professional does not lend itself to automatic testing. The tester starts with a checklist of items to test for each program, including user inputs and error conditions for that program.

The programs discussed in the test plan include the following:

- INSTDATA.EXE
- BLDACCTS.EXE
- ACCTS.EXE
- CPW.EXE

- MENU.EXE
- AUDREP.EXE
- UNPACKAR.EXE
- PACKAR.EXE
- FILECHK.EXE
- PCOPY.EXE
- SMCLOGON.EXE
- LOGON01.EXE
- LOGON02.EXE
- LOGON03.EXE
- PFILE.EXE
- PURGE.EXE
- BROWSE.EXE

There are various tools used in testing, including one called VIEWPRO which allows viewing the contents of the LOCKIT Professional board NVRAM contents.

Conclusion

Lockit Professional 2.10 satisfies the D2 requirement for Test Documentation.

Design Documentation

Requirement

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

- D1:

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

- D2:

There are no additional requirements for Design Documentation at the D2 class.

Applicable Features

The design document entitled *LOCKIT Professional Design Document* [3] submitted by Security Microsystems, Inc. provides a very good insight in the internals of Lockit Professional 2.10 and how the hardware works. The team was impressed that SMI included a significant amount of security relevant code paths in this document. The document also specifically answered the team's technical questions which came about from the one and only team-vendor meeting.

Conclusion

Lockit Professional 2.10 satisfies the D2 requirement for Design Documentation.

Rating Assignment

This section describes the composite feature rating and how it is determined. A composite rating is assigned to each evaluated feature and is based upon the individual ratings awarded in Chapter 3. The individual ratings are the rating for each feature and ratings for assurance and documentation supporting that feature. The chart below shows a 'Y' for each assurance

or documentation requirement that is sufficient to support the rating of each feature. An 'N' indicates that the assurance or documentation requirement is not sufficient. For features that have a rating of 'D', the assurances and documentation requirements are irrelevant, and are marked 'N/A'. Using the ratings attained in Chapter 3, the composite ratings for each of Lockit Professional 2.10's features are derived as shown in the following table.

Evaluated Features	Feature Rating	Assurance			Documentation				Supporting Function	Composite Rating
		Arch.	Integrity	Testing	SFUG	TFM	Testing	Design		
I&A	D1	N	Y	Y	N	N	Y	Y	Audit [1] DAC [2]	D
DAC	D1	N	Y	Y	N	N	Y	Y	I&A [3] AUD [4]	D
AUD	D	N/A	N/A	N/A	N/A	N/A	N/A	N/A	DAC [5] I&A [6]	D
OR	D2	N	Y	Y	N	N	Y	Y	DAC [7]	D

The CSSI requires that subsystems have *supporting functions* because some features rely on one another (e.g. an auditing subsystem needs user identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

- The supporting function is provided by another feature of the subsystem.
- The supporting function is provided within the feature, even though it may duplicate some functions of another feature.
- The supporting function is provided through an interface to other products.

If the supporting function is integrated within the product, it must be at the same level as

[1] I&A events are logged on the LOCKIT Professional 2.10 board.

[2] Authentication data is protected on the LOCKIT Professional 2.10 board. Programs which access the I&A data are protected by the DAC (menu) mechanism.

[3] The DAC mechanism (menus/access levels) gets user IDs from the I&A mechanism.

[4] The DAC mechanism has an interface with the auditing mechanism to report some security relevant events.

[5] The Audit trail is protected by the DAC mechanism (access levels, menus and encryption).

[6] The Audit mechanism gets user IDs from the I&A mechanism.

[7] SMCLOGON, CBOOT and WBOOT rely on DAC protection to provide OR correctly.

that of the feature to obtain the composite rating.

Evaluator's Comments

Design of Security Subsystems

Experience has shown us that a good security subsystem for a personal computer is one which monitors and handles activities at the system call level of MS/PC-DOS. LOCKIT Professional fails in this capacity, and the team feels that this makes it a less secure and certainly more intrusive security subsystem for a PC. The security shell in LOCKIT Professional has been placed at a high level in the software enviroment, and offers little or no protection at the lower levels.

An Intrusive Security Subsystem

LOCKIT Professional is a very intrusive security subsystem for a PC in that it limits user capabilities through a menu interface from which a user can only execute certain programs or perform certain operations. The security of the system is placed in jeapordy if the user is allowed to escape this menu enviroment. Program development can only be done by "trusted" individuals. Sophisticated programs with their own shell or menu enviroment would allow users to perform actions which cannot be controlled by LOCKIT Professional.

Burden on the System Administrator

The burden of system security is placed solely in the hands of the System Administrator who must very carefully set up all menus with all the correct options, and check all the programs which are placed in the LOCKIT Professional enviroment to make sure that these programs cannot circumvent the menu enviroment. This is difficult for the IBM PC enviroment where there are literally tens of thousands of software packages, most of which do not consider security at all.

Users who can delete their own files can also delete anyone else's files unless their menu is correctly set up to specify the path of the user's home directory. If a user can examine files

with the BROWSE utility, that user can examine another person's files unless the menu is set up correctly or the other user's files are encrypted automatically.

Every program installed on this system must be thoroughly checked to determine that it cannot perform undesirable actions. All to many programs provide a mini-shell enviroment or their own menu enviroment which allow users a great degree of freedom to perform various functions which the LOCKIT Professional system cannot audit.

Overall, a viable sense of security can be achieved under LOCKIT Professional but only if the System Administrator is willing to take on such a burden. The majority of people who are system administrators will not consider all the fine points of security and there is no documentation available that points out in a clear manner how to achieve this security. There are hints, suggestions, and pointers but no overall strategy provided by Security Microsystems, Inc..

Lack of System Call Auditing

LOCKIT Professional appears to be a derivative of LOCKIT I Extended which performs auditing at the MS/PC-DOS system call level. The team was mystified as to why this auditing was not carried through in LOCKIT Professional which is a better overall product.

Dangerous Default Menus

The default menus provided by LOCKIT Professional contain entries which were deemed by the evaluation team to be inappropriate for security. Menu names or entries are harmless if the program which they should invoke does not exist.

A Weak SFUG

While the LOCKIT Professional User's Guide was inadequate in describing overall security to users, the team felt that if users are permitted to read the TFM and System Administrators Manual, they would develop a much better understanding of how to run in a secure enviroment. If these two manuals were included as part of the SFUG, then the SFUG would meet the D2 SFUG requirement.

Bibliography

[1] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985

[2] Nilescom, LOCKIT III Professional Software System Integration and Test Plan , 1990, Proprietary

[3] Security Microsystems, Inc., LOCKIT Professional Design Document, 1990, Proprietary

[4] Security Microsystems, Inc., LOCKIT Professional System Administrator's Manual, 1990.

[5] Security Microsystems, Inc., LOCKIT Professional Trusted Facility Manual, 1990, Proprietary

[6] National Computer Security Center, A Guide to Understanding Discretionary Access Control in Trusted Systems, 30 September 1987.

[7] National Computer Security Center, Computer Security Subsytem Interpretation of the Trusted Computer System Evaluation Criteria, 16 September, 1988.

Evaluated Hardware Components

LOCKIT Professional Board Version 2.10

Evaluated Software Components

LOCKIT Professional Software Version 2.10, which includes the following programs:

ACCTS.DBF – User database containing encrypted logons, passwords, etc.
ACCTS.EXE – User database modifying program, works on ACCTS.DBF
ACCTS.HLP – Help information for ACCTS.EXE
AUDIT.HLP – Help information for AUDREP.EXE
AUDREP.EXE – Audit trail sorting and displaying program
AUTOBOOT.EXE – Enable/disable automatic boot option
BLDACCTS.EXE – Builds the initial ACCTS.DBF
BROWSE.EXE – Text file displaying program
CBOOT.EXE – Causes logout to perform a cold boot if renamed WBOOT.EXE
CPW.EXE – Program to allow a user to change their own passwords
DOS.MNU – Menu of DOS commands
FILECHK.CHK – CRC values of files checked
FILECHK.DAT – List of files checked by FILECHK.CHK
FILECHK.EXE – File verification and checksumming program
FILELIST – A list of all files on the LOCKIT Professional diskette
HINSTALL.EXE – Installs LOCKIT.ROM into the LOCKIT board
INSTALL.BAT – Installs all other LOCKIT Professional software
INSTALL1.BAT – Installs all other LOCKIT Professional software
INSTDATA.EXE – Sets certain LOCKIT Professional program parameters
INSTDATA.HLP – Help information for INSTDATA.EXE
KEYOFF.COM – Device driver to turn off keyboard during boot
KEYON.COM – Turns keyboard back on and verifies LOCKIT board
LOCKIT.ROM – LOCKIT Professional board software (firmware)
LOGON01.EXE – Menuing software overlay file
LOGON02.EXE – Menuing software overlay file
LOGON03.EXE – Menuing software overlay file

MENU.EXE	– Menu builder program
MENU.HLP	– Help information for the MENU.EXE program
NEW9.COM	– Re-enables the LOCKIT board after CTRL-ALT-DEL
NUMATTS.EXE	– Sets maximum number of invalid logon attempts
PACKAR.EXE	– Packs the audit trail file after it is unpacked
PCOPY.EXE	– Encryption/decryption program
PFILE.EXE	– File attribute setting program
PURGE.EXE	– File eraser (zeroes out file contents)
READ-ME.1ST	– File containing last minute information
SCREEN1.DOC	– Installation screen 1
SCREEN2.DOC	– Installation screen 2
SCREEN3.DOC	– Installation screen 3
SCREEN4.DOC	– Installation screen 4
SCREEN5.DOC	– Installation screen 5
SET-TIME.COM	– Sets the lunch-break automatic timeout
SMC_CLK.EXE	– Sets the DOS time/date from LOCKIT clock
SMC_DATE.EXE	– Sets the LOCKIT date from the keyboard
SMC_TIME.EXE	– Sets LOCKIT board clock from keyboard
SMCLOGON.EXE	– Menuing shell program
SMCLOGON.HLP	– Help information for SMCLOGON.EXE
SYSADM.MNU	– System Administrator's menu
SYSADM2.MNU	– Second half of System Administrator's menu
SYSTEM.MNU	– System or main menu
TESTSYS.BAT	– Verifies checksums of all system files
UNPACKAR.EXE	– Unpacks Audit Log file into ASCII text
VIOLS.EXE	– Display last 16 invalid logon attempts
WBOOT.EXE	– Causes logout to perform a warm boot
WHO.COM	– Returns user number logged on as errorlevel

Acronyms

ACL	– Access Control List
ADP	– Automated Data Processing
ASCII	– American Standard Code for Information Interchange
AT	– Advanced Technology
AUD	– Audit
BIOS	– Basic Input Output System
CPU	– Central Processing Unit
CRC	– Cyclic Redundancy Check
CSSI	– Computer Security Subsystem Interpretation
DAC	– Discretionary Access Control
DES	– Data Encryption Standard
DoD	– Department of Defense
DOS	– Disk Operating System
EPL	– Evaluated Products List
FAT	– File Allocation Table
I&A	– Identification and Authentication
IBM	– International Business Machines
ID	– Identifier
IN	– Interrupt
I/O	– Input/Output
MS-DOS	– Microsoft's Disk Operating System
MS/PC DOS	– Microsoft or Personal Computer DOS

NCSC – National Computer Security Center
NSA – National Security Agency
NSDD – National Security Decision Directive
NVRAM – Non-volatile random access memory
OR – Object Reuse
PC – Personal Computer
PC-DOS – IBM's version of Microsoft's DOS
POST – Power On Self-Test
PS/2 – Personal System 2
RAM – Random Access Memory
ROM – Read Only Memory
SA – System Administrator
TCB – Trusted Computing Base
TCSEC – Trusted Computer System Evaluation Criteria
TFM – Trusted Facilities Manual
TSR – Terminate and Stay Resident

MS-DOS System Calls

The tables below display all the BIOS interrupt vectors and the MS-DOS system calls. Some software interrupts have multiple function calls which are displayed in other tables.

Int Function Summary			
Hex	Dec	Function Name	MS-DOS Version
0	0	Divide by 0	1 2 3
1	1	Single step	1 2 3
2	2	Non-maskable interrupt (NMI)	1 2 3
3	3	Breakpoint	1 2 3
4	4	Overflow	1 2 3
5	5	Print screen	1 2 3
8	8	Timer tick	1 2 3
9	9	Keyboard input interrupt	1 2 3
0A	10	RESERVED	1 2 3
0B	11	Asynchronous communications port controller 1	1 2 3
0C	12	Asynchronous communications port controller 0	1 2 3
0D	13	Fixed disk controller	1 2 3
0E	14	Floppy disk controller	1 2 3
0F	15	Printer controller	1 2 3
10	16	ROM BIOS video services (see Note 2)	1 2 3
11	17	Equipment configuration check	1 2 3
12	18	Memory size check	1 2 3
13	19	ROM BIOS floppy disk services (see Note 2)	1 2 3
14	20	ROM BIOS serial port services (see Note 2)	1 2 3
15	21	Cassette I/O, PC/AT auxiliary functions	1 2 3
16	22	ROM BIOS keyboard services (see Note 2)	1 2 3
17	23	ROM BIOS printer control services (see Note 2)	1 2 3
18	24	ROM Basic	1 2 3
19	25	Bootstrap loader	1 2 3
1A	26	Set/read real time clock	1 2 3
1B	27	CTRL-Break handler	1 2 3
1C	28	Timer control	1 2 3
1D	29	Video parameter table (see Note 1)	1 2 3
1E	30	Disk parameter table (see Note 1)	1 2 3
1F	31	Graphics character table (see Note 1)	1 2 3
20	32	Program terminate (obsolete)	1 2 3

Note 1: The contents of the vector is used as a pointer only.
Note 2: See tables below

Int Function Summary (continued)			
Hex	Dec	Function Name	MS-DOS Version
21	33	MS-DOS system services (see Note 2)	1 2 3
22	34	Terminate vector	1 2 3
23	35	CTRL-C handler address	1 2 3
24	36	Critical error handler address	1 2 3
25	37	Absolute disk read	1 2 3
26	38	Absolute disk write	1 2 3
27	39	Terminate and stay resident	1 2 3
28	40	RESERVED (28-2E hex are all RESERVED)	1 2 3
2F	47	Print spool control	1 2 3
30	48	RESERVED (30-3F hex are all RESERVED by MS-DOS)	1 2 3
40	64	Floppy disk driver (PC/XT)	1 2 3
41	65	Fixed disk parameter table (see Note 1)	1 2 3
44	68	Graphics character table (codes 0-FF) (see Note 1)	1 2 3
67	103	Expanded memory system (EMS) services	1 2 3

Note 1: The contents of the vector is used as a pointer only.
Note 2: See tables below

Int 10H (16) Function Summary ROM BIOS Video Services			
Hex	Dec	Function Name	MS-DOS Version
0	0	Set video mode	1 2 3
1	1	Set cursor type	1 2 3
2	2	Set cursor position	1 2 3
3	3	Read cursor position	1 2 3
4	4	Read light pen position	1 2 3
5	5	Select display page	1 2 3
6	6	Init window or scroll contents up	1 2 3
7	7	Init window or scroll contents down	1 2 3
8	8	Read attribute and character at cursor	1 2 3
9	9	Write attribute and character at cursor	1 2 3
0A	10	Write charactor only at cursor	1 2 3
0B	11	Set color palette	1 2 3
0C	12	Write graphics pixel	1 2 3
0D	13	Read graphics pixel	1 2 3
0E	14	Write text in teletype mode	1 2 3
0F	15	Get current display mode	1 2 3
10	16	Set palette registers	1 2 3
11	17	RESERVED	1 2 3
12	18	RESERVED	1 2 3
13	19	Write string	1 2 3
FE	254	Get video buffer (Topview)	1 2 3
FF	255	Update video buffer (Topview)	1 2 3

Int 13H (19) Function Summary ROM BIOS Floppy Disk Services			
Hex	Dec	Function Name	MS-DOS Version
0	0	Reset floppy disk system	1 2 3
1	1	Get floppy disk system status	1 2 3
2	2	Read floppy disk	1 2 3
3	3	Write floppy disk	1 2 3
4	4	Verify disk sectors	1 2 3
5	5	Format disk track	1 2 3

Int 14H (20) Function Summary ROM BIOS Serial Port Services			
Hex	Dec	Function Name	MS-DOS Version
0	0	Initialize communications port	1 2 3
1	1	Write character to communications port	1 2 3
2	2	Read character from communications port	1 2 3
3	3	Communications port status request	1 2 3

Int 16H (22) Function Summary ROM BIOS Keyboard Services			
Hex	Dec	Function Name	MS-DOS Version
0	0	Read character from keyboard	1 2 3
1	1	Read keyboard status	1 2 3
2	2	Return keyboard flags	1 2 3

Int 17H (23) Function Summary ROM BIOS Printer Control Services			
Hex	Dec	Function Name	MS-DOS Version
0	0	Write character to printer	1 2 3
1	1	Initialize printer port	1 2 3
2	2	Printer status request	1 2 3

Int 21H (33) Function Summary				
Hex	Dec	Function Name	Input Type	MS-DOS Version
0	0	Program Terminate		1 2 3
1	1	Character input with echo		1 2 3
2	2	Character output		1 2 3
3	3	Auxiliary input		1 2 3
4	4	Auxiliary output		1 2 3
5	5	Printer output		1 2 3
6	6	Direct console I/O		1 2 3
7	7	Unfiltered character input without echo		1 2 3
8	8	Character input without echo		1 2 3
9	9	Output character string		1 2 3
0A	10	Buffered input		1 2 3
0B	11	Get input status		1 2 3
0C	12	Reset input buffer and then input		1 2 3
0D	13	Disk reset		1 2 3
0E	14	Set default disk drive	D	1 2 3
0F	15	Open file	F	1 2 3
10	16	Close file	F	1 2 3
11	17	Search for first match	F	1 2 3
12	18	Search for next match	F	1 2 3
13	19	Delete file	F	1 2 3
14	20	Sequential read	F	1 2 3
15	21	Sequential write	F	1 2 3
16	22	Create or truncate file	F	1 2 3
17	23	Rename file	F	1 2 3
18	24	RESERVED		1 2 3
19	25	Get default disk drive		1 2 3
1A	26	Set disk transfer area address		1 2 3
1B	27	Get allocation info for default drive		1 2 3
1C	28	Get allocation info for specified drive	D	2 3
1D	29	RESERVED		1 2 3
1E	30	RESERVED		1 2 3
1F	31	RESERVED		1 2 3
20	32	RESERVED		1 2 3
21	33	Random read	F	1 2 3
22	34	Random write	F	1 2 3
23	35	Get file size	F	1 2 3
24	36	Set random record number	F	1 2 3
25	37	Set interrupt vector		1 2 3
26	38	Create program segment prefix		1 2 3
27	39	Random block read	F	1 2 3
28	40	Random block write	F	1 2 3
29	41	Parse filename		1 2 3

A = ASCII string, D = Drive number, F = File control block, H = Handle

Int 21H (33) Function Summary (continued)				
Hex	Dec	Function Name	Input Type	MS-DOS Version
2A	42	Get system date		1 2 3
2B	43	Set system date		1 2 3
2C	44	Get system time		1 2 3
2D	45	Set system time		1 2 3
2E	46	Set verify flag		1 2 3
2F	47	Get disk transfer area address		2 3
30	48	Get MS-DOS version number		2 3
31	49	Terminate and stay resident		2 3
32	50	RESERVED		2 3
33	51	Get or set CTRL break flag		2 3
34	52	RESERVED		2 3
35	53	Get interrupt vector		2 3
36	54	Get free disk space	D	2 3
37	55	RESERVED		2 3
38	56	Get or set country		2 3
39	57	Create subdirectory	A	2 3
3A	58	Delete subdirectory	A	2 3
3B	59	Set current directory	A	2 3
3C	60	Create or truncate file	A	2 3
3D	61	Open file	A	2 3
3E	62	Close file	H	2 3
3F	63	Read file or device	H	2 3
40	64	Write to file or device	H	2 3
41	65	Delete file	A	2 3
42	66	Move file pointer	H	2 3
43	67	Get or set file attributes	H	2 3
44	68	Device driver control (IOCTL)	H,D	2 3
45	69	Duplicate handle	H	2 3
46	70	Force duplicate of handle	H	2 3
47	71	Get current directory	D	2 3
48	72	Allocate memory		2 3
49	73	Release memory		2 3
4A	74	Modify memory allocation		2 3
4B	75	Execute program		2 3
4C	76	Terminate with return code		2 3
4D	77	Get return code		2 3
4E	78	Search for first match	A	2 3
4F	79	Search for next match	A	2 3
50	80	RESERVED		2 3
51	81	RESERVED		2 3
52	82	RESERVED		2 3
53	83	RESERVED		2 3
54	84	Get verify flag	A	2 3

A = ASCII string, D = Drive number, F = File control block, H = Handle

Int 21H (33) Function Summary (continued)				
Hex	Dec	Function Name	Input Type	MS-DOS Version
55	85	RESERVED		2 3
56	86	Rename a file	A	2 3
57	87	Get or set file date and time	H	2 3
58	88	Get or set allocation strategy		3
59	89	Get extended error information		3
5A	90	Create temporary file	A	3
5B	91	Create new file	A	3
5C	92	Record locking	H	3
5D	93	RESERVED		3
5E	94	Get machine name/printer setup		3
5F	95	Assign list entry		3
60	96	RESERVED		3
61	97	RESERVED		3
62	98	Get program segment prefix address		3
63	99	Get lead byte table (MS-DOS 2.25 only)		2

A = ASCII string, D = Drive number, F = File control block, H = Handle

Int 67H (103) Function Summary Expanded Memory System [EMS] Services			
Hex	Dec	Function Name	MS-DOS Version
1	1	Get manager status	1 2 3
2	2	Get page frame segment	1 2 3
3	3	Get number of pages	1 2 3
4	4	Get handle and allocate memory	1 2 3
5	5	Map memory	1 2 3
6	6	Release handle and memory	1 2 3
7	7	Get Expanded memory manager (EMM) version	1 2 3
8	8	Save mapping context	1 2 3
9	9	Restore mapping context	1 2 3
0A	10	RESERVED	1 2 3
0B	11	RESERVED	1 2 3
0C	12	Get number of EMM handles	1 2 3
0D	13	Get pages owned by handle	1 2 3
0E	14	Get pages for all handles	1 2 3
0F	15	Get or set page map	1 2 3

*U.S. GOVERNMENT PRINTING OFFICE: 1991--526-252/40797

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **UNLIMITED DISTRIBUTION**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) **CSC-EPL-91/001**	5 MONITORING ORGANIZATION REPORT NUMBER(S) **S236,003**
6a. NAME OF PERFORMING ORGANIZATION **National Computer Security Center** 6b OFFICE SYMBOL *(If applicable)* **C71**	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS *(City, State and ZIP Code)* **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	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 Evaluation Report LOCKIT Professional 2.10**	
12 PERSONAL AUTHOR(S) Paul A Bicknell, Christine M Chiles, Hilary H Hosmer, Harold J Wolfe	
13a. TYPE OF REPORT **Final**	13b TIME COVERED FROM ____ TO ___
14 DATE OF REPORT *(Yr/ Mo/ Day)* **910327**	15 PAGE COUNT **73**
16 SUPPLEMENTARY NOTATION	

17 COSATI CODES		
FIELD	GROUP	SUB GR

18 SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
NCSC, I&A, DAC, AUDIT, CSSI, OR, LOCKIT Professional 2.10

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

The National Computer Security Center (NCSC) examined the security protection mechanisms provided by Security Microsystems, Inc.'s LOCKIT Professional 2.10. LOCKIT Professional 2.10 is a subsystem, not a complete trusted computer system. Therefore, it was evaluated against the *Computer Security Subsystem Interpretation* (CSSI). Specifically, the applicable requirements for this evaluation included Identification & Authentication (I&A), discretionary access control (DAC), audit, and object reuse. The evaluation team determined that the highest class at which LOCKIT Professional 2.10 satisfies the I&I, DAC, audit and object reuse requirements of the CSSI is class D.

This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21 ABSTRACT SECURITY CLASSIFICATION **UNCLASSIFIED**	
22a NAME OF RESPONSIBLE INDIVIDUAL **PATRICIA L. MORENO**	22b TELEPHONE NUMBER *(Include Area Code)* **(301)859-4458**	8b OFFICE SYMBOL **C71**

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE