



NATIONAL COMPUTER SECURITY CENTER

AD-A247 240



DTIC
ELECTE
MAR 9 1992
S C D

FINAL EVALUATION REPORT

OF

ALC Incorporated

TIGERSAFE (Zenith-version)

92-05767



26 September 1990

Approved for Public Release:
Distribution Unlimited

92 3 04 011

FINAL EVALUATION REPORT

ALC Group
Tigersafe
(Zenith version)



Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

NATIONAL COMPUTER SECURITY CENTER

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

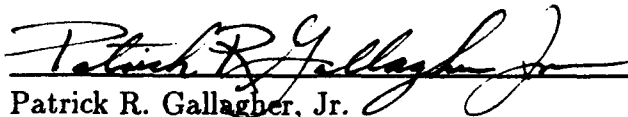
26 September 1990

CSC-EPL-90/005
Library No. S236,001

FOREWORD

This publication, the Final Evaluation Report ALC Tigersafe 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 ALC evaluation. The requirements stated in this report are taken from *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

26 September 1990

ACKNOWLEDGEMENTS

Team Members

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

Michael J. Oehler
Walter K. Roddy
1Lt Reggie Sharpless, USAF
Capt. Benton A. Wigney, USAF

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

For his contributions to this evaluation, acknowledgement is given to Steve Schneider, formerly of the NCSC.

Contents

FOREWORD *	i
ACKNOWLEDGEMENTS	ii
EXECUTIVE SUMMARY	v
Chapter 1 Introduction	1
Evaluation Process Background	1
Subsystem Evaluation Program	2
Document Organization	2
Chapter 2 System Overview	4
Product History	4
Product Overview	4
Security Relevant Portion (SRP)	4
Hardware Architecture	5
Software Architecture	6
SRP Protected Resources	9
Subjects	9
Objects	9
SRP Protection Mechanisms	10
Privileges	10
Identification and Authentication	11
Object Reuse	11
Chapter 3 Evaluation as a Subsystem	13
Features	13
Identification and Authentication	13
Object Reuse	15
Assurances	16
System Architecture	16
System Integrity	17
Security Testing	18
Documentation	20
Security Features User's Guide	20
Trusted Facility Manual	21
Test Documentation	21
Design Documentation	22
Rating Assignment	23

Chapter 4 Evaluator's Comments	25
Appendix A Evaluated Hardware Components	26
Appendix B Evaluated Software Components	27
Appendix C Glossary of Acronyms	28

EXECUTIVE SUMMARY

The National Security Agency (NSA) / National Computer Security Center (NCSC) examined the security protection mechanisms provided by ALC's Tigersafe for the Zenith 248 Personal Computer. Tigersafe 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 Identification and Authentication (I&A) and object reuse (OR). Tigersafe does not provide complete Discretionary Access Control (DAC) or Audit features, and was not rated in those categories.

The evaluation team determined that the highest rating at which Tigersafe satisfies the I&A and OR requirements of the CSSI is class D. The D rating in the evaluated features of I&A and OR resulted from Tigersafe's inability to meet all assurance and documentation requirements specified by the CSSI.

To obtain the level of trust described in this report, Tigersafe must be configured in accordance with the Trusted Facility Manual, or its equivalent, and properly administered. There are some programs and utilities that should not reside on the Zenith microcomputer. These include the following: DOS system files, programming languages, compilers, debuggers, Tigersafe's utilities, and other applications programs. Since Tigersafe only provides access control to its own utilities, those other files and programs which should be controlled must be deleted from the system, thus limiting its functionality.

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 any 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 an ADP system for the sole purpose of processing classified or sensitive information.

Introduction

In January 1990, the evaluation team began a product evaluation of ALC's Tigersafe as supplied for the Zenith Model 248 Personal Computer (IBM PC-AT compatible). The objective of this evaluation was to rate the Tigersafe product against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a rating for each of Tigersafe's evaluated features. This report documents the results of the evaluation. This evaluation applies to Tigersafe version 3.03.1 EN available from ALC Group of Coronado, California.

Material for this report was gathered by the evaluation team through documentation, interaction with company representatives, and through the use of Tigersafe.

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 or level 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 three appendices. Chapter 1 is an introduction. Chapter 2 provides an overview of the system's hardware and software architecture.

Chapter 3 provides a mapping between the requirements specified in the CSSI, and the Tigersafe's features that fulfill those requirements. Chapter 4 presents the evaluator's comments about Tigersafe. The appendices consist of identification of specific hardware and software components to which this evaluation applies, and a glossary.

System Overview

Product History

ALC - The Stealth Group is a privately held company specializing in add-on security products for IBM Personal Computers and compatibles. They have been in business for approximately five years. ALC is currently marketing the TIGERSAFE Security and Audit Trail Tracking Subsystem in several packages offering various levels of security and features, and physical security options to prevent subverting the system by removal or physical modification. ALC also markets an encryption package for use with the TIGERSAFE which was not included in this evaluation. This evaluation is of the TIGERSAFE Model 3.03.1 EN (for enhanced), installed as recommended by the documentation to provide the maximum security offered by the product.

Product Overview

The TIGERSAFE Model 3.03.1 EN was evaluated with multiple defined users in the configuration supplied for the Zenith Model 248 (IBM AT compatible). It allows up to fifteen users to share a Zenith PC running PC-DOS or MS-DOS version 2.1 and above. Tigersafe is a combined hardware and software product providing domain isolation on a small circuit card, a real-time program for device control and audit data processing, and a group of utility programs for configuring and monitoring the system. The Zenith version of the product additionally includes a jumper wire to prevent keyboard access to the Zenith Monitor Utility. The product can also be used in a network environment but was not evaluated in that configuration.

Security Relevant Portion (SRP)

The protection critical mechanism or the Security Relevant Portion (SRP) of Tigersafe, 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 hardware base of Tigersafe consists of a small, half-height, circuit card, with four integrated circuits (IC) and supporting circuitry. The circuit card is available in several versions using both 2K and 8K Random Access Memory (RAM) chips, however, this evaluation only applies to the 8K circuit card. The four IC's are a battery-backed RAM chip, two Programmable Array Logic chips (PALs), and an address chip. The RAM chip stores variables and some audit data for Tigersafe's operation. The two PALs contain the code for Tigersafe's execution. The address chip ensures that the system will recognize a valid card when the processor polls its address. The board interfaces to the BIOS only at address CE00. An external connector and jumper wire are part of the supporting circuitry. This wire prevents keyboard interrupts during start-up, precluding access to the Zenith ROM monitor and assuring that Tigersafe has control before access is granted to the user.

When power is applied to the system, a hex value is put into the instruction register. This causes a jump to the location of the machine's boot procedure in Read Only Memory (ROM). This ROM code executes a number of actions which cannot be interrupted because the jumper locks out the keyboard during the boot process. The ROM code:

1. Runs a reliability test of chips on the board.
2. Tests the extent of memory and the physical environment.
3. Fills in the Interrupt Vector Table in low memory.
4. Checks for optional equipment by polling the card slots.

At step four, Tigersafe asserts control. The *check for optional equipment* is done by scanning memory for additional devices on the bus. When Tigersafe senses its address during that scan, internal logic is executed to 'open' its on-board memory and respond. Seeing a response, the CPU examines Tigersafe's card to determine that it is a valid RAM card and reads the size identifier. The CPU then performs a CRC check to verify that the code within the Tigersafe is unchanged. If the checksum is valid, the CPU places Tigersafe's next byte into the instruction register. This marks the change of control from the computer's ROM boot sequence to Tigersafe's board.

The next step is to read the memory size value stored in the BIOS Data Area and reserve a section for its own use. Having made this change, Tigersafe relocates some of the code from its own ROM into that memory area. Tigersafe then replaces several interrupt vectors in DOS's low memory table so that the 8259 chip, which prioritizes all interrupts, will call this code. Since some interrupts are issued frequently and automatically, the code which protects devices attached to the PC is also executed automatically.

The alteration of the vector table allows Tigersafe to front-end a number ROM-BIOS routines. Part of the reserved system memory is used by the DEVTRACK program (see page 6, "Software Architecture") to organize data structures so that DEVTRACK can intercept the DOS software interrupts for I/O operations. This prepares Tigersafe to control whether individual users get access to hard drives, floppies, printers and com or serial ports. Finally, Tigersafe moves code that implements object reuse to this high memory area. After all the necessary code has been moved, Tigersafe checks the "Illegal Access" data table in its RAM data area to determine if the last time the PC was turned on, an illegal access was attempted. If so, a warning is printed to the screen and execution continues to the last step.

The last major step is to display the logon screen and open up the keyboard to poll for a user input. Tigersafe's code (on the board) is still in control and waiting for the password entry. The key strokes for the password are encrypted when received and stored in a temporary buffer. When the return key is pressed, the temporary buffer is compared to the value stored in Tigersafe's RAM. If a match is found, Tigersafe examines its own data areas to see if *user identification* is enabled (see page 11 "Identification and Authentication"). If not, control is passed back to the CPU to finish its boot sequence by continuing to examine the rest of the slots and then calling DOS. If enabled, it is checked before completing the boot process, just as the password was.

Software Architecture

This section describes the software components of Tigersafe's SRP. The software architecture of Tigersafe is a combination of real time software, firmware, and utility support programs. Firmware has already been discussed in the previous section (Hardware Architecture). Security relevant actions are all done by firmware contained on the Tigersafe card and the memory resident DEVTRACK program.

Tigersafe can be installed to provide three different levels of security. The administrator determines which level of security meets the needs of his organization by answering a questionnaire provided with the Tigersafe unit. Level 1 installation provides the highest level of Tigersafe security feature capabilities and is the installation level used for this evaluation. Specifying the desired installation level determines which programs on the distribution floppy disk will be copied by installation command files. At level 1, all security relevant program files are copied.

The utility TSMEMORY must be used prior to the Tigersafe card installation to check for any memory (ROM and RAM) addressing conflicts with existing add-on boards. TSMEMORY will alert the administrator if any adapter boards or drivers are in conflict with the Tigersafe addressing requirements. Tigersafe requires a fixed address so addressing conflicts must be

resolved prior to installing the Tigersafe card.

The DEVTRACK program performs most of Tigersafe's security relevant functions after system initialization. DEVTRACK intercepts DOS service requests and determines if they have any impact on Tigersafe programs or are requesting the use of a device. If the request is for a device, DEVTRACK compares the request to a master table of authorizations for the user. If the function requested is protected by DEVTRACK, or the user does not have the correct authorizations, the request will be either refused or ignored. Otherwise, the DEVTRACK program will pass control directly to the DOS routine without any further intervention. During this processing, DEVTRACK logs application program use and file use to their respective hard disk drive audit files. DEVTRACK is also responsible for providing security of deleted files. If enabled, DEVTRACK will overwrite the sectors of deleted files automatically for the user with alternating 1's and 0's.

The HWCONFIG utility is used by the administrator to configure hardware related functions:

- Enable/disable CMOS verification at bootup.
- Enable/disable RAM overwrite with 0's each time the LOCK utility is used.
- Enable/disable system devices (floppy disk drives, hard disk drives, serial (COM 1-4) ports, and parallel (LPT 1-4) ports).
- Enable/disable secure file deletion to overwrite deleted files with 0's and 1's (Tigersafeoverwrites full clusters in case a file is less than 512 bytes).
- Enable/disable the keyboard and floppy drive during system booting.
- Display the Tigersafe hardware security configuration status.
- Display the Tigersafe serial number and audit file names.

The SECURITY utility, used by the administrator, sets up the passwords and identifications for up to 15 End Users. These User IDs and passwords are used by the I&A mechanism to validate the users and to determine whether a user may access the floppy drive, hard disk, serial ports, and parallel ports. The SECURITY utility can also, optionally, prevent any duplicate End User passwords, define the maximum length of time an End User's password is valid and allow End Users to change their own passwords.

The MONITOR utility provides access to the Zenith MFM ROM monitor. The MFM monitor program allows setup parameters to be changed and the Zenith DEBUG and diagnostics programs to be executed. Only the Master Security Administrator (MSA) and the Department Level Administrator (DLA) have privileges to use this utility. On a Zenith 248 PC, the

MFM monitor would normally be called using the CTRL-ALT-INSERT and CTRL-ALT-RETURN key sequences. The Tigersafe intercepts the use of these key combinations, and does not allow access to the monitor function except through its own interface. Access to the ROM Monitor could allow even an unsophisticated user to circumvent Tigersafe's security features.

Tigersafe's equivalent of a logout is the LOCK utility. This utility is used by all users to return the PC to the initial logon screen. If used in conjunction with the SIGNOFF password, Tigersafe will clear extended/expanded memory and the 640K normal RAM memory with all 1's. Also, if configured, the LOCK utility will check the computer's 50 byte CMOS setup data against a copy of the setup data stored on the Tigersafe board. If the CMOS data has changed, the PC will not accept any further keyboard input, logs the violation in the audit trail, and prints a warning to the screen stating that the CMOS memory has been modified. Tigersafe's SIGNOFF utility allows the administrator to set the password used in conjunction with the LOCK utility to clear the PC's RAM memory.

The DELAY utility is used by the system administrator to configure the maximum number of illegal password entry attempts. Once the threshold is reached, the PC's keyboard is locked out, the screen is cleared, and the violation is logged with the date and time. The PC will have to be rebooted before any user can log in again. The DELAY utility also allows the administrator to set the amount of time that the PC may remain powered up and idle in the LOCK screen. When the time limit is reached, the DELAY utility will clear all RAM memory, lock out the keyboard, and clear the screen. The timed lockup feature is only effective from the LOCK screen, which can clear memory on entry, so its usefulness is questionable.

The CLOCK utility is used by the system administrator to link the computer's internal clock with the audit trails to log the date and time of events. This link is in the form of a clock driver chosen from a menu list of computer manufacturers and types. The installer specifies the manufacturer or model of the machine and the utility installs the proper driver software and links it to the audit programs. This should not be confused with the DOS time function, used to set the system clock, which has been protected to prevent altering the input to the audit trails. On protected systems the system clock can only be set by the administrators from the ROM Monitor utility.

Tigersafe's AUDIT utility allows the administrator to clear or display the four audit trail reports. The four reports are from the internal RAM-based session access log and the disk-based session access, program usage, and file usage logs, which are stored in ASCII format and accessible to all users. The audit trail reports can be viewed on screen or sent to a printer. The AUDITFN utility allows the administrator to enable any or all of the auditing functions and specify where to store the log files.

The PASSWORD utility is used by the administrator to change the Master Password, which is used to identify the administrator. The administrator may change the Master Keycode, which is used to authenticate an administrator, using the KEYCODE utility. Security relevant configuration actions require the use of both the Master Password and the Master Keycode. The manufacturer's intent is that one should be held by a Department Level Administrator (DLA), and the other by a Master Security Administrator (MSA), though implementation of such a policy is left to the site. The administrator may also enable the password option in the SECURITY utility to allow any users to use the PASSWORD utility to change their own passwords. When users are permitted to change their own passwords, the PASSWORD utility accepts user passwords and changes the password that is given for access.

SRP Protected Resources

This section describes the subjects and objects that Tigersafe mediates access between.

Subjects

The subjects are those processes and Tigersafe utilities that act on behalf of the system's users. A process is the abstraction of tasks which comprise an executing program. It consists of the current value of the program counter, registers, and associated variables. On a PC running DOS, all user processes execute in one unprotected mode. There is no memory separation for processes, nor is there a supervisor state or kernel to protect the operating system from user processes. It is the responsibility of subjects (programs) not to interfere with one another, a goal which is impossible to guarantee, since DOS does not provide memory separation.

Access to the Tigersafe utilities is controlled by password in the same manner as the system itself. However, once access is granted, they are subjects acting on behalf of a user (the system administrator), as is any other process.

Objects

Tigersafe's protected objects are the following:

The named objects:

- Floppy Disk Drives
- Serial Ports
- Parallel Ports
- Addressable RAM memory
- CMOS memory - The first 50 bytes of battery back-up memory
- The Tigersafe DEVTRACK program
- The Tigersafe audit data files

The storage objects:

- Files
- CMOS Memory
- Memory - including extended/expanded memory

SRP Protection Mechanisms

This section describes Tigersafe's privileges, I&A, and OR mechanisms.

Privileges

The Tigersafe system has three levels of user privilege, the Master Security Administrator (MSA), Department Level Administrator (DLA), and the end users. The Tigersafe manual refers to them as levels of password control but there is no difference in the I&A mechanism for access to the system using the Master Password or user passwords. The MSA is intended to be the highest level administrator and control the six character Master Keycode. The DLA is the second level administrator and is intended to control the six to twelve character Master Password. That administrative control is implicit in their possession of their Keycode or Password and neither has access to anything security relevant without the code controlled by the other. They are essentially on an equal level and both must be present to accomplish any configuration actions.

Identification and Authentication

When the boot sequence is interrupted by the Tigersafe, the user or administrator is presented with a logon screen requesting a password. The password may be six to twelve characters long and is controlled by the administrator. If *user identification* is enabled, and the user's password is successfully entered, the user's two character identifier would be requested. The user identifier is defined by the Tigersafe in a predictable sequence and cannot be changed. When the logon process is completed, the system will complete the boot process and leave the user at the DOS prompt. If the logon process is not successfully completed within the number of attempts selected by the MSA, the system will lock up, an entry will be made in the session access audit log, and the system must be rebooted by recycling power.

A separate I&A mechanism is required for system administration. The administrator performs administrator functions through use of Tigersafe utility programs. Access to Tigersafe utility programs requires use of both the Master Password (which serves as administrator identification) and the Master Keycode (which serves as the administrator authentication code).

The SECURITY utility program enables the system administrator to perform password configuration actions. Selection one of that menu allows enabling user ID authentication. Selection two allows the MSA to force unique passwords by having the system provide a one digit sequential numeric prefix to the password (such as "1TESTING" or the password "TESTING"). Selection three allows creating and editing user passwords. Selection four allows enabling password date control, and five allows the definition of expiration time periods for each user. The time periods may range from hours up to 180 days. Use of this option also requires enabling by user number under the "Date Limit" option of menu selection six.

Selection six of the SECURITY utility's menu allows the selection and editing of hardware access rights for each user. In addition to the date limit option noted above, each user may be allowed to change their own password, and each user may be allowed to use the Tigersafe controlled devices. Each user may (or may not) be allowed to use the floppy disk drives, hard drive, comm ports, or the printer ports. Devices are specified by type. It is not possible, for instance, to restrict access to drive B: while leaving drive A: available.

Object Reuse

Tigersafe provides object reuse on the storage objects as noted on page 9. This feature is activated by the administrator by enabling the "file overwrite", "CMOS clear", and "memory clear" options in the HWCONFIG utility. Once enabled, object reuse is provide in the following manner:

- File Overwrite - When the DOS ERASE or DELETE command is issued and this option is enabled, the disk sectors occupied by the designated file(s) will be overwritten. Tigersafe overwrites all space allocated to the file and not just the space currently used by the file. The administrator has the capability to specify how many times the sectors are to be overwritten, up to seven times, with alternating ones and zeros. The administrator may also enable the "verification" option which prevents clearing of the file allocation table, allowing the user to examine the file and verify that it was overwritten. While that feature may reassure some users, it must be noted that its use violates the requirements of Object Reuse since the file name may also "contain" information. The file name remains and the disk space is unavailable until the user takes explicit action in addition to viewing the overwritten file.
- CMOS Clear - During logon, this option compares the first 50 bytes of memory containing system setup parameters to a Tigersafe internal buffer. CMOS memory is then overwritten with the buffer contents. If they differ, a warning message is displayed on the screen.
- Memory Clear - During logout, this option clears main memory, extended memory, and expanded memory.

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 Tigersafe product are Identification and Authentication (I&A) and Object Reuse (OR). For each feature, this chapter states the requirements, describes Tigersafe'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 23 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

Features

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

Tigersafe requires that all users log in thru the login screen before taking any other actions. There are no apparent ways to circumvent this requirement. The passwords are sufficient to identify and authenticate users and administrators. Authentication data is stored in the isolated domain of the Tigersafe RAM and is not accessible to either authorized or unauthorized users. Tigersafe also provides for the auditing of security relevant I&A events.

Conclusion

Tigersafe satisfies the D2 feature requirement for I&A.

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

Tigersafe overwrote all user accessible storage objects and there are no obvious ways to circumvent the mechanism. It must be noted that there are multiple options which must all be activated to have an effective OR subsystem:

- RAM clear - extended/expanded memory.
- RAM clear - lower 640K memory.
- Enable secure file deletion.
- CMOS verification.

Conclusion

Tigersafe satisfies the D2 feature requirement for object reuse.

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

Although Tigersafe's board isolates its I&A code and data, it does not maintain a domain for execution of the remaining parts of the SRP. Therefore, these parts are not protected from external modification.

The controlled objects are defined on page 9. Other objects on the PC are accessible and not protected.

Conclusion

Tigersafe does not satisfy the D1 system architecture requirement.

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

- D1:

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

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

Applicable Features

Tigersafe automatically performs a CRC check of the firmware and data structures located on its card when the PC is powered on. Tigersafe does not provide any diagnostics for the hardware or software components of its SRP.

Conclusion

Tigersafe does not satisfy the D1 system integrity requirement.

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

The evaluation team tested Tigersafe in two phases, the first focusing on functional testing, and then a second phase of security testing. Tigersafe was installed to provide the maximum of three levels of security available with the product. The functional testing phase concentrated on providing the team assurance that the product was installed properly and functioned consistently with the instructions provided. The security testing phase focuses on determining if there are any apparent ways to bypass or defeat the security mechanisms.

Functional testing is basically testing the system as it might be installed in the field, using

DOS and any application programs that are not specifically forbidden by the instructions. All optional security features were turned on and several "accounts" were created for each member of the evaluation team. The system works as documented when one has the time and experience to interpret the instructions, which are poorly written and organized. Once an "account" is opened by entering the initial password at the SECURITY menu, it can only be changed and not deleted. The four audit logs are protected from modification and deletion by being set read-only but are viewable by all using either DOS or word processors. The Tigersafe utilities are protected from execution but are subject to deletion and spoofing by unsophisticated users.

The second phase of testing, security testing, consisted of exercising the system and looking for obvious flaws that would bypass or defeat the Tigersafe's protection mechanisms. Application programs, debuggers, utilities, and some locally written programs using both DOS and BIOS features were used. The team was not able to alter or bypass the authentication data on the circuit card itself or the I&A mechanism. However Tigersafe is vulnerable to an insider attack. Introducing such programs to a protected system may require a significant amount of work, depending on how well the system is managed, but once on the system. Tigersafe is not able to protect itself or system resources. Manipulating audit data and other disk based data structures such as the file containing password expiration dates was a simple matter using either DOS or word processors. While manipulating the audit mechanism, the link to the clock was broken and the system continued to log invalid data without noting errors. Team members were able to change Tigersafe data in reserved memory using readily available utilities. As testing progressed, operation of the Tigersafe utilities became very unpredictable and it was frequently necessary to reboot the system after the utilities would not exit properly.

Conclusion

Tigersafe does not satisfy the D1 security testing requirement.

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.

- D2:

There are no additional requirements at the D2 Class.

Applicable Features

Tigersafe supplies a pocket sized guide which briefly explains the protection mechanisms provided. This guide combines the administrative operations and instructions for users. It includes a short discussion on Tigersafe's available utilities, auditing, and how to log on and off the system.

Conclusion

Tigersafe satisfies the D2 Security Features Users Guide requirement.

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

ALC provides an appendix in their technical support manual which again describes the installation and use of the utilities, and how the features they control satisfy specific security goals. While there is some misuse of accepted computer security definitions, such as referring to keyboard lockout during bootup and master device disabling as Discretionary Access Control, the section does achieve its objective. It should be noted that ALC suggests using the Tigersafe encryption package to protect against unauthorized use of applications packages and files, but that is not an included part of this product.

Conclusion

Tigersafe satisfies the D1 Trusted Facility Manual requirement.

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.

Applicable Features

ALC supplied test documentation showing the procedures and results of product installation and the operation of some utilities. The documentation did not describe how the security mechanisms were tested nor the results of functional testing. This statement applies to each evaluated feature: I&A, and OR.

Conclusion

Tigersafe does not satisfy the D1 Testing Documentation requirement.

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.

Applicable Features

ALC failed to supply adequate design documentation. The document contained inaccuracies at the beginning of the evaluation and was never updated as the product was modified during the evaluation. Good technical detail was presented concerning how the Tigersafe interfaces with DOS and the PC, but they did not provide a design philosophy or how that is translated into the system's SRP.

Conclusion

Tigersafe does not satisfy the D1 Design Documentation requirement.

Rating Assignment

This section describes the composite rating and how it is determined. A composite rating is assigned to each evaluated feature and is based upon the individual ratings issued 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 Section 3, the composite ratings for each of Tigersafe'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	D2	N	N	N	Y	N	N	N	Audit ¹	D
OR	D2	N	N	N	Y	N	N	N	none	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 an aspect 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 that of the feature to obtain the composite rating.

¹ Authentication data is protected on the Tigersafe board. Tigersafe provides sufficient audit capability to support I&A.

Evaluator's Comments

The evaluation team feels that the Tigersafe provides additional security in its I&A mechanism that PC-DOS and MS-DOS clearly do not possess. During this evaluation, both the product and the documentation were greatly improved. The company was very responsive, and all problems identified to the company were quickly resolved.

The Tigersafe provides security features adequate for a benign environment but the administrators interface can be very annoying to use. Some functions are duplicated and similar options are not grouped together, making them unnecessarily complex. In one case, four options in three menus must be set to have a fully effective object reuse subsystem. In another case, options in three menus must be used to set password expiration dates. Audit trails, composed of four separate reports with no audit reduction capability, are difficult to correlate to get a clear picture of what has happened. The system does not record all failed commands in the audit log, so it is possible that there will be no audit record associated with some insider attempts to compromise the system.

Administrators should note that Tigersafe does not provide discretionary file protection. The CSSI permits a subset of the system's objects to be protected and does not limit the granularity of those objects. Subsystems are therefore permitted to control only a few resources with the remaining ones totally accessible. Tigersafe protects objects at the device level and by device type rather than specific devices. It is also notable that this is at the discretion of the administrator, not the user. Another feature, the User ID Authentication Code, serves no security purpose since it is short (two characters), system controlled, and easily guessed. Such devices may serve to identify users, as does a name, but they should not be confused with devices such as passwords which authenticate the identity of users, a legitimate security function.

The documentation improved greatly during the course of the evaluation, but it is still poorly structured and difficult even for knowledgeable persons to read. Some sections consist entirely of disconnected notes, rather than informative narrative. Users will have difficulty in finding documentation that will help solve certain problems caused inadvertently by users. For example: The evaluation team deleted AUTOEXEC.BAT during a test of protection mechanisms and Tigersafe worked as advertised, leaving a locked system. The team's efforts to recover from that were arduous. The team found it difficult to find guidance in the documentation and frequently had to guess at the proper action.

Evaluated Hardware Components

This appendix lists the ALC marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluation. The primary requirement for hardware is that the hardware function properly. This was verified by the diagnostic tests performed using the Zenith MFM-400 Monitor Utility. Those tests were repeated periodically to ensure that identified problems originated within the subsystem and not the system itself.

To operate in correspondence with the I&A and OR ratings, the security subsystem must contain the hardware components listed in this section.

The protected system covered by this evaluation is the Zenith Data Systems Model ZWX-0248-62 (the Zenith Z-248), IBM PC-AT compatible. It was supplied with one 40M hard disk, one DS/DD floppy disk, and one DS/HD floppy disk.

The Tigersafe board did not have any identifying features other than noting that it featured the 8Kbyte RAM chip. There is no version number or serial number on the circuit board other than the fabricators number for the "raw" board.

Evaluated Software Components

This section lists the programs that made up the Tigersafe software system as it was installed and evaluated. Tigersafe is designed to run under revisions 2.1, 3.1, 3.2, 3.3, 4.0 of PC-DOS, MS-DOS or IBM/DOS, although the Tigersafe audit trails only function under DOS 3.0 and above. This evaluation used MS-DOS version 3.1.

The software for version 3.03.1EN of the Tigersafe was delivered on two 5 1/4" floppy diskettes. The software consisted of the files listed below plus eight .DRV driver files for the CLOCK utility:

- Filename
- AUDIT.COM
- AUDITFN.COM
- CLOCK.COM
- DELAY.COM
- DEVTRACK.COM
- HWCONFIG.COM
- KEYCODE.COM
- LOCK.COM
- MONITOR.COM
- PASSWORD.COM
- SECURITY.COM
- SIGN.COM
- SIGNOFF.COM
- TIGERSAF.BIN
- TSINIT.COM
- TSINSTAL.COM

Glossary of Acronyms

ADP	Automatic Data Processing
BIOS	Basic Input-Output System
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSSI	Computer Security Subsystem Interpretation
DLA	Department Level Administrator
DAC	Discretionary Access Control
DOS	Disk Operating System
EEPROM	Electrically Erasable and Programmable Read Only Memory
EPL	Evaluated Products List
IC	Integrated Circuit
ID	Identification
I&A	Identification and Authentication
MAC	Mandatory Access Control
MS-DOS	MicroSoft Disk Operating System
MSA	Master Security Administrator
NCSC	National Computer Security Center
OR	Object Reuse
PC	Personal Computer
PAL	Programmable Array Logic
RAM	Random Access Memory
ROM	Read Only Memory
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual

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--SUM-90/005		5. MONITORING ORGANIZATION REPORT NUMBER(S) S236,001	
6a. NAME OF PERFORMING ORGANIZATION National Security Agency	6b. OFFICE SYMBOL <i>(if applicable)</i> C71	7a. NAME OF MONITORING ORGANIZATION National Computer Security Center	
6c. ADDRESS <i>(City, State and ZIP Code)</i> 9800 Savage Road Ft. George G. Meade, MD 20755-6000		7b. ADDRESS <i>(City, State and ZIP Code)</i> 9800 Savage Road Ft. George G. Meade, MD 20755-6000	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL <i>(if applicable)</i>	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS <i>(City, State and ZIP Code)</i>		10. SOURCE OF FUNDING NOS	
		PROGRAM ELEMENT NO	PROJECT NO
		TASK NO	WORK UNIT NO
11. TITLE <i>(Include Security Classification)</i> Final Evaluation Report ALC Group TIGERSAFE (Zenith)			
12. PERSONAL AUTHOR(S) Deborah M. Clawson, Michael J. Oehler; Shawn M. Rovanssek			
13a. TYPE OF REPORT Final	13b. TIME COVERED FROM ___ TO ___	14. DATE OF REPORT <i>(Yr, Mo., Day)</i> 900926	15. PAGE COUNT 28
16. SUPPLEMENTARY NOTATION			
17. COSATI CODES		18. SUBJECT TERMS <i>(Continue on reverse if necessary and identify by block number)</i>	
FIELD	GROUP	SUB GR	NCSC, I&A, OR, ALC Group, TIGERSAFE, CSSI
19. ABSTRACT <i>(Continue on reverse side if necessary and identify by block number)</i> The ALC Group TIGERSAFE (Zenith Version) has been evaluated by the National Computer Security Center (NCSC). The security features of TIGERSAFE were examined against the requirements specified by the COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988. The NCSC evaluation team has determined that TIGERSAFE satisfies the functional requirement for I&A/D2, and the functional requirements for OR/D2. TIGERSAFE failed to satisfy the assurance and documentation requirements and therefore it has been determined that the highest class at which the TIGERSAFE satisfies all the specified requirements of the CSSI is class I&A/D and OR/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 <i>(Include Area Code)</i> (301)859-4458	8b. OFFICE SYMBOL C71