

2



NATIONAL COMPUTER SECURITY CENTER

AD-A234 170

FINAL EVALUATION REPORT
OF
WANG LABORATORIES
MICROCONTROL

DTIC
ELECTE
APR 8 1991
S B D

11 October 1989

Approved for Public Release:
Distribution Unlimited

FINAL EVALUATION REPORT

WANG LABORATORIES INCORPORATED
MICROCONTROL

NATIONAL COMPUTER SECURITY CENTER

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

11 October 1989

CSC-EPL-89/008
Library No. S235,317

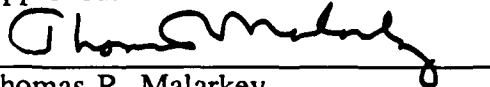
This page intentionally left blank.

Final Evaluation Report Wang MicroControl
Foreword

FOREWORD

This publication, the Final Evaluation Report of Wang's MicroControl, 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 MicroControl 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:



Thomas R. Malarkey
Deputy Chief,
Office of Product Evaluations
and Technical Guidelines
National Computer Security Center

11 October 1989

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	

Final Evaluation Report Wang MicroControl
Acknowledgements

ACKNOWLEDGEMENTS

Team Members

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

Captain Deborah M. Clawson, USAF

Michael J. Oehler

Shawn M. Rovanssek

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

CONTENTS

	FOREWORD	iii
	ACKNOWLEDGEMENTS	iv
	EXECUTIVE SUMMARY	vii
Section 1	INTRODUCTION	1
	Evaluation Process Background	1
	The NCSC Computer Security Subsystem Evaluation Program	1
	Document Organization	2
Section 2	SYSTEM OVERVIEW	5
	Security Relevant Portion	5
	Hardware Architecture	5
	Software Architecture	5
	SRP Protected Resources	6
	Subjects	6
	Objects	7
	SRP Protection Mechanisms	8
	Privileges	8
	Identification and Authentication	8
	Discretionary Access Control	10
	Audit	14
Section 3	EVALUATION AS AN I&A, DAC, AND AUDIT SUBSYSTEM	15
	Identification and Authentication	15
	Discretionary Access Control	16
	Audit	19
	System Architecture	20
	System Integrity	21
	Security Testing	22
	Security Features User's Guide	23
	Trusted Facility Manual	23
	Test Documentation	24
	Design Documentation	25
	Rating Assignment	26
Section 4	EVALUATOR'S COMMENTS	27
Appendix A	EVALUATED HARDWARE COMPONENTS	A-1
Appendix B	EVALUATED SOFTWARE COMPONENTS	B-1
Appendix C	GLOSSARY	C-1

This page intentionally left blank.

EXECUTIVE SUMMARY

The National Computer Security Center (NCSC) examined the security protection mechanisms provided by Wang's MicroControl Version 1.0650 and 1.0660. MicroControl 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), and audit.

The evaluation team determined that the highest class at which MicroControl satisfies the I&A, DAC, and the audit requirements of the CSSI is class D. A composite rating of D was awarded to these evaluated features because MicroControl could not meet all assurance and documentation requirements specified by the CSSI. See page 26 "Rating Assignment", for a description of each component in the rating.

To obtain the level of trust described in this report, MicroControl must be configured in accordance to the caveats of this report and the Workstation Administrator's Guide (WAG), included as part of MicroControl's documentation set. Additionally, administrators must be aware of the functions and capabilities of the programs residing on the system so that the greatest assurance can be achieved. Most notably, administrators must account for DOS's files, programming languages, compilers, utilities, and MicroControl's commands. Administrators may restrict access to these programs for certain users by using MicroControl's protection mechanisms.

Subsystems are designed to be installed on automatic data processing (ADP) systems. Specifically, subsystems are designed to add a level of assurance to an ADP system that has limited or ineffective security mechanisms. However, 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.

This page intentionally left blank.

INTRODUCTION

In May 1989, the National Computer Security Center (NCSC) began a product evaluation of Wang Laboratories Incorporated's MicroControl. The objective of this evaluation was to rate MicroControl against the *Computer Security Subsystem Interpretation* (CSSI), and to place it on the Evaluated Products List (EPL) with a final rating for each of MicroControl's components. This report documents the results of the evaluation. This evaluation applies to MicroControl Version 1.0650 and 1.0660 available from Wang Laboratories Incorporated.

Material for this report was gathered by the NCSC MicroControl evaluation team, through documentation, interaction with system developers, and through the use of MicroControl.

Evaluation Process Background

The National Computer Security Center (NCSC) 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, 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 NCSC 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.

The NCSC Computer Security Subsystem Evaluation Program

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

The goal of the NCSC's 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

Final Evaluation Report Wang MicroControl introduction

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 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 (TCSEC)*. 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 sections and three appendices. Section 1 is an introduction. Section 2 provides an overview of the system's hardware and software architecture. Section 3 provides a mapping between the requirements specified in the CSSI, and the features and assurances that fulfill those requirements. Section 4 presents the evaluation team's comments of the subsystem. The appendices identify specific hardware and software components to which the evaluation applies, and also a glossary of terms.

This report addresses MicroControl versions 1.0650 and 1.0660. Since the operation and functionality of both is similar, the report addresses both versions as one product, MicroControl. However, where distinct differences occur, the exact version is enunciated. Generally, version numbers will only be referenced in the I&A section where version 1.0650 uses an electronic token as part of the I&A process. The token allows the I&A information to be stored within the token providing a degree of portability. Version 1.0660 does not use the token. Instead, it maintains the I&A information within internal databases.

For consistency with documentation presented by Wang, this report uses the term "workstation" to refer to the Wang Professional Computer (PC) 200/300 series computer. However, the report will refrain from using the terms "labels", "access level", "Clearance",

Final Evaluation Report Wang MicroControl
Introduction

and "Mandatory Access Control" as stated in Wang's documentation, because they differ from that in the TCSEC.

This page intentionally left blank.

SYSTEM OVERVIEW

Security Relevant Portion

The protection-critical mechanism or the Security Relevant Portion (SRP) of MicroControl, consists of its hardware and software capabilities. A description of these components and their security relevant roles are described in the following two sections.

Hardware Architecture

MicroControl's board physically consists of 64K bytes of ROM, 32K bytes of static RAM, a clock, and controlling circuitry. This circuitry, called the Controlled Access Mechanism (CAM), is used to enable MicroControl's components in the address space of the workstation. Once enabled, a separate domain for execution is established. This domain allows MicroControl to enforce access mediation, to log audited events, and to perform I&A.

The processor enters this domain when a specific sequence of instructions is executed solely on MicroControl's board. No offboard reference to memory or to an I/O port can occur or the transition will fail. If the sequence is completed fully and only within the board, MicroControl's components will be enabled on the address bus. Otherwise, the transition is aborted. This assures that control of the processor is transferred only to MicroControl's code.

Once within MicroControl's domain, the processor can only reference the area enabled and still remain within the domain. All interrupts are masked out assuring control over the processor. Once MicroControl's operation is complete, an offboard reference will occur causing MicroControl's hardware to be disabled. Once disabled, MicroControl's isolated domain of execution is relinquished and the processor is transferred back to the user.

Software Architecture

This section describes the software relevant components of MicroControl's SRP including its internal programs, the MANAGER program, and commands. MANAGER and all commands reside outside of the CAM protected circuitry, but are still part of the SRP. Therefore, they must be protected in the fashion described below.

Internal Programs

No design documentation was supplied for this evaluation and therefore, the internal software which performs the security relevant actions for MicroControl cannot be described by the team. These programs are protected by and called through the hardware interface described above, "Hardware Architecture".

Final Evaluation Report Wang MicroControl System Overview

MANAGER Program

The MANAGER program is used by privileged users to set the security configuration (see page 8, "Privileges"). Once the configuration has been selected, the program will pass the proper parameters to the MicroControl board so that they are installed. Specifically, MANAGER prompts for machine access requirements (e.g. password length, password expiration period, the user's PID, etc.), the auditable events, the RAC assignment, and file protection.

Although non-privileged users are not allowed to execute the MANAGER program, the file is not protected from modification when installed. Therefore, administrators must decrease this incurred risk by protecting this file with the GROUP identifier when it resides on the workstation (see page 10, "Discretionary Access Control"). This assures that MANAGER is protected from modification by non-privileged users. It should be noted that protecting MANAGER from modification on disk does not render it absolutely safe from modification while executing. The nature of DOS programs is such that the presence of foreign code, such as a Terminate and Stay Resident (TSR) program or device driver, represents a source of modification to any executing program.

Command Files

The system is supplied with batch files used to call each command. The batch files pass the proper parameters to a program called TRIADCMD.EXE which in turn makes the proper call to MicroControl's board. The function of the command is then performed within the board and the result passed back to the system.

These commands allow all users to interact with MicroControl's capabilities and query many of its current settings. There are two types of commands, user and privileged. The user commands are used by all users to query or change that user's environment.

The privileged commands are the administrative interface to MicroControl. They allow the privileged user to maintain, monitor, and override the security configuration established by the MANAGER program. Only privileged users are allowed to issue these commands.

Like the MANAGER program, the batch files and TRIADCMD.EXE are not protected when installed. Since the batch files and TRIADCMD.EXE must be shared between users and the DAC mechanism is such that it will grant all or none access, MicroControl is not capable of preserving their integrity for all users even though they may be protected.

SRP Protected Resources

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

Subjects

The subjects in MicroControl are the processes performing user and system functions. A process is the abstraction of tasks which comprise a program. It consists of the current

value of the program counter, registers, and associated variables. On a workstation running MS-DOS, all user processes execute in a single state. There is no separation for these processes. MicroControl's processes however, executes within a separate domain after passing through the CAM mechanism.

Objects

The objects that MicroControl protects are files, memory, and devices.

Files

Files are the basic containers in which information is stored on the IBM PC. Although files do not differ conceptually, their physical representation and location do. MicroControl protects files on floppy, hard, and RAM drives.

Memory

Memory refers to the directly addressable locations of RAM. On the workstation, this RAM is contained within the 1M addressable area of the Intel 8086, or Intel 80286 in real mode. These locations are addressable to the granularity of a single byte.

Devices

MicroControl protects ten devices. The devices consist of disk drives and communication ports. Each device is located on the I/O bus at specific port addresses. Each device is defined discretely in the list below.

Disk Drive

Disk drives defined at port addresses 3F5H, 3F7H, 375H, and 377H.

Hard Disk

Hard drives defined at port addresses 320H to 323H.

Parallel Ports

The three parallel ports defined at addresses 278H, 27AH, 378H, 37AH, 3BCH, and 3BEH.

Asynchronous Ports

The two asynchronous ports defined at addresses 2F8H, 2F9H, 2FBH, 2FCH, 3F8H, 3F9H, 3FBH, and 3FCH.

Wang Local Office Connection

The WLOC defined at ports addresses 242H-243H, 282H-283H, 2A2H-2A3H, and 342H-343H.

Synchronous Data Link Controller (SDLC) Ports

The SDLC port defined at addresses 381H-389H and 38CH.

Final Evaluation Report Wang MicroControl System Overview

Network Port

The two network ports defined at addresses 361H to 363H, 369H, 36AH, and 36bH.

DCA IRMA Port

The DCA port defined at addresses 220H-227H.

ARCNET Port

The port addresses defined at 2E0H to 2EFH.

SRP Protection Mechanisms

This section describes MicroControl's privileges, I&A, DAC, and audit mechanisms.

Privileges

MicroControl permits only one type of privilege, the ability to implement administrative capabilities. These administrative capabilities are available to a single user, named the Workstation Administrator when MicroControl is installed. Thereafter, they can be distributed to other users if the Workstation Administrator defines assistant administrators. Assistant administrators are members of the Workstation Administrator's group (see page 9, "Group Structure").

All privileged users have the ability to execute the MANAGER program, access any protected file, and execute all of MicroControl's commands. These commands control audit capabilities, file protection, MicroControl's internal clock, and the ability to override the DAC protection on files. The ability to override DAC assures that users are unable to hold files hostage, regardless of the encryption mechanism.

Identification and Authentication

In order to access a machine on which MicroControl has been installed, a user must first pass through the I&A mechanism, a logon window. This window is automatically printed when the workstation is booted or after a prior logout. It requires that the proper information be presented before access is permitted. Before describing the exact logon process, this section describes the parameters used to control the logon process and MicroControl's group structure. The exact logon process is then discussed last.

Establishing the I&A Parameters

An administrator must assign a Primary Identifier (PID), Secondary Identifier (SID), the allowed periods for logon, and an RAC access state (see page 12, "Resource Access Control"). The PID is the user's unique qualifier and the SID is the group name. Additionally, the administrator can require users to enter their SID, and/or a project identifier for accounting purposes, during the logon process. The access periods represent the time of day in which the user is authorized to log on. The administrator can assign up to four different access periods each of which are specified by days of the week and

hours within the day. The administrator must then activate that user's account before the user may access the workstation.

Once this is completed, the administrator must then program an electronic token for version 1.0650. This token contains battery backed RAM on which certain I&A information is encoded for each user. This information includes the user's PID, password, its expiration date, RAC access state, and allowed time periods of usage. The token is then issued to each user so that it can be inserted into a receptacle during logon. Version 1.0660 contains the same information, but it is stored within MicroControl's internal database instead of a token. MicroControl's CAM assures that the information is protected from modification.

Since version 1.0650 stores the I&A information within the token, the token can be ported to various workstations that have the same Master Phrase (see page 10, "Discretionary Access Control") and have validated that user on the workstation. This provides some flexibility by allowing users to log onto different workstations while maintaining the I&A information within a single location, the token. The token also distributes I&A between the user's identity, the token, and typed password. However to provide this flexibility, the authentication data (password) resides on the token and, although it is encrypted within the token and not readily accessible, the token must be safeguarded by users.

Additionally, MicroControl can be configured such that after multiple logon failures, further attempts are suspended for a predetermined duration. An alarm can also be configured to warn those in the area. Both the lockout and alarm durations are defined by the administrator and cannot be circumvented by cycling power to the workstation after they sound.

Each workstation running MicroControl can have a maximum of sixty-four uniquely identified users including the Workstation Administrator. As one of these sixty-four users, MicroControl supports a guest user account for which no password or token is required to logon. The guest user account is not a part of the evaluated configuration.

The administrator can also establish the acceptable limits for passwords. This includes the minimum and maximum length (up to 10 characters), and the minimum and maximum password life. The life is the period of time in days that the password is valid. If a password is found to be invalid during a logon, the user will be required to update it based upon the current limits and then re-type it for confirmation.

Group Structure

The SID is used to determine the user's group affiliation. As mentioned above, the administrator can optionally require a user to enter the SID during the logon process. However, administrators are required to assign a user to a group because it is used for file mediation. See page 10, "Discretionary Access Control" for information on the GROUP identifier. Administrators are only permitted to assigned a user to a single group so considerable forethought is necessary in determining which users will need to share files.

Final Evaluation Report Wang MicroControl System Overview

An important example is the assignment of the Workstation Administrator's SID to other users. Users with this SID are allowed to execute privileged commands.

The Logon Process

In order to logon, the user enters a PID. A SID and/or an account identifier may also be required for individual users if configured by an administrator.

For version 1.0650, the user is then required to insert a token into the receptacle. MicroControl reads the I&A information from the token. MicroControl then prompts for a password.

After the user types the password, MicroControl compares the user-supplied information with the information read from the token. If the entered PID, SID, or password data does not match that of the token, access is denied without revealing the reason.

If the logon entries are correct, user access is subjected to a further test. MicroControl determines if the user is attempting to log on during a valid access period. Only then will access to the workstation be granted.

For version 1.0660, the user is only required to enter a password after enter the PID, and SID if required. The same comparisons are made, but instead of reading the information from a token, the data is obtained from its internal database.

MicroControl also supplies a featured called suspend which is related to the I&A mechanism. This feature is automatically invoked after a fixed period of workstation inactivity or by explicit user action (i.e., the SUSPEND command is issued). Upon invocation, the workstation screen is cleared, a 'Suspend' message is displayed, and the workstation is disabled. When any key is pressed, a logon window appears and the user must go through the same procedure as an initial logon. However, only the user who is suspended can be authenticated. All other users must re-boot the workstation to gain access, thereby causing the suspended user to be logged off. When a suspended session is restored by the appropriate user, the interrupted application is restored to the point at which it was suspended.

Discretionary Access Control

MicroControl's DAC capability is provided through two logical mechanisms called Cryptographic Access Control (CAC) and Resource Access Control (RAC). Generally, MicroControl's CAC mechanism monitors access to files by intercepting DOS and BIOS interrupts. The RAC mechanism prevents absolute port addressing. The following sections describe CAC and RAC. File access is then described in the last section.

Cryptographic Access Control

When a DOS or BIOS file operation is initiated, CAC mediates access to the file based upon the file ownership identifier encoded into the file and the current user identity. If access is allowed, CAC decrypts the file. A proprietary encryption algorithm known as SmartCypher is used to encrypt and decrypt files. This algorithm uses a key called the Master Phrase which forms the basis for MicroControl's cryptographic control. It assures that identical products do not necessarily represent the same accessible domain. This Phrase is incorporated into all protected files and tokens.¹

The evaluation team will not comment on the strength of encryption nor usage of the CAC mechanism, as these concerns are beyond the scope of a CSSI evaluation. The team found that the CAC's encryption scheme appeared to function as claimed and did not interfere with the encryption in ways other than intended.

File protection is based upon the file ownership identifier set by the OWNER command during a logged-on session. Users are able to choose an ownership identifier or combination of identifiers so that the file has the proper level of protection. Specifically, additional identifiers lengthen the cryptographic keystream of protected files. With these identifiers, it is possible to control access based upon who can access and/or where the data is located. The file ownership identifiers are: ME, GROUP, MACHINE, COMPANY, and PUBLIC. It is through these identifiers that the CAC mechanism permits access and consequentially decrypts files. A description of each is given below.

ME Files protected with the ME identifier are accessible only by the user who protected it. Access is based on the current user's PID. If it matches that of the user who protected the file, access is granted.

GROUP Files protected with the GROUP identifier are accessible only by users who have the same SID as the user who protected it. (see page 9, Group Structure").

MACHINE Files protected with the MACHINE identifier are accessible only on the workstation that it was created on and then, only by users that are allowed to access the workstation (i.e. through the I&A mechanism). This is made possible though a unique phrase given to each individual workstation by the administrator. Wang's documentation calls this phrase the Machine Identifier (MID).

¹The NCSC Computer Security Subsystem Evaluation program does not evaluate encryption nor can encryption be used to meet any of the CSSI requirements. Therefore, this report cannot be considered as a comment or endorsement of the strength of MicroControl's encryption algorithm.

Final Evaluation Report Wang MicroControl System Overview

COMPANY

Files protected with the COMPANY identifier are accessible by all users that are allowed to access the workstation. COMPANY protected files are also transportable to all workstations that have the same Configuration Identifier (CID). Similar to the MID, the CID is also a phrase entered by the administrator.

PUBLIC

Files protected with the PUBLIC identifier are accessible by all users that are allowed to access the workstation. They are not encrypted.

In addition to the individual identifiers, files can be protected with multiple identifiers. Such files are accessible only by users who can pass through each identifier protecting the file. These files have a higher degree of cryptographic protection (the keystream is lengthened) and tighter control on who/where the data can be used.

Executable file, such as COM or EXE files, can also be protected by an identifier. To execute the file, it must be unprotected (i.e. under the PUBLIC identifier) and then protected again when done.

If the OWNER command is not issued with an identifier during the session, MicroControl defaults to PUBLIC. All newly created files would then be accessible by any user. Specifically, MicroControl does not provide default protection until specified by the user. To obtain a greater level of trust, a default setting of OWNER ME should appear in the AUTOEXEC.BAT. Since batch files can not be protected and be issued, all users should check the identifier used to protect their files after login. Thereafter, users could still choose not to protect a file or change the settings by issuing the OWNER command with another identifier.

Resource Access Control

When a call is made to an I/O port address, the RAC mechanism determines if the data can be moved to or from the address. Conceptually, RAC is a limited implementation of DAC on devices because it can only permit or deny access (see page 7, "Objects"). For disk drives, this control is extended to permit either read, write, or no access to the drive. In either case, access is always based upon the permission recorded in an enumerated access state. This permission appears as "YES" or "NO" to the device in every state. For example, an administrator may allow "Hard Disk 0 READ = YES" for state 8. Administrators are allowed to define up to eight states and then define the permission allowed for each device in that state. These states are called "access levels" in Wang's documentation and should not be confused with the hierarchical portion of a security level as defined in the TCSEC.

Each user is then assigned one of these access states by the administrator during configuration. By default a user can only access those devices listed in his assigned state, however the administrator may configure the system so that all users have access to any devices listed in any logically lower state. This feature is referred to as Mandatory Access

Final Evaluation Report Wang MicroControl System Overview

Control (MAC) in the MicroControl documentation. In this report, this feature will be referred to hierarchical RAC in order to avoid confusion with MAC as described in the TCSEC.

File Access & Controlling Access

The order and the specific procedure for granting access to a file is unknown because design documentation was unavailable for the evaluation. Generally, RAC determines if authorization to the device is allowed and CAC determines if access to a file is allowed.

When a file is created, that file is assigned the access identifier(s) listed in the OWNER setting. The identifier is then encoded into the file. If multiple identifiers are active, the file will be protected by a combination of identifiers and users attempting access to the file must be permitted through each identifier before access is granted. There are two kinds of access to files: ALL or NONE. Any user with access to a file can read, write, execute (after converting it plain text), delete, and/or change the access identifiers of that file. Administrators should be aware that uncontrolled propagation of access rights can result from MicroControl's DAC. Although DOS directories are a special form of files, MicroControl does not control access to directories or sub-directories, only on the files within them.

After a file is created, the file's access identifiers can be changed by any user with access to the file. This occurs when either the PROTECT or the UNPROTECT command is executed, or when a copy is made. All users with access to a file can execute these commands. Executing the PROTECT command can change a file's access identifiers. The UNPROTECT command changes a file's access identifier to PUBLIC; converts it to plain text. If a user copies the file, the new file takes on the access identifiers in the user's OWNER setting at the time of the copy. For example, a user can share files with other group members by saving a file after executing an OWNER GROUP command or by executing PROTECT GROUP FILENAME command after the file has been created.

Administrators should be aware of MicroControl's DAC capabilities and limitations. The CAC mechanism protects file access through DOS and BIOS calls. The RAC mechanism prevents direct access to the I/O ports on which the devices reside. For a disk drive, RAC can be used to stop disk utilities and absolute control of the disk controller. However, it is impossible for the RAC mechanism to discriminate between a legitimate reference made by the operating system and by an illegitimate reference made by a disk editor or user written disk handler. MicroControl's RAC mechanism either allows or prevents all access. Therefore, if administrators permit access through RAC to the disk drives, they must be aware of the absolute addressing capability of the disk drives.

Final Evaluation Report Wang MicroControl System Overview

Audit

MicroControl provides the capability to create an audit trail of workstation activity. Audit must be selected from the MANAGER program before any specific event can be audited. The auditable events are:

- Logon
- Logoff
- Logon failure
- project identifier
- MS-DOS program execution
- Session suspend
- Failure to end suspend
- I/O access violations
- File access violations
- Session summary

The audit log for each user session contains the date and time of each event, the PID and SID, the RAC access state for the user, the machine identifier, the project code if configured, and the type of each event. The audit trail initially resides on MicroControl's static RAM. Its buffer is cyclically updated and is designed to hold 100 to 200 audit records.

As an evaluated subsystem, MicroControl must be configured to automatically write the audit records from this buffer to disk. This can be accomplished by enabling the "Audit Flush Enable" option. This option purges MicroControl audit buffer to disk when the user logs on and whenever it fills. Additionally, administrators must periodically copy the audit file to backup a medium so that the occupied disk space can be relieved.

EVALUATION AS AN I&A, DAC, AND AUDIT SUBSYSTEM

This chapter of the report maps MicroControl's I&A, DAC, and audit feature requirements, to the CSSI assurance and documentation requirements. The comparisons are made against the requirements at the highest level at which the evaluation team determined MicroControl to satisfy. Where MicroControl does not satisfy a requirement, the minimum requirement is stated and the deficiency enunciated.

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.

Final Evaluation Report Wang MicroControl Evaluation as an I&I, DAC, and Audit Subsystem

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

There are no apparent methods to bypass the login window and thus no other actions can occur before logon. In order to gain access to the workstation, users must identify and authenticate themselves.

MicroControl possesses the capability to identify specific users based upon their PID and SID. This includes specific system users such as the workstation administrators and assistant administrators. Note, MicroControl can be configured to accept guest users, but this configuration was not evaluated as it would not meet the D2 requirement.

Users can be uniquely authenticated after they type their password. For version 1.0650, the typed password is compared against the data read off an electronic token. For version 1.0660, the password is compared against an internal data base.

MicroControl possesses the capability to pass the identity of the user to the protected system, and its DAC and auditing components.

Conclusion

MicroControl satisfies the D2 Identification and Authentication requirement.

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

Final Evaluation Report Wang MicroControl Evaluation as an I&I, DAC, and Audit Subsystem

users to specify and control sharing of those objects by named individuals or defined groups or both.

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.

Applicable Features

MicroControl's provides discretionary access control between subjects and objects. The subjects are processes executing on the behalf of identified and authenticated users. The evaluation showed that the user identities were available to the DAC component. The identity of objects were also shown to be passed so that the access decision could be made. The objects in MicroControl are files, memory, and the MicroControl protected devices.

Final Evaluation Report Wang MicroControl Evaluation as an I&I, DAC, and Audit Subsystem

Files

The mechanism which allows subjects to share files are the ME, GROUP, MACHINE, COMPANY, and PUBLIC identifiers. These identifiers and how access mediation is performed, are described on page 10, "Discretionary Access Control". Essentially, MicroControl uses a mechanism called CAC to determine if access can be permitted based upon the identifier(s) protecting the file and the current user identity.

User's have the capability to protect a file with one or more of these identifiers. Once the identifier is specified other users have either complete or no access to a file (i.e. the set of authorizations). If access is granted, the user can alter the file or the file's access identifiers protecting it. MicroControl is not capable of controlling the propagation of access rights.

MicroControl is designed to mediate DOS and BIOS file operations to files. RAC assures that access to the physical sectors of a disk is prevented. Note, that RAC either permits access or denies it for both user processes and the operating system.

Memory

MicroControl only allows a single user to be on the workstation at a time. The subjects acting for that user are able to directly manipulate all of memory residing outside of CAM control. They may therefore be able to conflict with one another, but a user is responsible for his own domain and the subjects that execute within it.

MicroControl controls access to memory by assuring that the processes of other users are not present in memory after the user logs out. This is accomplished by warm booting the workstation.

Devices

MicroControl's RAC mechanism provides access control to the three parallel ports, two asynchronous communication ports, to the synchronous data link control adapter (SDLC), the network adapter, the DCA IRMA port, the ARCNET port, the WLOC port, and the disk drives (see page 7, "Objects").

The RAC mechanism as discussed on page 12, "Resource Access Control", can either permit or deny access to these devices based upon the configuration established by the administrator.

Although a DAC/D2 requirement, MicroControl's DAC mechanism has the capability to interface with the auditing component of itself.

Conclusion

MicroControl satisfies the D1 Discretionary Access Control feature requirement.

Final Evaluation Report Wang MicroControl
Evaluation as an I&I, DAC, and Audit Subsystem

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

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.

Final Evaluation Report Wang MicroControl Evaluation as an I&I, DAC, and Audit Subsystem

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

MicroControl was able to create and maintain an audit log that recorded the types of events listed on page 14, "Audit". For each of these events, the log lists the PID, SID, the machine name, time, and a line of text. This text line contains either the DOS command or the action initiated. If the action failed, the type of violation is displayed.

The audit log can only be read and manipulated by privileged users. Privileged users have the capability to process the audit log into readable text using the reduction tools supplied.

Conclusion

MicroControl satisfies the D2 feature requirement for Audit.

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

MicroControl's CAM mechanism maintains a protected domain for execution without placing a layer upon DOS. It also assures that its internal data base, internal code, and the internal audit buffer cannot be modified from an external source.

MicroControl architecture allows any accessible process (subject) to execute for a previously authenticated user. The architecture also protects the subset of objects as defined on page 7, "Objects". All other objects within the workstation are accessible and not protected.

Conclusion

MicroControl satisfies the D1 Subsystem 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.

Final Evaluation Report Wang MicroControl
Evaluation as an I&I, DAC, and Audit Subsystem

Interpretation

- D1

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

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

Applicable Features

MicroControl is supplied with a diagnostic routine to test the operation of the board. The diagnostic is initially executed during installation and can be executed thereafter by issuing SPDIAG.COM from DOS. However, no indication was given of its exact operation.

Conclusion

MicroControl does not satisfy the D1 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.

Final Evaluation Report Wang MicroControl
Evaluation as an I&I, DAC, and Audit Subsystem

Applicable Features

MicroControl's security mechanisms work as documented for the types of attacks it was designed to prevent. However, the introduction of a disk utility program will enable users to read (encrypted) sectors from the disk.

Conclusion

MicroControl does not satisfy the D1 Security Testing requirement.

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

A complete user manual is provided and describes MicroControl's protection mechanisms, logon procedure, commands, and other non security relevant capabilities.

Conclusion

MicroControl satisfies the D2 Security Features User's 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.

Final Evaluation Report Wang MicroControl
Evaluation as an I&I, DAC, and Audit Subsystem

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

The Workstation Administrator's Guide (WAG) details MicroControl purpose, installation, access control, MANAGER, the I&A mechanism, auditing, and commands. Within these sections its privileges are presented and how they are controlled (i.e. by the Workstation Administrator's SID). The WAG accurately reflects the product's integration into the overall system. However, all specific cautions and warnings needed to properly operate the subsystem are not described.

Conclusion

MicroControl does not satisfy 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

Wang failed to supply any testing documentation to indicate whether the product had been exercised.

Final Evaluation Report Wang MicroControl
Evaluation as an I&I, DAC, and Audit Subsystem

Conclusion

MicroControl does not satisfy the D1 Test 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

Wang failed to supply design documentation.

Conclusion

MicroControl does not satisfy the D1 Design Documentation requirement.

Final Evaluation Report Wang MicroControl
 Evaluation as an I&I, DAC, and Audit Subsystem

Rating Assignment

This section describes the composite feature rating and how it is determined. The composite rating for each evaluated feature is based upon the individual ratings awarded as previously described. These individual ratings are combined with ratings for assurances, documentation, and "supporting functions" (see discussion below). The resulting composite rating is equal to the lowest rating awarded in any one of the individual ratings or "supporting functions".

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

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

The "supporting function" must be at the same level as that of the feature to obtain the resulting rating.

Taking the values attained in Section 3 (above), the composite ratings for each of the three features of MicroControl are derived as shown in table 1. Note that MicroControl provides the supporting functions by integrating them within the feature. Since MicroControl does not provide all of the required assurance, documentation and supporting functions, MicroControl will be placed on the EPL as a D I&A, D DAC, and D Auditing Subsystem.

TABLE 1

EVALUATED FEATURE	INITIAL FEATURE RATING	LOWEST RATING (ASSURANCE)	LOWEST RATING (DOCUMENTATION)	REQUIRED SUPPORTING FUNCTION	SUPPORTING FUNCTION RATING	COMPOSITE FEATURE RATING
I&A	D2	D	D	AUDIT DAC*	D Yes	D
DAC	D1	D	D	I&A	D	D
AUDIT	D2	D	D	I&A DAC*	D Yes	D

* Audit and/or authentication data must be protected through DAC or domain isolation. Isolation is defined as any mechanism which prevents a subject from accessing the processes or data structures which provides the feature.

EVALUATOR'S COMMENTS

Administrators must exercise caution when programming tokens. Since they are portable among workstations with similar configurations, it is possible to configure multiple tokens or accidentally alter the data it contains. This will significantly impact on the accountability of the I&A mechanism. MicroControl displays warning screens to prevent this and they should be followed closely.

Both versions of MicroControl do not support the assignment of initial passwords to user accounts. As designed, the administrator need only define a user and program a token for version 1.0650. Once the administrator permits a user to log on and distributes the token for version 1.0650, that user is able to initiate the first session by typing in any valid password. MicroControl will then use it thereafter. This weakness can only be eliminated by administrative procedures. When an administrator creates an account, a password should be assigned and then invalidated so that it must be changed at the next successful logon.

MicroControl is capable of overwriting the data contents of files at deletion and MicroControl is also capable of calling DOS to clear memory when a user logs out. These capabilities may be appropriate for some installations. However, MicroControl should not be considered a complete object reuse subsystem because it does not revoke all information from all storage objects.

Although not a part of the evaluated configuration, MicroControl claims to provide protection of files residing on LANs and mainframe hosts. MicroControl also claims the ability to call DOS to clear memory when a user logs out and to overwrite files when deleted. MicroControl was not evaluated as an object reuse subsystem because it does not revoke all information from all storage objects. Although these capabilities are not a part of the evaluated configuration, they may be appropriate for some installations. These installations may want to research these capabilities further.

This page intentionally left blank.

Final Evaluation Report Wang MicroControl
Evaluated Hardware Components

EVALUATED HARDWARE COMPONENTS

This appendix lists the Wang marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by this subsystem evaluation. The primary requirement for hardware is that the hardware function properly. This was verified by the diagnostic tests performed by the MicroControl board, the SYSWATCH, and the SYSCHECK programs used only during installation.

To operate in correspondence with the I&A D, DAC D, and Audit D rating, the security subsystem must contain the hardware components listed in this section.

A MicroControl system board release 1.0650 and token receptacle. Any number of the electronic tokens used to gain access to the system.

OR

A MicroControl system board release 1.0660. It should be noted that the token receptacle for version 1.0660 is non-existent purportedly for TEMPESTing purposes.

The protected system covered by this evaluation is the Wang Professional Computer, 200/300 series.

This page intentionally left blank.

Final Evaluation Report Wang MicroControl
Evaluated Software Components

EVALUATED SOFTWARE COMPONENTS

This section lists the programs that make up the various divisions of MicroControl's software. The software for both versions is delivered on two disks, the configuration diskette and the Security Control Menu diskette. All files except the MANAGER program identical are identical regardless of the version. The files contained on both disks are listed below for reference:

General Files & Programs

~ARCHIVE.TRI	READ.ME	SPDIAG.EXE
ALLOWBRK.EXE	SAFECLK.EXE	TRISPAN.EXE
ATTN.COM	SCMENU.EXE	UCONTROL.DFT
PACKAGE.EXE	SCMENU.HLP	UCONTROL.HLP
PREPDIAG.COM	SCMENU.IDX	UCONTROL.IDX

Installation Programs

INSTALLM.BAT	SYSCHECK.EXE	SYSWATCH.COM
INSTALLU.BAT		

User Files & Commands

EXPORT.BAT	OWNERDIR.BAT	SPRINT.BAT
IMPORT.BAT	PROJECT.BAT	UNPROTEC.BAT
LOGOFF.BAT	PROTECT.BAT	VERSION.BAT
OWNER.BAT	SCRIPTER.BAT	WHO.BAT
SUSPEND.BAT		

Administrative Files & Commands

AUDIT.BAT	ORPHAN.BAT	PRINTC.EXE
AUDITACT.BAT	OVERRIDE.BAT	SETCLOCK.BAT
MANAGER.EXE	PRINTAAF.BAT	

MicroControl is designed to properly function with MS-DOS versions 2.1 to 3.2.

This page intentionally left blank.

GLOSSARY

ADP	Automatic Data Processing
CAC	Cryptographic Access Control
CAM	Controlled Access Mechanism
CID	Configuration Identifier
CSSI	Computer Security Subsystem Interpretation
DAC	Discretionary Access Control
EPL	Evaluated Products List
H	Hex
I&A	Identification and Authentication
I/O	Input and Output
LAN	Local Area Network
MAC	Mandatory Access Control
MID	Machine Identifier
MS-DOS	Microsoft Disk Operating System
NCSC	National Computer Security Center
PC	Professional Computer
PID	Primary Identifier
RAC	Resource Access Control
RAM	Random Access Memory
SDLC	Synchronous Data Link Controller
SFUG	Security Features User's Guide
SID	Secondary Identifier
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual
TSR	Terminate and Stay Resident
WAG	Workstation Administrator Guide
WLOC	Wang Local Office Connection

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE				
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT UNLIMITED DISTRIBUTION		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE				
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-89/008		5. MONITORING ORGANIZATION REPORT NUMBER(S) 5232,551 S235317		
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center	6b. OFFICE SYMBOL <i>(If applicable)</i> C12	7a. NAME OF MONITORING ORGANIZATION		
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>		
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 Wang Laboratories, Inc. MicroControl				
12. PERSONAL AUTHOR(S) Clawson, Deborah; Oehler, Michael; Rovansek, Shawn				
13a. TYPE OF REPORT Final	13b. TIME COVERED FROM ___ TO ___	14. DATE OF REPORT <i>(Yr, Mo., Day)</i> 891011	15. PAGE COUNT 43	
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 DAC CSSI	
19. ABSTRACT <i>(Continue on reverse side if necessary and identify by block number)</i>				
<p>THE National Computer Security Center (NCSC) examined the security protection mechanisms provided by Wang's MicroControl Version 1.0650 and 1.0660. MicroControl 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), and the audit requirements of the CSSI is class D. The overall D rating resulted from MicroControl's inability to meet all assurance and documentation requirements specified by the CSSI.</p> <p>This report documents the findings of the evaluation.</p>				
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED		21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL DENNIS E. SIRBAUGH		22b. TELEPHONE NUMBER <i>(Include Area Code)</i> (301)859-4458	8b. OFFICE SYMBOL C12	

DD FORM 1473, 83 APR

EDITION OF 1 JAN 73 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

U.S. GOVERNMENT PRINTING OFFICE: 1980 O-881 051