NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF FISCHER INTERNATIONAL WATCHDOG

VERSION 4.1

24 October 1986

SUBSYSTEM EVALUATION REPORT

FISCHER INTERNATIONAL

WATCHDOG VERSION 4.1

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

October 24,1986

Library No. S228,383

This page intentionally left blank.

FOREWORD

Accession For	
NTIS GRA&I	☑
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

This publication, the final evaluation of Fischer International's Watchdog Version 4.1, is 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 an evaluation of Fischer International's Watchdog Version 4.1 product. The requirements stated in this report are taken from DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, dated December 1985.

Approved:

October 24, 1986

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

ACKNOWLEDGEMENTS

Evaluation Team Members

Mark Gabriele
Paul Hager
Leon Neufeld

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

CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

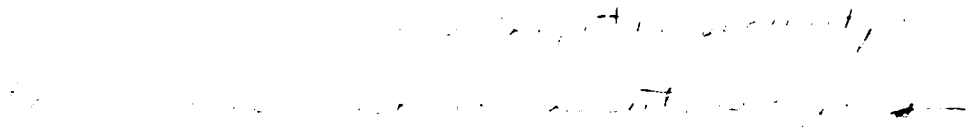
Watchdog Version 4.1 has been evaluated by the National Computer Security Center (NCSC). Because Watchdog is considered to be a security sub-system, rather than a complete trusted computer system, it was not evaluated against the entire class of security requirements as presented in the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria), dated December 1985. Instead, it was evaluated as to how well it implemented Discretionary Access Control (DAC), Identification and Authentication, Object Reuse, and Audit.

The NCSC evaluation team has determined that Watchdog Version 4.1, when configured as tested, is capable of applying the security features referenced above to data stored on the non-removable hard disk of an IBM PC/XT or a system of compatible architecture. (Here, and throughout the remainder of this report, "compatible" means IBM PC, IBM PC AT, IBM PC XT, IBM PC 3270, AT&T PC 6300, COMPAC, ITT XTRA, or ZENITH Z-150.) Watchdog can maintain user identification and authentication by requiring each user to enter a proper user ID and password prior to gaining access to Watchdog-protected resource menus and facilities. Watchdog can mediate user access actions, and with the aid of access control lists, determine which users are authorized to access protected files and directories. DAC is enforced through the use of user IDs and passwords. In the process of determining access to data areas and files protected by Watchdog, an audit record of user actions is maintained (e.g., user attempts to access protected data files, user logoff, logon, etc.). Once the current user logs off, Watchdog modifies the workspace so that the next user will not have access to any residual data (object reuse). Watchdog encrypts all data which is stored in its protected areas on the non-removable hard disk drive. During the course of the evaluation, the team made no attempt to evaluate the strength of the data encryption scheme used by Watchdog. The team only established that the data used in the functional testing was successfully transformed (encrypted/decrypted).

These security mechanisms can be maintained only if the code that implements them can be protected from unauthorized modification. However, because these mechanisms are implemented in single-state machine hardware, user/system isolation is very difficult to maintain. In systems with a single-state architecture, the user operates in the same memory space in which the security-related IBM DOS system functions. It becomes possible for a programer to change, destroy, or access important sections of code without the likelihood of detection.

Watchdog can be installed with various combinations of its security mechanisms implemented, and still offer the user some degree of security. However, in order to give the user maximum assurance that Watchdog's security mechanisms can be maintained, the NCSC recommends that Watchdog be configured in the mode tested (i.e., the optional high security configuration mode). This involves configuring both the Watchdog system software and hardware such that all non-privileged users are denied access to all DOS commands (IBM PC DOS system functions, especially direct I O commands). In addition, the system administrator must ensure that the application programs (including memory resident type) run by the non-privileged user do not allow him access to these DOS commands. In this configuration, there is some assurance that Watchdog security features will not be circumvented. However, the PC's functionality is reduced. Non-privileged users are no longer able to run compilers, assemblers, debuggers or any type of program which gives them access to IBM DOS system functions (e.g., DOS commands, direct I/O, etc.).

Even though this does result in the PC being placed in an application-restricted environment, we believe that such restrictions are necessary in order to maintain the integrity of Watchdog's security features. Once these particular capabilities are protected, Watchdog, in the configuration tested, does implement effective user identification and authentication, discretionary access control, event auditing, and object reuse on the IBM PC XT or compatible machine.



INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system 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 Sub-system Evaluation Program.

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

Introduction

Sub systems 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 sub system evaluation is limited to consideration of the sub system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub system's security-relevant performance in light of applicable standards and features outlined in the 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, a summary of the evaluation report will be placed on the Evaluated Products List

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

PRODUCT EVALUATION

Product Overview

Watchdog is a microcomputer software package which provides access control to programs and files while maintaining user separation (discretionary access control), user logon procedures (identification and authentication), auditing of user actions (audit), and elimination of previous users' data from memory (object reuse). In addition to these highly desirable security features, Watchdog also provides some protection against accidental or malicious formating of the non-removable disk or access to the data stored on the non-removable disk. Watchdog provides additional data protection by encrypting stored information. Watchdog also contains many additional features designed to enhance administrative management of the PC; however, the evaluation team did not formally test these features since they were not considered security-relevant.

Evaluation of Functionality

Discretionary Access Control

The Watchdog system allows for discretionary access control between objects (i.e., data areas and files) and subjects (individual users). Watchdog provides discretionary access control over those objects located on the section of the non-removable hard disk drive protected by the Watchdog software. Before providing any details of the Watchdog discretionary access control mechanism, it should be noted that non-privileged users can only access and execute objects through the use of Watchdog-provided menus. That is, ordinary users are only able to execute menu-listed programs (e.g., application programs). Only the System Administrator (SA) is able to construct and modify Watchdog menus.

Data areas represent file directories which can contain numerous subdirectories and files. A maximum of 256 data areas are under the control of the Watchdog system, including the IBM DOS system root directory. User access to each data area and file is set by the SA. By default, data areas are accessible to

the SA only. It is the SA who, upon Watchdog system initialization, first defines file and data area access for each of the system's registered users. At the request of a user, the SA can grant or deny access to these objects by adding or deleting entries in the appropriate object access tables. Access to objects is decided in reference to the user's ID. The SA can require that a user enter a correct password in order to gain access to particular data objects. Three "profile" tables are referenced by Watchdog during the process of mediating access control. Some access control information such as valid user IDs, passwords, and expiration dates is stored in these tables. The three tables used to control user access to data objects (discretionary access policy) are called the "System", "Area", and "User" Profile files. Only the SA can alter the contents of these access control files.

The System Profile table contains users' access permissions to those IBM DOS system capabilities which can affect data integrity, such as the ability to execute DOS commands. The Watchdog System Profile table will contain the user ID's of those users authorized to access such IBM DOS system functions. Passwords can be required of users requesting access to privileged IBM DOS system functions, data areas, or files. However, the SA should be aware that even if a user is restricted from accessing IBM DOS system functions by the System Profile setting, the user can still gain access to these IBM DOS system functions by use of "exit to DOS" features in some applications programs.

The Area Profile table contains information pertaining to each data area under Watchdog control. Such access information includes area name, area number, applicable area password(s), and the corresponding access permissions associated with that area (i.e., Read, Write, and Create/Delete). The SA may designate particular permissions as being global for a given data area. Should this be the case, all users having access to that area would automatically inherit that specific access permission. The SA may also deny access to an area for individual users, or globally for all users.

The User Profile table provides the Watchdog access control software with information on each PC user, such as user ID, passwords associated with each user ID (e.g., logon, area, and file passwords), a list of areas accessible to that user, and the particular access permissions the user may invoke for each area on the access list. The User Profile table is used most often during area file access checks and the user identification authentication process. The object and access

lists within the User Profile Table are used to define those specific access permissions available to each registered Watchdog user.

Only the System Administrator is able to alter the System, Area, and User Profile tables.

Identification and Authentication

Before gaining access to data areas and files under Watchdog control, each user must enter a valid user ID and corresponding password. Under Version 4.1, user ID's and passwords have no default minimum length; however, the SA can specify a minimum password default length for all users. Passwords have a maximum length of twelve characters. User ID's and passwords are alphanumeric. Upper and lower case letters are significant only in passwords. Initially, the SA assigns each user a unique user ID and password. Afterward, the users can select their own passwords.

User ID's and passwords are stored in the System Administration program. This program is stored on the System Administrator Diskette, which is maintained and protected by the SA. The SA uses this diskette to establish and change user ID's and passwords, area descriptions, and directory names. Upon Watchdog system generation, user ID's and passwords are copied to protected files within Watchdog's domain on the non-removable hard disk. In addition to being stored in protected files, both passwords and user ID's are encrypted. When a user enters his or her own password at logon, it is transformed and compared to the encrypted form stored on the non-removable disk. User ID's are decrypted to plain text prior to comparison and validation. Only the SA is authorized to set and delete user ID's. Users may have their logon password changed by requesting such action by the SA, or they may change it themselves.

There are three types of passwords on the Watchdog system: primary, alternate, and one-time. Primary passwords are changed infrequently and represent the major means by which Watchdog carries out user authentication and access control to data areas. For additional flexibility, the user may request that the SA designate an optional alternate password or he may designate one himself (this option is not recommended since it increases the possibility of successful password guessing). This alternate password would serve the same purpose as a primary password in that a user could enter the alternate password instead of the primary password. One-time passwords can be assigned by the SA

for instances in which a user will only temporarily require access to the Watchdog system or a data area. The one-time password is voided after its first use.

Additionally, the SA is able to preset a time limit of usage for a particular password, or define a maximum number of uses for any user's password. The Watchdog system also has a time-delay penalty to inhibit the guessing of passwords. After the first three unsuccessful attempts to enter a correct password, Watchdog delays the next logon prompt for 30 seconds. For every three subsequent incorrect password attempts, the time delay is doubled, and so on.

Object Reuse

Watchdog implements object reuse by modifying the user's data work space after he logs off. Residual information in transitive memory such as RAM and cache is changed between use by different users in such a way that the new user cannot gain any useful information from the prior user's process. Data stored on the non-removable hard disk is encrypted with each data area having a different encryption key. Some memory resident applications programs (e.g., Borland's Sidekick, etc.) which use common work space are not cleared between user sessions.

Audit

Watchdog provides comprehensive audit capabilities which may be employed to monitor use of the protected machine and any data which might be stored on its non-removable hard disk. Seven different types of audit reports may be selected, and the granularity of the audit may be adjusted from all users of the PC down to any individual user of the PC. The audit tools provide a convenient means of tracking PC usage from many different perspectives.

The audit mechanism gathers data on all successful logons, their times, and their user ID's. It also monitors the areas accessed, and can be set to monitor the use of any program specified by the System Administrator; however, the program-usage recording functions were not tested. There are seven different audit functions; during testing of the product, each of these seven was tested individually. It should be stressed that in this evaluation, the aim of the team was simply to test for functionality, and NOT to penetrate the security controls of the Watchdog system. The results of the testing follow:

Function 1: Detail - Session Only report.
This report shows the time and date the user or users of interest logged onto and off of the PC. This feature worked as documented.

Function 2: Detail - Area/Program report.
This report shows the areas logged into and programs executed by the specified user ID. Worked as documented, to the extent tested. However, functional testing did not include use of Watchdog "projects" or program tracking.

Function 3: Detail - Comprehensive report.
Shows all activity involving areas accessed, programs executed, and project ID's on which work was done during the logon session. Worked as documented.

Function 4: Summary - Session Only report.
Shows elapsed time between logon and logoff for a range of dates. Worked as documented.

Function 5: Summary - Area / Program report.
This report presents the same information as in the Detail Area / Program report, summarized so that date and time logged in and out are not given. This function contained a documentation error: Watchdog did not print the cumulative access time, as the documentation would indicate; it instead printed no times at all. Otherwise, Watchdog performed as documented.

Function 6: Exceptions Report.
This report shows security violations which have been recorded in the audit log, as well as PC activity which Fischer-Innis feels may be suspicious or inappropriate (for example, excessive usage). Several garbage records were generated. These garbage records caused no loss of audit data, and may have been caused either by hardware error or by Watchdog error. Removal of the garbage records is a straightforward but tedious process.

Function 7: Text File.
This function generates a sequential file of text which contains administrator-selectable

audit record information. The documentation for this area is incomplete; the "status" fields in the audit records are defined, but the audit documentation gives no indication as to what the meanings of the various status codes might be. Otherwise, this feature appeared to perform as documented.

Documentation

The Watchdog security software package consists of two documents, the Watchdog PC Data Security User Guide and the Watchdog PC Data Security System Administrator Guide.

Watchdog PC Data Security User Guide

This 60-page guide is intended for the end user. It describes to the user the protection features of Watchdog and gives him guidelines on their use. It includes the following sections.

Section 1 Introduction

This section gives the new user a brief overview of Watchdog's security features and explains how they are applied to protect system and user objects.

Section 2 Logging On

This section gives the new user details of the logon procedures. This section also includes examples of incorrect logon attempts and explains how a user can recover from logon errors.

Section 3 Locating Your Program

This section gives the user details of how storage areas are organized into different menus and sub-menus.

Section 4 Moving Within Watchdog

This section instructs the user on proper ways to move between the different storage areas.

Section 5 Building Sub-menus

This section gives the user additional details on how to use the special tools (the menu builder) provided by Watchdog to develop efficient nested sub-menus for data storage.

Section 6 Utilities

This section gives details of the DOS support utilities provided by Watchdog. The use of these utilities should be restricted to the most trusted users because these utilities can be used to circumvent Watchdog security mechanisms.

Section 7 Audit Trail

This section gives details of how the users can generate audit reports for their own system activity.

Section 8 Mailbox

This section gives the user details of the inter-office communications features available from Watchdog.

Glossary

This section includes definitions of some of the special names and terms used by Watchdog and an index to what sections of the manual they are in.

Watchdog System Administrator Guide

This 214-page guide is intended for the System Administrator and is designed to instruct him on the proper installation and administration of the Watchdog product. It is divided into the following eleven sections:

Section 1 Introduction

This section provides a general overview of the security and administrative features contained in the Watchdog product.

Section 2 Drives and Directories

This section contains a detailed overview of how the file directories and work areas are organized.

Section 3 Security Features

This section contains a description of the critical Watchdog security features. Included is a review of user passwords, area passwords, and system permissions. Also included in this section are details on the different features which can be used to maximize the security of the system.

Section 4 System Administration

This section describes the Watchdog System Administration Program (WDSA). Specifically, it outlines the process for changing user ID's, passwords, and permissions.

Section 5 Audit Trail

This section contains a description of the Audit Trail feature. A review of how Watchdog monitors system usage and generates audit reports is provided. Several errors were noted in this section (see the Audit section of this evaluation report, page 6).

Section 6 Area and Menu Management

This section contains information on how the System Administrator can organize programs and files to form various application menus.

Section 7 Installation Procedures

This section contains a detailed, step-by-step description of how the Watchdog software is installed.

Section 8 Troubleshooting Guide

This section contains information on how to resolve possible Watchdog problem conditions along with explanations of corresponding error messages.

Section 9 Appendices

This section consists of detailed descriptions of disk backup/restore, encrypted file transfer, and automatic batch file execution programs. Other general-support programs are also reviewed in this section.

Section 10 Advanced Topics

This section instructs the System Administrator on the procedure for constructing multiple system libraries.

Section 11 Glossary/Index

This section includes definitions of some of the special names and terms used by Watchdog and an index to what sections of the manual they are in.

This page intentionally left blank.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data stored on these systems. Initially, this protection was provided solely by the individual user who would simply remove and lock away diskettes which contained sensitive data. These physical and procedural controls isolated users and prevented them from intentionally or accidentally accessing or modifying other users' data. Since each user maintained physical possession of his own data and operating system, there was reasonably high assurance of maintaining data and code integrity. No other security mechanisms were deemed necessary, since the user would only be able to inflict damage to his own data or operating system.

However, with the advent of inexpensive and reliable hard disk drives, these procedural controls can no longer provide adequate user isolation and controlled sharing. It is now common practice to have many users share the same PC and store their data on the same hard disk memory unit. Users in this environment no longer have any assurance that their data can be protected from unauthorized access or modification, or even that the underlying operating system has not been subverted.

The task of providing security on the majority of microcomputers in use today is further complicated by the fact that their architectures have inherent security vulnerabilities. These vulnerabilities make it very difficult to implement protection mechanisms which isolate users from each other and provide a controlled sharing environment. This is because these systems are primarily single-state hardware machines and, as such, cannot easily support the more common security mechanisms found in larger, more fully integrated systems. Features such as multiple processor states (which provide for user process separation), privileged instructions (which limit user access to the trusted system processes), and memory protection (which prevents unauthorized user access to specific memory locations) are all mechanisms that help to maintain user isolation in a shared environment, but that are very difficult to implement on a single-state hardware machine.

Generally the security mechanisms can be maintained only if the code which implements them can be protected from unauthorized modification. However, in the case of the single state hardware machine, the non privileged user operates in the same memory space in which the security-related system functions. As a result, user isolation and data access control cannot be

maintained with any reasonable degree of assurance. In order to establish some minimal assurance that these security mechanisms can be maintained in this type of system, it is essential that all non-privileged users be restricted from accessing security-relevant system functions (e.g., all DOS commands, all I O commands, etc.).

PRODUCT TESTING

Testing Procedure

Testing represents a significant portion of a sub-system evaluation. The team developed a software test script which tested Watchdog discretionary access control (DAC), audit, identification and authentication, and object reuse functions. This functional test suite focused upon those security features identified in the Watchdog PC Data Security System Administrator Guide June 1986, Software Version 4.1. The evaluation results described by this report are valid only for the tested configuration (see below). The test suite consisted of two parts. The first was a Pascal program that attempted to read, write, and create files in every work area protected by Watchdog. Because each user possessed different access attributes, Watchdog was expected to selectively deny some of these attempts. The output of this test program was compared against Watchdog's attribute tables and audit reports. This testing was intended as a functional checklist to ensure that Watchdog's audit, DAC, and identification authentication mechanisms functioned as documented. Even though the team's testing of the DAC mechanism did involve attempts to locate flaws in the access control mechanism, the testing was functional in nature and did not attempt to circumvent or subvert the Watchdog security architecture. The second part of the test suite involved a series of manual memory searches. These searches were done after each user finished working in his work area but before he logged out. After the user's previous job (word processor documents in this case) had been located in memory, the user logged off and a different user logged on. The new user then searched memory in an effort to locate the previous user's job.

In order to afford the user the most protection, the test was run with Watchdog installed in the optional high-security configuration mode. First, all non-privileged users are denied access to all DOS command capabilities. The SA implements this by setting system permissions accordingly (see the Security Features chapter of the Watchdog SA guide). Permissions denied must include Exit to DOS, Changes to AUTOEXEC.BAT file (F5 in the Utility Section Menu), Control Diskette Booting, and User Supplied Command (F7 in the Utility Section Menu). The SA should limit access to these DOS functions (especially I O type) to only

the most privileged users because the DOS command instruction set provides knowledgeable users with the capability of circumventing Watchdog protection mechanisms.

Second, the PC XT was configured with only one floppy disk drive (drive "B") and one non-removable hard disk drive (drive "C"). When installing Watchdog, the "A" disk drive must be reconfigured as the "B" drive (by disconnecting the A drive connector and attaching the drive to the B drive connector on the drive controller cable - see details in the security configuration section of the System Administrator Guide , version 4.1, appendix F - Hardware Modifications for Preventing Diskette Booting). This is essential, because the normal IBM PC/XT or compatible operating system tries to "boot" first from the "A" drive. If the "A" drive is not found, the system defaults to the "C" drive. The "C" drive must be invoked at system start-up in order to have Watchdog's security protection mechanisms installed. Once Watchdog is installed, the B drive should only be used by the SA for system maintenance.

However, when such restrictions are implemented, the general functionality of the system is reduced. The non-privileged user must not be able to run compilers, assemblers, or any programs which allow direct DOS and I O access. The non-privileged user must be restricted solely to running application type programs available from the Watchdog system menus (e.g., word processors, data bases, spread sheets, etc.) The System Administrator must take special care to ensure that non-privileged users are not able to access DOS and I O type commands via application software. Application programs (e.g., some word processors, memory resident programs, etc.) which have exit to DOS or DOS sub shell features should not be used or should be modified so that these features no longer work.

Watchdog encrypts all data which is stored in its protected areas on the non removable hard disk. During the course of the evaluation, the team made no attempt to evaluate the strength of the data encryption scheme used by Watchdog. The team only established that the data used in the functional testing was successfully transformed (encrypted/decrypted).

Test Results

Watchdog version 4.1, when configured in the above manner, with the precautions noted, does maintain user isolation and controlled sharing of data objects on the non-removable hard disk. Even though this places the underlying system in an application-restricted environment with an associated reduction in functionality, the evaluation team feels that Watchdog, when installed in the optional high security configuration mode, provides an effective and reliable means of securing data on a single-state machine such as the IBM PC/XT. The product does provide a fully functional security overlay which requires user identification and authentication, maintains discretionary access control of data objects, implements a form of object reuse, and audits security-relevant user activity on the PC/XT.

This page intentionally left blank.

TEST PROGRAM

Pascal-language program used for testing

```
program read_write_create_test;

{this program exists solely to create, write to, and read from
files as a test for Watchdog, a program which is being evaluated
by the National Computer Security Center.  This program is
written in Borland International's Turbo Pascal}

{****** Operation of this program is as follows:
         Compile this source code into the file WATCHDOG;
         execute the command line:

         WATCHDOG [option] [filename]

         where [option] specifies the option from the following:
         R W C for Read, Write, or Create/Delete, and [filename]
         specifies the name of the file to be read from, written
         to, or created and deleted.

                                                              }

var
    garbage, {garbage to read from files}
    junk:  {the string of garbage retrieved from a file read}

          packed array [1..20] of char;

    filename:  {MS-DOS filename}
          string[36];

    option:  {selection of program operation}
          char;

    filevar:  {type of file we'll be playing with}
          file of char;

    i:  {loop counter}
          integer;


begin

  garbage:='Watchdog test 123456';
  option:=paramstr(1);
  filename:=ParamSTR(2);
```

```
  assign(filevar,filename);
  writeln (lst,'Parameters are:  option:  "',option,'" and file:
"',
    filename,'".');

case option of

'R','r':  begin

writeln(lst,'Attempting to READ from file:  ',filename);
   Reset(filevar);
   for i:=1 to 20 do
   Read(filevar, junk[i]);
   writeln(lst,'READ SUCCEEDED');
   end;

'W','w':  begin writeln(lst,'Attempting to WRITE to file:
'.filename);
   reset(filevar);
   for i:= 1 to 20 do
   write(filevar,garbage[i]);
   flush(filevar);
   writeln(lst,'WRITE SUCCEEDED')
   end;

'C','c':  begin
   writeln(lst,'Attempting to CREATE file:  ',filename);
              rewrite(filevar);
              close(filevar);
              erase(filevar);

    writeln(lst,'CREATE SUCCEEDED; file deleted');
    end;

else writeln(lst, 'Invalid Option.  Program terminates with no
action.');

end;

end.
```

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS NONE
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT DISTRIBUTION UNLIMITED
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-86/005	5 MONITORING ORGANIZATION REPORT NUMBER(S) S228,383
6a NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b OFFICE SYMBOL (If applicable) C12	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b ADDRESS (City, State, and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

(U) Sub-system Evaluation Report, Fischer International, Watchdog Version 4.1

12 PERSONAL AUTHOR(S)
Mark Gabriele, Paul Hager, Leon Neufeld

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Final	FROM _____ TO _____	861024	28

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Watchdog Fischer International NCSC TCSEC sub-system

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

Fischer International's Watchdog product was evaluated against identification and authentication, discretionary access control, object reuse and audit requirements of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. The product is an IBM PC/XT software package which, when properly installed, protects files and programs stored on the IBM PC/XT from unauthorized access. It also records system usages and permits the System Administrator to generate audit reports.

This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED

22a NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE (Include Area Code)	22c OFFICE SYMBOL
LTC Lloyd D. Gary, USA	(301)859-4458	C/C12

DD Form 1473, JUN 86 *Previous editions are obsolete.*