



NATIONAL COMPUTER SECURITY CENTER

AD-A247 251



FINAL EVALUATION REPORT
OF
EYEDENTIFY INC.
EIS System

92-05769



24 September 1990

Approved for Public Release:
Distribution Unlimited

92 8 04 013



FINAL EVALUATION REPORT
EyeDentify, Inc.
EIS System

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

NATIONAL
COMPUTER SECURITY CENTER

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

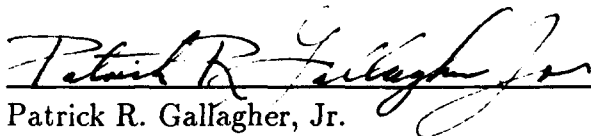
24 September 1990

CSC-EPL-90/006
Library No. S235,427

FOREWORD

This publication, the Final Evaluation Report of the EyeDentify EIS system 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 EyeDentify evaluation. The requirements stated in this report are taken from *Computer Security Subsystem Interpretation* of the *Department of Defense Trusted Computer System Evaluation Criteria* dated 16 September 1988.

Approved:



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

24 September 1990

ACKNOWLEDGEMENTS

Team Members

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

James J. Donndelinger
Charles Lavine

The Aerospace Corporation
El Segundo, CA

Contents

FOREWORD	i
ACKNOWLEDGEMENTS	ii
EXECUTIVE SUMMARY	iv
Chapter 1 Introduction	1
Evaluation Process Background	1
Subsystem Evaluation Program	2
Document Organization	2
Conventions	3
Chapter 2 Subsystem Overview	4
Product Overview	4
Security Relevant Portion (SRP)	5
Subsystem Hardware Architecture	5
Software Architecture	5
SRP Protection Mechanisms	8
Identification and Authentication	8
Chapter 3 Evaluation as a Subsystem	9
Features	9
Identification and Authentication	9
Assurances	10
System Architecture	10
System Integrity	12
Security Testing	13
Documentation	14
Security Features User's Guide	14
Trusted Facility Manual	15
Test Documentation	16
Design Documentation	17
Rating Assignment	18
Chapter 4 Evaluator's Comments	20
Appendix A Evaluated Hardware Components	22
Appendix B Evaluated Software Components	23

EXECUTIVE SUMMARY

The National Security Agency (NSA)/National Computer Security Center (NCSC) examined the security protection mechanisms provided by EyeDentify's EyeDentify Information Security (EIS) system. The EIS system uses biometric technology, retinal identification, as a means of identifying and authenticating individuals. The EIS system is a subsystem, not a complete trusted computer system. It was therefore evaluated against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC). The computer security feature evaluated was Identification and Authentication (I&A). The EIS system does not provide discretionary access control of files or storage objects, object reuse, or audit and was not rated in these categories.

The evaluation team determined that the highest rating at which the EIS system satisfies the I&A requirements of the CSSI is class D1. The EIS system provides I&A to the granularity of a single user, but does not meet all of the D2 I&A requirements.

To obtain the rated level of trust, the EIS system must be configured in accordance to the Trusted Facility Manual (TFM) and properly administered. The EIS system does not restrict access to DOS system files, programming languages, compilers, and other utilities. The EIS system does not provide access control to system objects or resources. The EIS system does not provide access control to the I&A database, but does provide access control to the commands stored in the EIS system. The commands initiated at the host computer must be protected by the host. The customer is responsible for writing and protecting the trusted code required to interact with the EIS system and to prevent access to the host until a user has been authenticated.

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

Introduction

In May 1989, the evaluation team began a product evaluation of EyeDentify's EIS system. The objective of this evaluation was to rate the EIS system against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a final rating for each of EIS system's features. This report documents the results of the evaluation. This evaluation applies only to EyeDentify's EIS system, which is one of many products provided by EyeDentify, Inc.

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

Evaluation Process Background

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

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

Subsystem Evaluation Program

The NCSC has recognized a need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the TCSEC. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

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

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

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

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria*. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the Information Systems Security Products and Services Catalog.

Document Organization

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

Chapter 3 provides a mapping between the requirements specified in the CSSI and the EIS system features that fulfill those requirements. Chapter 4 contains the evaluator's comments. The appendices identify specific hardware and software components to which the evaluation applies and provide references.

Conventions

The use of the word host refers to the computer system for which the EIS system provides identification and authentication.

Subsystem Overview

Product Overview

The EyeDentify Information Security (EIS) system is a biometric system that uses retinal identification technology to quickly and easily verify a person's identity.

The EIS system is used strictly as a means of identification. Once the EIS system verifies a user's identity, the host computer makes the necessary decisions, such as whether or not to allow access.

The EIS system does not have an access control mechanism. The customer is required to provide a mechanism to control access to the I&A database which is stored on the host computer. The database contains the users, their unique personal identification numbers (PINs) and digitized eye scans. The customer is also responsible for writing and protecting the trusted code required to interact with EIS system.

Before using the EIS system for identification, users must have an eye signature reference template created and stored on the host computer. This is done by taking a series of eye readings.

To take an eye reading on the EIS system, the user looks into the eye camera and fixates on a dot alignment target until a series of dots are lined up and perceived as one dot. This indicates the eye is in the proper position.

The user then presses the SCAN button. Using low-intensity infrared light, the eye camera (Icam) makes a 450-degree sweep of a portion of the retina centered at the fovea, or the area of sharpest vision. As it does this, the Icam takes 320 readings, measuring variations in reflection that indicate the pattern of blood vessels. This process produces a waveform that is converted into digital impulses and sent to the EIS system's microprocessor and then to the host computer, where it is stored as a 72-byte hex-ASCII eye signature.

After users are enrolled, the EIS system is used to verify a person's identity. In verification mode, a user enters a unique PIN on the host computer's keyboard and performs an eye scan. The host computer sends the corresponding eye signature to the EIS system where a comparison is done. If there is a match (above a threshold), the user is identified. In verification mode, only the first 40 bytes of the stored 72 bytes are used in the comparison.

Security Relevant Portion (SRP)

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

Subsystem Hardware Architecture

The hardware organization of the EIS system is depicted in Figure 2.1. The microprocessor is a Motorola 68000. The version of the EPROM is REV. 05-25-90 and can be verified at a site using the TFM. The EPROM contains EyeDentify's custom operating system and application software (commands).

The Random Access Memory (RAM) is used as a scratch pad, and the EEPROM is used to store the EIS system's parameters.

The parallel I/O controller controls one port and the serial controller controls two ports. There exists a separate interrupt control unit to handle interrupts.

There are three ports on the EIS system: two 25-pin serial ports labeled "Auxiliary" and "Terminal" and one 15-pin parallel port for the camera. The auxiliary port provides an EIA RS-232 DCE port for interfacing to the host computer. A complete description of this port is found in Appendix B of the design documentation. The terminal port provides an EIA RS-232 port for use with one of the compatible terminals listed in Appendix D of the TFM. This port is used to configure the EIS system's auxiliary port and other options as specified in the TFM. This port is also used to perform EIS system diagnostics.

It is possible to interact with the MC68000 through the auxiliary port, the terminal port, or through the commands provided by the EIS system. It is possible for a user to disconnect the auxiliary port and simulate commands if they know the proper format. The access control of the EIS system commands located in the host must be provided by the host system. Since the hardware is susceptible to tampering, a warning in the TFM informs the Security Administrator that the ports and box must be secured in some manner.

Software Architecture

EyeDentify has developed a customized operating system that only allows their menus, specified commands and programs used to perform digitizing and comparisons to be executed.

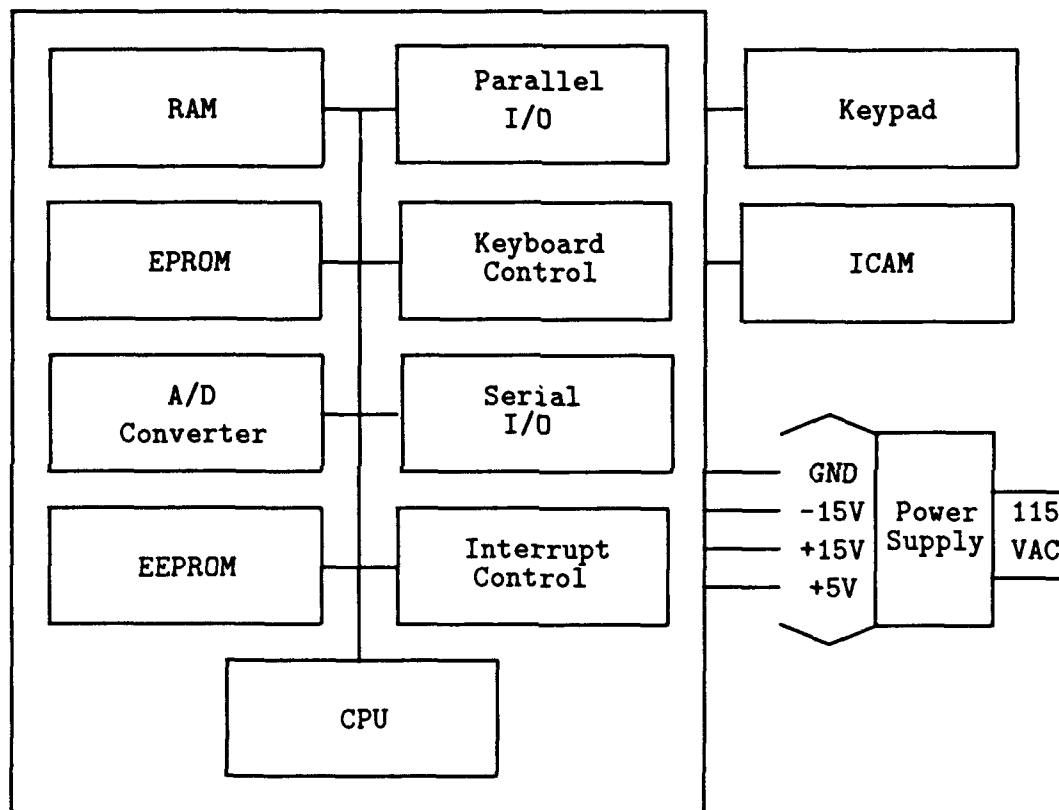


Figure 2.1: EyeDentify EIS system's Hardware Organization

The team did not examine documentation on EyeDentify's software that is used to digitize an eye scan. The team was only concerned with the software that interfaces to the host computer system. The design documentation provides a description and format for each command associated with the EIS system. The commands are separated into two groups, those initiated at the EIS system and those initiated at the host computer.

There are twelve commands that are initiated by the EIS system, they are:

- ACKnowledge
- NAK (Negative ACK)
- Transmit Eye Signature
- Verification Results
- Enrollment Results
- Timeout
- EIS System Malfunction Report
- Verification Canceled
- Reset Occurred
- Terminal Entry Text, with Response Requested
- Enrollment Canceled

There are eleven commands initiated by the host computer, they are:

- Enable EIS system
- Disable EIS system
- Activate Enrollment Mode
- Verification Mode
- Enable Verification Activation From EIS system
- Disable Verification Activation From EIS system
- Abort

- Status Report
- Retransmit Command - Command Format Checking
- Reset
- Send Text Response to EIS system

EyeDentify's customer is responsible for writing the code in their host computer to make use of these commands. The design documentation provides enough detailed information about each command to make writing code for the host a manageable task.

EyeDentify's customer is also responsible for protecting the database that contains the userIDs along with the associated PINs and eye signatures. If this database is corrupted the integrity of the EIS system would be lost.

SRP Protection Mechanisms

The EIS system provides Identification and Authentication (I&A) as its only feature. The host computer is responsible for protection of the I&A database as well as its trusted software.

Identification and Authentication

The EIS system is used strictly as a means of identification and authentication. Once the EIS system verifies a user's identity, the host system makes the necessary decisions thereafter.

Security relevant data or code is stored in the EIS system in either RAM, ROM or EEPROM. The code is stored in the ROM and EEPROM and cannot be modified by any user. It is possible for a user to remove the Auxiliary port connection to the host and synthesize the message dialog and circumvent the I&A mechanism. For this reason, there is a warning in the TFM stating the hardware and I/O ports must be secured. The host system is responsible for protecting the I&A database, the commands and any trusted code located in the host.

Evaluation as a Subsystem

This chapter presents the CSSI requirements (and interpretations) for the features that were evaluated. The computer security feature that was evaluated for the EIS system product is Identification and Authentication (I&A). For this feature, this chapter states the requirements, describes EIS system's efforts to meet those requirements, and concludes with a statement as to the level of requirements that have been satisfied. This pattern is continued for each of the CSSI requirements for assurance and documentation. Finally, a rating assignment section (see page 18 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

Features

Identification and Authentication

Requirement

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

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.

Applicable Features

The evaluation team has concluded that EyeDentify's EIS system provides Identification and Authentication to the granularity of a single user. When operating in verification mode (required mode of operation to meet the requirement), the user enters their unique PIN at the host computer's keyboard. The user then uses the Icam to perform an eye scan. The EIS system compares the eye reading to an eye signature that was determined during the enrollment procedure. The EIS system then returns a value back to the host computer where the value is a correlation between the eye signature and the eye scan just performed. The subsystem determines if access to the system should be granted, and the host simply enforces the decision. A correlation value of 0.70 and above is the range in which access should be granted. The EIS system can be configured to accept different values, but it will no longer be in the evaluated configuration. EyeDentify has documented results that show with a 0.70 correlation value the chance of a false acceptance is one in a million.

The eye signatures are stored in a database in the host computer and EIS system provides no protection for this file.

Conclusion

EIS system satisfies the D1 Identification and Authentication requirement.

Assurances

System Architecture

Requirement

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

Interpretation

- D1:

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

3.1.1.1 Execution Domain Protection

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

3.1.1.2 Defined Subsets

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

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

Applicable Features

The EIS system's I&A database is stored in the host system and the protection of this database is the responsibility of the host computer system.

The protection of the EIS system's hardware is the responsibility of the customer.

The subjects known to the EIS system are individual users, with an associated unique PIN and eye signature which are stored in the host computer system. As long as the hardware and I/O ports are protected this data cannot be corrupted at the EIS system. However, if there is no access control mechanism in the host computer this data could be corrupted.

Conclusion

EIS system satisfies the D1 System Architecture requirement.

System Integrity

Requirement

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

Interpretation

- D1:

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

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

Applicable Features

Chapter three in the TFM provides a discussion on how to perform diagnostics. It is necessary for a site to have a compatible terminal, listed in Appendix D of the TFM, in order to perform diagnostics. The trusted facility person can verify the keypad and camera work by using the diagnostic menu provided.

Conclusion

EIS system satisfies the D1 System Integrity requirement.

Security Testing

Requirement

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

Interpretation

- D1:

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

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

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

Applicable Features

EyeDentify provided the team with the software necessary to perform testing. The team requested the software be capable of issuing all commands and write to the screen the contents of each message being sent to verify the correctness of the design documentation and to ensure the correct values were being passed back and forth.

The testing was conducted with:

- The EIS system Controller Box:
 - Model Number 185-0071
 - Serial Number 101131
- The EIS system Camera:

- Model Number 185-0041
 - Serial Number 101130
- The Host System was an IBM PS/2:
 - Model Number 80

The evaluation team configured the EIS system as described in the TFM. The team then enrolled 21 people to perform security testing on the EIS system. Each person that was enrolled attempted to be verified against the other 20 people in the database. Five people that were not enrolled also attempted to be verified against the 21 people enrolled. This provided a total of 526 attempts and every attempt failed to bypass the I&A mechanism. The highest reading given to a false verification was a correlation value of 0.44, much lower than the threshold value of 0.70. Some of the participants wore contacts and this had no effect. Other tests included siblings, attempting a scan with a non-eye (blank), and a mirror.

Sometime after testing was completed it was discovered some debug code existed in the EPROMS that could be used to circumvent the EIS system. This debug code was removed and a new version of EIS was introduced. The team performed regression testing to ensure the EIS system performed as it did earlier.

Conclusion

EIS system satisfies the D1 Security Testing requirement.

Documentation

Security Features User's Guide

Requirement

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

Interpretation

- D1

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

Applicable Features

The security features user guide (SFUG) provides an introduction to biometrics and retinal identification. In addition, the SFUG provides a description of the enrollment process and how to perform an accurate eye scan.

Conclusion

EIS system satisfies the D1 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.

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 Trusted Facility Manual (TFM) consists of four chapters and four appendices. Chapter one is an introduction which provides background information on biometrics and the principles behind retinal identification. This chapter also provides an overview of the EIS system and of the TFM itself. Chapter two is a discussion of installation and maintenance. It provides a detailed description of how to electrically interface the EIS system with a host computer and provides a pointer to the design documentation for a description of the software interface. Chapter three discusses the need for a "Trusted Facility Person" and provides a method of ensuring the EIS system is configured as evaluated by the evaluation team. This chapter also provides the necessary warnings to the trusted personnel to ensure proper operation. Chapter four contains the necessary information required to correctly enroll users. Appendix A contains the technical specifications of the EIS system. Appendix B illustrates the acceptance diamond which is an important concept in obtaining acceptable eye scans. Appendix C discusses the use of eyeglasses. Appendix D provides a list of compatible terminals which are necessary for configuring and ensuring the integrity of the EIS system.

Conclusion

EIS system satisfies the D1 Trusted Facility Manual requirement.

Test Documentation

Requirement

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

Interpretation

- D1:

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the

subsystem being tested, the protected system, and other subsystems shall be described.

Applicable Features

EyeDentify has provided the evaluation team documentation which describes EyeDentify's testing philosophy, test plan and test procedures. EyeDentify has also provided documentation describing the actual test configuration and procedures used in determining their correlation value of 0.70 as producing one out of a million false verifications. EyeDentify has a quality assurance group to ensure adequate testing is performed.

Conclusion

EIS system satisfies 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

The design documentation consists of five chapters and four appendices. Chapter one is an introduction which provides background information on biometrics and the principles behind retinal identification and discusses EyeDentify's philosophy of protection. This chapter also provides an overview of the EIS system and of the design documentation itself. Chapter two provides an overview of the EIS system and host communication. Chapter three illustrates the command format required for communication. Chapter four provides a list and description of the commands that should be initiated by the host computer. Chapter five provides a list and description of commands initiated by the EIS system. The appendices provide the technical specifications, the RS-232 interface, the acceptance diamond, and the use of eyeglasses.

Conclusion

EIS system satisfies the D1 Design Documentation requirement.

Rating Assignment

This section describes the composite rating and how it is determined. A composite rating is assigned to each evaluated feature and is based upon the individual ratings issued in Chapter 3. The individual ratings are the rating for each feature and ratings for assurance and documentation supporting that feature. The chart below shows a 'Y' for each assurance or documentation requirement that is sufficient to support the rating of each feature. Using the ratings attained in Chapter 3, the composite ratings for each of EIS system's features are derived as shown in the following table.

Evaluated Features	Feature Rating	Assurance			Documentation				Supporting Function	Composite Rating
		Arch.	Integrity	Testing	SFUG	TFM	Testing	Design		
I&A	D1	Y	Y	Y	Y	Y	Y	Y	Audit ¹	D1

¹ Authentication data is protected on the EIS system board. The required supporting function, audit, is provided by another feature within the EIS system, but was not rated.

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

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

If the supporting function is integrated within the product, it must be at the same level as that of the feature to obtain the composite rating.

Evaluator's Comments

The EIS system provides I&A to the granularity of an individual user.

The EIS system does have some limitations. For instance:

- If a user has trouble focusing on the light emitted from the EIS system without eye-glasses, then they are unable to use the system unless they wear contacts.
- The I&A database and the customer developed trusted software need some type of access control.
- It is necessary for each site to have at least one compatible terminal for configuring the EIS system and performing diagnostics.

Bibliography

- [1] National Computer Security Center Computer Security Subsystem Interpretation, NCSC-TG-009 Version 1, 16 September 1988
- [2] EyeDentify Information Security (EIS) System Trusted Facility Manual, Manual Number 550-0045 REV A 5/90
- [3] EyeDentify Information Security (EIS) System Design Documentation Manual, Model Number 550-0046 REV A 5/90
- [4] EyeDentify Information Security (EIS) System Security Features User Guide, Model Number 550-0044 REV A 4/90

Evaluated Hardware Components

Evaluated Hardware Components consist of:

- EIS system Controller Box Model Number 185-0071
- EIS system Camera Model Number 185-0041

Evaluated Software Components

Evaluated Software Components consisted of EyeDentify's customized operating system and the EIS system commands residing in the 4 EPROMs, version REV. 05-25-90.

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--SUM-90/006			5. MONITORING ORGANIZATION REPORT NUMBER(S) S235,427		
6a. NAME OF PERFORMING ORGANIZATION National Security Agency		6b. OFFICE SYMBOL (If applicable) C71	7a. NAME OF MONITORING ORGANIZATION National Computer Security Center		
6c. ADDRESS (City, State and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000			7b. ADDRESS (City, State and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8c. ADDRESS (City, State and ZIP Code)			10. SOURCE OF FUNDING NOS		
11. TITLE (Include Security Classification) Final Evaluation Report Eyedentify Inc. EIS System			PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.
			WORK UNIT NO.		
12. PERSONAL AUTHOR(S) Deborah M. Clawson; Michael J. Oehler; Shawn M. Rovanseck					
13a. TYPE OF REPORT Final		13b. TIME COVERED FROM ____ TO ____		14. DATE OF REPORT (Yr, Mo., Day) 900924	
15. PAGE COUNT 23					
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) NCSC, I&A, Eyedentify, EIS System, CSSI		
FIELD	GROUP	SUB GR.			
19. ABSTRACT (Continue on reverse side if necessary and identify by block number) The Eyedentify Incorporated EIS System has been evaluated by the National Computer Security Center (NCSC). The security features of the EIS System were examined against the requirements specified by the COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988. The NCSC evaluation team has determined that the EIS System satisfies the functional requirement for I&A/D1, and also satisfies the assurance and documentation requirements. It has been determined that the highest class at which the EIS System satisfies all the specified requirements of the CSSI is class I&A/D1. This report documents the findings of the evaluation.					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL PATRICIA L. MORENO			22b. TELEPHONE NUMBER (Include Area Code) (301)859-4458		8b. OFFICE SYMBOL C71