Peripheral Sharing Switch

(PSS)

For Human Interface Devices

Protection Profile

Information Assurance Directorate

Version 2.0
Date 1 June 2010

Page left Blank Intentionally

Table of Contents

Foreword

This publication, "Peripheral Sharing Switch (PSS) for Human Interface Devices" Protection Parole, is issued by the Information Assurance Directorate (IAD) as part of its program to promulgate security standards for the components of information assurance solutions.

The base set of requirements used in this Protection Profile are taken from the Common Criteria for Information Technology Security Evaluation, Version 3.1. Further information, including the status and updates, of both this Profile and the Common Criteria, can be found on the Internet at "http://www.niap-ccevs.org/cc-scheme/cc_docs/".

Words which appear in SMALL CAPITALS are those which are formally defined in the Terms of Reference section.

Comments on this document should be directed to:

NIAP/CCEVS
National Security Agency
9800 Savage Road, Suite 6757
Fort George G. Meade, MD 20755-6757

or
scheme-comments@niap-ccevs.org.

1. Introduction

1.1 Identification

Title: Peripheral Sharing Switch (PSS) for Human Interface Devices.

Assurance Level: EAL 2 augmented with ALC_FLR.2

PP Version: 2.0, 1 June 2010.. Keywords: DEVICE sharing, multi-way SWITCH, PERIPHERAL switching, KEYBOARD-Video-MONITOR/Mouse (KVM) SWITCH.

1.2 Protection Profile Overview

This Protection Profile specifies U.S. Department of Defense minimum security requirements for PERIPHERAL SWITCHES; DEVICES which enable a single set of HUMAN INTERFACE DEVICES to be shared between multiple COMPUTERS. The profile limits the use of Universal Serial Bus (USB) connections to keyboard, mouse, and display. No other USB device shall be valid.

The Protection Profile is consistent with Common Criteria Version 3.1: Part 2, and Part 3 conformant (Evaluation Assurance Level 2).

2. Target of Evaluation Description

This document addresses a DEVICE, hereinafter referred to as a "Peripheral Sharing Switch" (PSS) or simply "SWITCH"--the Target of Evaluation (TOE)--permitting a single set of HUMAN INTERFACE DEVICES to be shared among two or more COMPUTERS (see Figure 1).

The TOE is normally installed in settings where a single USER with limited work surface space needs to access two or more COMPUTERS, collectively termed SWITCHED COMPUTERS (which need not be physically distinct entities). The USER may have a KEYBOARD, a visual display (e.g., MONITOR), and a POINTING DEVICE (e.g., mouse), no other peripheral device shall be connected to the switch. These are collectively referred to as the SHARED PERIPHERALS.

In operation, the TOE will be CONNECTED to only one COMPUTER at a time. To use a different COMPUTER, the USER must perform some specific action (e.g., push a button, turn a knob, etc.). The TOE will then visually indicate which COMPUTER was selected by the USER. Such indication is persistent and not transitory in nature.

The TOE must not have, and in fact must specifically preclude, any features that permit USER information to be shared or transferred between COMPUTERS via the TOE.

A PERIPHERAL PORT GROUP is a collection of DEVICE PORTS treated as a single entity by the TOE. There is one GROUP for the set of SHARED PERIPHERALS and one GROUP for each CONNECTED SWITCHED COMPUTER. Each SWITCHED COMPUTER GROUP has some unique associated logical ID. The SHARED PERIPHERAL GROUP ID is considered to be the same as that of the SWITCHED COMPUTER GROUP currently selected by the TOE.

Data Separation Security Function Policy (SFP): The TOE shall allow PERIPHERAL DATA and STATE INFORMATION to be transferred only between PERIPHERAL PORT GROUPS with the same ID.

The TOE itself is not concerned with the USER'S information flowing between the SHARED PERIPHERALS and the SWITCHED COMPUTERS. It is only providing a CONNECTION between the HUMAN INTERFACE DEVICES and a selected COMPUTER at any given instant.

SWITCHES of this type may differ significantly from the familiar "A/B" printer or serial port SWITCHES, where no constraints are placed on connections between devices. Some SWITCHES may provide enhanced features such as scanning (where it continually switches between the COMPUTERS until the USER performs an action to halt the switching), or video protocol conversion (e.g., Apple, Sun, PC, etc.) information in mixed COMPUTER environments. These enhancements must be examined to insure that information is not shared or transferred between COMPUTERS.

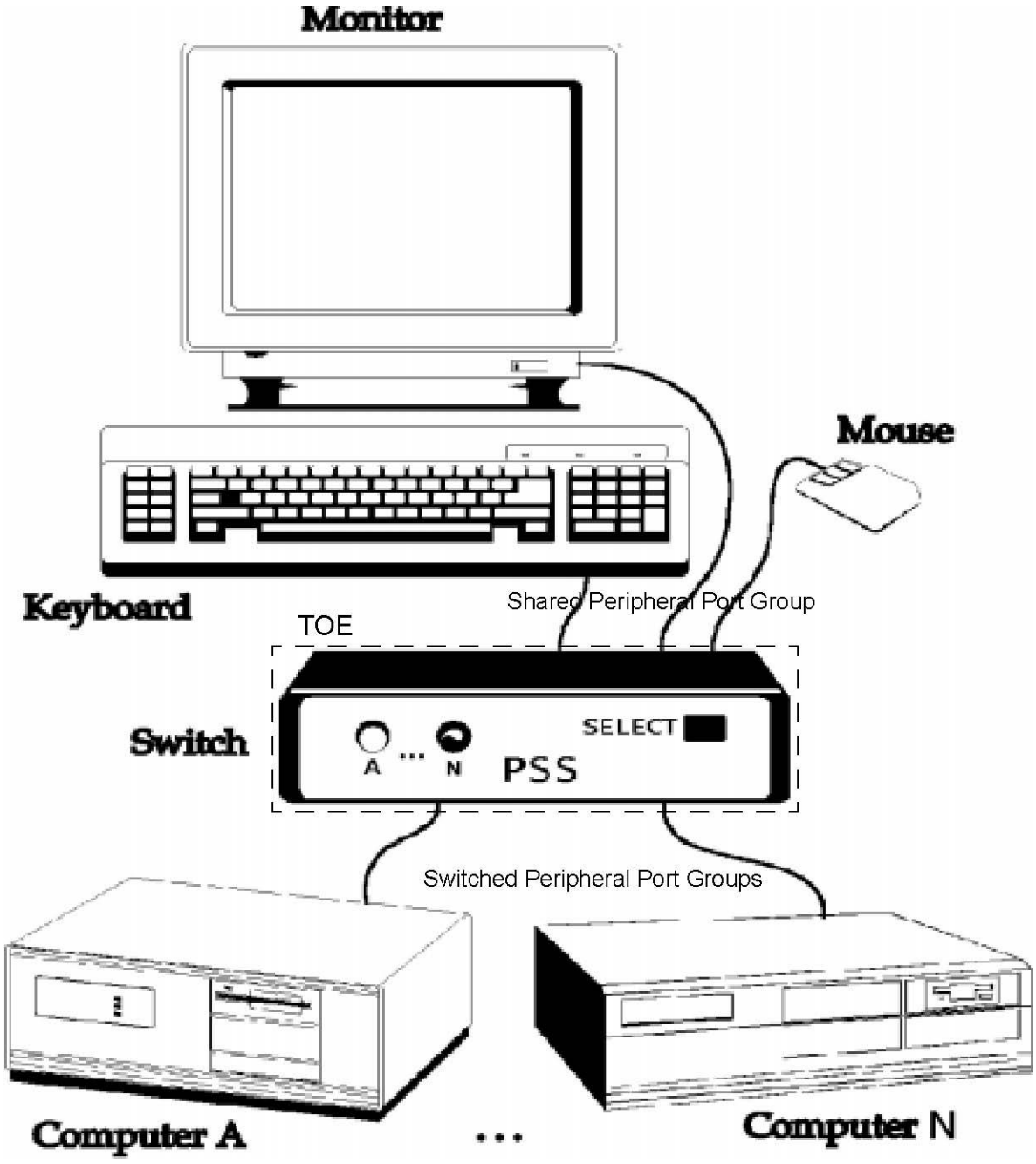

Figure 1: A Typical Configuration of Shared Peripherals

3. Target of Evaluation Security Environment

3.1 Secure Usage Assumptions

A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.

A.MANAGE The TOE is installed and managed in accordance with the manufacturer's directions.

A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.

A.PHYSICAL The TOE is physically secure.

3.2 Threats to Security

The asset under attack is the information transiting the TOE. In general, the threat agent is most likely (but not limited to) people with TOE access (who are expected to possess "average" expertise, few resources, and moderate motivation) or failure of the TOE or PERIPHERALS.

T.INVALIDUSB The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.

T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.

T.SPOOF Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

4. Security Objectives

4.1 Security Objectives for the Target of Evaluation

O.CONF The TOE shall not violate the confidentiality of information which it processes. Information generated within any PERIPHERAL GROUP COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP with a different GROUP ID.

O.INDICATE The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.

O.SELECT An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.

O.SWITCH All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.

O.USBDETECT The TOE shall detect any USB connection that is not a pointing device, keyboard, or display and will perform no interaction with that device after the initial identification.

4.2 Security Objectives for the Environment

All of the Secure Usage Assumptions are considered to be Security Objectives for the Environment. These Objectives are to be satisfied without imposing technical requirements on the TOE; they will not require the implementation of functions in the TOE hardware and/or software, but will be satisfied largely through application of procedural or administrative measures.

OE.ACCESS The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.

OE.MANAGE The TOE shall be installed and managed in accordance with the manufacturer's directions.

OE.NOEVIL The AUTHORIZED USER shall be non-hostile and follow all usage guidance.

OE.PHYSICAL The TOE shall be physically secure.

5. Information Technology Security Requirements

5.1 Target of Evaluation Security Requirements

Words which appear in italics are tailoring (via permitted operations) of requirement definitions.

5.1.1 User Data Protection (FDP)

5.1.1.2 **FDP_IFC.1** (Subset Information Flow Control)
[Dependencies: FDP_IFF.1]

1 The TSF shall enforce the Data Separation SFP on the set of PERIPHERAL PORT GROUPS, and the bi-directional flow of PERIPHERAL DATA and STATE INFORMATION between the SHARED PERIPHERALS and the SWITCHED COMPUTERS.

5.1.1.3 **FDP_IFF.1** (Simple Security Attributes)
[Dependencies: FDP_IFC.1 and FMT_MSA.3]

1. The TSF shall enforce the Data Separation SFP based on the following types of subject and information security attributes: PERIPHERAL PORT GROUPS (SUBJECTS), PERIPHERAL DATA and STATE INFORMATION (OBJECTS), and PERIPHERAL PORT GROUP IDs (ATTRIBUTES).
2. The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
   Switching Rule:
   PERIPHERAL DATA can flow to a PERIPHERAL PORT GROUP with a given ID only if it was received from a PERIPHERAL PORT GROUP with the same ID.
3. The TSF shall enforce the [No additional information flow control SFP rules.]
4. The TSF shall provide the following: [No additional SFP capabilities.]
5. The TSF shall explicitly authorize an information flow based on the following rules: [No additional rules.]
6. The TSF shall explicitly deny an information flow based on the following rules: [No additional rules.]

5.1.2 Security Management (FMT)

5.1.2.1 **FMT_MSA.1** (Management of Security Attributes)

[Dependencies: (FDP_ACC.1 or FDP_IFC.1) and FMT_SMR.1]

1. The TSF shall enforce the Data Separation SFP to restrict the ability to modify the security attributes PERIPHERAL PORT GROUP IDS to the USER.

Application Note: An AUTHORIZED USER shall perform an explicit action to select the COMPUTER to which the shared set of PERIPHERAL devices is CONNECTED, thus effectively modifying the GROUP ID associated with the PERIPHERAL DEVICES.

5.1.2.2 **FMT_MSA.3** (Static Attribute Initialization)
[Dependencies: FDP_MSA.1 and FMT_SMR.1]

1. The TSF shall enforce the Data Separation SFP to provide restrictive default values for security attributes that are used to enforce the SFP. Application Note: On start-up, one and only one attached COMPUTER shall be selected.
2. The TSF shall allow the *none* to specify alternative initial values to override the default values when an object or information is created.

5.1.3 Extended Requirements (EXT)

5.1.3.1 **EXT_VIR.1** (Visual Indication Rule)
[No dependencies]

1. A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided that is persistent for the duration of the CONNECTION.
   Application Note: Does not require tactile indicators, but does not preclude their presence.

5.1.3.2 **EXT_IUC.1** (invalid USB Connection)
[No dependencies]

1. All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, display). No further interaction with non-valid devices shall be performed.

5.2 Target of Evaluation Security Assurance Requirements

The TOE assurance requirements for this PP are EAL2 augmented by ALC_FLR.2 as shown in the table below. All assurance requirements are summarized in the table below.

Table 1 – Assurance Requirements: EAL2 Augmented

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw Reporting Procedures**
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Class ADV: Development

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

Class AGD: Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Class ALC: Life-cycle support

ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Class ATE: Tests

ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF interfaces to confirm that the TSF operates as specified.

Class AVA: Vulnerability assessment

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE

design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator *shall conduct* penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Application Note: The evaluator should test the system for buffer overflows, heap overflows, and string format problems.

6. Rationale

6.1 Security Objectives Rationale

Threat	Objective	Rationale
T.INVALIDUSB The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.	**O.USBDETECT** The TOE shall detect any USB connection that is not a pointing device, keyboard, or display and will perform no interaction with that device after the initial identification.	O.USBDETECT will detect the unauthorized connection so that it information from it can be ignored.
T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs	**O.CONF** The TOE shall not violate the confidentiality of information, which it processes. Information generated within any PERIPHERAL GROUP COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP with a different GROUP ID.	**O.CONF**: If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many

		PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS. Further, the purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER
T.SPOOF Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.	**O.INDICATE** The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected. **O.SELECT** An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED. Single push button, multiple push button, or rotary selection methods are used by most	**O.INDICATE**: The USER must receive positive confirmation of SWITCHED COMPUTER selection. **O.SELECT**: The USER must take positive action to select the current SWITCHED COMPUTER

	(if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.	
T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.	**O.CONF** The TOE shall not violate the confidentiality of information, which it processes. Information generated within any PERIPHERAL GROUPCOMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER CONNECTION. **O.SWITCH** All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.	**O.CONF**: If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS. Further, the purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER

		O.SWITCH: The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. It makes no sense to have, for example, video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER

6.2 Environmental Objectives Rationale

All of the Security Objectives for the Environment are considered to be Secure Usage Assumptions.

These objectives on the environment do not contain any IT security requirements because they are non-IT related objectives. Thus, the CC does not mandate it map to any requirements.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.	**OE.ACCES**S The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.	All authorized users are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate training, and follow all user guidance.
A.MANAGE The TOE is installed and managed in accordance with the manufacturer's directions.	**OE.MANAG**E The TOE shall be installed and managed in accordance with the manufacturer's directions.	Restates the assumption.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.	**OE.NOEVI**L The AUTHORIZED USER shall be non-hostile and follow all usage guidance.	Restates the assumption.
A.PHYSICAL The TOE is physically secure.	**OE.PHYSICAL** The TOE shall be physically secure.	The TOE, is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

6.3 Security Requirements Rationale

Objective	Requirements Addressing the Objective	Rationale
O.CONF The TOE shall not violate the confidentiality of information, which it processes. Information generated within any PERIPHERAL GROUPCOMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER	**FDP_ETC.1** (Export of User Data Without Security Attributes) **FDP_IFC.1** (Subset Information Flow Control) **FDP_IFF.1** (Simple Security Attributes) **FDP_ITC.1** (Import of User Data Without Security Attributes)	**FDP_ETC.1:** In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. Also included is configuration information such as KEYBOARD settings that must be reestablished each time the TOE switches between COMPUTERS. These DEVICES neither expect nor require any security

Objective	Requirements Addressing the Objective	Rationale
CONNECTION.		ATTRIBUTE information. The information content of the data passed through a CONNECTION is ignored. **FDP_IFC.1:** This captures the policy that no information flows between different PERIPHERAL PORT GROUP IDS. **FDP_IFF.1:** This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer. This requirement is a dependency of FDP_IFC.1. **FDP_ITC.1:** In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. These DEVICES neither expect nor require any security ATTRIBUTE information.
O.INDICATE The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected	**EXT_VIR.1** (Visual Indication Rule)	**EXT_VIR.1:** There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication.
O.SELECT An explicit action by the	**FMT_MSA.1** (Management of Security Attributes)	**FMT_MSA.1:** This restricts the ability to change selected PERIPHERAL

Objective	Requirements Addressing the Objective	Rationale
AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED. Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.	**FMT_MSA.3** (Static Attribute Initialization)	PORT GROUP IDs to the AUTHORIZED USER. This requirement is a dependency of FMT_MSA.3. **FMT_MSA.3:** The TOE assumes a default PERIPHERAL PORT GROUP selection based on a physical switch position or a manufacturer's specified sequence for choosing among the CONNECTED COMPUTERS (CONNECTED here implies powered on). This requirement is a dependency of FDP_IFF.1 and FDP_ITC.1.
O.SWITCH All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.	**FDP_IFF.1** (Simple Security Attributes)	**FDP_IFF.1:** This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer. This requirement is a dependency of FDP_IFC.1.
O.USBDETECT The TOE shall detect any USB connection that is not a pointing device, keyboard, or display and disable that connection.	**EXT_IUC.1** (invalid USB Connection)	**EXT_IUC.1:** Upon detection of an invalid USB connection, the switch will disable the connection and notify the user.

The set of security functional requirements can be partitioned into the following areas, analytically determined to be mutually exclusive and internally consistent.

Information Flow:	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1
Group ID Management:	FMT_MSA.1 FMT_MSA.3

6.4 Dependencies Not Met

FMT_SMR.1 (Security Roles)
The TOE is not required to associate USERS with roles; hence, there is only one "role", that of USER. This deleted requirement, a dependency of FMT_MSA.1 and FMT_MSA.3, allows the TOE to operate normally in the absence of any formal roles.

6.5 Mapping Tables

The indicated mappings do not necessarily imply that all aspects of the relations are resolved. For example, in Table 1, T.PHYSICAL is only partially addressed by O.NOPROG.

	O.CONF	O.INDICATE	O.SELECT	O.SWITCH
T.RESIDUAL	X			
T.SPOOF		X	X	
T.STATE	X			
T.TRANSFER	X			X

Table 1: Mapping of Threats to Objectives

	O.CONF	O.INDICATE	O.SELECT	O.SWITCH	O.USBDETECT
FDP_ETC.1	X				
FDP_IFC.1	X				
FDP_IFF.1	X			X	
FDP_ITC.1	X				
FMT_MSA.1			X		
FMT_MSA.3				X	
EXT_VIR.1		X			
EXT_IUC.1					X

Table 2: Mapping of Security Functional Requirements to Objectives

Dependency	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1		FMT_MSA.1	FMT_MSA.3	FMT_SMR.1
FDP_ETC.1	X						
FDP_IFC.1		X					
FDP_IFF.1	X					X	
FDP_ITC.1	X					X	
FMT_MSA.1	X						X
FMT_MSA.3					X		X
EXT_VIR.1							
EXT_IUC.1							

Table 3: Mapping of Security Functional Requirements Dependencies

Terms of Reference

Attribute

(See Peripheral Port Group ID)

Authorized User

A USER who has been granted permission to interact with the TOE and all of its CONNECTED PERIPHERALS.

Computer

A programmable machine. The two principal characteristics of a computer are: it responds to a specific set of instructions in a well-defined manner, and It can execute a prerecorded list of instructions (a software program). For the purposes of this document, any electronic DEVICE controlling the MONITOR, and accepting signals from the KEYBOARD and POINTING DEVICE (if any) will qualify. Examples of computers under this definition are IBM-class personal computers (and so-called clones), desktop workstations, and control console INTERFACES into "mainframe" computers.

Connected

A state in which information can be intentionally transferred.

Connection

A path for information flow between two or more DEVICES.

Device

A unit of hardware, outside or inside the case or housing for the essential COMPUTER that is capable of providing INPUT to the essential COMPUTER or of receiving OUTPUT or both. The term PERIPHERAL is sometimes used as a synonym for device or any INPUT/OUTPUT unit.

Group

(See Peripheral Port Group)

Human Interface Devices

Those PERIPHERALS which primarily allow a USER to directly observe and/or modify the operation/status of a COMPUTER. Examples include a keyboard, video MONITOR, mouse, and an optical head tracker. Modems, printers, hard drives, and scanners are not such devices.

Input Device

Any machine that feeds data into a COMPUTER. This includes scanners, touch screens, and voice response systems.

Interface

The CONNECTION and interaction between hardware, software, and the USER.

Keyboard

A DEVICE which converts the physical action of a USER such as the depressing of one or more buttons into electronic signals corresponding to the bitwise symbol for a character in some form of electronic alphabet. The most common example is the typewriter-like keyboard found on most home COMPUTERS, but the definition also includes braille keypads among other DEVICES.

Monitor

A COMPUTER OUTPUT surface and projecting mechanism that show text and other graphic images from a COMPUTER system to a user, using a Cathode Ray Tube (CRT),

Liquid Crystal Display (LCD), Light-Emitting Diode (LED), gas plasma, active matrix, or other image projection technology. The display (the terms display and monitor are often used interchangeably) is usually considered to include the screen or projection surface and the DEVICE that produces the information on the screen. In some COMPUTERS, the display is packaged in a separate unit called a monitor. Displays (and monitors) are also sometimes called Video Display Terminals (VDTs). Also included in this category are tactile braille OUTPUT DEVICES.

Object

(See Peripheral Data and State Information)

Output Device

Any machine capable of representing information from a COMPUTER. This includes display screens, printers, plotters, and synthesizers.

Peripheral

A DEVICE that is logically and electrically (or electromagnetically) CONNECTED to a COMPUTER, but normally mounted outside of the COMPUTER enclosure. MONITORS, KEYBOARDS, and POINTING DEVICES are all peripherals.

Peripheral Data

Information, including [buffered] STATE INFORMATION, sent from or to a PERIPHERAL.

Peripheral Port Group ("Group")/ Peripheral Port Group ID

A collection of HUMAN INTERFACE DEVICE PORTS treated as a single entity by the SWITCH. There is one Group for the set of SHARED PERIPHERALS and one Group for each SWITCHED COMPUTER directly CONNECTED to the SWITCH. Each SWITCHED COMPUTER Group has a unique logical ID. The shared Group ID is the same as that of the SWITCHED COMPUTER Group currently selected by the SWITCH.

Pointing Device

A DEVICE, which converts relative positioning motion from a human operator into positioning information on a MONITOR. Examples of Pointing Devices include a mouse, trackball, joystick, and touchpad.

Port

An external socket for plugging in communications lines and/or PERIPHERALS.

Residual Data

Any PERIPHERAL DATA stored in a SWITCH.

Shared Peripheral

(See Peripheral Port Group)

State Information

The current or last-known status, or condition, of a process, transaction, or setting. "Maintaining state" means keeping track of such data over time.

Subject

(See Peripheral Port Group)

Switch

A DEVICE permitting a single set of PERIPHERALS to be shared among two or more COMPUTERS. Synonymous with TOE in this document.

Switched Computer

(See Peripheral Port Group)

User

The human operator of the TOE.

Acronyms

CCIB Common Criteria Implementation Board

CCIMB Common Criteria Interpretations Management Board

CM Configuration Management

CRT Cathode Ray Tube

DAC Discretionary Access Control

EAL Evaluation Assurance Level

FCC Federal Communications Commission

FFRDC Federally Funded Research and Development Center

ID Identification

IEC International Electro-technical Commission

ISO International Standards Organization

ISSE Information Systems Security Engineer[ing]

ISSO Information Systems Security Organization

IT Information Technology

KVM Keyboard-Video-Mouse

LCD Liquid Crystal Display

LED Light-Emitting Diode

MAC Mandatory Access Control

PP Protection Profile

PSS Peripheral Sharing Switch

SFP Security Function Policy

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

USB Universal Serial Bus

VDT Video Display Terminal

References

1. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, CCIB-2006-09-001, 002, 003), September 2007.

2. ISSE Analysis - Electronic Computer Peripheral Switches, NSA/V23, draft dated 12 March 1999.

3. ISSE Analysis/Keyboard-Video-Mouse (KVM) Switches, NSA/V23, draft dated 5 August 1999.

4. National Information Assurance (IA) Glossary http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf