Avocent Cybex SwitchView SC Series Switches

Security Target

Document Version 4.0
2 December 2010

Prepared for:

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama, 35805-6201

Prepared by:

Computer Sciences Corporation
7231 Parkway Drive
Hanover, MD 21076

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

This Chapter presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Problem Definition).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 6, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Section 7, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 11.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the TOE Name. This ST targets an Evaluation Assurance Level (EAL) 4 (augmented with ALC_FLR.2) level of assurance.

ST Title	Avocent Cybex SwitchView SC Series Switches Security Target
ST Version	Version 4.0
Revision Number	Revision 1.8
Publication Date	December 2, 2010
Authors	Computer Sciences Corporation, Common Criteria Testing Lab Avocent Corporation
TOE Identification	Avocent Cybex SwitchView SC320 Model 520-633-501 Avocent Cybex SwitchView SC340 Model 520-634-501 Avocent Cybex SwitchView SC380 Model 520-635-501
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1R3, July 2009
ST Evaluation	Computer Sciences Corporation
Keywords	Device sharing, multi-way switch, peripheral switching, keyboard-video-monitor/mouse (KVM) switch

1.2 TOE Overview

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices: DVI-I video, Audio (input and output), USB keyboard, USB mouse, and Common Access Card (CAC) or SmartCard reader to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the

Avocent Cybex SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure. Also, any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide" switch.

The Avocent Cybex SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, USB mouse, and CAC or SmartCard reader. Each switch has a "select" button associated with each specific port. For the convenience of the operator, these models have USB ports on both the front and rear of the device.

A summary of the Avocent Cybex SwitchView SC series switches security features can be found in Section 1.4, TOE Description. A detailed description of the Avocent Cybex SwitchView SC series switches security features can be found in Section 7, TOE Summary Specification.

1.3 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1,Revision 3, CCMB-2009-07-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-003
[CEM]	Common Evaluation Methodology for Information Technology Security Evaluation, dated July 2009, Version 3.1, Revision 3, CCMB-2009-07-004
[PSS_PP]	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008

1.4 TOE Description

This Chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

1.4.1 Product Type

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices: DVI-I video, Audio (input and output), USB keyboard, USB mouse, and CAC or SmartCard reader, to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the Avocent Cybex SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

The Avocent Cybex SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, USB mouse, and CAC or SmartCard

reader. Each switch has a "select" button associated with each specific port. For the convenience of the operator, these models have USB ports on both the front and rear of the device.

1.4.2 Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Avocent Cybex SwitchView switch (see Table 1: TOE Models and Features), and its accompanying User and Administrator Guidance.

Table 1: TOE Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
Avocent Cybex SwitchView SC320	520-633-501	2	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader
Avocent Cybex SwitchView SC340	520-634-501	4	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader
Avocent Cybex SwitchView SC380	520-635-501	8	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader

In addition to having more (8) ports, the SwitchView SC380 also differs from the other two models (4-port SC340 and 2-port SC320) in how the internal hardware architecture controls selection and power indication LEDs; however, this well-documented difference does not alter the fact that all three models provide the same security functionality.

The TOE boundary does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. The following figure depicts the TOE and its environment.

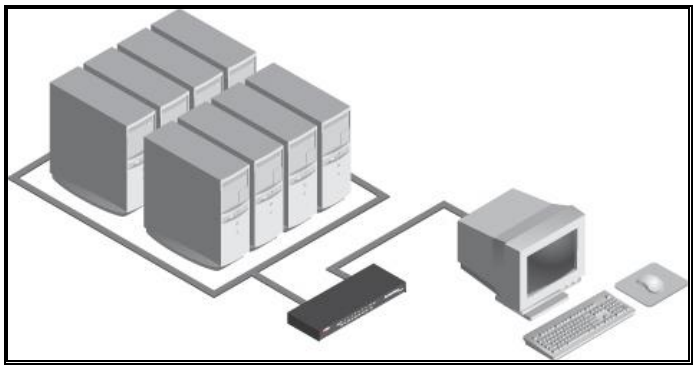

Figure 1: Depiction of TOE Deployment

1.4.3 Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

The TOE provides the following security features:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT)
- Tamper Detection (TSF_TMP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. In operation, the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP). Data Separation is accomplished as explained in section 7.1.1.

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides *select* switches, that allow the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel. Security Management is accomplished as explained in section 7.1.2.

Any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide" switch. If one of these models has been physically tampered with in this manner, the lights on the front of the TOE will all flash in unison to alert an administrator to the interference, and all TOE functions will be permanently disabled. Tamper Detection is accomplished as explained in section 7.1.3.

USB type-enforcement must be mandated by policy; only human interface and CAC or smart card reader devices are permitted in the evaluated configuration because type checking was not included in the PP to which this product claims conformance.

1.4.4 Evaluated Configuration

In its evaluated configuration, the TOE is connected to one or more computers and shared peripherals as described in the User Guidance delivered with the TOE.

2 CONFORMANCE CLAIMS

This section describes the conformance claims of this Security Target.

2.1 Common Criteria Conformance Claims

The Security Target is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 3, CCMB-2009-07-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 3, CCMB-2009-07-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- Part 2 extended
- Part 3 conformant
- Evaluation Assurance Level (EAL) 4+

2.2 Protection Profile (PP) Claims

This ST claims demonstrable compliance for the following PP:

> *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008 (hereafter referred to PSS PP in this section of the ST, for brevity)

2.3 Package Claims

This Security Target claims conformance to the EAL 4 package augmented with ALC_FLR.2.

2.4 Rationale

The TOE type in this ST (peripheral sharing switch) is the same as the TOE type for *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

The Security Problem Definition (Threats, Assumptions and Organizational Security Policies) and Objectives have been copied directly from PSS PP, and have not been modified. The statement of Security Requirements contains the SFRs and Extended Components from PSS PP and one additional extended requirement. By including all of the SFRs and Extended Components from PSS PP, and including an additional Extended Component that does not conflict with the other requirements, the statement of Security Requirements is necessarily at least as strict as the statement in PSS PP, if not more strict. The rationales for objectives, threats, assumptions, organizational security policies and security requirements have been copied from PSS PP and have been augmented to address the extended component that has been added to the ST.

3 SECURITY PROBLEM DEFINITION

The Security Problem Definition describes assumptions about the operational environment in which the TOE is intended to be used and represents the conditions for the secure operation of the TOE.

3.1 Definitions

In the Common Criteria, many terms are defined in Section 4 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

Authentication data	Information used to verify the claimed identity of a user.
Authorized User	A user who may, in accordance with the SFRs, perform an operation.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Subject	An active entity in the TOE that performs operations on objects.
User	See **external entity**.

In addition to the above general definitions, terminology that is specific to this ST is given in "Terms of Reference," Pages 47 - 49, of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

3.2 TOE Security Environment

The assumptions and threat identification combined with any organization security policy statement or rules requiring TOE compliance provides the definition of the security environment. It is necessary that a comprehensive security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- ***Physical security*** - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.
- ***Procedural security*** - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.

- ***Personnel security*** - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.2.1 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

Table 2: Environmental Assumptions

Assumptions	Description
A.ACCESS	An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
A.EMISSION	The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class A digital devices.]
A.ISOLATE	Only the selected COMPUTER'S video channel will be visible on the shared MONITOR.
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.
A.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, are a concern of the application scenario and not of the TOE.

3.2.2 Threats

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.2.1 Threats Addressed by the TOE

This section identifies the threats addressed by the TOE. 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 peripherals.

Table 3: Threats Addressed by the TOE

Threat	Description
T.BYPASS	The TOE may be bypassed, circumventing nominal SWITCH functionality.
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy.
T.LOGICAL	The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.
T.PHYSICAL	A physical attack on the TOE may violate the security policy.
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.STATE	STATE INFORMATION may be transferred to a PERIPHERAL PORT GROUP with an ID other than the selected one.
T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

3.2.2.2 Threats Addressed by the Operating Environment

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2, dated August 21, 2008, identifies no threats to the assets against which specific protection within the TOE environment is required.

3.2.3 Organizational Security Policies

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2, dated August 21, 2008, identifies no organization security policies (OSPs) to which the TOE must comply.

4 SECURITY OBJECTIVES

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the Operating Environment.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives of the TOE.

Table 4: Security Objectives for the TOE

Objectives	Description
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.CONNECT	No information shall be shared between SWITCHED COMPUTERS via the TOE. This includes STATE INFORMATION, if such is maintained within the TOE.
O.INDICATE	The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.
O.INVOKE	Upon switch selection, the TOE is invoked.
O.NOPROG	Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.
O.ROM	TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.
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.

4.2 Security Objectives for the IT 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 administrative measures.

Table 5: Security Objectives for IT Environment

Objectives	Description
OE.ACCESS	The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
OE.EMISSION	The TOE shall meet the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]
OE.ISOLATE	Only the selected COMPUTER'S video channel shall be visible on the shared MONITOR.
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.
OE.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, shall be a concern of the application scenario and not of the TOE.

4.3 Rationale for Security Objectives

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 6: Completeness of Security Objectives

	OBJECTIVES															
	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPORG	O.ROM	O.SELECT	O.SWITCH		OE.ACCESS	OE.EMISSION	OE.ISOLATE	OE.MANAGE	OE.NOEVIL	OE.PHYSICAL	OE.SCENARIO
T.BYPASS				X												
T.INSTALL													X			
T.LOGICAL					X	X										
T.PHYSICAL	X				X	X										
T.RESIDUAL	X	X														
T.SPOOF			X				X									
T.STATE	X	X														
T.TRANSFER	X	X						X								
A.ACCESS										X						
A.EMISSION											X					
A.ISOLATE												X				
A.MANAGE													X			
A.NOEVIL														X		
A.PHYSICAL															X	
A.SCENARIO																X

Table 7: Sufficiency of Security Objectives

Threats, Assumptions and OSPs	Objective	Rationale
T.BYPASS	O.INVOKE	O.INVOKE: The TOE must me invoked whenever a switch is made.
T.INSTALL	OE.MANAGE	OE.MANAGE: Installing and delivering the TOE in accordance with the manufacturer's instructions mitigates the risk of violation the security policy during delivery and installation.
T.LOGICAL	O.NOPROG O.ROM	O.NOPROG: The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information) may change. O.ROM: Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which

Threats, Assumptions and OSPs	Objective	Rationale
		prevents its modification.
T.PHYSICAL	O.CONF O.NOPROG O.ROM	O.CONF: If the PERPHERALS 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 of 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 the transfer is via the buffering mechanism in many KEYBOARDS. O.NOPROG: The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information may change. O.ROM: Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which prevents its modification.
T.RESIDUAL	O.CONF O.CONNECT	O.CONF: If the PERPHERALS 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 of 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 the transfer is via the buffering mechanism in many KEYBOARDS. O.CONNECT: The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from on SWITCHED COMPUTER is no to be shared with any other COMPUTER .
T.SPOOF	O.INDICATE O.SELECT	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.
T.STATE	O.CONF O.CONNECT	O.CONF: If the PERPHERALS 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 of DEVICES with bi-directional communications channels such

Threats, Assumptions and OSPs	Objective	Rationale
		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 the transfer is via the buffering mechanism in many KEYBOARDS. O.CONNECT: The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from on SWITCHED COMPUTER is no to be shared with any other COMPUTER.
T.TRANSFER	O.CONF O.CONNECT O.SWITCH	O.CONF: If the PERPHERALS 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 of 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 the transfer is via the buffering mechanism in many KEYBOARDS. O.CONNECT: The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from on SWITCHED COMPUTER is no 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 make no sense to have, for example video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER.
A.ACCESS	OE.ACCESS	All authorized users are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate training, and follow all guidance.
A.EMISSION	OE.EMISSION	Restates the assumption.
A.ISOLATE	OE.ISOLATE	Restates the assumption.
A.MANAGE	OE.MANAGE	Restates the assumption.
A.NOEVIL	OE.NOEVIL	Restates the assumption.
A.PHYSICAL	OE.PHYSICAL	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

Threats, Assumptions and OSPs	Objective	Rationale
		to access the TOE environment.
A.SCENARIO	OE.SCENARIO	Restates the assumption.

5 EXTENDED COMPONENTS DEFINITION

The Extended Components Definition describes components for security objectives which cannot be translated or could only be translated with great difficulty to existing requirements.

NOTE: The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008 contains extended components but does not include an Extended Components Definition. In order to comply with the Common Criteria, this ST provides the required definition.

5.1 Class EXT: Extended – Inspection

Visual confirmation provides the user with important information regarding the connection made through the TOE. This allows the user to confirm that their data are being securely transported to the proper computer.

5.1.1 Visual Inspection (EXT_VIR)

Family Behaviour

This family defines requirements for providing a means of determining which computer is connected to which set of peripheral devices.

Component leveling

EXT_VIR.1 Visual Indication Rule provides a visual indication of the connections between the computer and a set of peripheral devices.

Management: EXT_VIR.1

There are no management activities foreseen.

Audit: EXT_VIR.1

There are no auditable events foreseen.

EXT_VIR.1	**Visual Indication Rule**	
	Hierarchical to:	No other components
	Dependencies:	None
EXT_VIR.1.1	A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.	

Application Note: Does not require tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

5.2 Class EXP: Extended – Tampering

Tamper-proofing of the TOE protects all peripheral devices connected to that TOE. This prevents any alterations of the chips and circuits within the TOE. This in turn, prevents improper or corrupt data from being transferred to the peripheral devices connected to it.

5.2.1 Physical Tampering Security (EXP_TMP)

Family Behaviour

This family defines the response taken if the enclosure cover screws are removed.

Component leveling

EXP_TMP Prevention of Physical Tampering, the TSF shall disable all functions if the enclosure screws are removed.

Management: EXP_TMP.1

There are no management activities foreseen.

Audit: EXP_TMP.1

There are no auditable events foreseen.

EXP_TMP.1	**Prevention of Physical Tampering**	
	Hierarchical to:	No other components
	Dependencies:	None
EXP_TMP.1.1	The TSF shall permanently disable all TOE functions in the event of attempts to gain access to TOE internal circuitry through opening the enclosure via removing the enclosure cover screws.	

6 IT SECURITY REQUIREMENTS

This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.

- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subsections.

6.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on security functional components; *assignment*, *refinement*, *selection*, and *iteration* as defined in Section C.4 of Part 1 of the CC:

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].

- Iteration of a component is used when a component is repeated more than once with varying operations. Iterated components are given unique identifiers by an iteration number or name in parenthesis appended to the component and element identifiers.

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized text.*

Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

6.2 TOE Security Functional Requirements

The TOE satisfies the SFRs delineated in "Target of Evaluation Security Requirements," Section 5.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. The SFR's have been reproduced here merely for the convenience of the customer.

6.2.1 Class FDP: User Data Protection

6.2.1.1 FDP_ETC.1 Export of User Data Without Security Attributes

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 subset information flow control
FDP_ETC.1.1	The TSF shall enforce the [Data Separation SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

6.2.1.2 FDP_IFC.1 Subset Information Flow Control

Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.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].

6.2.1.3 FDP_IFF.1 Simple Security Attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	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)].
FDP_IFF.1.2	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].
FDP_IFF.1.3	The TSF shall enforce the [No additional information flow control SFP rules].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [No additional rules].

FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

6.2.1.4 FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the [Data Separation SFP] when importing user data, controlled under the SFP, from outside the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [No additional rules].

6.2.2 Class FMT: Security Management

6.2.2.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MSA.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.

6.2.2.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of Security Attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	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.

FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	None
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [none].

6.3 TOE Security Assurance Requirements

The security assurance components (EAL4 augmented with ALC_FLR.2) are specified in "Target of Evaluation Security Assurance Requirements," Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

Table 8: Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative user guidance
ALC: Life-cycle support	ALC_CMC.4 Product support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL4)
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.4 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

6.5 Explicitly Stated Requirements for the TOE

This ST contains the explicitly stated requirement for the TOE as specified in "EXT_VIR.1 (Visual Indication Rule)," Section 5.1.3, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. It has been reproduced here:

EXT_VIR.1	**Visual Indication Rule**
Hierarchical to:	No other components
Dependencies:	None
EXT_VIR.1.1	A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.
Application Note:	Does not require tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

This ST does contain an additional explicitly stated requirement for the TOE as specified below:

EXP_TMP.1	**Prevention of Physical Tampering**
Hierarchical to:	No other components
Dependencies:	None
EXP_TMP.1.1	The TSF shall permanently disable all TOE functions in the event of attempts to gain access to TOE internal circuitry through opening the enclosure via removing the enclosure cover screws.

6.6 Rationale for Assurance Level

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2. In this PP, the TOE environment is described as being exposed to a moderate level of risk (Reference Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008). As such, the Evaluation Assurance Level 4 is appropriate.

6.7 Rationale for Security Functional Requirements

Table 9 and Table 10 below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. These tables contain the original rationale from *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2 Rationales for the SFRs that have been added to this Security Target, that do not originate in *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, have been added to these tables.

Table 9: Completeness of Security Functional Requirements

SFRs	Objectives							
	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH
FDP_ETC.1	X	X						
FDP_IFC.1	X	X						
FDP_IFF.1	X	X						X
FDP_ITC.1	X	X						
FMT_MSA.1							X	
FMT_MSA.3								X
ADV_ARC.1				X				
ADV_ARC.1					X	X		
EXT_VIR.1			X					
EXP_TMP.1					X	X		

6.8 Security Requirements Rationale

Table 10: Sufficiency of Security Functional Requirements

Objectives	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 CONNECTION.	**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 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.

Objectives	Requirements Addressing the Objective	Rationale
O.CONNECT No information shall be shared between SWITCHED COMPUTERS via the TOE. This includes STATE INFORMATION, if such is maintained within the TOE.	**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 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.INVOKE Upon switch selection, the TOE is invoked.	**ADV_ARC.1** (Security architecture description)	**ADV_ARC.1:** addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The Data Separation SFP must be enforced at all times during TOE operation. This requires that the TSP functions always be invoked.

Objectives	Requirements Addressing the Objective	Rationale
O.NOPROG Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.	**ADV_ARC.1** (Security architecture description)	**ADV_ARC.1:** addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The TSF needs to ensure that it protects itself against changes, which might compromise its security functionality.
O.ROM TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.	**ADV_ARC.1** (Security architecture description)	**ADV_ARC.1:** addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The TSF needs to ensure that it protects itself against changes, which might compromise its security functionality.
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.	**FMT_MSA.1** (Management of Security Attributes) **FMT_MSA.3** (Static Attribute Initialization)	**FMT_MSA.1:** This restricts the ability to change selected PERIPHERAL 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.

Objectives	Requirements Addressing the Objective	Rationale
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.
None	**FMT_SMF.1**	The security requirements rationale in the Protection Profile is incomplete; the Protection Profile does not provide a mapping or rationale for the new requirement FMT_SMF.1. The requirement FMT_SMF.1, as written in the PP provides for no management functions to be performed. With no management functions to be performed and no management objective to contribute to, this requirement has nothing to be mapped to in the rationale of either the Protection Profile or this ST and is included only because it is required by the Protection Profile.
O.NOPROG Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.	**EXP_TMP.1** (Prevention of Physical Tampering)	**EXP_TMP.1**: The TSF needs to ensure that it protects itself against physical changes which might compromise its security functionality. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for physical tamper prevention.
O.ROM TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.	**EXP_TMP.1** (Prevention of Physical Tampering)	**EXP_TMP.1**: The TSF needs to ensure that it protects itself against physical changes which might compromise its security functionality. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for physical tamper prevention.

6.9 Rationale for SFR and SAR Dependencies

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. The rationale with respect to SFR and SAR dependencies from the PP is given in Sections 6.4 of the referenced PP.

Table 11: SFR Dependencies Satisfied

Functional Component ID	Dependency (ies)	Satisfied
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1	Yes
	FMT_MSA.3	Yes
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1
	FMT_MSA.3	Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_IFC.1
	FMT_SMR.1	No[1]
	FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	No[1]
FMT_SMF.1	None	N/A
EXT_VIR.1	None	Yes
EXP_TMP.1	None	N/A

[1] 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.

Table 11: EAL4 (Augmented with ALC_FLR.2) SAR Dependencies Satisfied

Assurance Component ID	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	Yes, hierarchically
ADV_FSP.4	ADV_TDS.1	Yes, hierarchically
ADV_IMP.1	ADV_TDS.3 ALC.TAT.1	Yes Yes
ADV_TDS.3	ADV_FSP.4	Yes
AGD_OPE.1	ADV_FSP.1	Yes, hierarchically
AGD_PRE.1	None	
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	Yes, hierarchically Yes Yes
ALC_CMS.4	None	
ALC_DEL.1	None	
ALC_DVS.1	None	
ALC_FLR.2	None	
ALC_LCD.1	None	
ALC_TAT.1	ADV_IMP.1	Yes
ASE_CCL.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	Yes Yes Yes, hierarchically
ASE_ECD.1	None	
ASE_INT.1	None	
ASE_OBJ.2	ASE_SPD.1	Yes
ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	Yes Yes
ASE_SPD.1	None	
ASE_TSS.1	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	Yes Yes Yes, hierarchically
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes, hierarchically Yes
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1	Yes Yes Yes
ATE_FUN.1	ATE_COV.1	Yes, hierarchically
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes, hierarchically Yes Yes Yes, hierarchically Yes

Assurance Component ID	Dependencies	Satisfied
AVA_VAN.3	ADV_ARC.1	Yes
	ADV_FSP.4	Yes
	ADV_TDS.3	Yes
	ADV_IMP.1	Yes
	AGD_OPE.1	Yes
	AGD_PRE.1	Yes

7 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

7.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1. Traceability to SFRs is also provided.

7.1.1 Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.

Signals processed by the TOE are shared peripheral device data, Data Display Channel information, and video signals. Specific versions of the TOE accommodate subsets of the listed signals to support popular types of computers. In all cases, the TOE ensures data separation for all signal paths using both hardware and firmware.

The basic arrangement of the microprocessors used for shared peripheral data ensures data separation in hardware by physical separation of the microprocessors connected to the user's peripheral devices from the microprocessors connected to the attached computers. In operation, the main processor moves data received from the shared peripherals to the microprocessor corresponding to the selected computer. The processor dedicated to the selected computer sends data to the computer. Separation is ensured in hardware by use of separate microprocessors for each of the computers and for the shared user peripheral devices.

Separation in firmware is ensured by firmware design consisting of dedicated functions and static memory assignment with no third-party library functions or multitasking executives.

In operation the TOE is not concerned with the content of user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer supporting the Data Separation Security Functional Policy – "the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID." The TOE interfaces ensure that confidentiality of information is not violated by isolating signals electrically and through firmware modules that ensure that information is passed only between the user peripherals and the selected computer.

Shared peripheral status for each computer is stored by the processor associated with each computer. The TOE does not have software to install, or boards to configure. The logic contained within the TOE is protected from unauthorized modification through the use of discrete components.

FUNCTIONAL REQUIREMENTS SATISFIED: FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1

7.1.2 Security Management (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides port-specific switches that allow(s) the human user to explicitly determine to which computer the shared set of peripherals is connected. This connection is visually displayed by an amber LED over the selected channel.

FUNCTIONAL REQUIREMENTS SATISFIED: FMT_MSA.1, FMT_MSA.3, EXT_VIR.1

7.1.3 Tamper Detection (TSF_TMP)

A switch inside the unit is activated when a screw used to fasten the top cover of the unit is removed. The tamper switch is powered by the main power supply or a dedicated battery so that it can always detect intrusions. After the switch is activated, TOE operation is disabled and the amber indicators on the front panel of the unit flash in unison. When the amber indicators are flashing in unison, operation of the TOE cannot be restored; the TOE must be replaced.

FUNCTIONAL REQUIREMENTS SATISFIED: EXP_TMP.1

8 ACRONYMS

8.1 Common Criteria Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

8.2 ST Acronyms

The following abbreviations are used in this Security Target to help describe the TOE, and the IT environment.

CAC	Common Access Card
DVI-I	Digital Video Interface - Integrated
IBM	International Business Machines, Inc.
LED	Light Emitting Diode
PC/AT	Personal Computer / Advanced Technology
USB	Universal Serial Bus

Acronyms specific to this ST and the referenced PP are given in “Acronyms,” Page 50 & 51, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008.