Avocent Cybex SwitchView SC Series Switches
Security Target

Document Version 6.0
Revision 2.6
August 12, 2014

Prepared by:

Avocent Corporation
4991 Corporate Drive
Huntsville, AL 35805-6201

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) 2 (augmented with ALC_FLR.2) level of assurance.

ST Title	Avocent Cybex SwitchView SC Series Switches Security Target
ST Version	Version 6.0
Revision Number	Revision 2.6
Publication Date	August 12, 2014
Authors	Computer Sciences Corporation, Common Criteria Testing Lab Avocent Corporation
TOE Identification	Avocent Cybex SwitchView SC620 Model 520-866-503 Avocent Cybex SwitchView SC640 Model 520-869-503 Avocent Cybex SwitchView SC740 Model 520-868-503 Avocent Cybex SwitchView SC620C Model 520-903-503 Avocent Cybex SwitchView SC640C Model 520-904-503 Avocent Cybex SwitchView SC740C Model 520-905-503
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1R4, September 2012
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, or USB 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' architecture to keep their private data separate. There is no software to install or boards to configure.

The Avocent Cybex SwitchView SCxx0 series of switches work with IBM PC and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, and USB mouse. The Avocent Cybex SwitchView SCxx0C series of switches work with IBM PC and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, USB mouse, and USB 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 the 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 September 2012, Version 3.1,Revision 4, CCMB-2012-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, Version 3.1, Revision 4, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, dated September 2007, Version 3.1, Revision 4, CCMB-2012-09-004
[PSS_PP]	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 7, 2010

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 to be shared among two or more computers.

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), a POINTING DEVICE (e.g., mouse), and SMARTCARD READER (e.g. Common Access Card reader). 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 doesn't 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.

The Avocent Cybex SwitchView SC series control DVI-I video, Audio (input and output), USB keyboard, USB mouse, and USB SmartCard reader to be shared among several computers (see Figure 1). Users who access secure and unsecure networks from one set of peripherals can rely on the Avocent Cybex SwitchView SC series of switches' architecture to keep their private data separate. There is no software to install or boards to configure.

The Avocent Cybex SwitchView SC series of switches work with IBM PC and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, USB mouse, and USB 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 the 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, listed as below:

- QUICK INSTALLATION GUIDE SwitchView™ SC620/640 2/4-Port DVI-I/USB Switches with Audio (590-1050-501A)
- QUICK INSTALLATION GUIDE SwitchView™ SC740 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1051-501A)
- QUICK INSTALLATION GUIDE SwitchView™ SC620C/640C 2/4-Port DVI-I/USB Switches with Audio (590-1137-501A)
- QUICK INSTALLATION GUIDE SwitchView™ SC740C 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1138-501A)

The environmental assumptions stated within this document constitute guidance for the proper installation of the TOE.

Table 1: TOE Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
Avocent Cybex SwitchView SC620	520-866-503	2	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, and USB mouse
Avocent Cybex SwitchView SC640	520-869-503	4	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, and USB mouse
Avocent Cybex SwitchView SC740	520-868-503	4	Dual-head, Dual-link DVI-I, Audio (input and output), USB keyboard, and USB mouse
Avocent Cybex SwitchView SC620C	520-903-503	2	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse, and SmartCard reader
Avocent Cybex SwitchView SC640C	520-904-503	4	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse, and SmartCard reader
Avocent Cybex SwitchView SC740C	520-905-503	4	Dual-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse, and SmartCard reader

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.

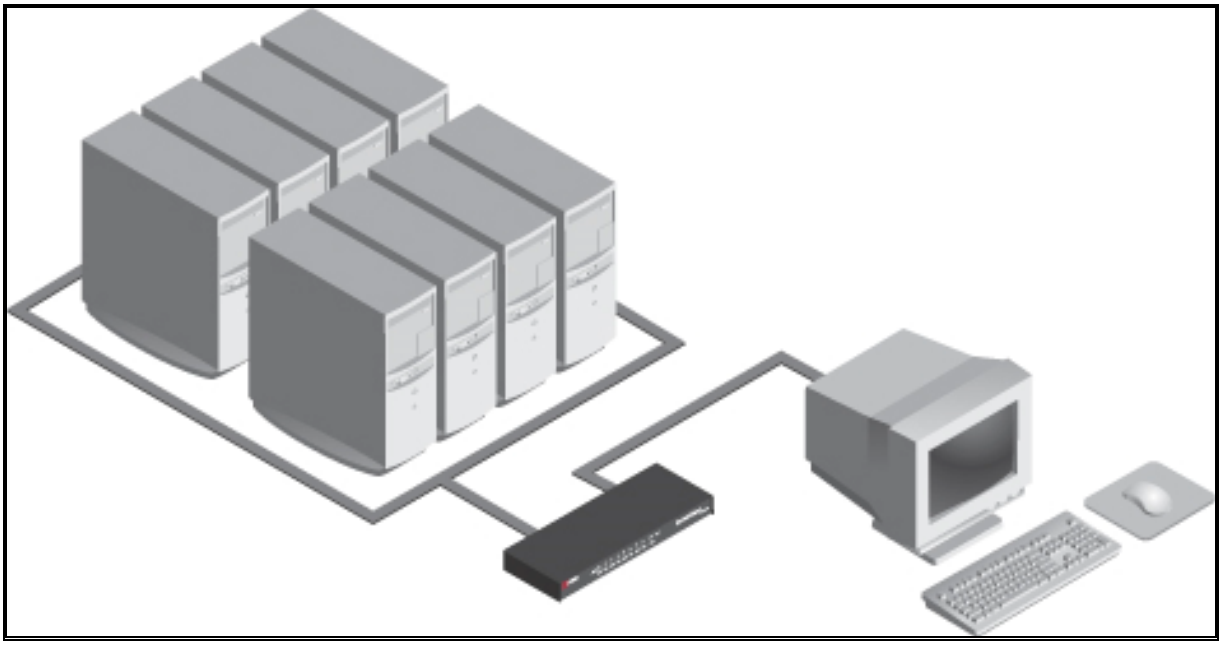

Figure 1: Depiction of TOE Deployment

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)
- Invalid USB Connection (TSF_IUC)
- Read-only ROMs (TSF_ROM)

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 2.1, dated September 7, 2010. 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.

All USB devices connected to the Peripheral switch are interrogated to ensure that they are valid (pointing device, keyboard, or SmartCard reader). No further interaction with non-valid devices is allowed to be performed. Invalid USB Connection Security Function is accomplished as explained in section 7.1.3.

TSF software embedded in TSF ROMs is contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly. Read-only ROMs is accomplished as explained in section 7.1.4.

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 4, CCMB-2012-09-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4, CCMB-2012-09-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4, CCMB-2012-09-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

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

2.2 Protection Profile (PP) Claims

None

2.3 Package Claims

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

3 SECURITY PROBLEM DEFINITION

The Security Problem Definition describes 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.

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**.

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.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

3.2.2 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 or peripherals.

Table 3: Threats Addressed by the TOE

Threat	Description
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.ROM_PROG	The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.
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.

3.2.2.2 Threats Addressed by the Environment

None.

3.3 Organizational Security Policies

None

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

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 or 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.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.

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

	O.CONF	O.INDICATE	O.ROM	O.SELECT	O.SWITCH	O.USBDETECT	OE.ACCESS	OE.MANAGE	OE.NOEVIL	OE.PHYSICAL
T.INVALIDUSB						X				
T.RESIDUAL	X									
T.ROM_PROG			X							
T.SPOOF		X		X						
T.TRANSFER	X				X					
A.ACCESS							X			
A.MANAGE								X		
A.NOEVIL									X	
A.PHYSICAL										X

Table 7: Sufficiency of Security Objectives

Threats, Assumptions and OSPs	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 SmartCard reader and will perform no interaction with that device after the initial identification.	O.USBDETECT will detect the unauthorized connection so that 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 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 for DEVICES with bi-directional communications channels such as KEYBOARD, POINTING DEVICES, and SMARTCARD READERS. 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 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.ROM_PROG The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-	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)	O.ROM: The threat of software (firmware) embedded in reprogrammable ROMs is mitigated by ensuring that the ROMs used in the TSF to hold embedded TSF data are not physically able to be re-programmed. Thus, even if an interface does exist to the ROM containing the embedded TSF code, high confidence can be obtained that that code (stored in the ROM) will remain unchanged.

Threats, Assumptions and OSPs	Objective	Rationale
enforcing components of the code and subsequent compromise of the data flowing through the TOE.	to a circuit assembly.	
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 (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.	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.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	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 for DEVICES with bi-directional communications channels such as KEYBOARD, POINTING DEVICES, and SMARTCARD READERS. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from

Threats, Assumptions and OSPs	Objective	Rationale
	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.	one COMPUTER system to another, resulting in compromise of sensitive information. An example of the transfer is 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 make no sense to have, for example video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER
A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.	OE.ACCESS 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 guidance
A.MANAGE The TOE is installed and managed in accordance with the manufacturer's directions.	OE.MANAGE The TOE shall be installed and managed in accordance with the manufacturer's directions.	Restates the assumption
A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.	OE.NOEVIL The AUTHORIZED USER shall be non-hostile and follow all usage guidance.	Restates the assumption

Threats, Assumptions and OSPs	Objective	Rationale
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.

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. This section defines three extended SFRs met by the TOE.

NOTE: The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile,* Version 2.1, dated September 7, 2010 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 Requirements

The TOE meets the following functional requirements:

- TOE's visual inspection or visual confirmation feature 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.
- TOE also ensures that all USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, or SmartCard reader). No further interaction with non-valid devices shall be performed.
- TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

The three extended functional requirements are not defined in the existing SFRs of CC Part 2, nor do they fit into any existing functional class of CC Part 2. Hence, a new functional class (i.e. Class EXT) is created. The new functional class includes three functional families, i.e. EXT_VIR, EXT_IUC, and EXT_ROM, in which each of the aforementioned three functional requirements is defined respectively.

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 that is persistent for the duration of the CONNECTION.

5.1.2 Invalid USB Connection (EXT_IUC)

Family Behaviour

This family defines the response taken if invalid USB connections are detected.

Component leveling

EXT_IUC.1 Invalid USB Connection, Upon detection of an invalid USB connection, the switch will disable the connection.

Management: EXT_IUC.1

There are no management activities foreseen.

Audit: EXT_IUC.1

There are no auditable events foreseen.

EXT_IUC.1 **Invalid USB Connection**

Hierarchical to: No other components

Dependencies: None

EXT_IUC.1.1 All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, or SmartCard reader). No further interaction with non-valid devices shall be performed.

5.1.3 Read-only ROMs (EXT_ROM)

Family Behaviour

This family describes that TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

Component leveling

EXT_ROM.1 Read-only ROMs, TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

Management: EXT_ROM.1

There are no management activities foreseen.

Audit: EXT_ROM.1

There are no auditable events foreseen.

EXT_ROM.1	**Read-only ROMs**	
	Hierarchical to:	No other components
	Dependencies:	None
EXT_ROM.1.1	TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.	

5.2 Rationale for Extended Security Functional Requirements

The TOE contains the following explicitly stated security functional requirements:

- EXT_VIR.1
- EXT_IUC.1
- EXT_ROM.1

EXT_VIR.1 was explicitly stated because the TOE is required to have visual inspection or visual confirmation feature to provide the user with important information regarding the connection made through the TOE and allow the user to confirm that their data are being securely transported to the proper computer. There is not any existing SFR of CC Part 2 which can meet this requirement.

EXT_IUC.1 was explicitly stated because the TOE is required to ensure that all USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, or SmartCard reader), and no further interaction with non-valid devices shall be performed. There is not any existing SFR of CC Part 2 which can meet this requirement.

EXT_ROM.1 was explicitly stated because the TOE is required to ensure that TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly. There is not any existing SFR of CC Part 2 which can meet this requirement.

Moreover, the aforementioned three extended SFRs cannot easily fit into existing CC components, families, and classes. Hence, a new class, i.e. Class EXT, is used to group the three requirements, and each of which belongs to a new family.

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.2 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 Security Policies

Data Separation Security Function Policy (SFP): The TOE shall allow PERIPHERAL DATA 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.

6.3 TOE Security Functional Requirements

6.3.1 Class FDP: User Data Protection

6.3.1.1 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.

6.3.1.2 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 between the SHARED PERIPHERALS and the SWITCHED COMPUTERS].

6.3.1.3 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 (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 authorize 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].

6.3.1.4 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].

6.3.2 Class FMT: Security Management

6.3.2.1 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, thus effectively modifying the GROUP ID associated with the PERIPHERAL DEVICES.

6.3.2.2 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.

6.3.2.3 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: [

- modify the security attributes PERIPHERAL PORT GROUP IDs

].

6.4 TOE Security Assurance Requirements

The security assurance components are as stated in Table 8 (EAL2+).

Table 8: Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.2 Security-enforcing Functional Specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative user guidance
ALC: 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 (augmentation of EAL2)
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.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA:Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.5 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

6.6 Explicitly Stated Requirements for the TOE

This ST contains the explicitly stated requirement for the TOE.

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 that is persistent for the duration of the CONNECTION.

Application Note: Does not require tactile indicators, but does not preclude their presence.

EXT_IUC.1 Invalid USB Connection

Hierarchical to: No other components

Dependencies: None

EXT_IUC.1.1 All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard, or SmartCard reader). No further interaction with non-valid devices shall be performed.

EXT_ROM.1 Read-only ROMs

Hierarchical to: No other components

Dependencies: None

EXT_ROM.1.1 TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

6.7 Rationale for Assurance Level

This ST is based on the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile,* Version 2.1. The claimed assurance level EAL2+ was chosen as the higher level of assurance under the Canadian Common Criteria scheme.

6.8 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.

Table 9: Completeness of Security Functional Requirements

SFRs	O.CONF	O.INDICATE	O.ROM	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	
FMT_SMF.1				X		
EXT_VIR.1		X				
EXT_IUC.1						X
EXT_ROM.1			X			

6.9 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 GROUP COMPUTER 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
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.

Objectives	Requirements Addressing the Objective	Rationale
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.	**EXT_ROM.1** (Read-Only ROMs)	EXT_ROM.1 implements the O.ROM objective directly. While there might be other ways to protect embedded TSF code on a ROM (programmable or not), the requirement stipulates an easily-verifiable implementation that ensures that the TSF code will not be overwritten.
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_SMF.1** (Specification of Management Functions)	**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. **FMT_SMF.1:** The TOE provides the TOE user with management function of modifying the PERIPHERAL PORT GROUP IDs.
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 SmartCard reader 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.

6.10 Rationale for SFR

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 7, 2010. 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	N/A
EXT_IUC.1	None	N/A
EXT_ROM.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.**

7 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE.

Note that the TOE's enclosure is sealed at the factory using labels made of tamper-evident material. Labels manufactured from this material are very difficult to remove and reapply without leaving obvious evidence of tampering especially since the TOE has indentations on the top and sides that contain such labels. Labels are imprinted with the Cybex Logo and a unique 8-digit serial number. They are applied over several screws as well. The TOE also has the warning label "WARNING: This switch has tamper-evident seals. Broken or removed seals will void the warranty". The Quick Installation Guide shipped with the switch contains the same warning.

Users of the TOE should establish a schedule for checking the seals for tampering and order a replacement unit from the vendor if evidence of tampering is found.

7.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 6.3 and 6.6. 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 2.1, dated September 7, 2010.

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.

The following testable assertion corresponds to the SFRs listed below: User generated keyboard, mouse, and microphone data can flow only to the user selected computer, only the user selected computer can send the data to the user's video display and speakers, and data can flow only between the SmartCard reader and selected computer.

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. The TOE also provides the TOE user with management function of modifying the PERIPHERAL PORT GROUP IDs.

The following testable assertions correspond to the SFRs listed below: Selecting a computer is possible; only users can select a computer to be connected to the peripherals; only one default computer selection is made by the switch itself upon computer power-up; users have clear visual indication of which computer is currently selected.

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

7.1.3 Invalid USB Connection (TSF_IUC)

The firmware in the TOE checks a USB device's class when this device is connected to the TOE and ensures that the device is valid, i.e. is a pointing device, a keyboard, or SmartCard reader. If the device is not valid, the TOE doesn't allow further interaction to be performed by the non-valid device; thus non-valid USB devices connected to the switch by the users will not be connected to any of the target computers.

The following testable via demonstration and analysis assertion corresponds to the SFR listed below: any USB device which is not a pointing device, a keyboard, or SmartCard reader connected to the switch by the users will not be connected to any of the target computers.

FUNCTIONAL REQUIREMENTS SATISFIED: EXT_IUC.1

7.1.4 Read-only ROMs (TSF_ROM)

TSF software embedded in TSF ROMs is contained in one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly because the processors are soldered directly to the boards and utilize Code Read Protection level 3 (CRP3), which prevents the device's flash memory from being modified, by an external entity. The processors corresponding to the computers attached and the main processor handling the shared peripherals do not use any external RAM/ROM. The firmware running on these processors does not contain any commands to update itself.

FUNCTIONAL REQUIREMENTS SATISFIED: EXT_ROM.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.

DVI-I	Digital Video Interface - Integrated
IBM	International Business Machines, Inc.
LED	Light Emitting Diode
PC	Personal Computer
USB	Universal Serial Bus