Cybex SwitchView SC Series Switches Security Target

For models with [EXP_TMP]

Document Version 2.01

Prepared for:

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

Prepared by:

Computer Sciences Corporation
7231 Parkway Drive
Hanover, MD 21076

Revisions to Document		
Date	**Version**	**Changes Made**
October 26, 2007	2.01	Removed incorrect model numbers from section 2.3

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 Environment).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, 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 Chapter 6, 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 4.

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	Cybex SwitchView SC Series Switches Security Target
ST Version	2.01
Revision Number	$Revision: 2.01 $
Publication Date	$Date: 2007/10/26 11:42:54 $
Authors	Computer Sciences Corporation, Common Criteria Testing Lab Avocent Corporation
TOE Identification	Cybex SwitchView SC120 Models 520-563-501, 520-563-502 Cybex SwitchView SC220 Models 520-564-501, 520-564-502 Cybex SwitchView SC140 Models 520-565-501, 520-565-502 Cybex SwitchView SC240 Models 520-566-501, 520-566-502 Cybex SwitchView SC180 Model 520-679-501 Cybex SwitchView SC280 Model 520-680-501
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
ST Evaluation	Computer Sciences Corporation
Keywords	Device sharing, multi-way switch, peripheral switching, keyboard-video-monitor/mouse (KVM) switch

1.2 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 August 2005, Version 2.3, CCMB-2005-08-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3, CCMB-2005-08-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3, CCMB-2005-08-003
[CEM]	Common Evaluation Methodology for Information Technology Security Evaluation, dated August 2005, Version 2.3, CCMB-2005-08-004
[PSS_PP]	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000

1.3 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.3.1 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 4.4.1.3.2 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.

1.3.2 Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and 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.
Authentication data	Information used to verify the claimed identity of a user.
Object	An entity within the TOE Security Function (TSF[1]) Scope of Control (TSC[2]) that contains or receives information and upon which subjects perform operations.
Subject	An entity within the TSC that causes operations to be performed.
Authorized User	A user who may, in accordance with the TOE Security Policy (TSP[3]), perform an operation.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.

In addition to the above general definitions, this Security Target provides the following specialized definitions: Terminology is specific to this ST is given in “Terms of Reference,” Page 38, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000.

1.3.3 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

As defined in the CC, Part 1, version 2.3:
1 TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
2 TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
3 TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

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

1.3.4 ST Acronyms

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

CAC	Common Access Card
IBM	International Business Machines, Inc.
LED	Light Emitting Diode
PC/AT	Personal Computer / Advanced Technology
PS/2	Personal System 2
VGA	Video Graphics Array
USB	Universal Serial Bus

Acronyms specific to this ST, and the referenced PP are given in “Acronyms,” Page 42, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000.

1.4 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, keyboard, video, mouse, Common Access Card (CAC) 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 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.

Various models of the SwitchView SC series of switches work with IBM PC/AT, PS/2 and Sun systems with support for VGA video and Common Access Card (CAC) reader. PS/2 or USB keyboard and mouse peripherals are supported through the rear of the unit. Each switch has a “select” button associated with each specific port.

A summary of the SwitchView SC series switches security features can be found in Section 2, TOE Description. A detailed description of the SwitchView SC series switches security features can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance

The TOE (Cybex SwitchView SC120 Model 520-563-501, 520-565-502; Cybex SwitchView SC220 Model 520-564-501, 520-564-502; Cybex SwitchView SC140 Model 520-565-501, 520-565-502; Cybex SwitchView SC240 Model 520-566-501, 520-566-502; Cybex SwitchView SC180 Model 520-679-501; Cybex SwitchView SC280 Model 520-680-501) is Part 2 extended, and Part 3 augmented (with ALC_FLR.2). The TOE is conformant to Evaluation Assurance Level (EAL) 4. Also, the TOE is conformant to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000.

2 TOE DESCRIPTION

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

2.1 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, keyboard, video, mouse, Common Access Card (CAC) 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 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.

Various models of the SwitchView SC series of switches work with IBM PC/AT, PS/2 and Sun systems with support for VGA and Common Access Card (CAC) reader. PS/2 or USB keyboard and mouse peripherals are supported through the rear of the unit. Each switch has a "select" button associated with each specific port.

2.2 Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one SwitchView switch (see Table 1: TOE Models and Features), and its accompanying User and Administrator Guidance. Updated User and Administrator Guidance can be downloaded from the http://www.avocent.com website at any time.

Table 1: TOE Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
SwitchView SC120	520-563-501, 520-563-502	2	USB, PS/2, VGA
SwitchView SC220	520-564-501, 520-564-502	2	USB, PS/2, VGA, CAC
SwitchView SC140	520-565-501, 520-565-502	4	USB, PS/2, VGA
SwitchView SC240	520-566-501, 520-566-502	4	USB, PS/2, VGA, CAC
SwitchView SC180	520-679-501	8	USB, PS/2, VGA
SwitchView SC280	520-680-501	8	USB, PS/2, VGA, CAC

The evaluated TOE configuration 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.

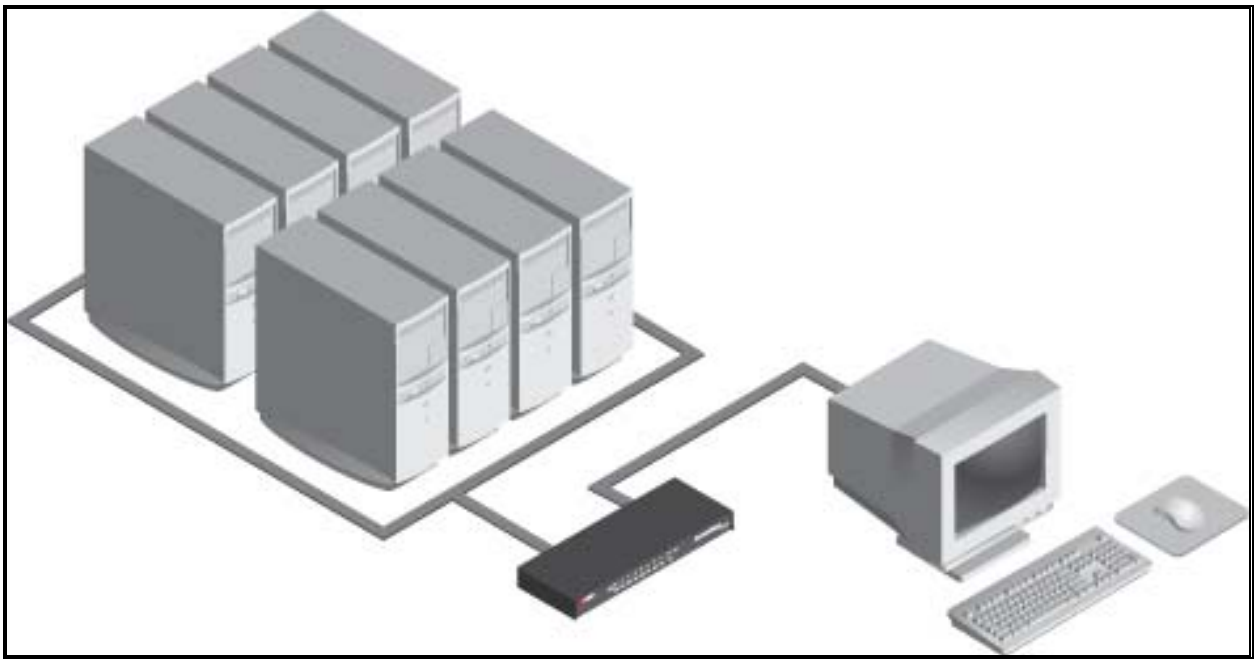

Figure 1: Depiction of TOE Deployment

2.3 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)

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 1.0, dated August 8, 2000. 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).

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.

2.4 TOE Features Outside of Evaluation Scope

There are no TOE features outside the evaluation scope.

3 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.

3.1 Assumptions

The specific conditions listed in "Secure Usage Assumptions," Section 3.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, are assumed to exist for the TOE.

3.2 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.

3.2.1 Threats Addressed by the TOE

"Threats to Security," Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, identifies threats to the assets against which specific protection within the TOE is required.

3.2.2 Threats Addressed by the Operating Environment

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, dated August 8, 2000, identifies no threats to the assets against which specific protection within the TOE environment is required.

3.3 Organizational Security Policies

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, dated August 8, 2000, 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

"Security Objectives for the Target of Evaluation," Section 4.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000 identifies the security objectives to address security concerns that are directly addressed by the TOE.

4.2 Security Objectives for the IT Environment

"Security Objectives for the Environment," Section 4.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, identifies security objectives to address security concerns that are directly addressed by the TOE environment.

5 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.

5.1 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 1.0, dated August 8, 2000. The SFR's have been reproduced here merely for the convenience of the customer.

5.1.1 User Data Protection (FDP)

FDP_ETC.1 **Export of User Data Without Security Attributes**

Hierarchical to: No other components.

FDP_ETC.1.1: The TSF shall enforce the [Data Separation SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2: The TSF shall export the user data without the user data's associated security attributes.

Dependencies: FDP_ACC.1 Subset access control
or
FDP_IFC.1 subset information flow control

FDP_IFC.1 **Subset Information Flow Control**

Hierarchical to: No other components.

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].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 **Simple Security Attributes**

Hierarchical to: No other components.

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 provide the following: [No additional SFP capabilities.]

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

Dependencies: FDP_IFC.1 Subset information flow control
and
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [Data Separation SFP] when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [No additional rules].

Dependencies: [FDP_ACC.1 Subset access control
or
FDP_IFC.1 Subset information flow control]
and
FMT_MSA.3 Static attribute initialisation

5.1.2 Security Management (FMT)

FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

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.

Dependencies: (FDP_ACC.1 Subset access control
or
FDP_IFC.1 Subset information flow control
and
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

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.

Dependencies: FDP_MSA.1 management of security attributes
FMT_SMR.1 Security roles

5.1.3 Protection of the TOE Security Functions (FPT)

Hierarchical to: No other components.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: None

FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: None

5.2 TOE Security Assurance Requirements

The security assurance components are specified in "Target of Evaluation Security Assurance Requirements," Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000. Additionally, the security assurance requirements have been augmented with ALC_FLR.2, which is drawn from CC Part 3 Security Assurance Requirements. This SAR has not been iterated or refined from Part 3.

5.3 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

This ST does contain the explicitly stated requirement for the TOE as specified in "EXT_VIR.1 (Visual Indication Rule)," Section 5.1.4.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000. It has been reproduced here:

EXT_VIR.1	**Visual Indication Rule**
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.
	Dependencies: None

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

EXP_TMP.1	**Prevention of Physical Tampering**
EXT_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.
	Dependencies: None

5.5 SFRs With SOF Declarations

The overall Strength of Function (SOF) claim for the TOE is SOF-medium (Reference "Threats to Security," Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000.

6 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.

6.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

6.1.1 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 1.0, dated August 8, 2000.

Signals processed by the TOE are keyboard data, mouse data, keyboard LED data, Data Display Channel information, analog video signals and USB status. 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 keyboard and mouse 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 keyboard and mouse 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 fixed polling loops, dedicated functions and static memory assignment with no third-party library functions or multitasking executives. This basic design results in a straightforward implementation suitable for independent verification to provide assurance of data separation.

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.

Keyboard LED 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.

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 flash in a unique pattern to alert an administrator to the interference, and all TOE functions will be permanently disabled.

FUNCTIONAL REQUIREMENTS SATISFIED: FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FPT_RVM.1, FPT_SEP.1, EXP_TMP.1

6.1.2 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

6.2 Assurance Measures

The TOE satisfies the CC EAL 4 assurance requirements as specified in "Target of Evaluation Security Assurance Requirements" Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000. The TOE additionally satisfies, and thus the Security Target is augmented with, the ALC_FLR.2 assurance requirement.

Per the conformance statement provided in Section 1.5 of this ST, the evidence requirements will be met with respect to presentation and content as specified in [CC_PART3] for each of the assurance requirements claimed.

7 PROTECTION PROFILE (PP) CLAIMS

This ST claims compliance for the following PP:

> *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000

As specified in Section 5 of this ST, the security requirements taken from the PP are referred back to the PP that this ST is claiming compliance with, and there were no operations performed on those requirements statements in the PP by this ST.

As specified in Section 4 of this ST, the security objectives are referred back to the PP that this ST is claiming compliance with, and there are no additional objectives. As specified in Section 5 of this ST, the security requirements taken from the PP are referred back to the PP that this ST is claiming compliance with. One additional explicitly stated requirement (EXP_TMP.1) has been added, its individual rationale is found in Section 8 of this Security Target.

8 RATIONALE

This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability	The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following: • security objectives to threats encountered • environmental objectives to assumptions met • SFRs to objectives met
Assurance Level	A justification is provided for selecting an EAL 4 level of assurance for this ST.
SOF	A rationale is provided for the SOF level chosen for this ST.
Dependencies	A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, without additional objectives. Consequently the security objectives rationale is provide in Section 6, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, and are claimed to be adequate for this ST.

8.2 Security Requirements Rationale

This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, without any operations performed on the IT security requirements specified in the cited PP. Consequently the security requirements rationale is provided in Section 6, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, and are claimed to be adequate for this ST for those requirements taken from the PP. Additional rationale for the augmented assurance requirements is found in Section 8.4.1 of this document. Rationale for the additional explicitly stated requirement (EXP_TMP.1) is as follows:

EXP_TMP.1 (Prevention of Physical Tampering)

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.

Objectives addressed: O.NOPROG, O.ROM

8.3 Rationale for Assurance Level

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0. 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 1.0, dated August 8, 2000). As such, the Evaluation Assurance Level 4 is appropriate.

8.4 Rationale for TOE Summary Specification

This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

The specified TSFs work together to satisfy the TOE SFRs. The following table provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 2: SFR to TSF Mapping

SFR	Name	TSF	Name
FDP_ETC.1	Export of User Data Without Security Attributes	TSF_DSP	Data Separation
FDP_IFC.1	Subset Information Flow Control	TSF_DSP	Data Separation
FPD_IFF.1	Simple Security Attributes	TSF_DSP	Data Separation
FDP_ITC.1	Import of User Data Without Security Attributes	TSF_DSP	Data Separation
FMT_MSA.1	Management of Security Attributes	TSF_MGT	Security Management
FMT_MSA.3	Static Attribute Initialization	TSF_MGT	Security Management
FPT_RVM.1	Non-bypassability of the TSP	TSF_DSP	Data Separation
FPT_SEP.1	TSF Domain Separation	TSF_DSP	Data Separation

SFR	Name	TSF	Name
EXT_VIR.1	Visual Indication Rule	TSF_MGT	Security Management
EXP_TMP.1	Prevention of Physical Tampering	TSF_DSP	Data Separation

8.4.1 TOE Assurance Requirements

Section 6.2 of this document identifies the Assurance Measures implemented by Avocent to satisfy the assurance requirements of EAL 4 as delineated in the table in Annex B of the CC, Part 3, and Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000. The Assurance Level is augmented with ALC_FLR.2, Flaw reporting procedures. This requirement ensures that instructions and procedures for the reporting, configuration management, and remediation of identified security flaws are in place.

8.4.2 TOE SOF Claims

The overall TOE SOF claim is SOF-medium because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 6.2 of the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, demonstrates that the security objectives for the TOE are satisfied by the security requirements. The SOF-medium claim for the TOE applies because the TOE protects against an attacker of average expertise, with few resources, and moderate motivation. The claim of SOF-medium ensures that the mechanism is resistant to a moderate attack potential.

8.5 Rationale For SFR and SAR Dependencies

This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, the rationale with respect to SFR and SAR dependencies from the PP is given in Sections 6.3 and 6.4 of the referenced PP. The augmented SARs have no dependencies and therefore require no dependency rationale.

The explicitly stated requirement EXP_TMP.1 does not contain any dependencies.

8.5.1 Rationale for Dependencies Not Met

Section 6.3 of the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0 contains a rationale for not having met the dependency on FMT_SMR.1. This PP was validated against Common Criteria v2.1. Since this validation, a dependency has been added to FMT_MSA.1. This new dependency is FMT_SMF.1, which did not exist in CC v2.1, and will not be met for the same basic reason that FMT_SMR.1 has not been met.

Due to the nature of the TOE, there are no security management functions to be performed. This *deleted* requirement, a dependency of FMT_MSA.1, allows the TOE to operate normally in the absence of any security functions to be managed.

8.6 Rationale for Explicitly Stated Requirements

By claiming conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, this ST contains an explicitly stated requirement. The rationale for this requirement is given in Section 6.2 of the referenced PP. This ST contains an additional explicitly stated requirement (EXP_TMP.1) beyond what is contained within the PP. The rationale for this requirement is given in Section 8.2 of this ST.

8.7 Internal Consistency and Mutually Supportive Rationale

The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a. The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b. The security functions of the TOE satisfy the SFRs as shown in Section 8.4. All SFR and SAR dependencies have been satisfied or rationalized as shown in Section 8.5 and described in Section 8.6.

c. The SARs are appropriate for the assurance level of EAL 4 and are satisfied by the TOE as shown in Section 8.4.1. EAL 4 was chosen to provide a medium level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d. The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.