Tripp Lite Secure KVM Switch Series
Security Target

File Name: Tripp Lite Secure KVM Switch Series Security Target.DOC
Version: 1.2
Date: 2011/09/01
Author: David Posner

Contents

1 ST Introduction

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Tripp Lite Secure KVM Switch, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the Tripp Lite Secure KVM Switch satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 ST and TOE Reference

ST Title: Tripp Lite Secure KVM Switch Series Security Target
TOE Identification:

- Tripp Lite Secure KVM Model B002-DUA2 (AG0027)
- Tripp Lite Secure KVM Model B002-DUA4 (AG0027)

ST Version: Version 1.2
Publication Date: 2011/09/01
Assurance Level: EAL 2 augmented with ALC_FLR.2
ST Author: David Posner

1.1.1 Document Conventions

The CC permits four types of operations to be performed based on security functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

a. Selection: Indicated by surrounding brackets and italicized text, e.g., [*selected item*].
b. Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].
c. Refinement: Indicated by underlined text, e.g., refined item for additions. ~~Deleted item~~ for deletion.

The functional security requirements beyond those defined in the claimed PP are identified by italicized text, e.g. *FMT_SMF.1*

1.2 TOE Overview

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

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

A PERIPHERAL PORT GROUP is a collection of DEVICE PORTS treated as a single entity by the TOE. There is one GROUP for the set of SHARED PERIPHERALS and one GROUP for each CONNECTED SWITCHED COMPUTER. Each SWITCHED COMPUTER GROUP has some unique associated logical ID (i.e. the SHARED PERIPHERALS PORT GROUP include the console monitor, USB mouse, USB keyboard, analog audio input device (e.g. microphone) and analog audio output device (e.g. speaker), while the SWITCHED COMPUTER PERIPHERAL PORT GROUP includes the DVI monitor connection, USB connection, and audio input/output connection). The SHARED PERIPHERAL GROUP ID is considered to be the same as that of the SWITCHED COMPUTER GROUP currently selected by the TOE.

1.2.1 TOE Type

The TOE has KVM (USB Keyboard, DVI-I Video, USB Mouse) switch functionality and a combination of 2/4 port KVM switch and audio (input & output) ports.

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 audio input/output devices. 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. The TOE will then visually indicate which COMPUTER is selected by the USER. Such indication is persistent and not transitory in nature.

1.2.2 Non-TOE hardware/software/firmware

There are no hardware/software/firmware components of the TOE that are outside of the scope of evaluation.

1.3 TOE Description

The TOE provides KVM (USB Keyboard, DVI-I Video, USB Mouse) switch functionality by combining a 2/4 port KVM switch and audio (input & output) ports. As a KVM switch, the TOE allows users to access two or four computers from a single set USB keyboard, USB mouse, and DVI-I monitor console.

In the Tripp Lite Secure KVM Switch, keyboard/mouse, video, and audio are processed by different chipsets. The keyboard/mouse is processed by an ASIC. The video signal is process by a video switch chipset and the audio is process by another analog switch (multiplexer). The video and audio chipset only switches between channels and allows the video/audio signal to pass through.

Setup is fast and easy; simply plug the KVM cables into their appropriate ports. There is no software to be configured, no firmware to be upgraded, no boards to be configured, no installation routines to be run, and no incompatibility problems. The only way to switch between computers is via the pushbuttons located on the unit's front panel. Since the TOE intercepts keyboard inputs directly, it can work on multiple computing platforms (PC (x86/x64), Macintosh PowerPC, and Sun Microsystems Sparc). The TOE is designed with its own unique security architecture. The TOE does not allow private data to be shared between the connected computers. And since the private data is totally separated, users can access connected computers using a single set of console via the TOE even when the computers are located on different networks (classified/unclassified).

1.4 TOE Boundaries

1.4.1 Physical Boundary

The following tables list the hardware/firmware components and the accompanying documents. They also identifying which are in the TOE and which are in the environment.

Hardware Components

TOE Model	Ports	Interface
B002-DUA2 (AG0027)	2	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio input (e.g. Microphone) and Analog Audio output (e.g. Speaker), Switch Buttons, LED indicators
B002-DUA4 (AG0027)	4	Dual Link DVI-I, USB Keyboard, USB mouse, Analog Audio input (e.g. Microphone) and Analog Audio output (e.g. Speaker), Switch Buttons, LED indicators

TOE/Environment	Component	Description
TOE	B002-DUA2 B002-DUA4	TOE Hardware
Environment	USB Keyboard	Member of Peripheral Group
Environment	USB Mouse	Member of Peripheral Group
Environment	DVI Monitor	Member of Peripheral Group
Environment	Audio Input/Output (e.g. Speaker and Microphone)	Member of Peripheral Group
Environment	Host Computers	Computer Environment

Firmware Components

TOE Model	Firmware
B002-DUA2 (AG0027)	FW v1.0.064
B002-DUA4 (AG0027)	

Guidance Documents

The guidance documents that accompany the TOE are:

TOE Model	AGD_OPE/AGD_PRE Guidance
B002-DUA2 (AG0027)	Tripp Lite Secure KVM Switch Series Guidance v1.3.pdf
B002-DUA4 (AG0027)	

1.4.2 Logical Boundaries

The Logical Scope and Boundary of the TOE consists of the security functions and features provided by the TOE. The security functions include Information Flow Control (TSF_IFC), Security Management (TSF_MGT), and Self Protection (TSF_SPT).

1.4.2.1 Information Flow Control (TSF_IFC)

Per the request of the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 07, 2010. Data Separation Security Function Policy (SFP) is implemented in the TOE. The TOE shall allow PERIPHERAL DATA to be transferred only between PERIPHERAL PORT GROUPS with the same ID. The TOE processes mainly keyboard/mouse data, keyboard LED data, Data Display Channel information, video signals, audio data and USB status. The TOE is neither concerned with the USER's information in the shared computers nor the 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. As long as the guidance is followed by the Administrator while configuring and using the TOE, only valid USB devices are accepted by the TOE. Therefore the user information flows are safe. A more detailed explanation of TSF_IFC implementation is described in Section 7.1.1.

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

1.4.2.2 Security Management (TSF_MGT)

There are two (B002-DUA2) or four (B002-DUA4) pushbuttons on the TOE front panel. The only method to access the computers via TOE is by pushbuttons. By pressing the pushbutton, the user can explicitly determine which port is to be selected or which computer to switch to. The user can explicitly determine which computer is connected to the shared set of peripherals. There are two LED indicators (one green, one orange) located above each pushbutton. The green LED indicator of a specific port lights up when there is a computer connected to that port and powered on (the green LED indicator is lit when there is a powered-on USB connection between the TOE and any connected computers). Once a specific computer is selected by the user, which means the share set of peripherals switches to that port of computer, the orange LED indicator lights. An explanation of TSF_MGT implementation is described in

Section 7.1.2

1.4.2.3 Self Protection (TSF_SPT)

This function is intended to protect the set of peripheral devices connected to the TOE. Any attempt to open the TOE will trigger a Tamper Detection switch. Once the TOE is physically tampered, the LED lights on the front panel flash to alert and remind the administrator that this has occurred. All TOE functions are disabled.

The firmware of the TOE is embedded in one-time-programmable ROMs inside the ASIC which is permanently attached (non-socketed) to a circuit assembly. So there is no way to modify the firmware. A more detailed explanation of TSF_SPT implementation is described in Section 7.1.3

2 Conformance Claims

2.1 Common Criteria Conformance

-

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.
  - Part 2 Extended
  - Part 3 Conformant

2.2 Protection Profile Conformance

This ST claims demonstrable compliance to the Protection Profile:
Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1 dated September 7, 2010

2.3 Evaluation Assurance Level

EAL 2+ (augmented with ALC_FLR.2 (Flaw reporting procedures))

3 Security Problem Definition

The security problem definition shows the threats, Organizational Security Policies (OSPs) and assumptions that must be countered, enforced and upheld by the TOE and its operational environment.

3.1 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

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 Organizational Security Policies

None.

3.3 Assumptions

The following usage assumptions are made about the intended environment of the TOE.

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.

Application Note: The installed USB devices connected to the TOE do not buffer and transfer data to any COMPUTERS other than the currently CONNECTED COMPUTER.

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

A.PHYSICAL The TOE is physically secure.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE

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

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

O.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, or display and will not perform any interaction with that device after the initial identification.

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

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

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

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

OE.PHYSICAL The TOE shall be physically secure.

5 Extended Components Definition

This section specifies the extended SFRs for the TOE.

5.1 Class EXT: Extended

This class provides four families specifically concerned with Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for

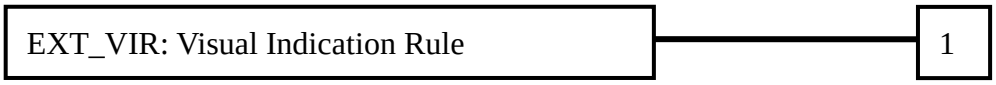
- EXT_VIR.1 Visual Indication Rule
- EXT_IUC.1 invalid USB Connection
- EXT_ROM.1 Read-Only ROMs
- *EXT_TMP.1 Physical Tampering Security*

5.1.1 Visual Indication Rule (EXT_VIR)

Family Behaviour

This family defines requirements for the visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided for the duration of the CONNECTION.

Component leveling



Management: EXT_VIR.1

No management activities are foreseen.

Audit: EXT_VIR.1

No auditable events are foreseen.

EXT_VIR.1 Visual Indication Rule

Hierarchical to: No other components

Dependencies: None

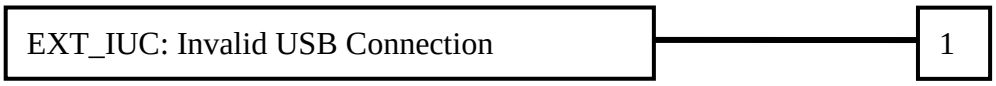
EXT_VIR.1.1 A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided that is persistent for the duration of the CONNECTION.

5.1.2 Invalid USB Connection (EXT_IUC)

Family Behaviour

This family defines the requirements for the interrogation of all USB devices connected to the Peripheral switch to ensure that they are valid (pointing device, keyboard, display).

Component leveling



Management: EXT_IUC.1

No management activities are foreseen.

Audit: EXT_IUC.1

No auditable events are 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, display). No further interaction with non-valid devices shall be performed.

5.1.3 Read-Only ROMs (EXT_ROM)

Family Behaviour

This family defines the requirements for the TSF software/firmware which must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

Component leveling

Management: EXT_ROM.1

No management activities are foreseen.

.

Audit: EXT_ROM.1
No auditable events are foreseen.

EXT_ROM.1	Read-Only ROMs	
	Hierarchical to:	No other components
	Dependencies:	None

EXT_ ROM.1.1	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.

5.1.4 Physical Tampering Security (EXT_TMP)

Family Behaviour
This family defines the requirements for the protection of the set of peripheral devices connected to the TOE. Any attempt to open the enclosure will trigger a Tamper Detection switch. Once the Tamper Detection switch is triggered, all TOE functions are disabled.

Component leveling

Management: *EXT_TMP.1*
No management activities are foreseen.

Audit: *EXT_TMP.1*
No auditable events are foreseen.

EXT_TMP.1	*Physical Tampering Security*	
	Hierarchical to:	No other components
	Dependencies:	None

EXT_TMP.1.1	*Any attempt to open the enclosure of the TOE will trigger a Tamper Detection switch. Once the Tamper Detection switch is triggered, all TOE functions are disabled.*

6 Information Technology Security Requirements

6.1 Target of Evaluation Security Requirements

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

6.1.1 User Data Protection (FDP)

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

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

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

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

6.1.2 Security Management (FMT)

6.1.2.1 **FMT_MSA.1** (Management of Security Attributes)
[Dependencies: (FDP_ACC.1 or FDP_IFC.1) FMT_SMR.1, and *FMT_SMF.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.

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

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

6.1.2.3 ***FMT_SMF.1*** *(Specification of Management Functions)*
[No dependencies*]*

*1. The TSF shall be capable of performing the following management functions: [*selection of the CONNECTED PERIPHERAL PORT GROUP*]*.
   Application Note: This SFR is missing in the PSS PP which is required by FMT_MSA.1.

6.1.3 Extended Requirements (EXT)

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

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

6.1.3.2 **EXT_IUC.1** (Invalid USB Connection)

[No dependencies]

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

6.1.3.3 **EXT_ROM.1 (**Read-Only ROMs)

[No dependencies]

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.

6.1.3.4 ***EXT_TMP.1*** (*Physical Tampering Security*)

[No dependencies]

1. Any attempt to open the enclosure of the TOE will trigger a Tamper Detection switch. Once the Tamper Detection switch is triggered, all TOE functions are disabled.

6.2 Target of Evaluation Security Assurance Requirements

The following table describes the TOE security assurance requirements drawn from Part 3 of the CC. The security assurance requirements represent EAL2 augmented with ALC_FLR.2.

Assurance Class	Assurance Components	
	Identifier	**Name**
ADV: Development	ADV_ARC.1	Security architecture description
	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 procedures
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
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

7 TOE Summary Specification

This section summarizes the security functions and describes the security functions implemented in the TOE. This section also describes the applied assurance measures needed to ensure the correct security function implementation

7.1 TOE Security Functions

The security functions performed by the TOE include Data Separation (TSF_IFC), Security Management (TSF_MGT), and Self Protection (TSF_SPT)

7.1.1 Information Flow Control (TSF_IFC)

Per the requirement of the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 07, 2010, Data Separation Security Function Policy (SFP) is implemented in the TOE. The TOE shall allow PERIPHERAL DATA to be transferred only between PERIPHERAL PORT GROUPS with the same ID. The TOE processes mainly keyboard/mouse data, keyboard LED data, Data Display Channel information, video signals, audio data and USB status. The TOE itself is neither concerned with the USER'S information in the shared computers nor the 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. As long as the guidance is followed by the Administrator while configuring and using the TOE, only valid USB devices are accepted by the TOE. Therefore the user information flows are safe.

The TOE deals with the following type of signals: keyboard data (including its LED), mouse data, USB status, audio (input/output) data and video signals. The TOE collects subsets of the signals and transfers them to the connected switched computers. There is no data or information flowed between CONNECTED COMPUTERS.

By using specifically designed hardware and firmware, the TOE ensures data separation for all paths of signals. The user data is not stored or buffered for video and audio data in the TOE. The keyboard and mouse data are not stored but are buffered and sent to the CONNECTED COMPUTER. These buffers are zeroed before the PERIPHERAL GROUP ID is changed. However the keyboard Num/Cap/Scr lock status for each COMPUTER is kept in the TOE to resume lock status of the keyboard.

There is no possibility to forward the buffered data to the next selected COMPUTER. In the firmware, specially designed functions are dedicated for Data Separation Functions. Static memory is assigned for these functions without any third-party libraries or multitasking executives.

Concerning the audio (input/output), the audio data separation mechanism is the same as the above mechanism. No data will be buffered and sent to other computer.

In operation the TOE itself is neither concerned with the USER'S information in the shared computers nor with the information flowing between the SHARED PERIPHERALS and the SWITCHED COMPUTERS. It only provides a single 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."
FUNCTIONAL REQUIREMENTS SATISFIED: FDP_IFC.1, FDP_IFF.1

All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device and keyboard). No further interaction with non-valid devices shall be performed.
FUNCTIONAL REQUIREMENTS SATISFIED: EXT_IUC

7.1.2 Security Management (TSF_MGT)

There are two (B002-DUA2) or four (B002-DUA4) pushbuttons on the TOE front panel. The only method to access the computers via TOE is by pushbuttons. By pressing the pushbutton, user can explicitly determine which port he wants to select or which computer he wants to switch to, which means the user can explicitly determine which computer is connected to the shared set of peripherals. There are also two LED indicators (one green, one orange) located above each pushbutton. The green LED indicator of a specific port lights up when there is a computer connected on that port and it is powered on. Once a specific computer is selected by the user, which means the share set of peripherals switches to that port of computer, the orange LED indicator lights up.
FUNCTIONAL REQUIREMENTS SATISFIED: FMT_MSA.1, FMT_MSA.3, TMT_SMF.1, EXT_VIR.1, FDP_IFF.1

7.1.3 Self Protection (TSF_SPT)

This function is intended to protect the set of peripheral devices connected to the TOE. Any attempt to open the TOE will trigger a Tamper Detection switch. The Tamper Detection switch inside the TOE is powered by a dedicated battery. This switch will be triggered once the enclosure cover of the TOE is opened. Once the Tamper Detection switch has been triggered, the orange LED lights on the front panel flash to alert and remind the administrator of this event. All TOE functions and the TOE itself are disabled. None of the operations can be restored. Since the ROM inside the TOE is OTP (One time programmable), there is no way for the user to reset or recover the system once the firmware runs into the disable loop after the switch is triggered. The TOE has to be returned to Tripp Lite. Tripp Lite will either exchange it for new hardware or they will change the main board with a new one and send the unit back to the customer. The contact information is listed as follows:

Tripp Lite World Headquarters

Website:	http://www.tripplite.com
Address:	1111 W. 35th Street
	Chicago, IL 60609 USA
Phone:	+1-773-869-1233
Fax:	+1-773-869-1177
E-mail:	techsupport@tripplite.com

For customers outside the US, please email to intlservice@tripplite.com, or headquarters listed below for more detailed information
www.tripplite.com/support

FUNCTIONAL REQUIREMENTS SATISFIED: EXT_TMP

The OTP ROM in the ASIC is soldered on the PCB to ensure that the firmware inside the TOE will not be modified or corrupted.
FUNCTIONAL REQUIREMENTS SATISFIED: EXT_ROM

8 Rationale

8.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and each security objective addresses at least one assumption or threat.

8.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats that the TOE is intended to counter, and to those assumptions that must be met.

This ST claims conformance to the [PSS_PP] with identical security objectives for the TOE. Therefore the security objectives rationale provided in "[PSS_PP] - Section 6.1" are claimed to be consistent with this ST.

8.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those threats that the environment is expected to counter, and to the assumptions that must be met.

This ST claims conformance to the [PSS_PP] with identical security objectives for the Environment. Therefore the security objectives rationale provided in "[PSS_PP] - Section 6.2" are claimed to be consistent with this ST.

8.2 Rationale for Security Requirements

In this section, the security objectives are mapped to the functional requirements and the rationale is provided for the selected EAL and its components and augmentation.

8.2.1 Rationale for TOE security functional requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives.

This ST claims conformance to the [PSS_PP] with identical security objectives and security functional requirements (except: *EXT_TMP.1 Physical Tampering Security*) for the TOE. Therefore the security objectives rationale provided in "[PSS_PP] -

Section 6.3" are claimed to be consistent with this ST. The rationale of the additional security functional requirements (*EXT_TMP.1 Physical Tampering Security*, *FMT_SMF.1 Specification of Management Functions*) is provided in the following:

Objective	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_TMP.1 Physical Tampering Security*	*EXT_TMP.1* implements the O.ROM objective indirectly. Any attempt to open the enclosure of the TOE will trigger a Tamper Detection switch. Once the Tamper Detection switch is triggered, all TOE functions are disabled. Therefore this requirement ensures that the TSF code will not be overwritten or modified.
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_SMF.1 Specification of Management Functions*	*FMT_SMF.1* allows an AUTHORIZED USER to explicitly press the port selection pushbutton located on the TOE's front panel. According to the pressed pushbutton, the TOE generates the corresponding SHARED PERIPHERAL GROUP ID. Each SWITCHED COMPUTER GROUP has a unique logical ID according to the connected ports. All DEVICES in a SHARED PERIPHERAL GROUP will be CONNECTED to the SWITCHED COMPUTER GROUP whose SWITCHED COMPUTER GROUP ID is the same as the SHARED PERIPHERAL GROUP ID.

NOTE: There is some previous information (no longer necessary), FDP_ETC.1 and FDP_ITC.1, which remains in "[PSS_PP] - Section 6.3".

8.2.2 Rationale for Security Assurance Requirements (SAR)

EAL2 augmented with ALC_FLR.2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor and assume the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2 augmented with ALC_FLR.2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The assurance claim is consistent to meet the requirements of a Basic Robustness TOE environment.

8.2.3 Dependencies Rationale

The dependency of FMT_SMR.1 is not to meet with CC. The rationale is as follow.

FMT_SMR.1 (Security Roles)

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

8.3 TOE Summary Specification Rationale

This section contains a table which relates the security functional requirements to the TOE security functions. The rationale that the security functions cover the security functional requirements is provided in Section 7.1 TOE Security Functions.

	Information Flow Control (TSF_IFC)	Security Management (TSF_MGT)	Self Protection (TSF_SPT)
FDP_IFC.1	X		
FDP_IFF.1	X	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
EXT_TMP.1			X

9 Acronyms & Reference

9.1 Acronyms

CC Common Criteria

DVI-I Digital Video Interface - Integrated

LED Light Emitting Diode

USB Universal Serial Bus

9.2 Reference

[PSS_PP] *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 7, 2010