



Argon Corp Ruggedized KVM Switch Security Target

Document Version: .11

May 3, 2011

Prepared For:

Argon Corp
343 Great Neck Road
Great Neck, NY 11021

Prepared By:

CSC
7231 Parkway Drive
Hanover, MD 21076



This page is intentionally blank.

Table of Contents

1	SECURITY TARGET INTRODUCTION.....	6
1.1	ST AND TOE IDENTIFICATION	6
1.2	TOE OVERVIEW.....	7
1.2.1	<i>Usage and Major Security Features.....</i>	7
1.2.2	<i>TOE Type.....</i>	7
1.2.3	<i>Required Non-TOE Hardware, Firmware and Software</i>	7
1.3	TOE DESCRIPTION.....	8
1.3.1	<i>Physical Scope of the TOE</i>	8
1.3.2	<i>Logical Scope of the TOE.....</i>	8
1.3.3	<i>Evaluated Configuration</i>	9
2	CONFORMANCE CLAIMS.....	10
2.1	COMMON CRITERIA CONFORMANCE CLAIMS.....	10
2.2	PROTECTION PROFILE CONFORMANCE CLAIMS	10
2.3	PACKAGE CLAIMS	10
2.4	CONFORMANCE CLAIMS RATIONALE.....	10
3	SECURITY PROBLEM DEFINITION	11
3.1	ASSUMPTIONS	11
3.2	THREATS	11
3.2.1	<i>Threats Addressed by the TOE.....</i>	12
3.2.2	<i>Threats addressed by the IT Environment.....</i>	12
3.3	ORGANIZATIONAL SECURITY POLICIES	12
4	SECURITY OBJECTIVES	13
4.1	SECURITY OBJECTIVES FOR THE TOE.....	13
4.2	SECURITY OBJECTIVES FOR THE ENVIRONMENT	13
4.3	RATIONALE	14
5	EXTENDED COMPONENTS DEFINITION	19
5.1	CLASS EXT: EXTENDED – INSPECTION	19
5.1.1	<i>Visual Inspection (EXT_VIR).....</i>	19
6	SECURITY REQUIREMENTS.....	20
6.1	CONVENTIONS.....	20
6.2	TOE SECURITY POLICIES.....	20
6.2.1	<i>Data Separation SFP (TSP_DSP).....</i>	20
6.3	SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE	20
6.3.1	<i>Class FDP: User Data Protection.....</i>	21

6.3.2	<i>Class FMT: Security Management</i>	22
6.3.3	<i>Class EXT: Extended – Inspection</i>	23
6.4	SECURITY ASSURANCE REQUIREMENTS FOR THE TOE	23
6.5	SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT	24
6.6	RATIONALE FOR SECURITY FUNCTIONAL REQUIREMENTS	24
6.7	RATIONALE FOR SECURITY ASSURANCE REQUIREMENTS	27
6.8	RATIONALE FOR DEPENDENCIES	27
6.8.1	<i>Security Functional Requirement Dependencies</i>	27
6.8.2	<i>Security Assurance Requirement Dependencies</i>	27
7	TOE SUMMARY SPECIFICATION	29
7.1	TOE SECURITY FUNCTIONS	29
7.1.1	<i>Data Separation (TSF_DSP)</i>	29
7.1.2	<i>Security Management (TSF_MGT)</i>	30
8	GLOSSARY	31
8.1	TERMS	31
8.2	ACRONYMS	31

1 Security Target Introduction

This Chapter presents Security Target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

- a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).
- b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4, 5 and 6, Security Objectives, Extended Components Definition, and IT Security Requirements, respectively).
- c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 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 associated TOE. This ST targets Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2.

ST Title:	Argon Corp Ruggedized KVM Switch Security Target
ST Version:	.11
Publication Date:	May 3, 2011
Authors:	CSC Security Testing and Certification Laboratories, Argon Corp
TOE Identification:	Argon Corp Ruggedized KVM Switch Part Number 90731
ST Evaluator:	CSC Security Testing and Certification Laboratories
Keywords:	Argon, Security Target, Protection Profile, KVM Switch, peripheral sharing, keyboard, mouse, video, audio, rugged

1.2 TOE Overview

1.2.1 Usage and Major Security Features

The TOE is a ruggedized peripheral sharing switch (PSS) based on the Avocent SwitchView SC Series SC440 hardware, which was Common Criteria evaluated as VID-10327¹. This PSS is protected from the elements (e.g. water, wind, debris) by an aluminum case. The switch has a remote set of buttons (connected to the switch by a 12-foot cable) that are large enough to be operated by users who are wearing gloves or other protective equipment. The indicator lights for this TOE are also located on the remote selection device, a custom extension to the Avocent switch, and are plainly visible to users. Due to the inaccessible environment that this PSS is designed to be deployed in, there are no selection buttons or indicator lights on the switch case itself. The PSS is controlled remotely. The Remote Controls under evaluation are: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

The Argon Ruggedized KVM Switch Part Number 90731 (hereafter referred to as the “Argon 90731 Switch”) connects a single set of human interface input and output devices (e.g. keyboard, mouse, video, audio) to one or more computers. The switch passes data between the input/output devices and the computer(s); it is not concerned with and does not modify or otherwise interfere with the content of the data.

The Argon 90731 Switch works with IBM PC compatible and Sun systems and has ports for USB keyboard, USB mouse, DVI-I video, audio (input and output), and USB Common Access Card (CAC) or SmartCard reader. The switch has a “select” button (connected via a 12-foot cable) associated with each specific port. A CCID Smart Card reader or a CAC reader can be used with the Argon 90731 Switch, but this capability is not included in the evaluated configuration.

A summary of the Argon 90731 Switch security features can be found in Section 1.3, TOE Description. A detailed description of the Argon 90731 Switch security features can be found in Section 7, TOE Summary Specification.

1.2.2 TOE Type

The TOE is a ruggedized peripheral sharing switch (PSS) that connects a single set of human interface devices to one or more computers.

1.2.3 Required Non-TOE Hardware, Firmware and Software

The TOE does not require any external hardware to provide its standard functionality; however, it must be connected to one or more human interface devices and computers in order to be useful as a peripheral sharing switch.

¹ All Avocent and Cybex trademarks and copyrights are acknowledged.

1.3 TOE Description

This section provides context for the TOE evaluation by identifying the logical and physical scope of the TOE, as well as its evaluated configuration.

1.3.1 Physical Scope of the TOE

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Argon 90731 Switch, and its accompanying User and Administrator Guidance. The switch is capable of connecting one set of human interface peripherals (as described in Section 1.2.1) to up to four computers as depicted in the figure below.

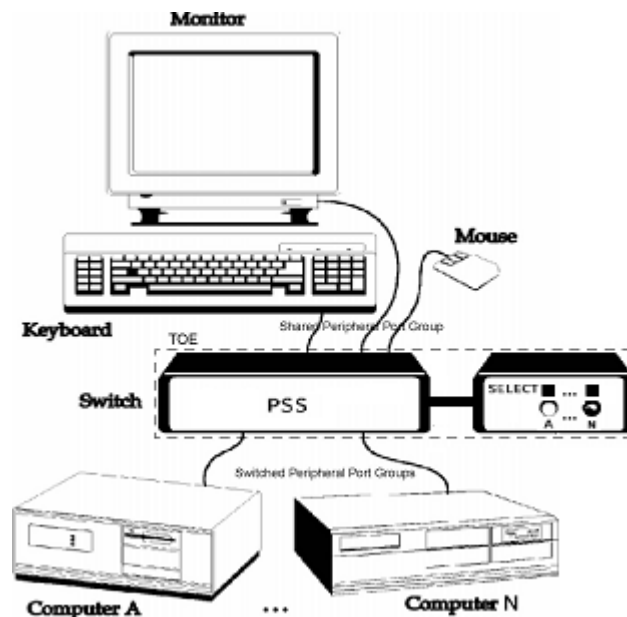


Figure 1: Example depiction of TOE usage

1.3.2 Logical Scope of the TOE

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 1.2, dated August 21, 2008. In operation, the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP). Data Separation is accomplished as explained in section 7.1.1.

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. To select or switch computers, the TOE utilizes remote select switches and LEDs, 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 remotely by an LED near or integrated into the selected channel button. Security Management is accomplished as explained in section 7.1.2.

1.3.3 Evaluated Configuration

In its evaluated configuration, the TOE is connected to a set of human interface devices and one or more computers. The human interface devices and computer(s) are not a part of the TOE. One feature of the TOE that is outside of the scope of the evaluation is the use of smart cards which is not allowed in the evaluated configuration.

The Remote Controls under evaluation are: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

For the TOE to meet an EAL4 assurance level in a Common Criteria evaluated configuration, the selected remote control indicator light must never be dimmed so that it is not visible to the user.

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 1, CCMB-2006-09-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 1, CCMB-2006-09-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 1, CCMB-2006-09-003

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

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

2.2 Protection Profile Conformance Claims

This Security Target claims demonstrable conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008 (referred to in this ST as “PSS PP”).

2.3 Package Claims

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

2.4 Conformance Claims Rationale

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

The Security Problem Definition (Threats, Assumptions and Organizational Security Policies) and Objectives have been copied directly from PSS PP, and have not been modified. The statement of Security Requirements contains the SFRs and Extended Components from PSS PP. By including all of the SFRs and Extended Components from PSS PP, the statement of Security Requirements is necessarily at least as strict as the statement in PSS PP, if not more strict. The rationales for objectives, threats, assumptions, organizational security policies and security requirements have been copied from PSS PP.

3 Security Problem Definition

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

Note: The content in this section is taken directly from PSS PP and is copied here for completeness.

3.1 Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Security Target are based on the condition that all of the assumptions described in this section are satisfied.

Table 1: Assumptions for the TOE

Assumption	Definition
A.ACCESS	An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
A.EMISSION	The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]
A.ISOLATE	Only the selected COMPUTER'S video channel will be visible on the shared MONITOR.
A.MANAGE	The TOE is installed and managed in accordance with the manufacturer's directions.
A.NOEVIL	The AUTHORIZED USER is non-hostile and follows all usage guidance.
A.PHYSICAL	The TOE is physically secure.
A.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, are a concern of the application scenario and not of the TOE.

Application Note: *Since assumptions cannot be made about the TOE itself in a Common Criteria evaluation, the ST author interprets A.PHYSICAL (copied directly from PSS PP) to assume that the environment provides physical protection for the TOE.*

3.2 Threats

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.

3.2.1 Threats Addressed by the TOE

Table 2: Threats to Addressed by the TOE

Threat	Description
T.BYPASS	The TOE may be bypassed, circumventing nominal SWITCH functionality.
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy.
T.LOGICAL	The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.
T.PHYSICAL	A physical attack on the TOE may violate the security policy.
T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.
T.SPOOF	Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.
T.STATE	STATE INFORMATION may be transferred to a PERIPHERAL PORT GROUP with an ID other than the selected one.
T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

3.2.2 Threats addressed by the IT Environment

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

3.3 Organizational Security Policies

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

4 Security Objectives

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

- Security objectives for the TOE, and
- Security objectives for the environment.

Note: The content in this section is taken directly from PSS PP and is copied here for completeness.

4.1 Security Objectives for the TOE

This section describes the security objectives that the TOE shall fulfill.

Table 3: Security Objectives for the TOE

Objective	Definition
O.CONF	The TOE shall not violate the confidentiality of information which it processes. Information generated within any PERIPHERAL GROUPCOMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER CONNECTION.
O.CONNECT	No information shall be shared between SWITCHED COMPUTERS via the TOE. This includes STATE INFORMATION, if such is maintained within the TOE.
O.INDICATE	The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.
O.INVOKE	Upon switch selection, the TOE is invoked.
O.NOPROG	Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components.
O.ROM	TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.
O.SELECT	An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.
O.SWITCH	All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.

4.2 Security Objectives for the 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 4: Security Objectives for the Non-IT Environment

Objective	Definition
OE.ACCESS	The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
OE.EMISSION	The TOE shall meet the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]
OE.ISOLATE	Only the selected COMPUTER'S video channel shall be visible on the shared MONITOR.
OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
OE.NOEVIL	The AUTHORIZED USER shall be non-hostile and follow all usage guidance.
OE.PHYSICAL	The TOE shall be physically secure.
OE.SCENARIO	Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, shall be a concern of the application scenario and not of the TOE.

4.3 Rationale

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 5: Completeness of Security Objectives

Threats, Policies, Assumptions	Objectives															
	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH		OE.ACCESS	OE.EMISSION	O.ISOLATE	OE.MANAGE	OE.NOEVIL	OE.PHYSICAL	OE.SCENARIO
T.BYPASS				X												
T.INSTALL													X			
T.LOGICAL					X	X										
T.PHYSICAL	X				X	X										
T.RESIDUAL	X	X														

T.SPOOF			X				X									
T.STATE	X	X														
T.TRANSFER	X	X					X									
A.ACCESS									X							
A.EMISSION										X						
A.ISOLATE											X					
A.MANAGE												X				
A.NOEVIL													X			
A.PHYSICAL														X		
A.SCENARIO																X

NOTE: The security objectives rationale in the Protection Profile is incomplete; while mapping T.INSTALL to OE.MANAGE, the Protection Profile does not provide a rationale for the mapping. This ST provides this rationale in the table below:

Table 6: Sufficiency of Security Objectives

Threats, Policies, and Assumptions	Summary	Objectives and rationale
T.BYPASS	O.INVOKE	The TOE must be invoked whenever a switch selection is made.
T.INSTALL	OE.MANAGE	(See note above) Installing and delivering the TOE in accordance with the manufacturer's instructions mitigates they risk of violation of the security policy during delivery and installation.
T.LOGICAL	O.NOPROG	The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information) may change.
	O.ROM	Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which prevents its modification
T.PHYSICAL	O.CONF	If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information.

Threats, Policies, and Assumptions	Summary	Objectives and rationale
		An example of this is transfer via the buffering mechanism in many KEYBOARDS.
	O.NOPROG	The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information) may change.
	O.ROM	Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which prevents its modification.
T.RESIDUAL	O.CONF	If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.
	O.CONNECT	The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER.
T.SPOOF	O.INDICATE	The USER must receive positive confirmation of SWITCHED COMPUTER selection.
	O.SELECT	The USER must take positive action to select the current SWITCHED COMPUTER.
T.STATE	O.CONF	If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many

Threats, Policies, and Assumptions	Summary	Objectives and rationale
		<p>PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.</p>
	O.CONNECT	<p>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.</p>
T.TRANSFER	O.CONF	<p>If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.</p>
	O.CONNECT	<p>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.</p>
	O.SWITCH	<p>The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. It makes no sense to have, for example, video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER.</p>
A.ACCESS	OE.ACCESS	<p>All authorized users are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate training, and follow all user guidance.</p>

Threats, Policies, and Assumptions	Summary	Objectives and rationale
A.EMISSION	OE.EMISSION	Restates the assumption.
A.ISOLATE	A.ISOLATE	Restates the assumption.
A.MANAGE	OE.MANAGE	Restates the assumption.
A.NOEVIL	OE.NOEVIL	Restates the assumption.
A.PHYSICAL	OE.PHYSICAL	The TOE, is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
A.SCENARIO	OE.SCENARIO	Restates the assumption.

5 Extended Components Definition

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

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

5.1 Class EXT: Extended – Inspection

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

5.1.1 Visual Inspection (EXT_VIR)

Family Behaviour

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

Component leveling

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

Management: EXT_VIR.1

There are no management activities foreseen.

Audit: EXT_VIR.1

There are no auditable events foreseen.

EXT_VIR.1 Visual Indication Rule

Hierarchical to:	No other components
Dependencies:	None

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

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

6 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

All operations performed on the Security Functional Requirements or the Security Assurance Requirements need to be identified. For this purpose the following conventions shall be used.

- Assignments will be written in [normal text with brackets]
- Selections will be written in underlined and italic text.
- Refinements will be written **bold**
- Iterations will be performed on components and functional elements. The component ID defined by the Common Criteria (e.g. FDP_IFC.1) will be extended by an ID for the iteration (e.g. "(RULE 1)"). The resulting component ID would be "FDP_IFC.1 (RULE 1)".

6.2 TOE Security Policies

The following Security Function Policy (SFP) is copied directly from PSS PP.

6.2.1 Data Separation SFP (TSP_DSP)

The TOE shall allow PERIPHERAL DATA and STATE INFORMATION to be transferred only between PERIPHERAL PORT GROUPS with the same ID.

6.3 Security Functional Requirements for the TOE

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

Table 7: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
FDP_ETC.1	Export of user data without security attributes

Functional Component ID	Functional Component Name
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.1	Import of user data without security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
EXT_VIR.1	Visual indication rule

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 and STATE INFORMATION 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: <ul style="list-style-type: none"> ○ [PERIPHERAL PORT GROUPS (SUBJECTS), ○ PERIPHERAL DATA and STATE INFORMATION (OBJECTS), and ○ PERIPHERAL PORT GROUP IDs (ATTRIBUTES)].

- FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[Switching Rule: PERIPHERAL DATA can flow to a PERIPHERAL PORT GROUP with a given ID only if it was received from a PERIPHERAL PORT GROUP with the same ID].
- FDP_IFF.1.3 The TSF shall enforce the [No additional information flow control SFP rules].
- FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [No additional rules].
- FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [No additional rules].

6.3.1.4 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.*

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: [none].

6.3.3 Class EXT: Extended – Inspection

6.3.3.1 EXT_VIR.1 **Visual Indication Rule**

Hierarchical to: No other components

Dependencies: None

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

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

6.4 Security Assurance Requirements for the TOE

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

Table 8: Security Assurance Requirements

Assurance Class	Assurance Components
-----------------	----------------------

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

6.5 Security Requirements for the IT Environment

There are no security functional requirements for the IT Environment.

6.6 Rationale for Security Functional Requirements

The tables below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. These tables contain the original rationale from *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2.

NOTE: The security requirements rationale in the Protection Profile is incomplete; the Protection Profile does not provide a mapping or rationale for the new requirement FMT_SMF.1. The requirement FMT_SMF.1, as written in the PP, provides for no management functions to be performed. With no management functions to be performed and no management objective to contribute to, this requirement has nothing to be mapped to in the rationale of either the Protection Profile or this ST and is included only because it is required by the Protection Profile.

Table 9: Completeness of Security Functional Requirements

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

Table 10: Sufficiency of Security Functional Requirements

Objectives	SFRs	Purpose
O.CONF	FDP_ETC.1	In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. Also included is configuration information such as KEYBOARD settings that must be reestablished each time the TOE switches between COMPUTERS. These DEVICES neither expect nor require any security ATTRIBUTE information. The information content of the data passed through a CONNECTION is ignored.
	FDP_IFC.1	This captures the policy that no information flows between different PERIPHERAL PORT GROUP IDS.
	FDP_IFF.1	This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer. This requirement is a dependency of FDP_IFC.1.
	FDP_ITC.1	In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. These DEVICES neither expect nor require any security ATTRIBUTE information.

Objectives	SFRs	Purpose
O.CONNECT	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	EXT_VIR.1	There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED. Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication.
O.INVOKE	ADV_ARC.1	Addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The Data Separation SFP must be enforced at all times during TOE operation. This requires that the TSP functions always be invoked.
O.NOPROG	ADV_ARC.1	Addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The TSF needs to ensure that it protects itself against changes, which might compromise its security functionality.
O.ROM	ADV_ARC.1	Addresses the non-bypassability and domain separation aspects of the TSF. The architecture will contribute to this objective by ensuring that the TSF can protect itself from users. The TSF needs to ensure that it protects itself against changes, which might compromise its security functionality.
O.SELECT	FMT_MSA.1	This restricts the ability to change selected PERIPHERAL PORT GROUP IDS to the AUTHORIZED USER. This requirement is a dependency of FMT_MSA.3.
	FMT_MSA.3	The TOE assumes a default PERIPHERAL PORT GROUP selection based on a physical switch position or a manufacturer's specified sequence for choosing among the CONNECTED COMPUTERS (CONNECTED here implies powered on). This requirement is a dependency of FDP_IFF.1 and FDP_ITC.1.

Objectives	SFRs	Purpose
O.SWITCH	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.

6.7 Rationale for Security Assurance Requirements

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

6.8 Rationale for Dependencies

6.8.1 Security Functional Requirement Dependencies

The table below is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

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 ²
	FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	No ²
FMT_SMF.1	None	N/A
EXT_VIR.1	None	Yes

6.8.2 Security Assurance Requirement Dependencies

SAR dependencies identified in the CC have been met by this ST as shown in the table below.

Table 12: EAL4 (Augmented with ALC_FLR.2) SAR Dependencies Satisfied

² 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.

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

7 TOE Summary Specification

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

7.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 6.3. Traceability to SFRs is also provided.

7.1.1 Data Separation (TSF_DSP)

FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1

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

Signals processed by the TOE are keyboard data, mouse data, keyboard LED data, Data Display Channel information, digital/ analog video signals, audio data, CAC or SmartCard data and USB status. A CCID Smart Card reader or a CAC reader can be used with the Argon 90731 Switch, but this capability is not included in the evaluated configuration. 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 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.

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.

7.1.2 Security Management (TSF_MGT)

FMT_MSA.1, FMT_MSA.3, EXT_VIR.1

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. Electrical signals for the built in Channel select buttons and corresponding LED indicators (which are inaccessible within the chassis) are routed to an internal connector on the chassis. An external mate to this connector is attached to a 12 foot extension cable to which a remote control box is connected. The remote control box buttons and LED indicators connect to the signal lines from the target and allow channel switching and its corresponding indication.

To select or switch computers, the TOE provides port-specific switches (attached to a 12-foot cable), that allow the human user to explicitly determine to which computer the shared set of peripherals is connected. This connection is visually displayed by an LED near or integrated in the select button for the selected channel. The first computer to be powered on will be the default selected computer until the user selects another. Because the TOE uses electrical (hardware) signals, not software logic, to change signal paths for attached computer peripherals, peripheral port group IDs are not explicit.

8 Glossary

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

8.1 Terms

There are no additional terms in this Security Target.

8.2 Acronyms

Acronym	Definition
A.	assumption (when used in hierarchical naming)
CAC	Common Access Card
CC	Common Criteria
DVI-I	Digital Video Interface - Integrated
EAL	evaluation assurance level
IBM	International Business Machines, Inc.
IT	information technology
LED	Light Emitting Diode
O.	security objective (of the TOE) (when used in hierarchical naming)
OE.	security objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PC	Personal Computer
PP	protection profile
SFP	security function policy
SFR	security functional requirement
ST	security target
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE security policy
USB	Universal Serial Bus
VGA	Video Graphics Array