National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cybex SwitchView SC, Model 520-147-004/Model 520-319-003

Report Number: CCEVS-VR-03-0041
Dated: 31 July 2003
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Margaret T. Webster-Butler
Ronald J. Bottomly
National Security Agency
Ft. Meade, MD 20755

Technical Oversight Panel
Vicky Ashby, MITRE
Jim Brosey, Mitretek

Common Criteria Testing Laboratory

Evaluation Team
Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Table of Contents

1. Executive Summary

The Target of Evaluation (TOE), the Cybex SwitchView SC, Model 520-147-004/Model 520-319-003 was evaluated by Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL) in the United States, beginning on 15 January 2003, and completed on 31 July 2003. The evaluation was for the Evaluation Assurance Level 4 (EAL4). The evaluation was conducted in conformance with the Common Criteria (CC) for Information Technology Security Evaluation, parts 1, 2, 2a, and 3; the Common Evaluation Methodology for Information Technology Security (CEM), parts 1 and 2; and, the Peripheral Sharing Switch for Human Interface Devices Protection Profile, (PSS_PP) v1.0, dated 8 August 2000. The evaluation was conducted in accordance with the rules and regulations of the NIAP Common Criteria Evaluation and Validation Scheme, and the conclusions of CSC in their Evaluation Technical Report (ETR) were consistent with the evidence adduced. CSC concluded that the Common Criteria requirements of EAL4 had been met for the TOE.

The Cybex SwitchView SC Series Switches Security Target (ST) and Section 10 of this report, (Validator's Comments/Recommendations), identifies the specific version and models of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Cybex SwitchView SC product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

1.1. Evaluation Highlights

Dates of Evaluation: 15 January 2003 through 31 July 2003
Evaluated Product: Cybex SwitchView SC, Model 520-147-004/Model 520-319-003
Developer: Avocent/Cybex Corporation, 4991 Corporate Drive, Huntsville, AL 35805
CCTL: CSC, 132 National Business Parkway, Annapolis Junction, MD 20701
Evaluation Class: EAL4
PPs Claimed: Peripheral Sharing Switch for Human Interface Devices Protection Profile, (PSS_PP) v1.0, dated 8 August 2000
Validation Team: Margaret T. Webster-Butler, National Security Agency
Ronald J. Bottomly, National Security Agency

2. Product Identification

ST: Cybex SwitchView SC Series Switches Security Target v1.0, dated 23 June 2003

TOE Identification: Cybex SwitchView SC Series Switches Model 520-147-004 and Model 520-319-003

The TOE is a hardware device, hereinafter referred to as a "Peripheral Sharing Switch" (PSS), or simply "switch," that permits a single set of human interface devices, (i.e., keyboard, video, or mouse), to be shared among two or more computers. The SwitchView SC series of switches' architecture is designed to keep users' private data completely separate and secure at all times when accessing secure and unsecure networks. Firmware, to control proper signals for each peripheral port, is burned onto a microprocessor chip inside the TOE hardware. There is no software to install or boards to configure. No portion of the product was excluded from the TOE boundary.

The SwitchView SC series of switches work with IBM PC/AT and PS/2 systems with support for VGA and SVGA video. PS/2 keyboard and PS/2 mouse peripherals are supported through the rear of the unit. With the SwitchView SC, Model 520-147-004, the user can cycle through the available computer channels via the Select button on the front panel. With the SwitchView SC, Model 520-319-003, there is a Select button associated with each specific port.

3. Security Policy

The TOE provides the following security functions:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT)

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 a *select* switch, or switches in the case of the SwitchView SC Plus, that allow(s) 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.

The PSS_PP identifies no organization security policies (OSPs) to which the TOE must comply.

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

The specific conditions listed in "Secure Usage Assumptions," Section 3.1, of the PSS_PP are assumed to exist for the TOE. These conditions are:

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.

4.2 Clarification of Scope

None.

4.3 Interpretations

The CSC evaluation team performed an analysis of the international and national interpretations and identified those that were applicable and had an impact on the TOE evaluation. Those interpretations were applied when the CEM work units were started.

The following sections provide the number and title of the applicable interpretations and the CEM class in which they were considered.

Applicable National Interpretations

None.

Applicable International Interpretations

116 Indistinguishable work units for ADO_DEL

4.4 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. Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards).

4.4.1 Threats Addressed by the TOE

"Threats to Security," Section 3.2, of the PSS_PP identifies threats to the assets against which specific protection within the TOE is required. The threats are:

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.

4.4.2 Threats Addressed by the TOE Environment

The PSS_PP identifies no threats to the assets against which specific protection within the TOE environment is required.

5. Architectural Information

The TOE is a hardware device, hereinafter referred to as a "Peripheral Sharing Switch" (PSS), or simply "switch," that permits a single set of human interface devices, (i.e., keyboard, video, or mouse), to be shared among two or more computers. The SwitchView SC series of switches' architecture is designed to keep users' private data completely separate and secure at all times when accessing secure and unsecure networks. Firmware, to control proper signals for each peripheral port, is burned onto a microprocessor chip inside the TOE hardware. There is no software to install or boards to configure. No portion of the product was excluded from the TOE boundary.

The SwitchView SC series of switches work with IBM PC/AT and PS/2 systems with support for VGA and SVGA video. PS/2 keyboard and PS/2 mouse peripherals are supported through the rear of the unit. With the SwitchView SC, Model 520-147-004, the user can cycle through the available computer channels vial the *Select* button on the front panel. With the SwitchView SC, Model 520-319-003, there is an additional *Select* button associated with each specific port.

5.1 Physical Boundaries

The following components comprise the TOE: the Cybex SwitchView SC, Model 520-147-004 or the Cybex SwitchView SC Plus, Model 520-319-003. For each of these, the TOE is the entire product as identified by the model number; no part of the product was excluded from the evaluation. The evaluated TOE configuration does not include any peripherals or computer components, including the cables or their associated connectors, attached to the TOE.

5.2 Logical Boundaries

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

The TOE provides the following security functions:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT).

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 a *select* switch, or switches in the case of the SwitchView SC Plus, that allow(s) 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.

6. Delivered Product

The delivered product consisted of the following items:

1. A packing list on the outside of the sealed box
2. Within the sealed box, the TOE resided inside its own box, surrounded by a form fitting plastic case
3. Either the SwitchView SC or SwitchView SC Plus Installer/User Guide, depending on which model was purchased.
4. SwitchView SC Plus Quick Installer/User Guide with the SwitchView SC Plus purchase.

For a longer list of the major pieces of evidence examined during the evaluation, see section 14 of this report.

7. IT Product Testing

7.1 Examination of Vendor Tests

Avocent, the vendor, provided test plans, procedures, test results and a test coverage document for the testing of each Security Functional Requirements (SFR) within each of the TOE Security Functions (TSF_MGT and TSF_DSP). The evaluation team examined the test coverage analysis and found that Avocent provided a correspondence between the tests provided for evaluation and the functional specification.

At Avocent's laboratory, the evaluation team reproduced the entire Avocent test suite. The evaluation team used the same test equipment that Avocent used, in particular 2 keyscopes – one

monitored the keyboard input to the TOE, the other monitored the output of the TOE. (The KeyScope is a test instrument that monitors signals on the interface used to connect keyboards and mice to personal computers, commonly called a PS/2 interface. It provides connections for the keyboard or mouse, for a computer and for a serial device, such as a CRT terminal or computer with terminal emulation software. KeyScope monitors data on a PS/2 interface and generates a serial data stream displaying the data in ASCII coded hexadecimal format. It identifies the direction of data transmission and shows line errors using plain text messages. It allows the operator to observe communications between a keyboard or mouse and a computer.) The evaluation team found this sufficient to verify the basic functionality of the TOE and the proper execution of its security functions.

The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TOE Security Functions was appropriate for this EAL4 evaluation.

7.2 Evaluation Team Independent Tests

The evaluation team performed all Avocent tests. In every case, the evaluation team concluded that the expected results matched the team's actual results. The evaluation team did not devise any additional independent test cases since it was determined that Avocent had performed every conceivable test already.

7.3 Strength of Function

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim. The overall SOF claim for the TOE made in this ST was expressed as a medium SOF rating.

The evaluation team determined that the most viable attack to the TOE would be by disassembly of the TOE, which would require extensive knowledge of the hardware of the TOE. The replacement of the chip containing the firmware would be the easiest to carry out and would require minimal physical access to the TOE since programming of the chip could take place anywhere. The expertise required and the knowledge of the TOE would be considerable. In addition the equipment to program a chip is considered specialized. The results of this

computation provide a value of 20 that equates to an SOF rating of medium (using the SOF attributes as outlined in the CEM). The evaluation team supported the rating of SOF-medium.

7.4 Vulnerability Analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate any TOE Security Policies.

The evaluation team determined that direct access to the TOE security functions is not possible without disassembling the TOE. Thus, penetration is not possible via the product control, i.e., user/administrator interfaces. The only access to the TOE security functions is through the keyboard and mouse ports. These ports do not carry security parameters and have a well-defined and documented protocol. The TOE validates all keyboard/mouse signals as valid prior to accepting that data, thus, there is no possibility of introducing a processing error through bad data inputs. The TOE does not run an operating system and has very little shared memory buffers to launch an attack through. Since the firmware is burned in and executed directly from the ROM, the likelihood of a data driven attack from the keyboard or mouse is low (?) .

The video switch does not pass any information through the microprocessors; thus it is not possible to manipulate the TSP through the video connections.

No configuration items are provided for the security functionality of the TOE; thus it cannot be configured in an insecure state. The security functionality is inherent in the design and internal functioning of the TOE.

Modification of the TOE would require disassembly and modification to the hardware or firmware of the TOE, which requires extensive knowledge and expense on the part of an attacker. Precautions and processes for the protection of the TOE are made during production when the TOE is at its most vulnerable point. Any postproduction modifications would be externally visible by the disturbance of the tamper resistant tape applied during production.

Even given the unlikely possibility that a TOE was opened and an attempt was made to extract the firmware, the microprocessor is programmed in such a way that an encryption key is needed to extract the firmware. Thus, extracting the firmware, reverse engineering it and re-installing a modified version of it, is well beyond the attack potential of EAL4.

Based upon analysis performed by the developer and the evaluation team, and supported by the evaluation team testing, it was concluded that penetration of the TOE was unlikely and that the TOE met the criteria for EAL4.

8. Evaluated Configuration

The environment configuration used to test both models of the TOE was:

1. The KeyScope computer, an Intel®-based PC running Windows 2000 with the Hyperterminal terminal emulation software installed.
2. Attached Computers - For any given test, because operation of the TOE is independent of the operating system used, the type of attached computer is irrelevant as long as the following are true:

Interface	**Interface Specifications that must be met**
Keyboard	Keyboard Meets the requirements of keyboard specifications in IBM Technical Reference S84F-9809-00.
Mouse	Meets the requirements of mouse specifications in IBM document S68X-2229-00.
Video	Meets the requirements of specifications for Display Connector Signals on page 105 of the Video Subsystem section of IBM Document S84F-9809-00.

For this particular test effort, the attached computers were Intel®-based PCs. Each computer was loaded with Windows NT 4.0. Unique text documents were stored on each computer to allow each computer to be readily identified by the video it displayed. The documents contained the text "Computer A" through "Computer H", corresponding to the eight computers used during testing. The text documents were also used to capture and display keyboard input and to verify mouse operation.

9. Results of the Evaluation

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures (CCEVS_PUB 3). The validation team observed that the evaluation and all of its activities were in accordance with the CC, the CEM and CCEVS. The validation team therefore, concludes that the evaluation and its results of **pass** are complete.

9.1 Assurance Content

The evaluation provides for Assurance at the EAL 4 level without augmentation. The assurance components are shown in the table below:

EAL4 Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_AUT.1 Partial CM Automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and Operation (ADO)	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools

Tests (ATE)	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability assessment (AVA)	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

10.Validator Comments/Recommendations

Throughout this evaluation, both switch boxes have been referred to by their manufacturing model number, which is printed on the underside of each one. In maintaining Avocent's configuration management standards, policies and procedures, manufacturing changes would result in a new manufacturing model number and part number for that switch box. Only the model and part numbers listed below are the evaluated EAL 4 configuration:

4-port switch box corresponds with: Model 520-147-004 and Part Number 10040-SC
8-port switch box corresponds with: Model 520-319-003 and Part Number 10080SC-AM

As with any evaluation, this evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The product has been evaluated at the assurance level of EAL 4 and it has been determined that it meets its functional claims.

The validation team observed that the evaluation and all of its activities were in accordance with the CC the CEM, and CCEVS practices; and that the CCTL presented appropriate CEM work units and rationale. The validation team therefore concludes that the evaluation, and its results of **pass,** are complete and correct.

11. Annexes

None, the remainder of this page is blank.

12. Security Target

The Security Target is provided separately.

ST: Cybex SwitchView SC Series Switches Security Target v1.0, dated 23 June 2003

13. List Of Acronymns And Glossary Of Terms

The following acronyms are provided for reference:

ACM	Assurance Configuration Management
ADO	Assurance Delivery and Operation
AGD	Assurance Guidance Documents
ADV	Assurance Development
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
EAL	Evaluation Assurance Level
NIST	National Institute of Standards and Technology
SF	Security Functions
SFR	Security Functional Requirements
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	TOE Security Policy

The following terms are provided for reference:

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (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.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

14. Documentation

The evidence used in this evaluation is based upon the product and the following documentation:

[AVO_ADO]	Delivery for the SwitchView SC, Document ADO_DEL.2, Revision 2, 20 September 2002
[AVO_AGD]	SwitchView SC Installer/User Guide
[AVO_AGDSC]	SwitchView SC Plus Installer/User Guide
[AVO_BOM2]	SwitchView SC Manufacturer Bill of Materials (BOM)
[AVO_CMP]	SwitchView SC Configuration Management Plan
[AVO_COM]	KEIL Software, C51 Compiler, Optimizing 8051 C Compiler and Library Reference, User's Guide 04.95
[AVO_DVS]	SwitchView SC Development Security (DVS)
[AVO_EMP20]	EMP-20 Programmer User's Manual v.2.0
[AVO_FS]	SwitchView SC Facility Security
[AVO_FTP]	Functional Test Plan for SwitchView SC v 1.0
[AVO_KEIL]	KEIL Software, 8051 Utilities BL51 Code Banking Linker/Locator, LIB51 Library Manager, OC51 Banked Object File Converter, OH51 Object Hex Converter, User's Guide 04.95
[AVO_LCD]	Global Product Development Procedure
[AVO_MBR]	Manufacturer BOM Report
[AVO_MPS]	Avocent document Mouse Data Packet Structures version 1.1
[AVO_PCADU]	P-CAD 2002, PCB Design
[AVO_QIG]	SwitchView SC Plus Quick Installer/User Guide
[AVO_RVN]	Avocent Raven Interprocessor Communications Document
[AVO_SDD]	SwitchView SC and SwitchView SC Plus Design Document
[AVO_ST]	SwitchView SC Series Switches, Security Target, Version: 1.0
[AVO_TC]	Test Cases for Cybex SwitchView SC Series Switches under Common Criteria, v 0.4
[AVO_TCD]	SwitchView SC Series Switches Test Coverage and Depth Analysis, Version 1.0
[AVO_VA]	Vulnerability Assessment Evidence for Cybex SwitchView SC Series Switches, EAL4 Evaluation Effort Version 0.1
[CSC_SV]	CSC, Avocent Site Visit, Cybex SwitchView SC Series Switches, dated May 21, 2003
[IBM_MTR]	IBM document S68X-2229-00 PS/2 Mouse Technical Reference
[IBM_TCI]	IBM document S84F-9809-00 PS/2 Tech Ref-Common Interface
[PP]	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0 8 August 2000
[PSS_PP]	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 1.0 8 August 2000

The evaluation and validation methodology was drawn from the following:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.
[CC_PART2A]	Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.
[CEM_PART1]	Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.
[CEM_PART2]	Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.
[CCEVS_PUB 1]	Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.
[CCEVS_PUB 2]	Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000
[CCEVS_PUB 3]	Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, January 2002.
[CCEVS_PUB 4]	Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001
[CCEVS_PUB 5]	Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.