National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cybex SwitchView SC Series Switches for Models with [EXP_TMP]

Report Number: CCEVS-VR-VID10309-2008

Dated: 30 January 2008

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

Ken Elliott
The Aerospace Corporation
Columbia, MD

Shaun Gilmore
NSA

Common Criteria Testing Laboratory

Computer Sciences Corporation
7231 Parkway Drive
Hanover, Maryland 21076

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Cybex SwitchView SC Series Switches for Models with [EXP_TMP], Cybex SwitchView SC120 Models 520-563-501, 520-563-502; Cybex SwitchView SC220 Model 520-564-501, 520-564-502; Cybex SwitchView SC140 Models 520-565-501, 520-565-502; Cybex SwitchView SC240 Models 520-566-501, 520-566-502; Cybex SwitchView SC180 Model 520-679-501; Cybex SwitchView SC280 Model 520-680-501, the target of evaluation (TOE), performed by Computer Sciences Corporation the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on January 02, 2008. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Avocent Corporation. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, dated August 2005 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices, keyboard, video, mouse, Common Access Card (CAC) reader, to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

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

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

Table 1: Models and Features

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

The evaluated TOE configuration does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before January 21, 2007.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 2: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	SwitchView SC 120 Model 520-563-501 SwitchView SC 120 Model 520-563-502 SwitchView SC220 Model 520-564-501 SwitchView SC220 Model 520-564-502 SwitchView SC140 Model 520-565-501 SwitchView SC140 Model 520-565-502 SwitchView SC240 Model 520-566-501 SwitchView SC240 Model 520-566-502 SwitchView SC180 Model 520-679-501 SwitchView SC280 Model 520-680-501
Protection Profile	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000
Security Target	*Cybex SwitchView SC Series Switches for Models with [EXP_TMP]Security Target* Version 2.01, October 26, 2007
Dates of evaluation	January 2007 through January 2008
Evaluation Technical Report	*Evaluation Technical Report for Cybex SwitchView SC Series Switches for Models with [EXP_TMP]*, Version 1.0, January 28, 2008
Conformance Result	Part 2 extended and Part 3 EAL 4 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005
Sponsor	Avocent Corporation
Developer	Avocent Corporation
Evaluators	Halvar Forsberg, Gregory Bluher, and Christa Lanzisera of Computer Sciences Corporation
Validation Team	Ken Elliott of The Aerospace Corporation and Shaun Gilmore of CCEVS

3. SECURITY POLICY

The TOE enforces the following security policies:

3.1. Data Separation Policy

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, dated August 8, 2000.

Signals processed by the TOE are keyboard data, mouse data, keyboard LED data, Data Display Channel information, analog video signals and USB status. Specific versions of the TOE accommodate subsets of the listed signals to support popular types of computers. In all cases, the TOE ensures data separation for all signal paths using both hardware and firmware.

The basic arrangement of the microprocessors used for keyboard and mouse data ensures data separation in hardware by physical separation of the microprocessors connected to the user's peripheral devices from the microprocessors connected to the attached computers. In operation, the main processor moves data received from the shared keyboard and mouse to the microprocessor corresponding to the selected computer. The processor dedicated to the selected computer sends data to the computer. Separation is ensured in hardware by use of separate microprocessors for each of the computers and for the shared user peripheral devices.

Separation in firmware is ensured by firmware design consisting of fixed polling loops, dedicated functions and static memory assignment with no third-party library functions or multitasking executives. This basic design results in a straightforward implementation suitable for independent verification to provide assurance of data separation.

In operation the TOE is not concerned with the content of user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer supporting the Data Separation Security Functional Policy – "the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID." The TOE interfaces ensure that confidentiality of information is not violated by isolating signals electrically and through firmware modules that ensure that information is passed only between the user peripherals and the selected computer.

Keyboard LED status for each computer is stored by the processor associated with each computer. The TOE does not have software to install, or boards to configure. The logic contained within the TOE is protected from unauthorized modification through the use of discrete components.

Any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide" switch. If one of these models has been physically tampered with in this manner, the lights on the front of the TOE will flash in a unique pattern to alert an administrator to the interference, and all TOE functions will be permanently disabled.

3.2. Security Management Policy

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides select switches, that allow the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel.

4. ASSUMPTIONS

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located within a facility providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE.

4.2. Personnel Security Assumptions

It is assumed that an authorized user possesses the necessary privileges to access the information transferred by the TOE – users are authorized users. It is also assumed that the TOE is installed and managed in accordance with the manufacturer’s directions. It is assumed that the authorized user is non-hostile and follows all usage guidance.

4.3. Operational Security Assumptions

It is assumed that 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]. It is also assumed that only the selected computer’s video channel will be visible on the shared monitor. It is assumed that vulnerabilities associated with the attached devices (shared peripherals or switched computers), or their connection to the TOE, are a concern of the application scenario an not of the TOE.

4.4. Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

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.

4.5. Organizational Security Policies

The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, dated August 8, 2000, identifies no organization security policies (OSPs) to which the TOE must comply.

5. ARCHITECTURAL INFORMATION

5.1. Logical Scope and Boundary

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

The TOE provides the following security features:

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

5.2. Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, dated August 8, 2000. 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).

5.3. Data Separation (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides select switches, that allow the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel.

5.4. Physical Scope and Boundary

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

The evaluated TOE configuration does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. The following figure depicts the TOE and its environment.

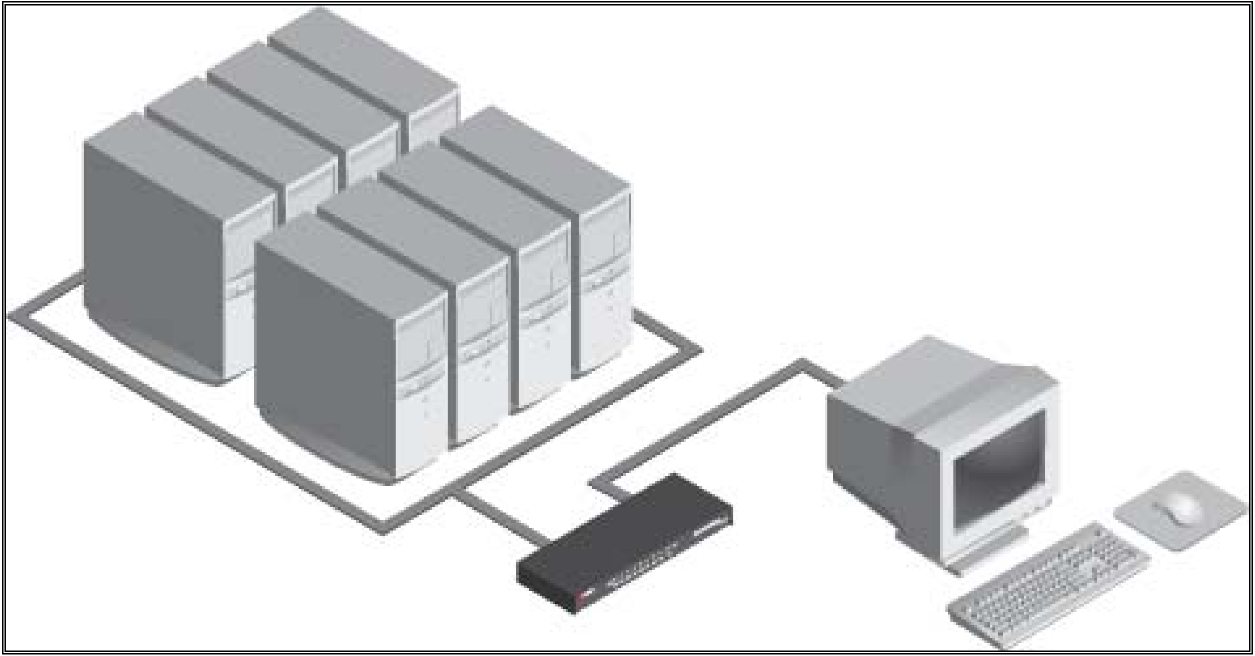


Figure 1: Depiction of TOE Deployment

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Cybex SwitchView SC Series Switches for Models with [EXP_TMP]. Note that not all evidence is available to customers. The following documentation is available to the customer:

- Quick Installation Guide, SwitchView SC Switch for models: 120/140/220/240 (590718501A.pdf)
- Quick Installation Guide, SwitchView SC Switch for models: 180/280 Draft (SwitchView SC180-280 Draft.pdf)

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

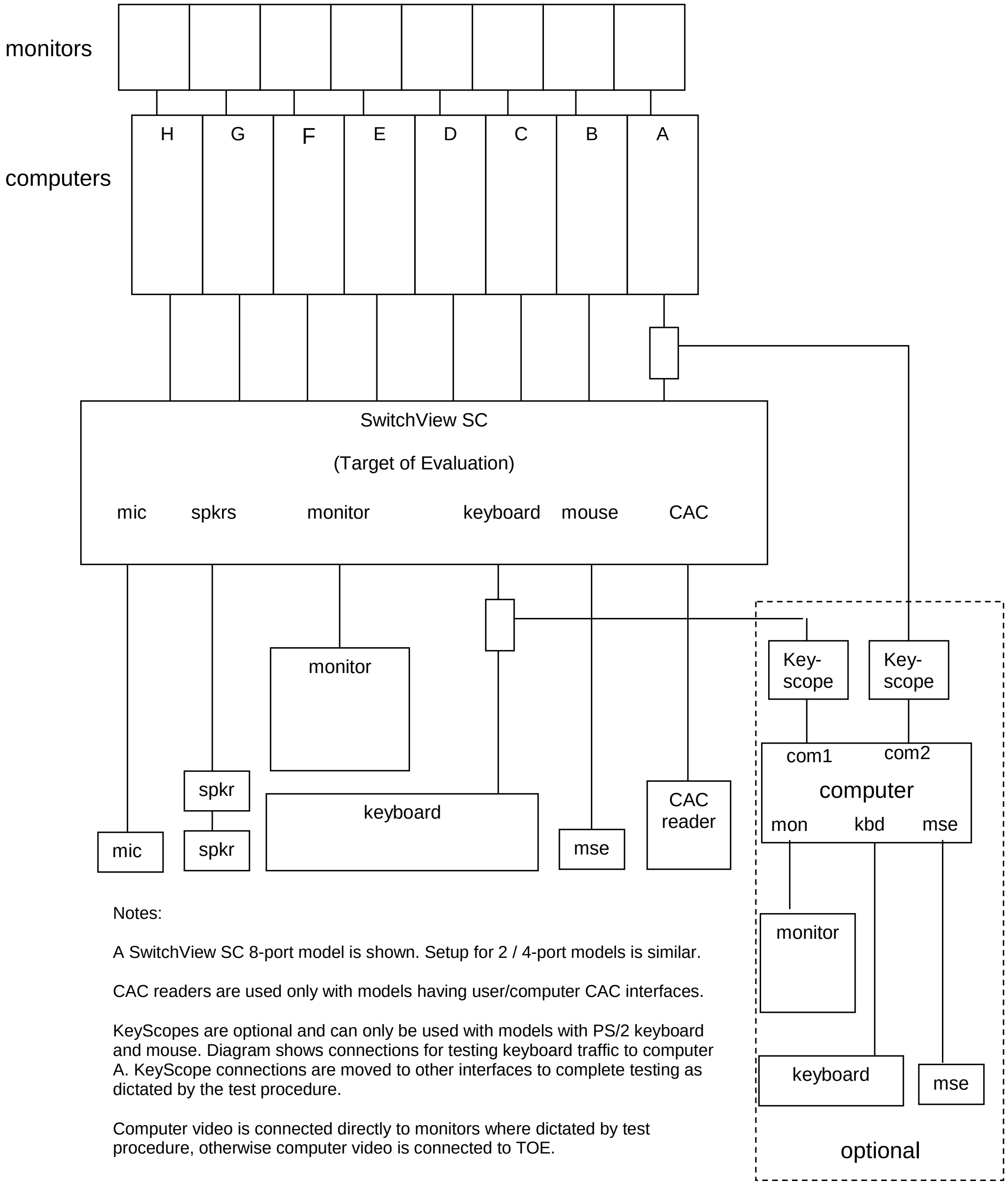
This section describes the testing efforts of the Developer and the evaluation team.

7.1. Developer testing

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included with each of the tests in the TOE Test Procedures. Each test case was assigned an identifier that was used to reference it throughout the testing evidence.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 4. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagram depicts the test environment that was used by the Developers. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored a portion of this test configuration during Independent testing.



Notes:

A SwitchView SC 8-port model is shown. Setup for 2 / 4-port models is similar.

CAC readers are used only with models having user/computer CAC interfaces.

KeyScopes are optional and can only be used with models with PS/2 keyboard and mouse. Diagram shows connections for testing keyboard traffic to computer A. KeyScope connections are moved to other interfaces to complete testing as dictated by the test procedure.

Computer video is connected directly to monitors where dictated by test procedure, otherwise computer video is connected to TOE.

7.2. Evaluation team independent testing

The evaluation team conducted independent testing both at the CCTL and the Developer's facilities. For the testing at the CCTL, the TOE was delivered by common carrier, UPS, and a signature receipt was required. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target. The evaluation team then tested the tamper detection security functionality.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated a portion of the Sponsor's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

The evaluators examined the ADV evidence listed in Section 1.2 above as well as a subset of the implementation representation and selected to run the developer's tests only for the following specific 8 models:

- 520-564-502 was selected to represent the 2-port switches SC120 and SC220 because it is functionally and electronically identical to the previous SC220 model 520-564-501 and differs from the two SC120 models 520-563-501 and 520-563-502 only by having the additional CAC functionality. The 520-564-502 firmware is identical to the firmware in the rest of SC120 and SC220 switches.
- 520-566-502 was selected to represent the 4-port switches SC140 and SC240 because it is functionally and electronically identical to the previous SC240 model 520-566-501 and differs from the two SC140 models 520-565-501 and 520-565-502 only by having the additional CAC functionality. The 520-566-502 firmware is identical to the firmware in the rest of SC140 and SC240 switches.
- 520-680-501 was selected to represent the 8-port switches SC180 and SC280 because it differs from the SC180 model 520-679-501 only by having the additional CAC functionality. The 520-680-501 firmware is identical to the firmware in 520-679-501.

The evaluators chose to run all of the developer's tests for the eight models selected above with the following exceptions:

- The CAC Reader functionality is identical for SC220, SC240, and SC280 since they have identical firmware and the hardware architecture differs only in number of ports it supports, the evaluators ran the Separation of CAC Reader Input Data tests only for the 2 port model SC220 (520-564-502).

- Developers tested User Data Protection for SC220, SC240, and SC280 by running each test twice using PS/2 output cables (with KeyScopes when testing with PS/2 user keyboard) first and USB output cables second. Since SC220, SC240, and SC280 have identical firmware and the hardware architecture differs only in number of ports it supports, the evaluators ran the User Data Protection tests for SC220 (520-564-502) with each set of cables, but ran the corresponding tests for SC240 (520-566-502) and SC280 (520-680-501) with PS/2 output cables (using KeyScopes when testing with PS/2 user keyboard) only.

Each TOE Security Function was exercised at least once, and the evaluation team verified each test passed.

7.3. Vulnerability analysis

The evaluation team gained assurance that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, and the evaluation team's Vulnerability Analysis.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerability in the product and to show that it is not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis and an in depth analysis (to the code level) of the TOE design evidence, the evaluation team came to the conclusion that obvious penetration attempts are not possible through the TOE external interfaces. As indicated in the design documentation, direct access to the TOE security functions is not possible without disassembly of the TOE, thus penetration is not possible via the product control, i.e., user/administrator interfaces. Additionally, 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.

8. EVALUATED CONFIGURATION

The evaluated configuration of the Cybex SwitchView SC Series Switches for Models with [EXP_TMP], as defined in the Security Target, consists of one of the evaluated models. Please see the Security Target for the TOE model numbers.

The Cybex SwitchView SC Series Switches for Models with [EXP_TMP] must be configured in accordance with the following Guidance Documents:

- Quick Installation Guide, SwitchView SC Switch for models: 120/140/220/240 (590718501A.pdf)
- Quick Installation Guide, SwitchView SC Switch for models: 180/280 (SwitchView SC180-280.pdf)

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Computer Sciences Corporation has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 augmented with ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on December 20, 2007. A final Validation Oversight Review (VOR) was held on January 24th, 2008 and final changes to the VR were completed on January 30, 2008.

10. VALIDATOR COMMENTS

The evaluation team performed a very thorough analysis job, including tracing schematics and analyzing the firmware included in the product.

11. ANNEXES

None

12. SECURITY TARGET

Cybex SwitchView SC Series Switches for Models with [EXP_TMP], Version 2.01, 26 October 2007.

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the Cybex SwitchView SC Series Switches for Models with [EXP_TMP].
- **Attack:** An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Authentication:** Verification of the identity of a user.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.3, August 2005. CCMB-2005-08-001.

2.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.3, August 2005. CCMB-2005-08-002.

3.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.3, August 2005. CCMB-2005-08-003.

4.) Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005 CCMB-2005-08-004.

5.) Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

6.) Avocent Corporation/Computer Sciences Corporation. *Cybex SwitchView SC Series Switches for Models with [EXP_TMP] Security Target* Version 2.01, October 26, 2007

7.) Computer Sciences Corporation. *Evaluation Technical Report Cybex SwitchView SC Series Switches for Models with [EXP_TMP],* Version 1.0, January 28, 2008.