National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Avocent SwitchView SC Series Switches SC420, SC440, and SC540

Report Number: CCEVS-VR-VID10327-2009
Dated: 21 April 2009
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

Mike Allen (Lead Validator)
Jandria Alexander (Senior Validator)
Ken Elliott (TVOR TOP Chair)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Computer Sciences Corporation (CSC)
7231 Parkway Drive
Hanover, Maryland 21076

Table of Contents

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 and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Avocent SwitchView SC Series Switches: Cybex SwitchView SC420 Model 520-753-502, Cybex SwitchView SC440 Model 520-721-502, and Cybex SwitchView SC540 Model 520-728-502. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of Avocent SwitchView SC Series Switches was performed by Computer Sciences Corporation, the Common Criteria Testing Laboratory, in Hanover, Maryland USA and was completed on 2 March 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Avocent Corporation. The ETR and test report used in developing this validation report were written by CSC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1, dated September 2007 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, dated September 2007. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Avocent SwitchView SC Series Switches Security Target. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 with ALC_FLR.2. The product is conformant to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, version 1.2, dated August 21, 2008. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

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: USB keyboard, DVI-I video, USB mouse, audio (input and output), and Common Access Card (CAC) or SmartCard 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' architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

The SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for USB keyboard, USB mouse, DVI-I video, audio (input and output), and USB Common Access Card (CAC) or SmartCard reader. Each switch has a "select" button associated with each specific port.

The physical boundary of the TOE consists of one SwitchView switch (see Table 1: 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 SC420	520-753-502	2	USB keyboard, USB mouse, USB Smart Card reader, proprietary USB HID target channel selector (not currently in production), audio (speaker and microphone), DVI-I video monitor interfaces.
SwitchView SC440	520-721-502	4	USB keyboard, USB mouse, USB Smart Card reader, proprietary USB HID target channel selector (not currently in production), audio (speaker and microphone), DVI-I video monitor interfaces.
SwitchView SC540	520-728-502	4	USB keyboard, USB mouse, USB Smart Card reader, proprietary USB HID target channel selector (not currently in production), audio (speaker and microphone), dual-head DVI-I video monitor interfaces.

The evaluated TOE configuration does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. The evaluated TOE configuration **EXCLUDES** the usage of a proprietary USB target selection/indication device which was under development by Avocent at one time if such device becomes available for purchase at some time in the future.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence reviewed.

During this evaluation, the Validators monitored the activities of the CSC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security

Target (ST). Therefore, the Validators conclude that the CSC findings are accurate, the conclusions justified, and the conformance claims correct.

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 information technology (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;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals 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 SC420 Model 520-753-502; SwitchView SC440 Model 520-721-502; SwitchView SC540 Model 520-728-502
Protection Profile	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, version 1.2*, dated August 21, 2008
Security Target	*Cybex SwitchView SC Series Switches Security Target, Version 3.0* March 2, 2009
Dates of evaluation	October 2008 through March 2009
Evaluation Technical Report	*Avocent SwitchView SC Series: SC420, SC440, SC540,* Version 1.0, March 2, 2009
Conformance Result	Part 2 extended and Part 3 conformant, EAL 4 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, September 2007 and all applicable NIAP and International Interpretations effective on October 30, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on October 30, 2008
Sponsor	Avocent Corporation, 4991 Corporate Drive, Huntsville, Alabama 35805
Developer	Avocent Corporation, 4991 Corporate Drive, Huntsville, Alabama 35805
Common Criteria Testing Lab	Computer Sciences Corporation (CSC), Hanover, MD
Evaluators	Gregory Bluher and Christa Lanzisera of CSC
Validation Team	Ken Elliott, Jandria Alexander and Mike Allen of The Aerospace Corporation

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 1.2, dated August 21, 2008.

Signals processed by the TOE are keyboard data, mouse data, keyboard LED data, Data Display Channel information, analog video signals, Common Access Card (CAC) or SmartCard reader data, audio data 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 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 the firmware design consisting of 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.

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.

3.3 Anti-tamper Policy

Any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide"switch (TSF_TMP). If one of these models has been physically tampered with in this manner, the lights on the front of the TOE will all flash in unison to alert an administrator to the interference, and all TOE functions will be permanently disabled. At this point the TOE must be returned to the manufacture for replacement.

4 Assumptions and Clarification of Scope

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 A 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 and not of the TOE.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- The attached peripheral devices (keyboard, video display, etc.) have memory which may contain persistent data when switched between attached computers. The TOE ST makes no Claim to clear this data. Risks associated with this persistent data are considered beyond the scope of the TOE and are the responsibility of the user.

- The authentication associated with a CAC device is broken upon switching to another computer and the user will need to re-authenticate with each switch operation.

- At some point in the future, Avocent may make available a USB selection capability that provides selection of the target computer via the USB interface. If this becomes possible, the user must understand that this capability was not part of the evaluated configuration and use of the USB selector will invalidate the evaluation.

- When power is applied to the switch, if all the amber lights are found flashing, the tamper switch has been tripped and the device will no longer operate and must be replaced.

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),
- Security Management (TSF_MGT), and
- Tamper Detection (TSF_TMP).

5.1.1 Data Separation (TSF_DSP)

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

5.1.2 Security Management (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides 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.

5.1.3 Tamper Detection (TSF_TMP)

A switch inside the unit is activated when a screw used to fasten the top cover of the unit is removed. The tamper switch is powered by the main power supply or a dedicated battery so that it can always detect intrusions. After the switch is activated, TOE operation is disabled and the amber and green indicators on the front panel of the unit flash in unison. When the amber and green indicators are flashing in unison, operation of the TOE cannot be restored; the TOE must be replaced.

5.2 Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one SwitchView switch (see Table 1), 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.

The evaluated TOE configuration does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. The evaluated TOE configuration excludes the usage of a proprietary USB target selection / indication device if such device becomes available for purchase. The following figure depicts the TOE and its environment.

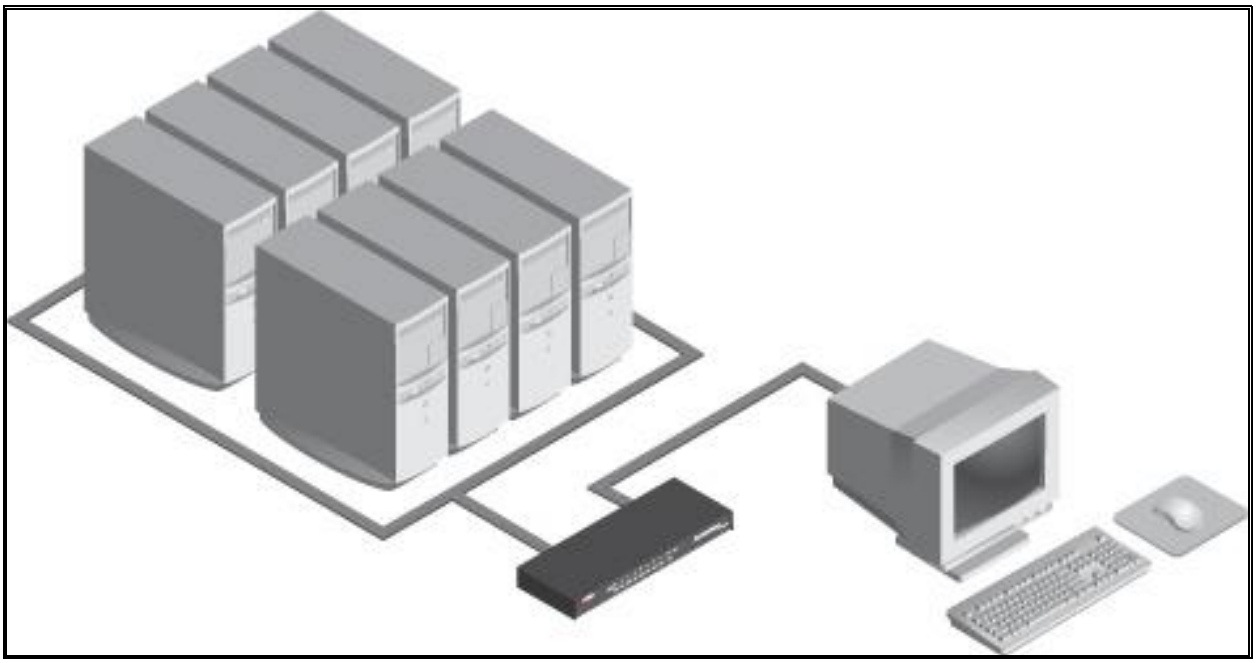


Figure 1: Depiction of TOE Deployment

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 Avocent SwitchView SC Series Switches SC420, SC440, and SC540. Note that not all evidence is available to customers. The following documentation is available to the customer:

- Quick Installation Guide, SwitchView SC420/440 (590822501C (SC420 and SC440 Guidance).pdf)
- Quick Installation Guide, SwitchView SC540 (590823501B (SC540 Guidance).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

Test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

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.

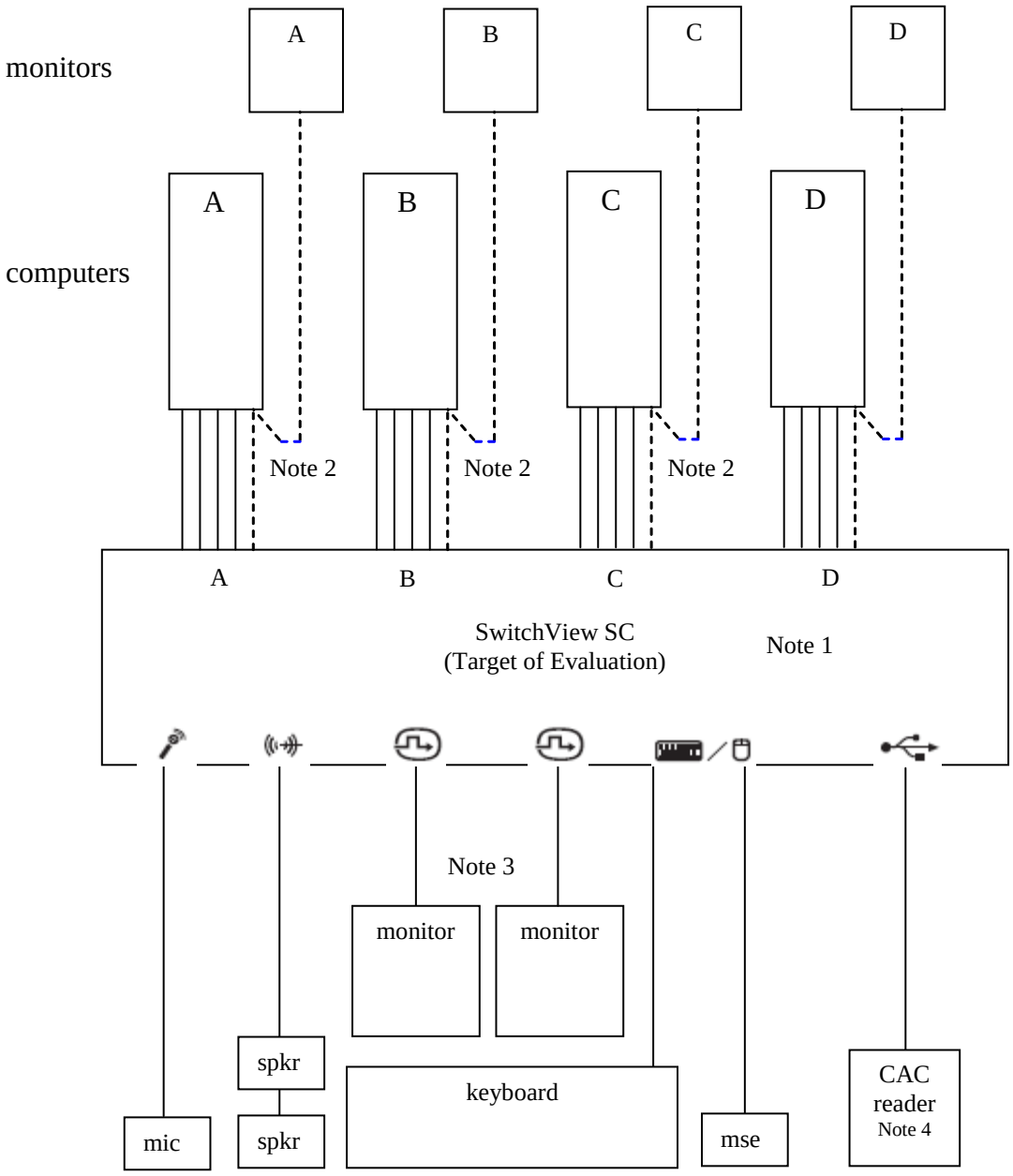
7.2 Evaluation Team Independent Testing

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, FedEx, 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. 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



Note:
1. Four-port model is illustrated. Omit ports C and D for two-port model.
2. Connect computer video directly to monitors where dictated by test procedure – Smart Card Reader tests, otherwise connect computer video to TOE. It is also acceptable to use a single monitor, moving it from computer to computer during the test.
3. Dual-head DVI video model is illustrated. Omit one monitor for single-video models.
4. CAC reader also refers to Smart Card Reader.

- 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 all 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 of the ST as well as a subset of the implementation representation and selected to run the developer's tests for all three models under evaluation. Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

7.3 Vulnerability Testing

The evaluation team gained assurance that the TOE does not contain exploitable flaws or weaknesses in the TOE based 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 search of the public vulnerability sites to determine the thoroughness of the analysis.

Based on the results of the team'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 Avocent SwitchView SC Series Switches SC420 Model 520-753-502, SC440 Model 520-721-502, and SC540 Model 520-728-502, as defined in the Security Target, consists of one of the evaluated models. The Avocent SwitchView SC Series Switches SC420, SC440, and SC540 must be configured in accordance with the following Guidance Documents:

- Quick Installation Guide, SwitchView SC420/440 (590822501C (SC420 and SC440 Guidance).pdf)
- Quick Installation Guide, SwitchView SC540 (590823501B (SC540 Guidance).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 3.1R2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R2.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Avocent SwitchView SC Series Switches SC420 Model 520-753-502, SC440 Model 520-721-502, and SC540 Model 520-728-502 meet the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

- The attached peripheral devices (keyboard, video display, etc.) have memory which may contain persistent data when switched between attached computers. The TOE ST makes no Claim to clear this data. Risks associated with this persistent data are considered beyond the scope of the TOE and are the responsibility of the user.

- The authentication associated with a CAC device is broken upon switching to another computer and the user will need to re-authenticate with each switch operation.

- At some point in the future, Avocent may make available a USB selection capability that provides selection of the target computer via the USB interface. If this becomes possible, the user must understand that this capability was not part of the evaluated configuration and use of the USB selector will invalidate the evaluation.

- When power is applied to the switch, if all the amber lights are found flashing, the tamper switch has been tripped and the device will no longer operate and must be replaced.

11 Security Target

The Security Target is identified as Cybex SwitchView SC Series Switches Security Target, Version 3.0, March 2, 2009. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirement(s)
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control

- **Administrator:** Role applied to user with full access to all aspects of the Cybex SwitchView SC Series Switches.
- **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.
- **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.
- **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.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, revision 1.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, revision 2.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, revision 2.

4.) Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, revision 2.

5.) Avocent Corporation/Computer Sciences Corporation. *Cybex SwitchView SC Series Switches Security Target, Version 3.0,* March 2, 2009.

6.) Computer Sciences Corporation (CSC). *Evaluation Technical Report Avocent SwitchView SC Series: SC420, SC440, and SC540,* Version 1.0, March 2, 2009.

7.) Quick Installation Guide, SwitchView SC420/440 (590822501C (SC420 and SC440 Guidance).pdf)

8.) Quick Installation Guide, SwitchView SC540 (590823501B (SC540 Guidance).pdf)

9.) NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001