

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

SecureSwitch® Fiber Optic A/B/C Switch Revision A

Report Number: CCEVS-VR-05-0088

Dated: January 14, 2005

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

Timothy J. Bergendahl
The MITRE Corporation
Bedford, MA 01730

Common Criteria Testing Laboratory

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road
Columbia, MD 21046

Evaluation Team

Brian Pleffner
Anthony Busciglio
Jeffrey Burke

Table of Contents

| | |
|---|-----------|
| I. Executive Summary | 4 |
| II. Identification | 5 |
| III. Security Policy | 7 |
| IV. Threats and Assumptions | 7 |
| V. Security Functional Requirements..... | 9 |
| VI. Assurance Requirements | 9 |
| VII. Evaluated Configuration | 10 |
| VIII. TOE Testing..... | 10 |
| IX. Validation Process and Conclusions | 11 |
| X. Validator Comments/Recommendations | 11 |
| XI. Documentation..... | 11 |
| ANNEXES | 12 |

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

I. Executive Summary

The purpose of this Validation Report (VR) is to document the results of the evaluation of the SecureSwitch® Fiber Optic A/B/C Switch Revision A (hereafter SecureSwitch®), a product of Market Central, Inc., Pittsburgh, PA.

Evaluation of the SecureSwitch® at EAL4, augmented with AVA_CCA.1 and AVA_VLA.3, was performed by the COACT, Inc. Common Criteria Testing Laboratory (CCTL), Columbia, MD, and the Common Criteria Evaluation and Validation Scheme (CCEVS). Evaluation results identified in this validation report (VR) were drawn from the *SecureSwitch® Fiber Optic A/B/C Switch Revision A Evaluation Technical Report* (ETR) prepared by the COACT, Inc. CCTL, and the CCEVS (for AVA_CCA.1 and AVA_VLA.3).

This Validation Report is not an endorsement of the SecureSwitch® product by any agency of the United States Government, and no warranty of the product is either expressed or implied.

The SecureSwitch® product does not claim conformance to any protection profile.

The SecureSwitch® Fiber Optic A/B/C Switch Revision A is a fiber optic network switch that connects up to three different full-duplex networks, one at a time, to a full-duplex host. It features all-optical switching using a proprietary mirrored switching mechanism to connect the host port to the selected network port, while providing a minimum of 75 dB of isolation between all unconnected ports.

The SecureSwitch® is completely transparent to optical signaling rates, formats, and protocols. Model #5101180 supports SC connections and Model #5101182 supports ST connections. Both models are 62.5/125 µm multimode, dual-fiber systems. Also available are 19-inch rackmount versions of these switches.

Typical applications include connecting a host computer to three different classifications of networks, up to and including Top Secret. By leaving one network port of the SecureSwitch® unconnected, the SecureSwitch® can also provide a position that leaves the host computer disconnected and isolated from all networks.

A Strength of Function (SOF) claim is not made since no probabilistic or permutational mechanisms are associated with the TOE.

The TOE was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999 [CCV2.1], including applicable International and National Interpretations, and the *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 1: Evaluation Methodology, August 1999

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

[CEMV1.0]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4].

The Security Target (ST) for the SecureSwitch® product is contained within the document *SecureSwitch Fiber Optic A/B/C Switch Revision A Security Target*, F4-0205-001, February 14, 2005 [ST_F4], authored by COACT, Inc. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex C of Part 1 of [CCV2.1].

The project, which also involved evaluation of the associated Security Target, was completed on January 14, 2005.

All copyrights and trademarks are acknowledged.

II. Identification

2.1 TOE, CC, and CEM Identification

TOE: SecureSwitch® Fiber Optic A/B/C Switch Revision A

Developer: Market Central, Inc.
500 Business Center Drive
Pittsburgh, PA 15205-1333

CCTL: COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999 [CCV2.1].

Interpretations: International: 004; 008; 019; 031; 049; 064; 069; 075; 084; 085; 116; 127; 128; 133

National: I-0405; I-0427

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, August 1999 [CEMV1.0].

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

2.2 TOE Overview

The TOE is the SecureSwitch® Fiber Optic A/B/C Switch Revision A. The all-hardware TOE, which is shown in Figure 1, is a fiber optic network switch that connects up to three different full-duplex networks, one at a time, to a full-duplex host.



Figure 1. Front panel (top) and back panel (bottom) views of the TOE.

The TOE uses a proprietary mirrored switching mechanism with specially designed spherical mirrors to provide isolation of a minimum 75 dB between all ports.

To control the switching mirrors, the user selects one of three radio buttons on the front of the device. These buttons are marked A, B, and C, and correspond to network ports A, B, and C on the back of the device (Network Ports). There are also three LEDs marked A, B, and C on the front of the device to indicate which Network Port is selected.

One or more of the Network Ports may be left disconnected (no fiber is connected) to provide a switch position that causes the Common Port to be disconnected from all networks.

The TOE features all-optical switching using a proprietary mechanism consisting of five independent mirrors (Mirror Switch). The switching action is controlled by rotating the mirrors. The rotation mechanism is managed electronically. The TOE is completely transparent to optical signalling rates and supports ST, and SC connectors for 62.5 / 125

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

micrometers multimode, dual fiber systems. Other size fiber systems are available as well.

The device specifications include:

- Sensitivity: 750 to 1450 nanometers;
- Crosstalk Tolerance: exceeds 75 dB;
- Insertion Loss: 4.5 dB @ 1300 nm;
- Vibration Tolerance: 15 Gs on 3 axes per FOTP-11;
- Physical Shock: 15 Gs on 3 axes per FOTP-14;
- Switching Speed: 5 milliseconds typical, 10 milliseconds maximum;
- Operating Temperature: -10° C to +65° C;
- Size Table-top Enclosure: 2.5” H x 8” W x 6.3” D;
- Size Rack-mount Enclosure: 2U (3.5”) H x 19” W x 6.25” D;
- Weight Table-top: 3 pounds;
- Weight Rack-mount: 6 pounds including power supply;
- Power: 5 volts DC from included power module.

III. Security Policy

The security policy for the TOE is as follows.

- The TOE shall not allow network ports to be connected to each other;
- The TOE shall provide isolation between all ports, with the crosstalk tolerance exceeding 75 dB;
- The TOE shall provide the user with the ability to connect the common port to each of the three network ports, one at a time.

IV. Threats and Assumptions

4.1 Threats

Attackers are assumed to be of low attack potential. Applicable threats are shown in the table below.

| Threat | Description |
|--------------------|--|
| T.DIRECT | A remote attacker captures data of a separate network while the attacker’s network is connected to that separate network by the TOE. |
| T.CROSSTALK | A remote attacker captures data of a separate network while the |

**SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088**

| Threat | Description |
|-----------------|--|
| | attacker's network is not connected to that separate network by the TOE. |
| T.ATTACK | A remote attacker performs malicious activity against the Host computer while the attacker's network is connected to the Host computer by the TOE. |

4.2 Environmental assumptions

The personnel and physical environment assumptions required to ensure the security of the TOE are shown in the table below.

| Personnel Assumptions | |
|---|---|
| Assumption | Description |
| A.INSTALL | The User has connected between one and three distinct networks on Network Ports A, B, and C. The User has connected a computer on the Common Port that has a full-duplex network interface. |
| A.NOEVILUSER | The User is non-hostile. |
| A.COMPETENT | The User follows all user guidance when using the TOE. |
| Physical Environment Assumptions | |
| Assumption | Description |
| A.ENVIRON | The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware. |

4.3 Usage assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL4 assurance requirements.

| | |
|------------------|---|
| ADO_DEL.2 | Detection of modification |
| ADO_IGS.1 | Installation, generation, and start-up procedures |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |

V. Security Functional Requirements

The security functional requirements are shown in the table below.

| From Part 2 of the CC, V2.1 | |
|--------------------------------------|-----------------------------------|
| FDP_IFC.2 | Complete information flow control |
| FDP_IFF.1 | Simple security attributes |
| FPT_RVM.1 | Non-bypassability of the TSP |
| FPT_SEP.1 | TSF domain separation |
| Explicitly-stated requirement | |
| SSR_ISO.1 | Optical isolation |

VI. Assurance Requirements

The SecureSwitch® satisfies the EAL4 security assurance requirements, augmented with AVA_CCA.1 and AVA_VLA.3, as identified in Part 3 of the *Common Criteria* [CCV2.1]. These requirements are displayed in the table below.

| Assurance Component ID | Assurance Component Name |
|-------------------------------|---|
| ACM_AUT.1 | Partial CM automation |
| ACM_CAP.4 | Generation support and acceptance procedures |
| ACM_SCP.2 | Problem tracking CM coverage |
| ACM_DEL.2 | Detection of modification |
| ADO_IGS.1 | Installation, generation, and start-up procedures |
| 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 |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |
| ALC_DVS.1 | Identification of security measures |
| ALC_LCD.1 | Developer defined life-cycle model |
| ALC_TAT.1 | Well-defined development tools |
| ATE_COV.2 | Analysis of coverage |
| ATE_DPT.1 | Testing: high-level design |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing - sample |
| AVA_CCA.1 | Covert channel analysis |
| AVA_MSU.2 | Validation of analysis |
| AVA_SOF.1 | Strength of TOE security function evaluation |

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

| Assurance Component ID | Assurance Component Name |
|-------------------------------|------------------------------------|
| AVA_VLA.2 | Independent vulnerability analysis |
| AVA_VLA.3 | Moderately resistant |

VII. Evaluated Configuration

The evaluated configuration is the SecureSwitch® Fiber Optic A/B/C Switch Revision A TOE.

VIII. TOE Testing

Testing of the SecureSwitch took place on October 18, 2004, at COACT, Inc., and on October 29, 2004, at Market Central, Inc. The COACT, Inc. evaluation team executed all of the developer tests as well as several tests they devised. Aspects of testing included:

- Verification that the three LEDs operate correctly on power-up;
- Verification that the pushbutton switches and associated LEDs operate correctly when depressing a switch button;
- Verification of the position of the internal mirrors by measuring the insertion loss and isolation between the Common Port and the three network ports based on the position of the internal mirror assemblies when a specific pushbutton is selected;
- Verification that there is at least 75 dB of isolation between all ports that are not currently connected by the position of the mirror switch;
- Verification that when power to the TOE is lost, the user will still have access to the last network the switch was connected to.

The Evaluation Team also conducted penetration testing based on the developer's vulnerability analysis, as well as on the Team's vulnerability analysis. Aspects of penetration testing included:

- Examination of the delivery procedures to determine if an attacker with low attack potential could compromise a TOE delivery by exchanging the TOE with a pre-modified substitute;
- Examination of the delivery procedures to determine if an attacker with low attack potential could compromise a TOE delivery by modifying the TOE in a fashion that would allow one connected network to be able to see another connected network, without such a modification being detected.

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

IX. Validation Process and Conclusions

The COACT Inc. Evaluation Team followed the procedures outlined in CCEVS Scheme Publication #4, *Guidance to Common Criteria Testing Laboratories* [CCEVS4].

The Evaluation Team concluded that the TOE was CC Part 2 extended and CC Part 3 conformant, and recommended that an EAL4 certificate rating be issued for the TOE.

The Validation Team agreed with the conclusion of the COACT, Inc. Evaluation Team (for EAL4), and recommended to CCEVS Management that a certificate be issued for the SecureSwitch® Fiber Optic A/B/C Switch Revision A.

X. Validator Comments/Recommendations

- Testing activities conducted by the COACT, Inc. CCTL were thorough and very professionally executed.

XI. Documentation

Documentation applicable to the SecureSwitch® Delivery Procedures, Installation and Generation, Administrator Guidance, and User Guidance is identified in the table below.

| |
|---|
| Delivery Procedures |
| <i>SecureSwitch® Fiber Optic A/B/C Switch Revision A Delivery and Operation</i> , Rev 00096, November 15, 2004. |
| Installation and Generation |
| <i>SecureSwitch® Fiber Optic A/B/C Switch Revision A (Manual)</i> , Rev 00086, October 19, 2004. |
| Administrator and User Guidance |
| <i>SecureSwitch® Fiber Optic A/B/C Switch Revision A (Manual)</i> , Rev 00086, October 19, 2004. |

Additional documentation, most of which is proprietary, was available to the Evaluation Team during the evaluation of the SecureSwitch®.

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

ANNEXES

Annex A: Glossary

| Acronym | Expansion |
|----------------|---|
| CC | <i>Common Criteria for Information Technology Security Evaluation.</i> [Note: Within this Validation Report, CC always means Version 2.1, August 1999.] |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Criteria Testing Laboratory |
| EAL | Evaluation Assurance Level |
| dB | Decibel |
| ETR | Evaluation Technical Report |
| NIAP | National Information Assurance Partnership |
| LED | Light-Emitting Diode |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| PP | Protection Profile |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |

SecureSwitch® Fiber Optic A/B/C Switch Revision A
CCEVS-VR-05-0088

Annex B: Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS):
(www.niap.nist.gov/cc-scheme).
- COACT, Inc. (www.coact.com)
- Market Central, Inc. (www.mctech.com)

CCEVS Documents

- [CCV2.1] *Common Criteria for Information Technology Security Evaluation*,
Version 2.1, August 1999.
- [CEMV2.1] *Common Methodology for Information Technology Security Evaluation*,
Version 1.0, Part 2. Evaluation Methodology, August 1999.
- [CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February
2000.
- [CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0,
March 2000.

Security Target

- [ST_F4] *SecureSwitch Fiber Optic A/B/C Switch Revision A Security Target*,
Document No. F4-0205-001, February 14, 2005, authored by COACT,
Inc.