Market Central, Inc.

SecureSwitch® Fiber Optic Switch
Revision A, B, C, D

Security Target

June 2015

Document prepared by

Ark Infosec Labs Inc.
www.arkinfosec.net

Document History

Version	Date	Author	Description
1.0	30 Mar 2015	Ark Infosec	Release for evaluation.
1.1	8 Apr 2015	Ark Infosec	Address OR1.
1.2	1 Jun 2015	Ark Infosec	Address OR3 and CB OR1.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the SecureSwitch® Fiber Optic Switch Revision A, B, C, D Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is an optical switch that allows a single host to connect to multiple networks, one at a time, whilst maintaining separation between the networks. The TOE user manually switches between networks.

3 The TOE uses a proprietary mirrored switching mechanism with specially designed mirrors to provide isolation of a minimum 75 dB between all unselected ports. The mirrors are positioned electronically to control the switching action.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	SecureSwitch® Fiber Optic Switch Revision A, B, C, D
Security Target	SecureSwitch® Fiber Optic Switch Revision A, B, C, D Security Target, v1.2

1.3 Conformance Claims

4 This ST supports the following conformance claims:

a) CC version 3.1 Release 4

b) CC Part 2 extended

c) CC Part 3 conformant

d) Evaluation Assurance Level (EAL) 2

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

5 The TOE is an optical switch.

2.2 Usage

6 The TOE is used when it is necessary to connect a single host to multiple networks whilst maintaining separation between the networks, such as those of different security classifications. As shown in Figure 1 below, to use the switch, the user selects the radio button on the front of the device (or on a connected remote control) that corresponds to the desired network. This connects the selected network to the host. LEDs (and dry contact relay closures on revision B, C & D models) indicate which network is selected.

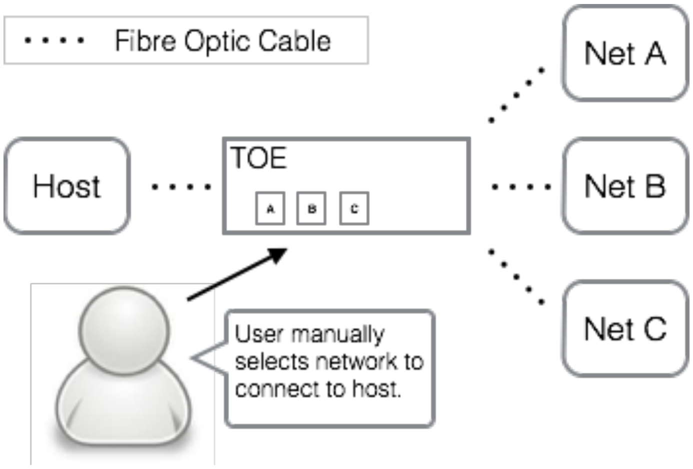

Figure 1: TOE usage scenario

7 Figure 2 and Figure 3 show the TOE (Revision A) front and back panels. The radio buttons with integrated LEDs on the front indicate the selected network. The A/B/C ports on the back connect to the isolated networks and the Common port connects to the host.

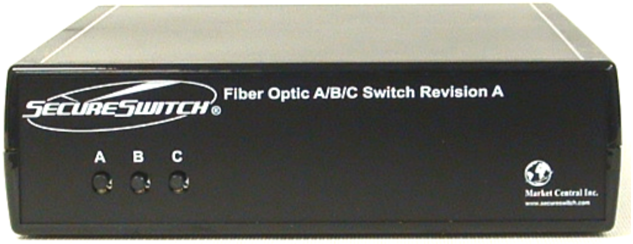

Figure 2: Front Panel SecureSwitch® Revision A

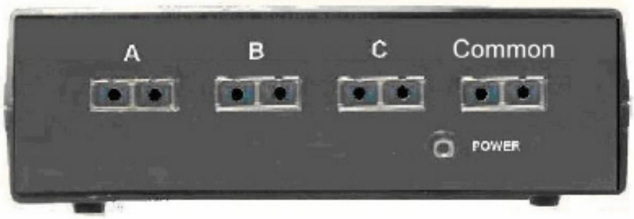

Figure 3: Back Panel SecureSwitch® Revision A

8 The TOE is available in four different revisions as follows. In all cases, the firmware and security enforcing mechanisms are the same:

a) **Revision A.** Multimode Fiber Optic A/B/C switch.

b) **Revision B.** Multimode Fiber Optic A/B/C switch with remote control ports and switched AC power outlet.

c) **Revision C.** Multimode Fiber Optic A/OFF/C switch with remote control ports and switched AC power outlet.

d) **Revision D.** Single mode Fiber Optic A/B/C switch with remote control ports and switched AC power outlet.

9 Each TOE revision is available in tabletop, 1U tabletop and rackmount enclosures as shown in the following figures.

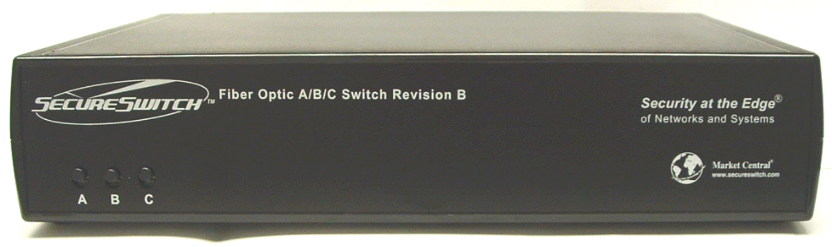

Figure 4: Tabletop SecureSwitch® Revision B

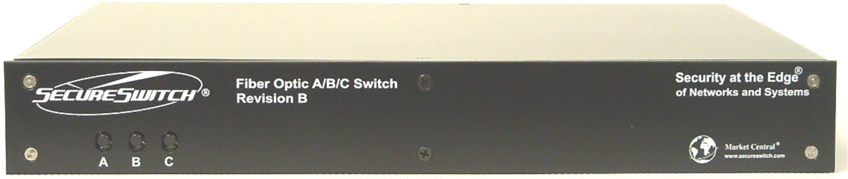

Figure 5: 1U Tabletop SecureSwitch® Revision B

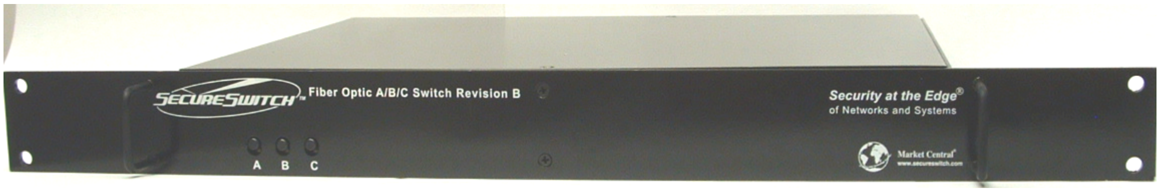

Figure 6: Rackmount SecureSwitch® Revision B

2.3 Security Functions

10 The TOE provides the following security functions:

a) **Switching.** An internal Mirror Switch allows optical communications to travel between the Common Port and one of the network ports at a time. When the user selects a different network, the Mirror Switch is repositioned to allow the host device that is connected to the Common Port to communicate with the selected network port. Each radio button has a corresponding LED that indicates which network port currently selected. Only one button/network can be selected at a time.

b) **Isolation.** Due to the use of fiber-optic signals and the proprietary mirrored switching mechanism design, the TOE provides an isolation of a minimum of 75 dB between all unselected ports.

2.4 Physical Scope

11 The physical boundary of the TOE is the entire SecureSwitch® device. This includes the buttons, the LEDs, the Mirror Switch, the ports, as well as the internal electronics that operate the mirrored switching mechanism.

12 Each TOE revision is available in multiple configurations as shown in Table 3. These configurations differ in terms of type of fiber-optic connectors, enclosure, remote status and control interfaces, switched AC power outlet and power delay for the AC power outlet (allows connected equipment to power down for the given time delay when switching between networks). In all variants, the firmware and security enforcing mechanisms are the same.

Table 3: TOE variants and part numbers

Part #	Revision	Connectors (network/ common)	Enclosure	Remote Status & Control	Power Delay
5101180	Revision A	SC/SC	Tabletop	No	None
5101180-1U	Revision A	SC/SC	1U Tabletop	No	None
5101182	Revision A	ST/ST	Tabletop	No	None
5101182-1U	Revision A	ST/ST	1U Tabletop	No	None
5101183	Revision A	SC/SC	Rackmount	No	None
5101184	Revision A	ST/ST	Rackmount	No	None
5101185	Revision B	ST/SC	Tabletop	Yes	15s
5101185-60	Revision B	ST/SC	Tabletop	Yes	60s
5101185-1U	Revision B	ST/SC	1U Tabletop	Yes	15s
5101185-1U-60	Revision B	ST/SC	1U Tabletop	Yes	60s
5101186	Revision B	ST/SC	Rackmount	Yes	15s
5101186-60	Revision B	ST/SC	Rackmount	Yes	60s

Part #	Revision	Connectors (network/ common)	Enclosure	Remote Status & Control	Power Delay
5101191	Revision C	ST/SC	Tabletop	Yes	15s
5101191-60	Revision C	ST/SC	Tabletop	Yes	60s
5101191-1U	Revision C	ST/SC	1U Tabletop	Yes	15s
5101191-1U-60	Revision C	ST/SC	1U Tabletop	Yes	60s
5101192	Revision C	ST/SC	Rackmount	Yes	15s
5101192-60	Revision C	ST/SC	Rackmount	Yes	60s
5101177	Revision D	ST/SC	Tabletop	Yes	15s
5101177-60	Revision D	ST/SC	Tabletop	Yes	60s
5101177-1U	Revision D	ST/SC	1U Tabletop	Yes	15s
5101177-1U-60	Revision D	ST/SC	1U Tabletop	Yes	60s
5101178	Revision D	ST/SC	Rackmount	Yes	15s
5101178-60	Revision D	ST/SC	Rackmount	Yes	60s

2.4.1 Guidance Documents

13 The TOE includes the following guidance documents:

a) Market Central, Inc. Manual ver 1, SecureSwitch® Fiber Optic A/B/C Switch Revision A

b) Market Central, Inc. Manual ver 1, SecureSwitch® Fiber Optic A/B/C Switch Revision B with Switched AC Power Outlet

c) Market Central, Inc. Manual ver 1, SecureSwitch® Fiber Optic A/OFF/C Switch Revision C with Switched AC Power Outlet

d) Market Central, Inc. Manual ver 1, SecureSwitch® Fiber Optic A/B/C Switch Revision D with Switched AC Power Outlet

2.4.2 Non-TOE Components

14 The TOE is not reliant on any external components.

2.5 Logical Scope

15 The logical scope of the TOE comprises the security functions defined in section 2.3.

3 Security Problem Definition

3.1 Threats

16 Table 4 identifies the threats addressed by the TOE.

Table 4: Threats

Identifier	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 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.

3.2 Organizational Security Policies

17 None.

3.3 Assumptions

18 Table 5 identifies the assumptions related to the TOE's environment.

Table 5: Assumptions

Identifier	Description
A.INSTALL	The User has connected up to three (depending on TOE revision) distinct networks to the TOE Network Ports. 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.
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. TOE connected optical cabling and equipment shall be protected from unauthorized physical access.

4 Security Objectives

4.1 Objectives for the Operational Environment

19 Table 6 identifies the objectives for the operational environment.

Table 6: Operational environment objectives

Identifier	Description
OE.INSTALL	The User has connected up to three (depending on TOE revision) distinct networks to the TOE Network Ports. The User has connected a computer on the Common Port that has a full-duplex network interface.
OE.NOEVILUSER	The User is non-hostile.
OE.COMPETENT	The User follows all user guidance when using the TOE.
OE.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.

4.2 Objectives for the TOE

20 Table 7 identifies the security objectives for the TOE.

Table 7: Security objectives

Identifier	Description
O.NOCONNECT	The TOE will not allow two Network Ports to directly connect (i.e., no information flow is permitted).
O.ISOLATION	The TOE will provide isolation between all ports.
O.SWITCH	The TOE will provide the User with the ability to connect the Common Port to each of the three Network Ports, one at a time.

5 Security Requirements

5.1 Conventions

21 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

5.2 Extended Components Definition

22 Table 8 identifies the extended component that is incorporated into this ST.

Table 8: Extended Components

Component	Title	Rationale
FDP_ISO.1	Optical Isolation	No existing CC Part 2 SFRs address hardware port shielding and isolation. Since the purpose of optical isolation is to protect user data from unintended disclosure via crosstalk, a new family was created within the User Data Protection (FDP) class.

5.2.1 Secure Virtual Container (FDP_ISO)

5.2.1.1 Family Behavior

23 This family provides requirements that address the protection of user data unintended disclosure via crosstalk by means of optical isolation. Crosstalk occurs when a signal transmitted on one circuit or channel of a transmission system creates an undesired effect in another circuit or channel.

5.2.1.2 Component Leveling

FDP_ISO: Optical Isolation
1

24 FDP_ISO.1 Optical isolation addresses protection of user data from unintended disclosure via crosstalk.

5.2.1.3 Management: FDP_ISO.1

25 The following actions could be considered for the management functions in FMT:

a) None

5.2.1.4 Audit: FDP_ISO.1

26 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) None

FDP_ISO.1 Optical Isolation

Hierarchical to: No other components.

Dependencies: None

FDP_ISO.1.1 The TSF shall ensure that there is a minimum of 75 dB of isolation between all ports that are not currently connected by the position of the Mirror Switch.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FDP_IFC.2	Complete Information Flow Control
FDP_IFF.1	Simple Security Attributes
FDP_ISO.1	Optical Isolation

5.3.1 User Data Protection (FDP)

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the *SecureSwitch Flow Control Policy* on *optical signals on the Common Port and each of the Network Ports* and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the *SecureSwitch Flow Control Policy* based on the following types of subject and information security attributes: *the position of the Mirror Switch*.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *Information may only flow between the Common Port and a single Network Port if the position of the Mirror Switch is in the single position that corresponds to that Network Port.*

FDP_IFF.1.3 The TSF shall enforce the *no additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *no explicit authorization rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *no explicit denial rules*.

FDP_ISO.1 Optical Isolation

Hierarchical to: No other components.

Dependencies: None

FDP_ISO.1.1 The TSF shall ensure that there is a minimum of 75 dB of isolation between all ports that are not currently connected by the position of the Mirror Switch.

5.4 Assurance Requirements

27 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2.

Table 10: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Switching

Related SFRs: FDP_IFC.2, FDP_IFF.1

28 The SecureSwitch® device has a front panel with three radio buttons labeled A, B, and C (B is replaced by OFF in Revision C). Revision B, C and D versions of the TOE also have three remote control inputs on the rear panel labeled A, B and C (B is replaced by OFF in Revision C) plus a Ground connection labeled G. Only one front panel radio button or only one rear panel remote control input can be selected at a time.

29 Each front panel button and each rear panel remote control input corresponds to a Network Port on the rear of the device (except in the case of the ‘OFF’ button and the ‘OFF’ remote control input on Revision C).

30 Each Network Port has a corresponding front panel LED that indicates if that Network Port is currently selected. Revision B, C and D versions of the TOE also have three sets of remote control outputs on the rear panel labeled A, B and C (B is replaced by O in Revision C) that correspond to each Network Port, and that indicate if that Network Port is currently selected.

31 Another port on the rear of the TOE labeled Common is for connection to a host computer. The information flows from each of these ports are the only information flows in the TOE.

32 Inside the SecureSwitch® device is a Mirror Switch. The Mirror Switch is a specially designed set of miniature mirror movements that allow optical communications to travel between the Common Port and one of the Network Ports at a time. When the Mirror Switch is repositioned, the Common Port can communicate with a different Network Port. There is a single position for each Network Port.

33 The radio buttons on the front of the device and the rear panel remote control inputs on the revision B, C and D versions of the TOE control the Position of the Mirror Switch. When button ‘A’ is pressed, or when remote control input ‘A’ is connected to the ‘G’ pin, an electro-mechanical mechanism rotates the mirror to the position designated for Network Port ‘A’. The same applies to buttons ‘B’ and ‘C’ and remote control inputs ‘B’ and ‘C’. In Revision C of the TOE, selecting the ‘OFF’ radio button or the ‘OFF’ remote control input performs the same positioning of the mirror, however the related fiber optic path and port has been removed thereby terminating the network connection.

34 The TOE is a self-contained unit that forwards information signals but is not affected by those signals.

6.2 Isolation

Related SFRs: FDP_ISO.1

35 Due to the use of fiber optic signals and the proprietary proprietary mirrored switching mechanism design, the TOE provides a minimum of 75 dB of isolation between all unselected ports. This high isolation was designed to comfortably meet the industry standard 65 dB isolation rating.

7 Rationale

7.1 Security Objectives Rationale

36 Table 11 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 11: Security Objectives Mapping

	T.DIRECT	T.CROSSTALK	T.ATTACK	A.INSTALL	A.NOEVILUSER	A.COMPETENT	A.ENVIRON
O.NOCONNECT	X						
O.ISOLATION		X					
O.SWITCH			X				
OE.INSTALL				X			
OE.NOEVILUSER					X		
OE.COMPETENT						X	
OE.ENVIRON							X

37 Table 12 provides the justification to show that the security objectives are suitable to address the security problem.

Table 12: Suitability of Security Objectives

Element	Justification
T.DIRECT	**O.NOCONNECT.** The TOE will not allow Network Ports to be connected to each other, directly addressing the threat of a direct connection.
T.CROSSTALK	**O.ISOLATION.** By providing isolation between ports, the only way for information to pass between ports is according to the TOE's information flow control policy.
T.ATTACK	**O.SWITCH.** The User has the ability to disconnect from a network from which malicious activity originates.
A.INSTALL	**OE.INSTALL.** The objective satisfies the assumption by providing the assumed installation configuration.
A.NOEVILUSER	**OE.NOEVILUSER.** The objective satisfies the assumption by

Element	Justification
	providing there will be no evil users.
A.COMPETENT	**OE.COMPETENT.** The objective satisfies the assumption by providing the User will follow guidance.
A.ENVIRON	**OE.ENVIRON.** The objective satisfies the assumption by providing the assumed operating conditions.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

38 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices.

7.2.2 SFR Rationale

Table 13: Security Requirements Mapping

	O.NOCONNECT	O.ISOLATION	O.SWITCH
FDP_IFC.2	X		X
FDP_IFF.1	X		X
FDP_ISO.1	X	X	

Table 14: Suitability of SFRs

Objectives	SFRs
O.NOCONNECT	**FDP_IFC.2** & **FDP_IFF.1** specify that only information may flow between the Common Port and a single Network Port at a time, never two Network Ports. **FDP_ISO.1** supports this objective, because it requires all ports be isolated from each other by a minimum of 75dB. This includes one Network Port to the next, thereby supporting the objective of not allowing a connection between Network Ports.
O.ISOLATION	**FDP_ISO.1** requires all ports be isolated from each other by a minimum of 75dB. This will prevent crosstalk and provide isolation between ports.
O.SWITCH	**FDP_IFC.2** & **FDP_IFF.1** define the SecureSwitch Flow Control Policy in accordance with O.SWITCH.

Table 15: SFR dependencies

SFR	Dependency	Rationale
FDP_IFC.2	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met by inclusion of FDP_IFC.2.
	FMT_MSA.3	Not met. Not included as there are no objects or attributes that can be created that affect the SecureSwitch Flow Control Policy. Rather, the policy is determined by one attribute alone, the position of the Mirror Switch.
FDP_ISO.1	None	Met

7.3 TOE Summary Specification Rationale

39 Table 16 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 16: Map of SFRs to TSS Security Functions

	Switching	Isolation
FDP_IFC.2	X	
FDP_IFF.1	X	
FDP_ISO.1		X