National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 2.1, September 7, 2010

Report Number:	**CCEVS-VR-PP-0016**
Dated:	**31 July 2015**
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base Requirements
InfoGard Laboratories, Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Peripheral Sharing Switch for Human Interface Devices, Version 1.2 Protection Profile, also referred to as PSSHID21. It presents a summary of the PSSHID21 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the PSSHID21 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Belkin Secure DVI-I KVM Switch. The evaluation was performed by the InfoGard Laboratories, Inc. Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, California, United States of America, and was completed in September 2010. This evaluation addressed the base requirements of the PSSHID2.

The information in this report is largely derived from the Security Target, written by the InfoGard Laboratories CCTL, and the product Validation Report, written by NIAP.

The evaluation determined that the PSSHID21 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the PSSHID21, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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

The validation team found that the evaluation showed that the PSSHID21 meets the requirements of the APE components. The evaluation technical report (ETR) has been provided in order to confirm that the conclusions of the testing laboratory are consistent with the evidence produced.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the PSSHID21 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Belkin Secure DVI-I KVM Switch, provided by Belkin International, Inc. The evaluation was performed by the InfoGard Laboratories, Inc. Common Criteria

Testing Laboratory (CCTL) in San Luis Obispo, California, United States of America, and was completed in August 2011.

The PSSHID21 contains a set of “base” requirements that all conformant STs must include. There are no optional requirements defined by the PP.

The following identifies the PP subject to the evaluation/validation, and to the supporting information from the base evaluation performed against this PP.

Protection Profile	*Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 2.1, 07 September 2010*
ST (Base)	Belkin International, Inc Belkin® Secure DVI-I KVM Switch Security Target, Version 1.2, August 1, 2011
Evaluation Technical Report (Base)	Evaluation Technical Report For the NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Peripheral Sharing Switch (PSS) (Proprietary), Version 1.1, April 22, 2013
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	InfoGard Laboratories, Inc., San Luis Obispo, CA
CCEVS Validators	Franklin Haskell, The Mitre Corporation Olin Sibert, Orion Security Solutions, Inc.

3 PSSHID Description

The PSSHID21 specifies U.S. Department of Defense minimum-security requirements for peripheral sharing switches permitting a single set of human interface devices to be shared among two or more computers, wherein the use of Universal Serial Bus (USB) connections are limited to keyboard, display and mouse, with no other USB devices valid. The normal installation for the TOE is with a single user in limited work surface space accessing two or more computers as switched computers, with a keyboard, monitor, and pointing device connected to the switch as the shared peripherals. In operation, the TOE is connected to one computer at a time, with the user performing a specific action, such as pushing a button, to begin using a different computer. The TOE will then indicate the computer selected by the user in a persistent and non-transitory manner. The TOE treats a collection of device ports as a single entity, called the peripheral port group. There is one group for each connected switched computer, and one group for the set of shared peripherals. Every switched computer group has a unique associated logical ID, and the shared peripheral group ID is considered to be the same as that of the switched computer group currently selected by the TOE.

The peripheral sharing switch must preclude any features permitting user information to be shared or transferred between computers. The TOE only provides a connection between a selected computer and the human interface devices at any given time, but is not concerned with the user’s data flowing between the switched computers and the shared peripherals. Wherein a peripheral sharing switch provides enhanced features such as scanning or video protocol conversions, these enhancements must be examined to ensure that information is not transferred or shared between computers.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.ACCESS	It is assumed that authorized users possess the necessary privileges to access the data transferred by the TOE, and thus users are authorized users.
A.MANAGE	It is assumed that the TOE is installed and managed in accordance with the manufacturer's directions.
A.NOEVIL	It is assumed that the authorized user follows all usage guidance and is not hostile.
A.PHYSICAL	It is assumed that the TOE is kept physically secured.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.INVALIDUSB	An unauthorized USB device is connected to the peripheral switch by an authorized user.
T.RESIDUAL	Residual data may be transferred between peripheral port groups with different IDs.
T.ROM_PROG	If an attacker modifies the TSF such that the embedded code in reprogrammable ROMs is overwritten, the separation-enforcing components of the code would be compromised, and would lead to the subsequent compromise of the information flowing through the TOE.
T.SPOOF	A user may intentionally or unintentionally act as if a set of shared peripherals are connected to one computer when they are in fact connected to a different computer.
T.TRANSFER	Through the TOE, a connection between computers may allow data transfer.

4.3 Organizational Security Policies

There are no applicable organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.CONF	The TOE shall not violate the confidentiality of information which it processes, so that information generated within any peripheral group connections is not accessible by any other peripheral group with a different group ID.
O.INDICATE	The Authorized user shall receive a clear, unambiguous indication of which switched computer has been selected.
O.ROM	The TOE software/firmware shall be protected against unauthorized modification, with the embedded software contained in mask=programmed or one-time programmable read-only memory permanently attached (non-socketed) to a circuit assembly.
O.SELECT	To select the computer to which the shared set of peripheral devices is connected, an explicit action shall be used by the authorized user. Automatic switching based on scanning shall not be used as a selection identification.
O.SWITCH	All devices in a shared peripheral group shall be connected to no more than one switched computer at a time.

The following table contains security objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.ACCESS	The authorized user shall possess the necessary privileges to access the information transferred by the TOE. Users are authorized users.
OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
OE.NOEVIL	The authorized user shall be non-hostile and follow all usage guidance.
OE.PHYSICAL	The TOE shall be physically secure.

5 Requirements

As indicated above, requirements in the PSSHID21 are comprised of the "base" requirements. The following table contains the "base" requirements that were validated as part of the Belkin evaluation activity referenced above.

Requirement Class	Requirement Component
FDP: User Data Protection	FDP_IFC.1: Subset Information Flow Control
	FDP_IFF.1: Simple Security Attributes
FMT: Security	FMT_MSA.1: Management of Security Attributes

Requirement Class	Requirement Component
Management	FMT_MSA.3: Static Attribute Initialization
EXT: Extended Requirements	EXT_VIR.1: Visual Indication Rule
	EXT_IUC.1: Invalid USB Connection
	EXT_ROM.1: Read-only ROMs

6 Assurance Requirements

The following are the assurance requirements contained in the MDFPP20:

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Architectural Design with Domain Separation and Non-bypassibility
	ADV_FSP.2: Security-enforcing Functional Specification
	ADV_TDS.1: Basic Design
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative User Guidance
ALC: 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
	ALC_FLR.2: Flaw Reporting Procedures
ATE: Tests	ATE_COV.1: Evidence of Coverage
	ATE_FUN.1: Functional Testing
	ATE_IND.2: Independent Testing - Conformance
AVA: Vulnerability Assessment	AVA_VAN.2: Vulnerability Analysis

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

8 Glossary

The following definitions are used throughout this document:

- **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.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[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] Infogard, Evaluation Technical Report For the NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Peripheral Sharing Switch (PSS) (Proprietary), Version 1.1, April 22, 2013.

[7] InfoGard Laboratories, Inc. *Belkin® Secure DVI-I KVM Switch Security Target*, Version 1.2. February 28, 2013.

[8] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, 07 September 2010.