National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Data Diode Version 1 and Data Diode Version 2

Report Number: **CCEVS-VR-2-0026**
Dated: **19 November 2002**
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

Elizabeth A. Foreman
Jeffrey C. Gilliatt
Mitretek Systems,
Fall Church, Virginia

Paul A. Olson
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of the Owl Data Diode (Data Diode Version 1 and Data Diode Version 2) was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 31 October 2002. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM),Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. 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 adduced. This Validation Report is not an endorsement of the Owl Data Diode product by any agency of the US Government and no warranty of the product is either expressed or implied.

The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Evaluation Details

Evaluation Completion: 31 October 2002

Evaluated Product: Data Diode Version 1 and Data Diode Version 2

Developer:
Owl Computing Technologies, Inc.
19 North Salem Road (2nd Floor)
P.O. Box 313
Cross River, NY 10518

CCTL:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300

Columbia, MD 21046

Validation Team: Jeffrey C. Gilliatt and Elizabeth A. Foreman, Mitretek Systems, Inc., 3150 Fairview Park South, Falls Church, VA 22042-4519

Paul A. Olson, National Security Agency, Fort Meade, MD

Evaluation Class: EAL2

Completion Date: 31 October 2002

1.2 Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

1. Unique Identification of Configuration Items in the Configuration List (003)
2. Meaning of "clearly stated" in APE/ASE_OBJ.1 (043)
3. Use of Documentation Without C & P Elements (051)
4. Aspects of Objectives in TOE and Environment (084)
5. SOF Claims Additional to Overall Claim (085)
6. Indistinguishable Work Units for ADO_DEL (116)

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

1. Empty Selection or Assignments (407)
2. Configuration Items in The Absence of Configuration Management (412)
3. Evaluation of the TOE Summary specification: Part 1 Vs Part 3 (418)
4. Content of PP Claims Rationale (426)
5. Identification of Standards (427)

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

Name (T = Threat)	Threat
T.FULL_DUPLEX	If the receive photodiode on a Send-only NIC can sense light from the light source, then a subject executing on a workstation, in which the TOE in installed, could cause an information flow contrary to the direction of the information flow established when the TOE was installed.
T.INCORRECT_FLOW	A Receive-Only Data Diode NIC can receive a send request over the PCI Bus to send information. A Send-Only Data Diode NIC can receive a listen-on-this-port request

Name (T = Threat)	Threat
	over the PCI Bus. A NIC that allows requests from the PCI Bus that are inconsistent with the direction of the information flow, could cause an information flow contrary to the direction of the information flow established when the TOE was installed.
T.TAMPERING	A person, with sufficient time, tools [e.g., soldering iron, wire, propane torch, new physical network connectors], and access to the TOE, can change the information flow through a Data Diode NIC and violate the policy.

2 Identification

2.1 ST and TOE Identification

ST: Owl Computing Data Diode Common Criteria Security Target (EAL2), Version 4.0,

31 October 2002

TOE Identification: Data Diode – Version 1, Data Diode – Version 2

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

The TOE is a pair of Data Diode NIC network interface cards. Each card has two external interfaces. One external interface is the PCI Bus of the host in which the Data Diode NIC is installed. The other interface is the fiber optic network connection physically located on the card. Each Data Diode NIC has two network connections, one for incoming traffic, and one for outgoing traffic. However only one connection can be active for one type of card. Therefore it requires a pair of Data Diode NIC cards to communicate from a sending host to a receiving host. The purpose of the Data Diode NIC is to provide assurance that one-way operation occurs at the physical interface between a network sender and receiver. Enabling only a single photodiode on the sender and a single light detector on the receiver insures one-way information flow over a fiber-optic line. A machine cannot have both a send and a receive card. The Data Diode NIC is provided in two models, the send-only and receive-only NICs.

This Data Diode NIC was developed to support higher-level application software packages to provide secure one-way network communications. Owl markets and sells application programs that utilize the Data Diode Technology for specific data transfers, however only the TOE is the Data Diode NIC.

The information flow policy enforced by the Data Diode NIC does not rely on passwords, authentication, or encryption to protect host data. Rather the physics of a photo-detector and light emitting diode enforce the TSP.

The Target of Evaluation (TOE) is either one of two versions of the Data Diode NIC hardware card offered by Owl. The difference in Version 1 and Version 2 of the TOE is strictly limited to throughput. Either version of the TOE is offered as a single Data Diode as a send-only NIC or as a receive-only NIC, or as a pair of Data Diode NICS for two-way communication. Owl uses a proprietary protocol to translate light impulses into data, however the protocol is not part of the TOE and is not required to meet the TSF. Any host that supports a PCI Bus is sufficient for the correct operation of the TSF; therefore the host is not part of the TOE.

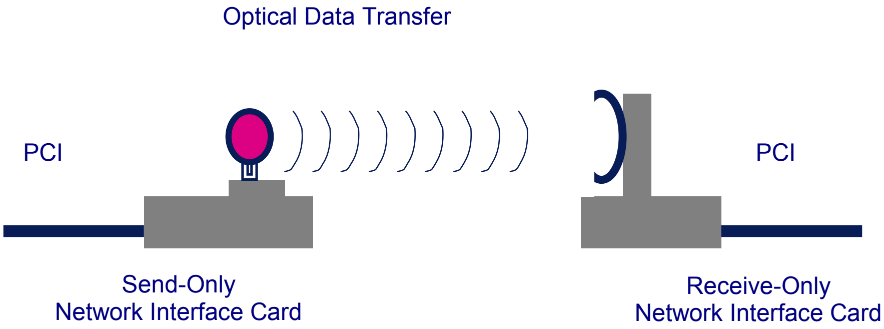

Figure 1 - High Level view of the Data Diode Interface

A pair of Data Diode NIC cards is required to move packet data directly between a send-only communication card and a receive-only communication card. The data is formatted, framed and queued in the "Send-Only Communication Card" once across the PCI Bus. The output of the "Send-Only Communication Card" is a fiber optic cable connected to a "Receive-Only Communication Card". Data is then transferred from the "Receive-Only Communication Card" across the PCI Bus, for availability to application programs.

The TOE consists of a send-only optical communication card and a receive-only optical communication card whereby packets of data move uni-directionally from a send-only optical communication card to a receive-only communication card. The data is staged, queued, segmented and framed in the "Send-Only Communication Card" for packet transfers across the PCI Bus. The output of the "Send-Only Communication Card" is an optical photo-diode, which transfers information by way of a fiber optic cable connected to optical receiver in the "Receive-Only Communication Card". Data packets are then received with a photo-detector and reassembled into the original message by the "Receive-Only Communication Card".

2.2 IT Security Environment

The Target of Evaluation (TOE) is comprised of two Data Diode NIC integrated circuit cards. Each card is connected to a standard PCI slot in a computer. Each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode NIC is a send-only card, and the other type of data diode NIC is a receive-only card. Both types of cards are modified ATM Segmentation and Reassembly integrated cards for PCI-based networking applications.

Each Data Diode NIC has two external interfaces. Each type of Data Diode NIC (receive-only, and send-only) has a Peripheral Component Interconnect (PCI) bus interface that accepts buffers of information from the host (send-only) or puts buffers of information on the PCI Bus for the host (receive-only). The data and control information from the PCI Bus to the Data Diode NIC are received by the ATM Segmentation and Reassembly (SAR) controller. The SAR connects directly to the PCI Bus and exchanges data and control information between the PCI Bus and the TOE. The SAR uses host memory to change packet (buffered) information that it receives from the PCI Bus interface and serializes the byte stream for the ATM Phy chip, an internal TOE subsystem. The ATM SAR also receives a serial byte stream from the ATM Phy and blocks the data into a buffered packet format before placing packets on the PCI Bus. Although the SAR is part of the TOE and exports an interface to PCI Bus, the SAR provides no TSF.

Each type of Data Diode NIC card has a transceiver that physically provides two ports for a network fiber-optic connection. There is one receive port and one send port. The send port exports light pulses to a receive port that receives light impulses. To export light pulses over the send port, the transceiver converts electrical voltage received over an internal TOE interface into light impulses. To import light pulses over the receive port; the transceiver converts light impulses into electrical voltage that are sent over an internal TOE interface.

Therefore, each of the host computers that participate in the one-way data transfer that the Data Diodes provide must contain a Peripheral Component Interconnect (PCI) bus interface to which the appropriate (send-only or receive-only) Data Diode card can be attached.

3 Security Policy

The Owl Data Diode TOE provides two security services. Their descriptions in the following sections were taken from the ETR, Part 1 (Non-Proprietary version).

3.1 Information Flow Protection

A Data Diode NIC physically can only provide network traffic flow in one direction over any single network connection and this TSP is enforced at the physical level. One send-only Data Diode NIC communicating with a receive-only Data Diode NIC is required for communication between them over the ports that they are exporting.
If a host attempts to send traffic over a receive-only Data Diode NIC, buffers of data may be sent through the host device driver over the PCI Bus to the receive-only Data Diode NIC. The receive-only NIC will process the buffer, and convert binary to voltage. But when transceiver goes to transmit the light impulses, there is no light source since it has been physically disconnected. Also the send port has been physically blocked so that no light impulses can be transmitted. When the host does not receive a response from a connection request, it is up to the host protocol to deal with no response to the connection request. The TSF is maintained even though the host has attempted to send information through a receive-only Data Diode NIC.

If a host attempts to listen for traffic over a send-only Data Diode NIC, no signals/bits/buffers/voltage will be received by the device driver listening on the PCI Bus for data from the send-only Data-Diode NIC. The send-only Data Diode NIC has had the photodiode physically disconnected. Also the receive port has been physically blocked so that no light impulses can be received. When the host does not receive a response while listening for data from the send-only Data Diode NIC, it is up to the host protocol to deal with no data. The TSF is maintained even though the host has attempted to receive information through a send-only Data Diode NIC.

3.2 TOE Self Protection

The Data Diode NIC protects itself by not exporting an interface that can modify the TOE. The only interfaces exported are the PCI Bus interface and the network fiber optic interface. Neither interface can alter the TSF since the TOE has been physically modified to enforce the TSF and the TOE would have to be physically modified to violate the TSF.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. Since the TOE operates at the physical level, which is below the level of protocols or binary logic, it is unaffected by buffer content or network traffic.

4 Assumptions

4.1 Personnel Assumptions

A.NOEVIL Authorized administrators and installers are non-hostile.

4.2 Physical Assumptions

A.PHYSICAL The TOE is physically secure.

A.CONNECTION A protected fiber optic connection exists between any pair Data Diode NICs

4.3 Host Assumptions

A.ADMIN Only a trained trusted administrator installs the TOE into a host.

5 Architectural Information

The high level design describes three subsystems for each type of card:

- Segmentation and Reassembly Component (SAR)
- ATM Physical Packet Interface Chip
- Optical Transceiver.

Each Data Diode NIC has two external interfaces. Each type of Data Diode NIC (receive-only, and send-only) has a Peripheral Component Interconnect (PCI) bus interface that accepts buffers of information from the host (send-only) or puts buffers of information on the PCI Bus for the host (receive-only). The data and control information from the PCI Bus to the Data Diode NIC are received by the ATM Segmentation and Reassembly (SAR) controller. The SAR connects directly to the PCI Bus and exchanges data and control information between the PCI Bus and the TOE. The SAR uses host memory to change packet (buffered) information that it receives from the PCI Bus interface and serializes the byte stream for the ATM Phy chip, an internal TOE subsystem. The ATM SAR also receives a serial byte stream from the ATM Phy and blocks the data into a buffered packet format before placing packets on the PCI Bus.

Each type of Data Diode NIC card has a transceiver that physically provides two ports for a network fiber-optic connection. There is one receive port and one send port. The send port exports light pulses to a receive port that receives light impulses. To export light pulses over the send port, the transceiver converts electrical voltage received over an internal TOE interface into light impulses. To import light pulses over the receive port; the transceiver converts light impulses into electrical voltage that are sent over an internal TOE interface.

6 Documentation

Purchasers of the Owl Data Diode product receive the *Secure DFTS Secure Directory File Transfer System OEM Install User's Manual*, version N.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer conducted the same tests on each of the two versions of the Data Diode TOE: Version 1 and Version 2. The developer tested the interfaces identified in the Functional Specification and the High-Level Design. Each test is directly mapped to the security function tested. The developer tested both of the TOE Security Functions: Information Flow and TOE Self Protection.

The developer's tests completed successfully and the developer archived all test results in the Configuration Management repository.

The developer tested a pair of Data Diode Version 1 products and a pair of Data diode Version 2 products. Each test configuration consisted of two computers with an ATM network between them.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The Evaluation Team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run all of the tests that the developer performed. This ensured that the Evaluation Team adequately addressed both security functions. The Evaluation Team used the developer's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team conducted a brainstorming session to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team’s ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

The evaluated configuration consisted of a pair of Data Diode NIC network interface cards: one receive-only Data Diode NIC and one send-only Data Diode NIC. Each card was installed into a separate host and connected directly through a fiber optic cable. Additionally, to prevent a violation of the information flow policy, each host did not contain any additional Network Interface Cards.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The evaluation determined the Data Diode TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL) 2 requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for Owl Data Diode Part II" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> 6.1 Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Data Diode ST is a CC compliant ST.
>
> 6.2 The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:
>
> - Secure DFTS Secure Directory File Transfer System OEM Install User's Manual, Software Versions Msend 1.06, Mrecv 1.46, Driver Version 1.16, Documentation Revision N, October 18, 2002

the Data Diode TOE (Data Diode, Version 1, and Data Diode, Version 2) satisfies the Owl Computing Technologies Incorporated, Data Diode Security Target, Version 4.0, October 31, 2002.

10 Evaluator Comments/Recommendations

The evaluation team had no recommendations concerning the Data Diode TOE.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as Owl Computing Data Diode Common Criteria Security Target (EAL2), Version 4.0, 31 October 2002.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

ATM PHY. The ATM PHY is a high performance physical layer inter-face chip on the Data Diode NIC that generates and receives high-speed data streams. The ATM PHY receives 53-byte ATM cells from the SAR and produces analog signals that are passed to the transceiver. The interface into the ATM PHY from the SAR uses the UTOPIA protocol and the interface to the transceiver is SONET over analog power pins.

Data Diode. A network interface card consisting of three functional components; the "Segmentation and Reassembly Component (SAR)", the ATM physical packet interface chip (PHY), and the fiber optic communication interface (transceiver). These components are purchased from Integrated Device Technologies as a complete integrated card; then, the transceiver is modified by Owl to restrict communication to always receive or always send.

Data Diode Host. A network connected host where the network connections are provided by a single photodiode to send or a single light detector to receive.

Data Diode System. A pair of Data Diode NICs, one send-only and one receive-only, that are necessary to communicate from one Data Diode host to another Data diode Host.

Gateway. Also called a router, a gateway is a program or a special-purpose host that transfers network traffic with an identifiable network address from one network to another until the final destination is reached.

Host. A general term for a computer system. Once specific application software or hardware is installed on a host it assumes the role of Data Diode Host, gateway, receiving Host, Sending Host.

NIC. Network Interface Card that provides the physical interface to a network.

PCI Bus Interface. The Peripheral Component Interconnect bus interface is the device driver interface into the TOE from the host computer. The PCI Bus is an open architecture bus structure to control devices. Composed of a PCI BIOS, CPU, CPU cache, system cache, system memory, PCI Bridge, and Peripheral bus.

Receive-only Data Diode. An ATM SAR controller for PCI-based networking applications integrated circuit card that has been permanently modified by Owl so that the transceiver has no light source but does have a photo-detector.

Receiving Host. A host receiving network traffic though a receive-only Data Diode NIC that receives traffic from the network using a light detector to receive light impulses through a fiber-optic cable.

SAR. The Segmentation and Reassembly (SAR) chip on the Data Diode NIC accepts buffer information from the Peripheral Component Interconnect (PCI) bus interface on a host computer and produce complete 53-byte ATM cells from the buffered information it receives. These cells are sequential packets for the ATM physical packet interface chip (PHY).

Sending Host. A host sending network traffic though a send-only Data Diode NIC that sends traffic over the network using a photodiode to send light impulses through a fiber-optic cable.

Send-only Data Diode. An ATM SAR controller for PCI-based networking applications integrated circuit card that has been permanently modified by Owl so that the transceiver has no photo-detector but does have a light source.

SONET Protocol. The interface between the ATM PHY and the transceiver provides both Transmission Convergence (TC) and Physical Media Dependent (PMD) sub-layer functions of an ATM PHY suitable for ATM networks.

UTOPIA Protocol. The UTOPIA (Universal Test and Operations PHY Interface for ATM) interface is the protocol used between the SAR and the ATM PHY. UTOPIA is a standard data path handshake protocol.

14 Bibliography

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

- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, Parts 1, 2, and 3

- 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.

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

- Owl Computing Data Diode Common Criteria Security Target (EAL2), Version 4.0, 31 October 2002

- ETR Part 1 (Non-Proprietary)