Owl Computing Technologies®

White Paper

Secure. Reliable. Fast

# All Data Diodes Are Not Equal

Author: Jeffrey Menoher

Document Version: r03c
Publish Date: 9/6/2013

## Abstract

This paper describes various implementations of physical one-way data transfer systems, generically called data diodes, and shows that some implementations are clearly better than others in terms of quality of service, reliability, and security.

The paper provides a taxonomy of one-way designs and goes on to explain how specific hardware/software pipeline architectures achieve the highest performance in terms of both security and quality of service. The most secure pipeline architectures provide a deep protocol break that assures robust isolation between standard IP communication networks while simultaneously providing high assurance of data integrity.

The DualDiode Technology® one-way hardware pipeline architecture from Owl Computing Technologies, Inc (OwlCTI) is described in some detail, as it is widely deployed and has proven reliable and scalable in a variety of government agencies and commercial enterprises. Among all types of data diodes, DualDiode technology stands out for its high quality of service, high performance, and high degree of security. DualDiode technology also provides multi-channel data transfer concurrency for mixed data types.

## Problem

Sensitive high-value networks must remain isolated and yet provide data access to authorized users on demand, which increases risk of network attack.

## Solution

A well-engineered data diode mitigates network attack threats by restricting information flow to one-way data transfer only. Hardware diodes cannot be breached by network attack.

## Keywords

data diode, DualDiode, cyber threat mitigation, one-way data transfer

## Table of Contents

1 Introduction .......... 1
1.1 Overview .......... 1
1.2 Scope .......... 2
2 Taxonomy of Data Diodes .......... 2
2.1 One-Way Cable Assemblies .......... 3
2.1.1 Serial Communication .......... 3
2.1.2 Ethernet Fakeout .......... 3
2.2 Commercial Off The Shelf (COTS) Media Converter Systems .......... 4
2.3 Complex Software .......... 4
2.4 Firewall-Enabled One-Way Policy .......... 5
2.5 Intentionally-Designed One-Way Hardware .......... 6
3 Virtues of Intentionally-Designed Diodes .......... 6
3.1 Error Control .......... 6
3.2 Security Policy Administration .......... 6
3.3 Self-Protection .......... 7
4 Data Diode State of the Art .......... 7
4.1 The DualDiode .......... 7
4.1.1 DualDiode Hardware .......... 7
4.1.2 Deep Non-Routable Protocol Break .......... 9
4.1.3 Multichannel Data Transfer Concurrency .......... 10
4.1.4 Integrity Verification .......... 10
4.1.5 Defense In Depth .......... 10
4.2 Industry Standard Interfaces .......... 11
5 Summary .......... 11
6 References .......... 11

## Table of Figures

Figure 1: Conceptual One-Way Interface between Networks .......... 1
Figure 2: RS-232 with Modified Cable .......... 3
Figure 3: Ethernet Fakeout Method of Enforcing One-way Data Transfer .......... 3
Figure 4: Ethernet Fakeout with Split Fiber .......... 4
Figure 5: Software Enforced One-way Transfer Policy .......... 5
Figure 6: Paired Firewalls Configured to Enforce One-Way Dataflow Policy .......... 5
Figure 7: DualDiode Card Installation .......... 8
Figure 8: The DualDiode: One-Way Data Transfer Hardware at both Ends of Link .......... 8
Figure 9: DualDiode Non-Routable Protocol Break .......... 9
Figure 10: DualDiode Protocol Stack .......... 10

# 1 Introduction

Significant hardening of existing networks is achieved by separating inter-network communications into one-way data transfers. One-way data transfers naturally complement the inherently different security checks required for transferring data to (read-up) or from (read-down) any isolated high-security domain. Among other advantages, one-way data transfers deny the possibility of network probing for vulnerability; a prelude for cyber-attacks.

One-way data transfer systems are routinely used to allow cyber assets on isolated Industrial Control System (ICS) networks to export real-time operational state information to the Internet for purposes of remote monitoring, while protecting the ICS network from any inbound data flow that may include malware.

This paper describes various implementations of physical one-way data transfer systems, also generically called data diodes, and shows that some implementations are clearly better than others in terms of quality of service, reliability, and security.

## 1.1 Overview

Data diodes are one-way data transfer systems that are used to isolate high-security networks from external threats, while allowing them to import or export data at high speed in a controlled manner.

Data diodes are often compared with firewalls, which may be configured to pass data in one direction only. However, data diode security policies may be implemented in hardware, software, or both, and often bear little resemblance to firewalls.

When one-way data transfer security policy is rendered in hardware, it is physically impossible to send messages of any kind in the reverse direction. Physical one-way links cannot be hacked with software, and are used by the US Department of Defense (DoD) and Intelligence Community (IC) for isolating their high-security networks.

Hardware-enforced data diodes are considered the most secure. The US National Institute of Standards and Technology (NIST) provides a specific security control, AC-4.7, that describes hardware-enforced one-way information flow control as a threat-mitigation method.

A conceptual one-way interface between networks is shown below in Figure 1.

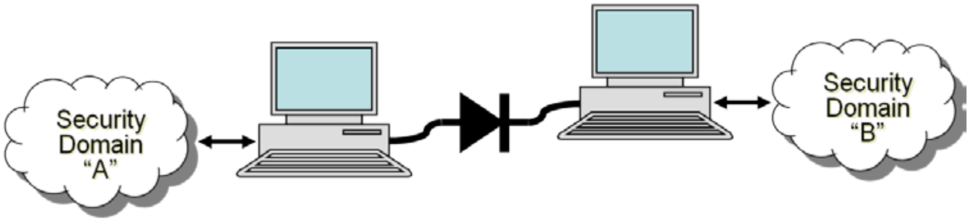

**Figure 1: Conceptual One-Way Interface between Networks**

It is easy to implement a simple hardware-enforced one-way data transfer system. It is more difficult to engineer a high-performance one-way data transfer system that presents high quality of service and is also easy to implement.

A simple implementation may be achieved by modifying an RS-232 serial communication cable by clipping the return wire. Douglas Jones of the University of Iowa describes such an implementation in detail [1].

Another class of devices similar in function to one-way mechanisms are data pumps. A practical implementation of a data pump includes multiple microprocessors and buffer memory, with the most published design being that of the US Naval Research Institute [2]. Jones and Bowersox reject data pumps not just because they are very complex, but also because they support a reverse channel for handshaking. In secure implementations, even a single bit transmitted in the reverse direction cannot be permitted [3].

## 1.2 Scope

This paper describes various implementations of physical one-way data transfer systems, and shows that some implementations are clearly better than others in terms of quality of service, reliability, and security.

Many data diode implementations have proven unreliable, slow, and insecure; in some cases openly exposing their one-way functionality to the point of requiring additional safeguards. This paper shows how these limitations can be overcome with the use of solid engineering design methods.

The paper provides a taxonomy of one-way designs and goes on to explain how hardware can complement operating system drivers and application proxy software to create a reliable, scalable, physical one-way "protocol break" between standard IP communication networks.

# 2 Taxonomy of Data Diodes

Traditional one-way transfers include the following general configuration types. Each type has unique advantages and disadvantages.

| Method | Examples |
|---|---|
| One-way cable assembly | RS-232 with clipped return line |
| Ethernet fakeout | Three servers partially connected with cables |
| Media converter | RJ45 to optical fiber, partially connected |
| Complex software programs | Trusted OS security policy rules, encryption |
| Firewall enabled policy | Box in the middle, UDP routing rules |
| One-way system hardware<br>(OwlCTI Implementation) | One-way hardware at send and receive points, DualDiode |

The one-way transfer configuration types listed above are complimentary in the sense that multiple types may be deployed concurrently in the same overall cross-border communication solution to reinforce security.

## 2.1 One-Way Cable Assemblies

### 2.1.1 Serial Communication

One-way cable assembly refers to a one-way security policy rendered in the communication cables (not in appliances or computing platforms) linking otherwise isolated networks. Historically, one-way data transfer has often been realized by modifying the cable of a two-way RS-232 connection (clipping the RX wire) as shown in Figure 2. In this and other cable assembly architectures, a change in cable arrangement, whether accidental or intentional, defeats the security policy. RS-232 suffers from low throughput and lack of data transfer integrity verification. An extension of the RS-232 method is the Sandia solution: an RS232 cable assembly with fiber conversion – US Patent 5,703,562 [4].

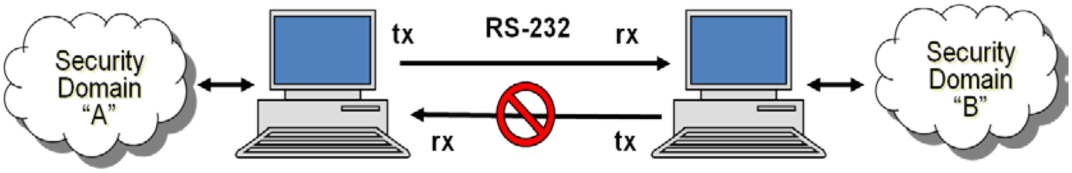

**Figure 2: RS-232 with Modified Cable**

### 2.1.2 Ethernet Fakeout

Another method to enforce one-way security policy using novel cable arrangements is the "Ethernet Fakeout" method, where two computers are partially connected using standard Ethernet two-way protocols and a third computer provides enough feedback to the sending computer to effect forward data transmission [5]. There are two methods popularly used.

The simpler Ethernet Fakeout method is illustrated below in Figure 3. This method provides just enough feedback capability to allow the Ethernet protocol to move data forward, but is inherently slow due to limitations in link-layer protocol implementation. Logically, it is very similar to the RS-232 method described above.

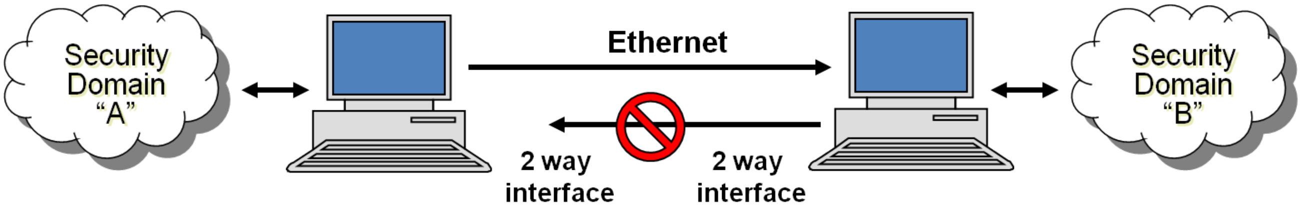

**Figure 3: Ethernet Fakeout Method of Enforcing One-way Data Transfer**

Ethernet Fakeout systems have been known to present poor quality of service and reliability, as implementations of individual network interfaces are designed to rely on acknowledgements for error correction. Both inlet and outlet interfaces maintain the same IP communication protocol, including IP routing information embedded in the data. In other words, there is no protocol break and the protocol is routable.

A second implementation of the Ethernet Fake-out method is shown below in Figure 4.

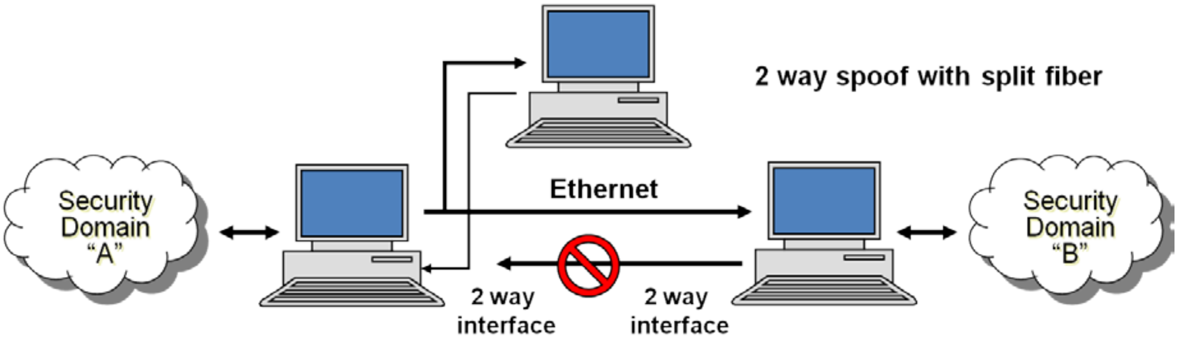

**Figure 4: Ethernet Fakeout with Split Fiber**

The second fakeout method uses a split fiber at the source domain outlet to allow the link-layer protocol to advance at higher speed (between the data source and "spoof" platform),m but still does not engage error-correction logic between the data source and the data destination. Once again, there is no protocol break, the protocol is routable, and the transmission method is prone to errors and data loss.

## 2.2 Commercial Off The Shelf (COTS) Media Converter Systems

A media converter is a simple networking device that makes it possible to connect two dissimilar media types such as twisted pair with fiber optic cabling. They are usually designed to connect high-bandwidth fiber optic cabling-based systems with legacy copper-based cabling systems. Typically, these are inherently two-way communication devices.

Utilizing unmodified, bidirectional, off-the-shelf products to enforce one-way security policies presents inherent vulnerabilities, similar in nature to one-way cable systems. Media converters remove the need for link-layer fakeout, but still fail to engage link-layer error correction, and they are just as prone to data loss as fake-out systems. Typical media converter systems maintain the same communication protocol across both inlet and outlet transmission media, including IP routing information embedded in the data. There is no protocol break, and the protocols are routable.

Media converters are typically connected in a manner similar to the RS-232 method described above. Since media converters provide few security functions, additional equipment must be integrated in order to achieve security goals. Once again, security of the entire system devolves to cable arrangements, which may be casually tampered with, and interfacing software, which is vulnerable to hacking.

## 2.3 Complex Software

Complex software programs refer to applications and operating system configurations that are designed to move data from one network to another in unidirectional fashion. Examples include configurable security policies that enforce specific read-only or write-only access rules in Trusted Solaris [6] and Security-Enhanced Linux [7] that are used to create secure gateways for information flow between network security domains. An example of software-enforced one-way security policy is illustrated in Figure 5.

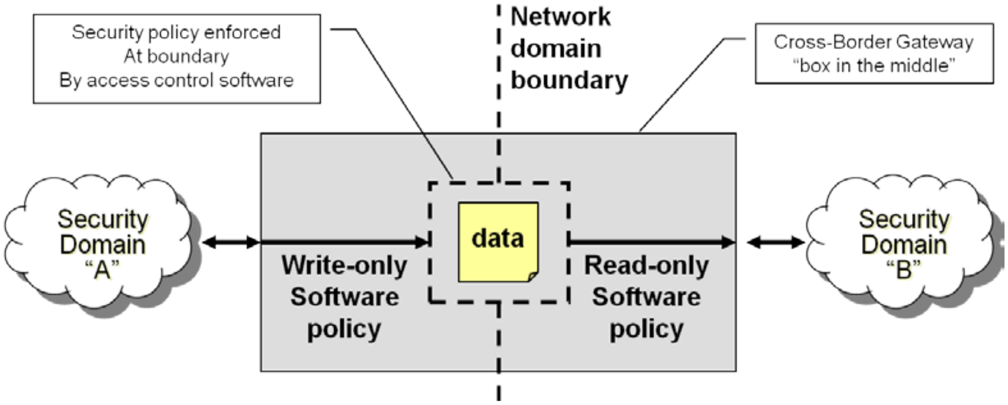

**Figure 5: Software Enforced One-way Transfer Policy**

Complex software solutions may or may not include encryption, which may be used to enforce one-way data transfer policies. Asymmetric encryption keys enable one user with write-only access to encrypt data while another user with read-only access uses a different key to decrypt, thus ensuring that readable data only flows in one direction.

Complex software security solutions, even well-crafted ones, are still subject to cyber attack and are often more vulnerable than they seem. The more complex the software, the more venues tend to be available for cyber attack. A recent paper shows how malicious software can compromise security of an operating system without root privileges in an undetectable manner [9, 10]. Administration of software solutions is also complicated by ambiguity in defining the cross-border boundary, where security policies are enforced in a platform or data storage area between otherwise-isolated network domains. Such architectures are often called "box-in-the-middle" designs and can be difficult to administer effectively.

## 2.4 Firewall-Enabled One-Way Policy

Firewall-enabled policy refers to a configuration of one or more firewalls to pass data in one direction only. While a single firewall may be configured to enforce a one-way data transfer security (passing its data from the inside to the outside interface), a pair of firewalls configured back-to-back provides stronger hardware implementation, as shown below in Figure 6. Firewalls configured back-to-back present their external faces to separate isolated networks.

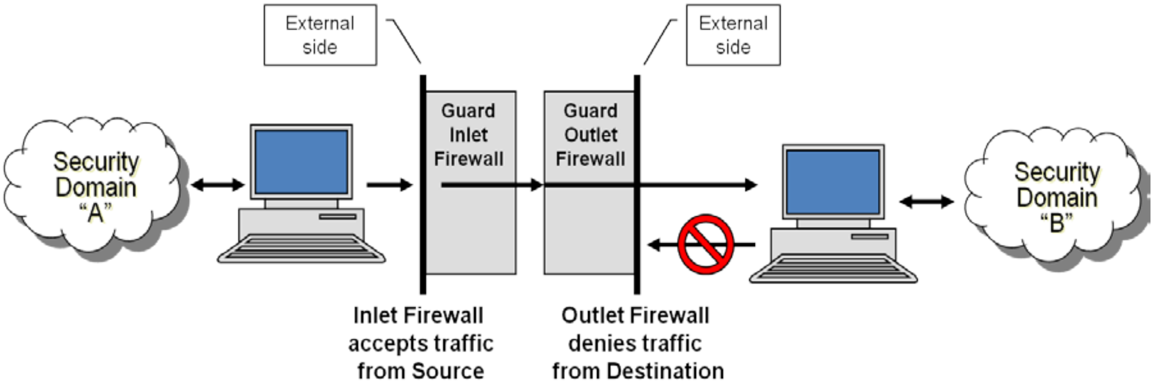

**Figure 6: Paired Firewalls Configured to Enforce One-Way Dataflow Policy**

In effect, the firewall solution is another complex software implementation on Commercial Off The Shelf (COTS) appliance platforms that continues to present a variety of vulnerabilities. Firewalls are associated with a variety of domain boundary ambiguities and administration issues.

Due to their commodity nature and high degree of configurability, firewalls are particularly prone to the "Swiss Cheese" security configuration problem. Here, an ever-increasing number of data routes and protocols are permitted to pass through the firewall, each providing new venues of software attack, until the firewall is almost completely permeable.

### 2.5 Intentionally-Designed One-Way Hardware

One-way system hardware refers to rendering a one-way security policy in one or more computing platforms using specially-designed hardware. In general, this is the most secure one-way policy enforcement method. Security is typically enforced by circuitry on the Communication Cards in either the Sender or Receiver or both. Architectures in which specialized hardware enforces one-way security policy at both terminals of a cable or fiber optic link are the most secure and are described in detail below.

The idea of one-way networking is not new. In April 1997, the UniDirectional Link Routing (UDLR) group was formed to "provide a solution for the support of unidirectional links on the Internet" [8].

## 3 Virtues of Intentionally-Designed Diodes

One-way data transfer systems present a unique set of technical and policy challenges, most of which are related to the absence of any form of message acknowledgement. For this reason, the highest performance and reliability is presented by systems whose hardware is intentionally-designed for one-way data transfer.

### 3.1 Error Control

One of the main challenges in creating a one-way transfer is managing error control. Data loss can occur when the receiving-side buffers are overrun in hardware or memory. In two-way communication system protocols, such as TCP, acknowledgements allow intelligent retransmission of data. In true one-way transfer systems, this is not possible.

Data loss can be minimized by the use of redundancy, either by sending the same data more than once, or by including additional information such as Forward Error Correction (FEC) codes to reconstruct lost data if enough good data has been received. Another technique is to pace the sent data with sufficient time resolution to ensure that the receiver is always able to receive data. Detection of lost data can be done at the hardware or software level by tagging data with sequence numbers to ensure detection of lost packets. Data within a packet can be verified through checksum, length checks, and format/schema validations. Correct reassembly of multiple packets can be verified through digest calculations such as SHA or MD5.

### 3.2 Security Policy Administration

Effective administration of a one-way inter-network data transfer system depends strongly on a clear definition of the inter-network boundary. Box-in-the-middle solutions present problems in this regard. When the network boundary runs through the internals of a separate platform or machine, it can be difficult to assign administration responsibilities for source-side and destination-side components of the cross-boundary communication system. Absence of effective administration and auditing oversight can create vulnerabilities.

A much better solution is to split the diode architecture into two separately-administered interfacing components, each administered separately in a manner compatible with the networks to which they are connected. Such split-platform pipeline architectures present numerous advantages in security and configurability.

## 3.3 Self-Protection

Security policies rendered in software or hardware are subject to various forms of attack by malicious entities. An attack may occur in the form of hands-on physical tampering, or via communications across networks. In order to protect security systems from physical attack, they are customarily located in protected areas subject to access by authorized personnel only.

One limitation of one-way cable assemblies and system hardware is that direct physical access can alter the hardware-enforced policies. External cable solutions present the greatest vulnerability to physical tampering, because cables can be easily removed and replaced. Hardware solutions embedded in gateway platforms are much better, with a chassis that can be locked and mounted within additional sealed enclosures.

In complex software and firewall-enabled policies, where the interfaces are already bidirectional, the one-way policy enforcement is inside the machine memory. Such software solutions must be deployed on hardened operating systems [6, 7] and in such a manner that they are resistant to cyber attack.

The best security policy implementation presents multiple layers of security rendered in both hardware and software. Such systems present “Defense in Depth” and are the most highly resistant to attack.

# 4 Data Diode State of the Art

There are numerous economic advantages in designing a data processing system from high-quality COTS technologies. Quality of service may be ensured at relatively low cost by carefully selecting the finest commercially-available components and protocols while integrating them in unique ways.

## 4.1 The DualDiode

This section provides details of a one-way system hardware design for one-way transfers as developed by Owl Computing Technologies, Inc [11].

To sustain line speed performance, the underlying hardware utilizes an Asynchronous Transfer Mode (ATM) protocol originally developed for high-bandwidth, long distance communication. ATM naturally comprises two separate one-way communication channels, each of which does not require acknowledgment. When implemented as a unidirectional point-to-point connection, there is no need for a two-way set up mechanism such as the MAC protocol for Ethernet.

### 4.1.1 DualDiode Hardware

DualDiode hardware comprises a pair of one-way communication cards that are specifically engineered to transfer data in one direction only. The Send-only card is installed in the Send Host Server platform, and the Receive-only card is installed in the Receive Host Server platform as shown below in Figure 7. The two cards (and the two platforms) communicate through a single optical fiber that connects the communication cards.

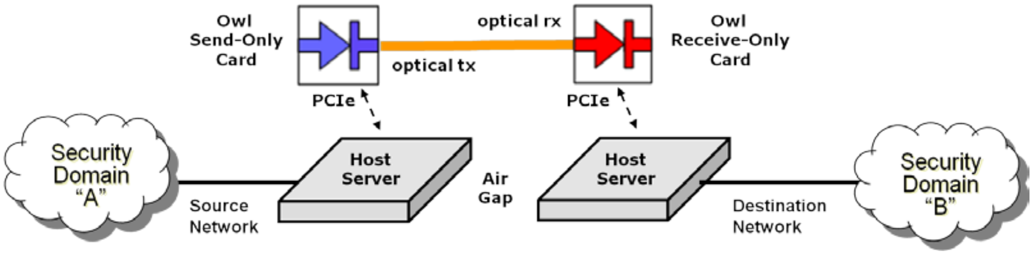

**Figure 7: DualDiode Card Installation**

Once cards are installed in their respective host servers, the servers operate as Send and Receive communication gateways for their respective networks as shown below in Figure 8.

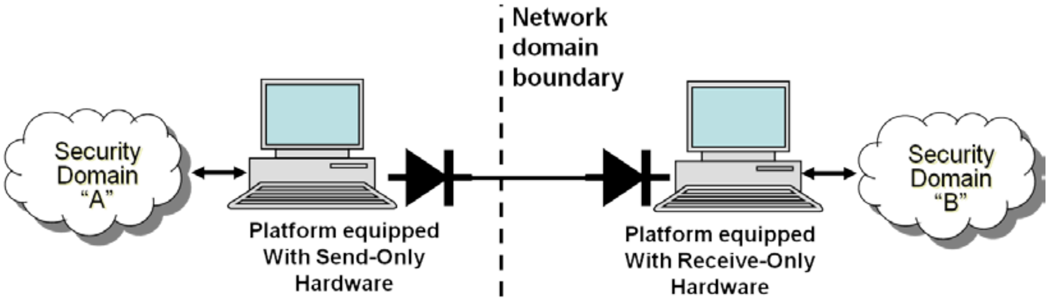

**Figure 8: The DualDiode: One-Way Data Transfer Hardware at both Ends of Link**

Note that the DualDiode system comprises a hardware pipeline architecture that contains two diodes and a clear network boundary located between the diodes. Should one diode fail, the other continues to hold; the connected networks remain highly isolated. All failures result in a state where no data transfer is possible, an inherently safe failure state.

The following diagram, Figure 9, shows the DualDiode hardware implementation in context with hardware driver software and data transfer interface software applications.

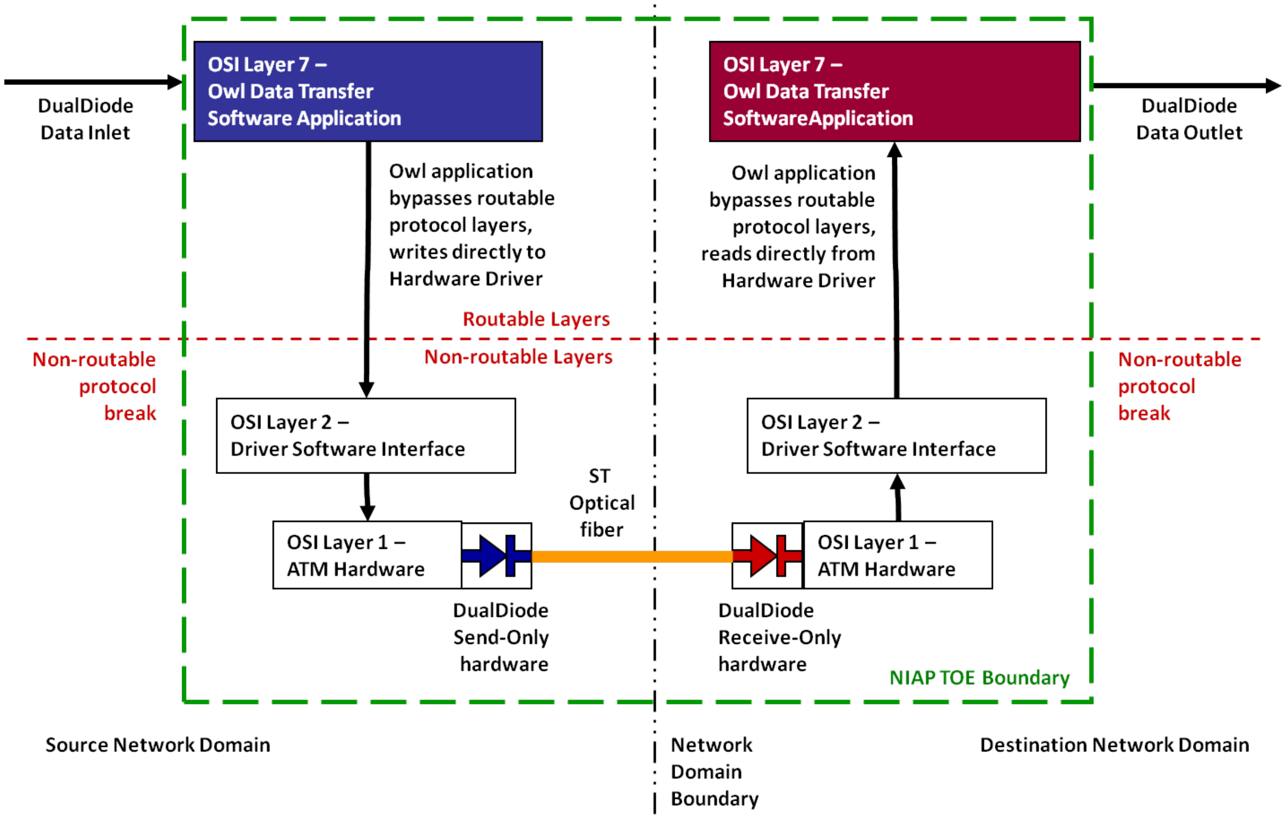
OSI Layer 7 – Owl Data Transfer Software Application
DualDiode Data Inlet
Owl application bypasses routable protocol layers, writes directly to Hardware Driver
OSI Layer 7 – Owl Data Transfer SoftwareApplication
DualDiode Data Outlet
Owl application bypasses routable protocol layers, reads directly from Hardware Driver
Routable Layers
Non-routable Layers
Non-routable protocol break
Non-routable protocol break
OSI Layer 2 – Driver Software Interface
OSI Layer 2 – Driver Software Interface
ST Optical fiber
OSI Layer 1 – ATM Hardware
OSI Layer 1 – ATM Hardware
DualDiode Send-Only hardware
DualDiode Receive-Only hardware
NIAP TOE Boundary
Source Network Domain
Network Domain Boundary
Destination Network Domain

**Figure 9: DualDiode Non-Routable Protocol Break**

### 4.1.2 Deep Non-Routable Protocol Break

ATM, an Open Systems Interconnection (OSI) layer 2 technology, is used to provide packetized data streaming with high quality of service and low latency.

ATM, as implemented in Owl hardware, is not routable (ATM cells do not retain source and destination information). IP information is not sent across the one-way link. Instead, static IP routes are defined by mapping tables that reside in the Send server and Receive server on either side of the diode interface. Neither table alone can be used to construct the other, and neither table alone provides IP routing information that might compromise security of the overall system.

The DualDiode protocol stack is shown below in Figure 10. Note that data integrity is verified at each step during the data reassembly process [17].

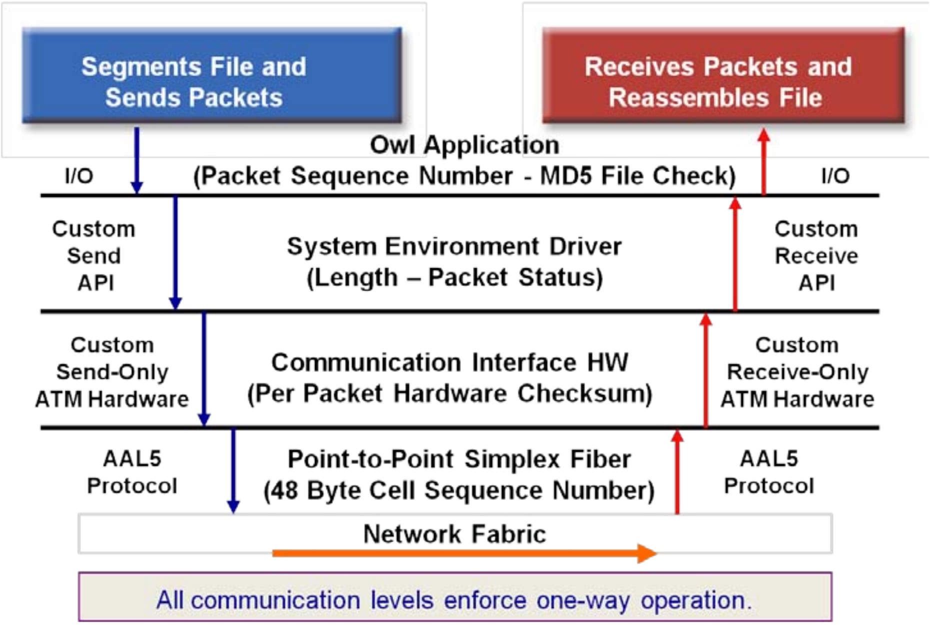
Segments File and Sends Packets
Receives Packets and Reassembles File
Owl Application
I/O
(Packet Sequence Number - MD5 File Check)
I/O
Custom Send API
System Environment Driver (Length – Packet Status)
Custom Receive API
Custom Send-Only ATM Hardware
Communication Interface HW (Per Packet Hardware Checksum)
Custom Receive-Only ATM Hardware
AAL5 Protocol
Point-to-Point Simplex Fiber (48 Byte Cell Sequence Number)
AAL5 Protocol
Network Fabric
All communication levels enforce one-way operation.

**Figure 10: DualDiode Protocol Stack**

### 4.1.3 Multichannel Data Transfer Concurrency

ATM natively contains mechanisms that enable multiple independent virtual channel connections that can provide different quality of service pacing levels to match traffic shaping requirements of concurrent data transfers.

DualDiode technology also provides multichannel data transfer concurrency for mixed data types. Files, UDP packets, TCP streams, and IP packets may all be streamed through a single hardware instance of DualDiode technology without data loss.

### 4.1.4 Integrity Verification

At the ATM cell level, data integrity is verified in hardware using CRC methods and advanced hash algorithms at higher levels. DualDiode transfer systems do not lose data, and no forward error correction methods are required.

Multiple levels of data integrity checking, along with inherently high quality of service of ATM technology, enable the DualDiode to move terabyte-size files consistently and without error, as well as moving large numbers of very small files efficiently.

### 4.1.5 Defense In Depth

In DualDiode systems, each level of the system supports and/or redundantly enforces one-way operation. The entire system operates as an assured hardware pipeline. Since there are two hardware-enforced data diodes in the system, either side can suffer a total breach of hardware and software security, and the diode on the other side will still hold.

In order to provide additional security, Owl software applications in each server platform are also arranged in an assured pipeline architecture. This is to insulate the data diode hardware from any vulnerabilities inherent in the communications stack.

At each step of the way, the hardware and software ensure that the only failure mode is no transfer of data. In other words, if the DualDiode fails, it fails into a safe state. This is validated in Common Criteria testing referenced by NIAP at [12, 13, 14, 15]. Since the security features are not modifiable using any method of software execution, the only attack is physical substitution.

## 4.2 Industry Standard Interfaces

Data rendered as files or as streaming packets may be transferred through the DualDiode seamlessly using industry-standard protocols. When DualDiode technology is used in streaming applications, edge servers operate like routers.

Software applications at the data diode inlet perform IP filtering, and will deny socket access to machines whose IP addresses are not recognized, if configured to do so. Files may be transferred directly through the DualDiode or via TCP proxies. From a data integrity verification perspective, the processes are the same.

A variety of special-purpose industrial communication protocols are supported by modular interface software, including the OSIsoft PI historian and MODBUS.

# 5 Summary

This paper describes various implementations of physical one-way data transfer systems, and shows that some implementations are clearly better than others in terms of quality of service, reliability, and security.

While many data diode implementations have proven unreliable, slow, and insecure, this paper has shown how specific hardware/software pipeline architectures achieve the highest performance in terms of both security and quality of service. The most-secure pipeline architectures provide a deep protocol break that ensures robust isolation between standard IP communication networks while simultaneously providing high assurance of data integrity. DualDiode technology implements these features.

Among all types of data diode, DualDiode technology stands out for its high quality of service, high performance, and high degree of security. DualDiode technology also provides multichannel data transfer concurrency for mixed data types.

# 6 References

1. *http://homepage.cs.uiowa.edu/~jones/voting/diode/*
2. Myong H. Kang, Ira S. Moskowitz, and Stanley Chincheck, “The Pump: A Decade of Covert Fun”, Center for High Assurance Computer Systems, Naval Research Laboratory, Washington, DC, 20375; URL *http://www.acsac.org/2005/papers/Kang.pdf*
3. Douglas W. Jones, Tom C. Bowersox, “Secure Data Export and Auditing using Data Diodes”. USENIX/ACCURATE Electronic Voting Technology 06, 2006 Vancouver, B.C., Canada
4. Curt A. Nilsen, “Method for transferring data from an unsecured computer to a secured computer”, United States Patent 5,703,562, Sandia Corporation, December 30, 1997
5. Jason Westmacott, “Unidirectional Networking”, GIAC Security Essential Certification Practical Assignment Version 1Ab, © SANS Institute 2003
6. Glenn Faden, “Solaris Trusted Extensions, Architectural Overview”, © April 2006, Sun Microsystems, Inc. Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN, Web *sun.com*

7. Chris Runge, “The Path to Multi-Level Security in Red Hat Enterprise Linux”, 2006 Red Hat, Inc, available via URL: *http://www.redhat.com*
8. Jason Westmacott, “Unidirectional Networking”, GIAC Security Essential Certification Practical Assignment Version 1Ab, © SANS Institute 2003
9. Dan Tsafrir, Yoav Etsion and Dror G. Geitelson, “General-Purpose Timing: The Failure of Periodic Timers”, Technical Report 2005-6, School of Computer Science and Engineering, the Hebrew University February 2005, Jerusalem, Israel
10. Dan Tsafrir, Yoav Etsion, Dror G. Feitelson, “Secretly Monopolizing the CPU Without Superuser Privileges”, 16th USENIX Security Symposium
11. *http://www.owlcti.com/products/how-dual-diode-works.html*
12. “Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification”, Owl Computing Technologies, Inc., Dec 8, 2006, available through URL *http://www.niap-ccevs.org/cc-scheme/vpl* and from Owl Computing Technologies, Inc.
13. “Validation report: Owl Computing Technologies Data Diode Network Interface Card Version 4”, Report Number CCEVS-VR-07-0018, February 01, 2007, Version 1.0, National Information Assurance Partnership (NIAP), available through URL *http://www.niap-ccevs.org/cc-scheme/vpl*
14. “Assurance Continuity Maintenance Report for Owl Computing Technologies Dual Diode Network Interface Card Version 6”, Maintenance Report Number CCEVS-VR-07-0018a, Oct 16, 2007, National Information Assurance Partnership (NIAP), available through URL *http://www.niap-ccevs.org/cc-scheme/vpl*
15. NIAP Common Criteria, URL *http://www.niap-ccevs.org/cc-scheme/*
16. J. Menoher, R, Mraz, “CWID 2007 Data Diode Case Study”, Invited ACSAC 2007 Presentation
17. J. Menoher, “Technical Notes on Data Integrity Verification”, OwlCTI internal White Paper, Sept 22, 2010

END OF DOCUMENT