

## INTRODUCTION

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 way.

Significant hardening of existing networks are achieved by separating inter-network communications into one-way data transfers. One-way data transfers naturally compliment 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. Intelligent utilization of one-way data transfer also simplifies creation of data archives whose contents cannot be deleted, corrupted, or repudiated.

Data diodes are often compared with firewalls, but their security policies are most often rendered in the wiring or hardware and they do not operate the same way. One-way communications across a two-way channel poses an unacceptable security risk for data to leak in the reverse direction. It is physically impossible to send messages of any kind in the reverse direction through a hardware-enforced data diode. Physical one-way links cannot be hacked with software, and are used by the government intelligence community for isolating their high security networks.

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

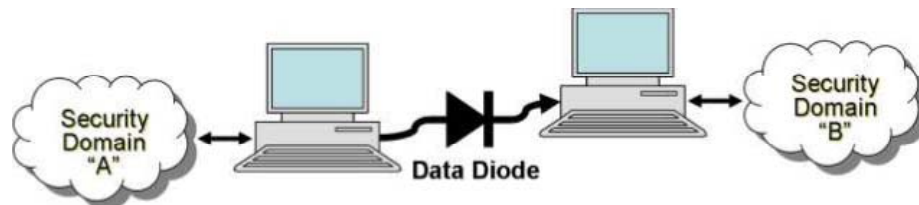


Figure 1: Conceptual One-way Interface between Networks

A Cross Border Solution may be defined as software and/or hardware that mediates controlled transfers of information across security boundaries. It is trusted to allow sharing of data across boundaries. It enforces a defined security policy.

## MOTIVATION AND RELATED WORK

The need to move data securely from one domain to another, while protecting the security levels of both environments, is central to the operation of sharing information between government entities. Whether distributing information from centralized, highly secure IT centers or bringing in information from unsecured sources, IT managers require absolute assurance that the cross border communication path is free from security compromise.

The need for secure Cross Border information sharing is increasing, driven by the requirements for international cooperation in fields of economics, law enforcement, and counter terrorism. File sizes and channel capacity requirements are increasing for all communication venues. High resolution imagery and real-time streaming media are also straining existing communication infrastructures to their limits.

The simplistic design of a secure one-way transfer system maps to well-established models of data security and integrity, which are described in greater detail in the following text. One-way transfer design also maps to higher levels of government certification and accreditation processes such as the Evaluation Assurance Level (EAL) system which is part of the 'Common Criteria' [21], developed by and accepted by the international community as the baseline standard for security specifications and evaluations. Furthermore, these devices integrate well for information sharing between sensitive networks, such as coalition communications and cross boarder communications within Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) requirements.

An intriguing example of the pervasive applications of data diodes is in the domain of electronic voting. Jones and Bowersox [18] provide a prototype design description of a low bandwidth data diode for pervasive use in voting systems. In this system, the data diode is used to publish timely election results to an open system such as the internet. To safeguard the voting systems the vendors currently recommend using an air gap with 'sneakernet technology' to carry data across the gap. Unfortunately, this requires the use of write-once media but is wasteful in resources and time. 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. The most published design being that of the US Naval Research Institute [14]. Jones and Bowersox reject data pumps not only because they are very complex, but, because they support a reverse channel for handshaking. In secure implementations, even a single bit transmitted in the reverse direction cannot be permitted.

## IP CONVENTIONS AS RELATED TO ONE-WAY DATA TRANSFER

The Open Systems Interconnection (OSI) Reference Model for communications and computer network protocol design has seven layers, listed from top (layer 7) to bottom (layer 1) as follows: Application, Presentation, Session, Transport, Network, Data Link, and Physical layers. A layer is a collection of related functions that provides services to the layer above it and receives service from the layer below it. Internet Protocol (IP) is a layer 3 'Network' protocol. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) rely on IP services and are layer 4 'Transport' protocols.

IP itself is a connectionless protocol. A connectionless protocol is a protocol in which there is no persistent logical connection established between the points that are communicating, and each unit of data received is treated as being independent. UDP is a connectionless protocol over IP, and is naturally suited to implementing one-way communications. Delivery of UDP packets is not assured, and no acknowledgment is required when UDP packets are received. TCP is a connection-oriented protocol over IP, and normally requires two-way communications. The TCP protocol offers a significant benefit of assured data delivery. It will be shown later in this paper how the benefits of one-way communication may be integrated with TCP connections using TCP proxies.

Media Access Control (MAC) address is a Layer 2 identifier that serves to identify a particular piece of network hardware. Thus network cards (or built-in network adapters) in two different computers will have different MAC addresses. Layer 2 network protocols like MAC address are designed to be globally unique. Address Resolution Protocol (ARP) is used to translate IP (Layer 3) addresses to MAC addresses.

In large scale telecommunication infrastructures, Asynchronous Transfer Mode (ATM), a layer 2 technology, is used to provide packetized data streaming with high quality of service and low latency. Significantly, ATM segregates all two-way communications into independent one-way data paths. ATM relies on cell-switching technology. ATM cells have a fixed length of 53 bytes, which allows for very fast switching. ATM creates pathways between end nodes, called virtual circuits, which are

identified by the VPI /VCI values. The ATM Adaption Layer 5 (AAL5) provides point-to-point and point-to-multipoint (ATM layer) connections used to carry computer data such as TCP/IP.

### MODELS OF DATA SECURITY AND INTEGRITY

The Bell-LaPadula model [9,10,11] focuses on data confidentiality and access to classified information. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. The clearance/classification scheme is characterized by the phrase: "no read up, no write down". Such a security policy prevents unauthorized access to secret information.

The Biba Data Integrity Model [12] describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Data integrity models favor a read-up write-down data transfer paradigm -- one-way downward.

Note that both of these security models favor one-way data transfer security policies, though they point in different directions. The Biba Data Integrity model favors a one-way deployment that pushes data from a high integrity source to lower integrity destination. The Data Security model favors one-way push from a low confidentiality domain to a high confidentiality domain.

Another model, the Assured Pipeline model by Boebert and Kain [13], provides a formalism for defining data flow controls to assure overall system security. This refers to the case where some function (like crypto) absolutely positively has to happen between a predecessor operation (message prep) and a successor (message release). Assured Pipeline architectures may be constructed by connecting a sequence of processing nodes with one-way data transfer systems. A combination of one-way data transfer systems and processor security controls assure that the processing steps occur in proper order and cannot be bypassed. A recent paper by Zeldovich [17] describes how the imposition of data flow security controls can secure applications built from mostly untrusted code.

### TAXONOMY OF ONE-WAY DATA TRANSFER SYSTEMS

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

Method	Examples
Sneakernet	Manual transfer of CDS, disks
One-way cable assembly	RS-232, Ethernet variants
Complex software programs	Trusted OS security policy rules, encryption
Firewall enabled policy	Box in the middle, UDP routing rules
One-way system hardware	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.

## SNEAKERNET

Sneakernet refers to the practice of manually moving data from one network to another on a portable physical medium such as a write-once CD or tape. While sneakernet throughput can be very high (data throughput at a Blockbuster video checkout counter is a compelling example), sneakernet is also prone to high latency, and the media used to effect the cross domain data transfer must often be destroyed afterward according to standing security policies. An additional consideration is that human-enforced security policies are known to be vulnerable to human error [16]. Human error and human slowness are strong justifications for automating secure data transfer functions to the greatest extent possible.



Figure 2: Sneakernet - Manual Transfer of Physical Storage Media across Air Gap

## ONE-WAY CABLE ASSEMBLY

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 3. 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.

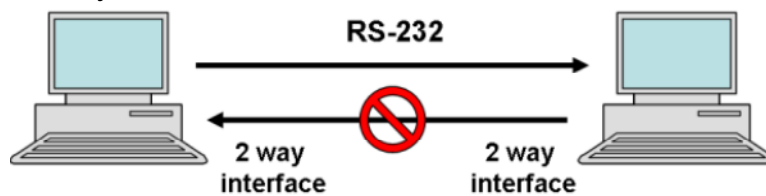


Figure 3: RS-232 with Modified Cable

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 [22]. The Ethernet Fakeout method is illustrated in Figure 4.

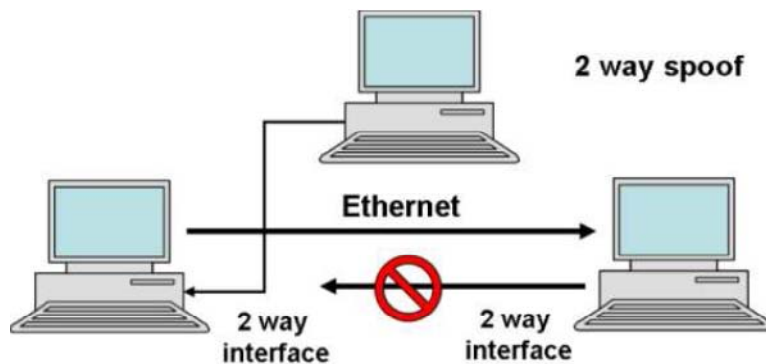


Figure 4: Ethernet Fakeout Method of Enforcing One-way Data Transfer

## COMPLEX SOFTWARE PROGRAMS

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 [23] and Secure Linux [24] 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.

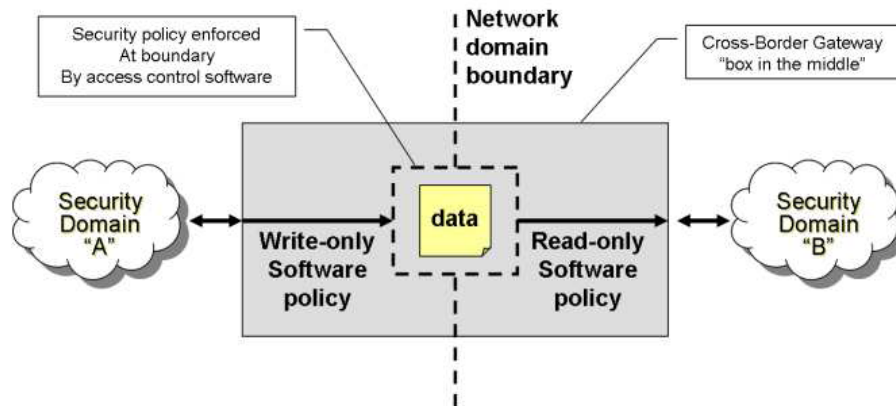


Figure 5: Software Enforced One-way Transfer Policy

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 assuring 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 may compromise security of an operating system without root privileges in an undetectable manner [28,29]. Administration of software solutions is also complicated by ambiguity in defining the cross-border boundary when 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 may be difficult to administer effectively.

## FIREWALL ENABLED POLICY

Firewall enabled policy refers to a configuration of one or more firewalls to pass data in one direction only. A pair of firewalls may be configured to operate like a hardened one-way data transfer device as shown in Figure 6. Firewalls configured back-to-back present their external faces to separate isolated networks. In effect, this is another box-in-the-middle configuration using Commercial Off-The-Shelf (COTS) appliances that is subject to domain boundary ambiguity and associated administration issues.

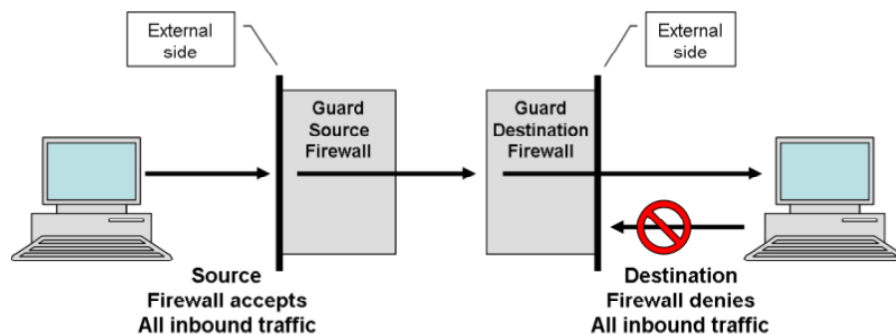


Figure 6: Paired Firewalls Configured to Enforce One-Way Dataflow Policy

## ONE-WAY SYSTEM 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 network interface cards in either the Sender or Receiver or both. A hardware-enforced Send-only architecture is shown in Figure 7. 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.

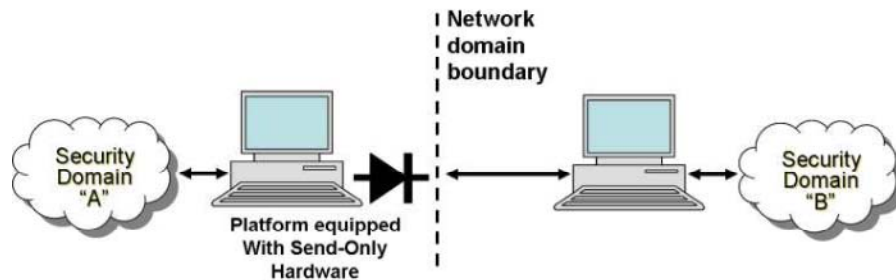


Figure 7: One-way Link Enforced with Send-only Special Hardware

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]. In March 2001, the UDLR issued RFC 3077 describing a mechanism to emulate full bidirectional connectivity between nodes that are directly connected by a unidirectional link [5].

## CHALLENGES

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. Additional challenges are related to the special-purpose character of many one-way data transfer systems, which were created by organizations whose security requirements are extreme. The most significant challenges are described below.

## MANAGING 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, we have the ability to acknowledge transfers to 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 send data with sufficient time resolution to insure 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 insure 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 done through digest calculations such as SHA or MD5.

## PERFORMANCE

One-way transfer systems have traditionally been the bottleneck for communication projects. Many one-way systems that were but from components optimized for two-way transfers, such as Firewall Enabled Policy and One-way Cable Assembly systems, do not incorporate sufficient memory buffers to support line rate one-way transfers. The designs were done with the knowledge that return line acknowledgments would pace the data to insure receive buffer availability; the result being that these systems needed to operate at reduced speed capability to support one-way transfers.

One-way systems designed with Trusted OS Policy configuration use tagging of each individual data record to enforce data movement policies. This adds overhead and delay in every hop as the data moves through the system.

Sneakernet operation is unique in that buffering of data is not a problem but extremely long latencies in the movement of data can be seen as the human in the loop transports the data.

## **SECURITY POLICY ADMINISTRATION**

Effective administration of a one-way cross border 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.

## **SELF PROTECTION**

Security policies rendered in software or hardware are subject to various forms of attack by malicious entities. Security policies rendered in physical hardware must be deployed in environments where physical security is provided. External cable solutions present the greatest vulnerability to physical tampering. Hardware solutions embedded in gateway platforms are much better. Software solutions must be deployed on hardened operating systems [23,24] and in such a manner that they are resistant to cyber attack. Malware scanning and intrusion detection systems are routinely deployed in conjunction with one-way data transfer systems to augment security assurance for the cross border data transfer solution.

## **INHERENT VULNERABILITIES REQUIRING MITIGATIONS**

One limitation of One-way Cable Assemblies and System Hardware is that direct physical access can alter the hardware-enforced policies. In Complex Software and Firewall enabled policies, where the interfaces are already bi-directional, the one-way policy enforcement is inside the machine memory. Sneakernet policy enforcement is as good as the human in the loop.

## **VALIDATION FOR CERTIFICATION, ACCREDITATION AND AUDITS**

A physical focused piece of hardware that enforces one-way movement is simpler to validate than a trusted operating system or embedded software used within Complex Software or Firewalls, respectively. Also, a orthogonal, independent piece of hardware is not impacted by software updates to the operating system or firewall application. Whereas, software-based one-way systems may require retesting after software upgrades and patches are provided.

## **PROJECTS VS. PRODUCTS**

Utilizing bi-directional off-the-shelf products to enforce one-way security policies in software presents a project mentality. This being that the policy is created for a specific role, implementation, or installation. To reuse these mechanisms in follow-on installations would require examination of the entire system to ensure the policies are correctly enforced. Enforcing the one-way security policy in separate orthogonal hardware means that other aspects can change with the security enforcement stays the same.

## ENGINEERING DESIGN CASE STUDY

In this section, we provide details of a One-way System Hardware design for one-way transfers as developed by Owl Computing Technologies [26]. To sustain line speed performance, the underlying hardware utilizes an Asynchronous Transfer Mode (ATM) protocol used for long distance communication, since acknowledgments are not required when using the AAL5 [27] transport layer. This is done without the need for a two-way set up mechanism such as the MAC protocol for Ethernet.

ATM natively contains a quality of service (QOS) mechanism in the hardware send logic. This offers fine grain pacing support at the 48-byte data cell level. This enables the hardware to accurately pace data to the receiver independent of software and operating system timers, which have been known to be problematic in maintaining accuracy of long periods of sustained activity. Additionally, multiple independent virtual channel connections can be provided different QOS pacing levels to match traffic shaping requirements of concurrent transfers.

Figure 8 displays an interesting extension of the Hardware Enforced Methodology incorporated in the system. The one-way policy is enforced at both domains of the point to point communications. This, in effect, creates 2 data diodes in series and creates a DualDiode. Each hardware mechanism is protected within the server housing rather than outside, as in Cable Assembly or Fire Wall Box security. The advantage is that either side can independently validate and verify their one-way policy independent of the other domain. This saves time and effort in auditing installations when the domains are truly communicating across borders or disjoint government agencies.

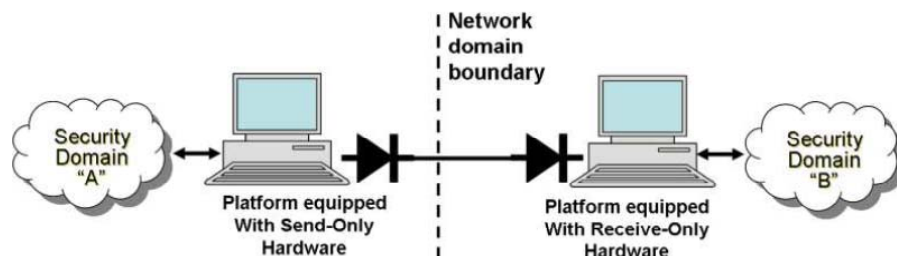


Figure 8: The DualDiode – Hardware-enforced One-way Data Transfer at both Ends of Cross Domain Link

Figure 9 displays additional features of this implementation, where each level of the system supports and/or redundantly enforces one-way operation. In the case of a file transfer, the send side (blue) segments a file into packets with headers and metadata. The send application inserts sequence numbers, naming information about the file and a digest calculation for data verification. These packets are passed to a system driver that validates the length and returns a packet status to the original application. The return status information also communicates QOS information for pacing the data. The system driver is independent of the existing communication stack used for traditional TCP/IP communications. This is to insulate the data diode hardware from any vulnerabilities inherent in the communications stack.

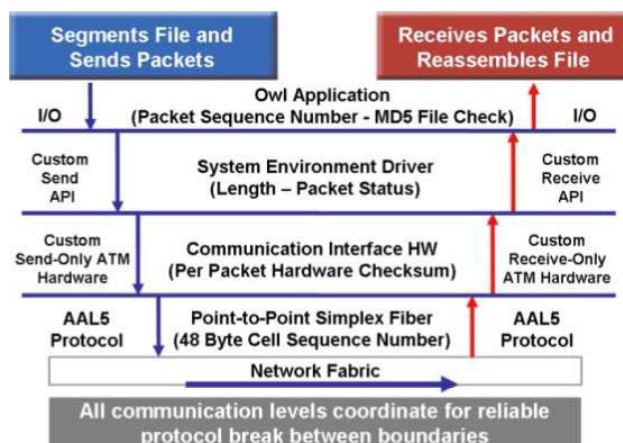


Figure 9: Data Diode Operation at Various Network Layers

The data packet is queued for transport to the network through the ATM network hardware. The hardware itself is state machine-based, rather than CPU programmed, to reduce the possibility of errors in program downloads and the improper enforcement of the one-way policy. Packets are scheduled for the link layer transport at 48-byte cell granularity. These are then received by the complementary receive hardware.

Network cells are then reassembled into the original communication packets and a hardware checksum is validated prior to writing these to the host. The host driver then examines the length and packet status from the hardware and, if good, forwards the data to the receiving application. The receive (red) application reassembles the packets into the original file and validates the file arrived intact.

At each step of the way, the hardware and software coordinates such that the only failure mode is no transfer of data. This is validated in Common Criteria Testing reference by NIAP at [21,30,31,32]. Since the security features are not modifiable, the only attack is physical substitution.

### CROSS BOUNDARY CASE STUDY

DualDiodes from Owl Computing were deployed in an international information sharing exercise known as the Coalition Warrior Interoperability Demonstration (CWID). CWID is an annual international information sharing exercise between NATO governments, and between military, intelligence, and civilian emergency response networks within and across government borders [25].

In CWID 2007, DualDiodes were deployed in Trials 1.56 'DualDiode' and 3.27 'Integrated Information Management System (IIMS)' in the general configuration shown in Figure 10. Information was shared between armed services personnel of the US, Canada, and New Zealand without compromising network security. DualDiodes were integrated with antivirus scanning software, with mandatory human review process enforcement software, and with SharePoint Web Servers from Microsoft Corporation in order to provide web-based user interfaces.

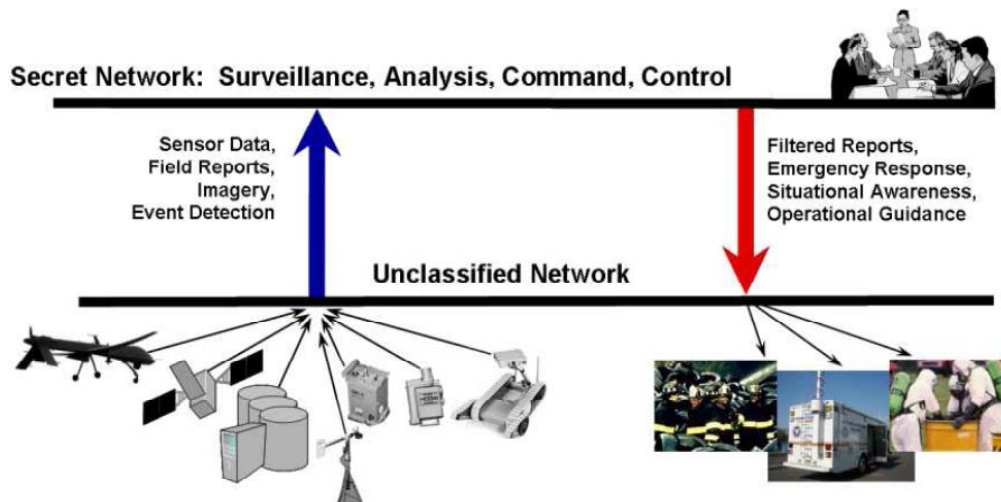


Figure 10: CWID 2007 Data Diode Deployment in Command/Control Communications Infrastructure

## TCP Proxies for Network Interfacing

TCP/IP socket-based proxy software may be deployed on both ends of a hardware enforced Data Diode, providing seamless connectivity and easy integration into standard networks as shown in Figure 11.

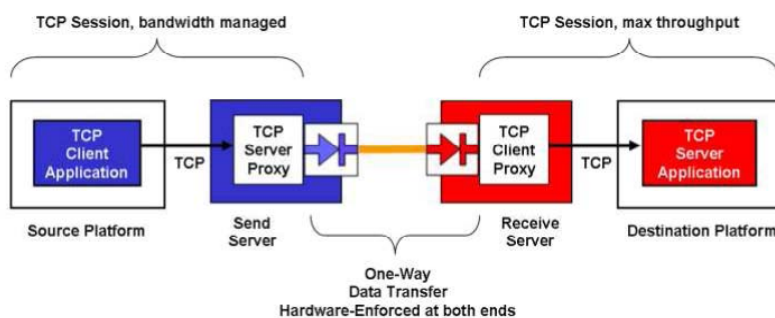


Figure 11: TCP Proxies on Both Sides of Data Diode

Once TCP socket connectivity is established on both ends of the DualDiode link, TCP packet payloads are passed across the data diode as a continuous stream without passing IP information across the link. IP routes are defined in the form of complimentary channel mapping tables. The incoming IP sources addresses are mapped to anonymized channel numbers in a configuration file residing at the data diode inlet. Channel numbers are mapped to destination IP addresses in a separate configuration file located at the data diode outlet. Taken together, both configuration files establish static IP routes through the data diode system. Neither configuration file alone can be used to construct a complete static route that might compromise security of the overall system.

A TCP/IP client program in the user source machine connects to the inlet of the data diode, which operates as a TCP/IP server proxy. The TCP server proxy at the data diode inlet performs IP filtering, and will deny socket access to machines whose IP addresses are not recognized, if configured to do so. The data diode outlet operates as a TCP/IP client proxy and requests a socket connection to TCP/IP destination. All data relayed over the data diode is transferred to the destination machine over a TCP/IP socket. Closing the socket on the data diode inlet will close the socket on the data diode outlet.

## SUMMARY

Data diodes or one-way transfer systems have been in place for secure sharing of information for many years. These have traditionally been projects developed to move specific data for specific platforms. Due to recent events, the need for secure cross border information sharing is increasing in volume, variety and frequency to the point that these traditional solutions are being overrun. A more formal and systematic approach to this area is required. To this end, this paper provides a taxonomy definition of one-way architecture types. Namely, Sneakernet, Complex Software, Firewall Box, Cable Assembly, and System Hardware. The challenges of creating one-way architectures over traditional bidirectional methods are presented. Case studies of a state-of-the-art one-way transfer hardware design, a cross boarder application scenario, and how two-way communication protocols such as TCP can be proxied across a one-way link.

### About Owl Computing Technologies, Inc.

Owl Computing Technologies, Inc. is a privately owned and funded U.S. company. Owl delivers NIAP Common Criteria EAL-4 certified one-way cross domain systems & electronic perimeter defense solutions to transport and protect an organization's most sensitive data between discrete domains of varying security levels and policies. Information sharing Secured by Owl® is enforced with Owl Computing proprietary DualDiode® data diode technology. DualDiode one-way transfer systems guards against data leakage and protects networks from unauthorized access. Owl systems meet the highest levels of information protection within the U.S. Department of Defense, the Intelligence community, & the Power Generation industry, delivering secure, reliable, information transfer of multiple data sources and types across single DualDiode systems -- any file size or data type. [www.owlcti.com](http://www.owlcti.com)

## References

1. RFC 768: User Datagram Protocol. URL: <http://www.ietf.org/rfc/rfc0768.txt>
2. RFC 791: Internet Protocol. URL: <http://www.ietf.org/rfc/rfc0791.txt>
3. RFC 793: Transmission Control Protocol. URL: <http://www.ietf.org/rfc/rfc0793.txt>
4. RFC 826: Address Resolution Protocol. URL: <http://www.ietf.org/rfc/rfc0826.txt>
5. RFC 3077: A Link-Layer Tunneling Mechanism for Unidirectional Links. URL: <http://www.ietf.org/rfc/rfc3077.txt>
6. RFC 3164: The BSD syslog Protocol. URL: <http://www.ietf.org/rfc/rfc3164.txt>
7. RFC 3452: Forward Error Correction (FEC) Building Block. URL: <http://www.ietf.org/rfc/rfc0793.txt>
8. UniDirectional Link Routing Group. URL: <http://www.udcast.com/udlr/> URL: <http://www.ietf.org/html.charters/udlr-charter.html>
9. D. Elliott Bell, Leonard J. LaPadula, 'Secure Computer Systems: Mathematical Foundations', (c)1973, MITRE Corporation
10. D. Elliott Bell, Leonard J. LaPadula, 'Secure Computer Systems: Unified Exposition and MULTICS Interpretation', (c) 1976, MITRE Corporation
11. D. Elliott Bell, 'Looking Back at the Bell-La Padula Model', ACSAC conference, December 2005, Proc. 21st Annual Computer Security Applications Conference: 337-351. Doc. 10.1109/CSAC.2005.37. URL: [www.acsac.org/2005/papers/](http://www.acsac.org/2005/papers/)
12. K. J. Biba, 'Integrity Considerations for Secure Computer Systems', MTR-3153, The Mitre Corporation, April 1977
13. William Earl Boebert, R.Y. Kain. 'A Practical Alternative to Hierarchical Integrity Policies'. Proceedings of the 8th National Computer Security Conference, 1985
14. J. Menoher, R. Mraz, 'CWID 2007 Data Diode Case Study', Invited ACSAC 2007 Presentation
15. J. Menoher, J. Hope, A. Holmes, R. Cooper, R. Mraz, 'Transferring Large Files in Real-Time', Owl Computing Technologies, Inc., presented at the 2nd International Workshop on Operating System Interference in High Performance Applications (OSIHPA) 2006, in conjunction with the PACT-06 <http://www.pactconf.org/> September 16-20, 2006, Seattle, WA. Paper available at URL: <http://osihpa.cs.utep.edu/>
16. Lorrie Faith Cranor, 'A Framework for Reasoning About the Human in the Loop'. Carnegie Mellon University. URL: <http://www.usenix.org/events/upsec08/tech/>
17. Nikolai Zeldovich, Silas Boyd-Wickizer, and David Mazieres, 'Securing Distributed Systems with Information Flow Control'. Stanford University. URL: <http://www.usenix.org/event/nsdi08/tech/zeldovich.html>
18. 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

19. 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>
20. 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
21. NIAP Common Criteria, URL: <http://www.niap-ccevs.org/cc-scheme/>
22. Jason Westmacott, 'Unidirectional Networking', GIAC Security Essential Certification Practical Assignment Version 1Ab, (c) SANS Institute 2003
23. Glenn Faden, 'Solaris Trusted Extensions, Architectural Overview', (c) 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
24. Chris Runge, 'The Path to Multi-Level Security in Red Hat Enterprise Linux', 2006 Red Hat, Inc, available via URL: <http://www.redhat.com>
25. Coalition Warrior Interoperability Demonstration (CWID). URL: <http://www.cwid.js.mil/c/extranet/home>
26. <http://www.owlcti.com/products/how-dual-diode-works.html>
27. <http://www.ipmplsforum.org/tech/atm-specs.shtml>
28. Dan Tsafir, 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
29. Dan Tsafir, Yoav Etsion, Dror G. Geitelson, 'Secretly Monopolizing the CPU Without Superuser Privileges', 16th USENIX Security Symposium
30. '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.
31. '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>
32. '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>