DSTO

Data Diodes (U)

M. Stevens and M. Pope

DEPARTMENT ◆ OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Data Diodes (U)

M. Stevens and M. Pope

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-TR-0209

ABSTRACT (U)

Technical Report

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables more sensitive or highly classified computer networks to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction. This paper discusses several ways to implement a data diode and some implications of the alternatives.

RELEASE LIMITATION

Access additional to the initial distribution list is limited to the Defence Community of Australia, UK, USA, CAN and NZ. Others MUST be referred to the Chief, Information Technology Division, Electronics and Surveillance Research Laboratory.

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

DSTO Electronics and Surveilla ce Research Laboratory
PO Box 1500
Salisbury, South Australia, 5108

Telephone: (08) 259 7053
Fax: (08) 259 5619

AR-009-336
July 1995

DOD ONLY

Embassy of Australia
Attn: Joan Bliss
Head. Pub. Sec. -Def/Sci.
1601 Massachusetts Ave., NW
Washington, DC 20036

Conditions of Release and Disposal

1. *This document is the property of the Australian Government; the information it contains is released for defence purposes only and must not be disseminated beyond the stated distribution without prior approval.*

2. *The document and information it contains must be handled in accordance with security regulations applying in the country of lodgement, downgrading instructions must be observed and delimitation is only with specific approval of the Releasing Authority as given in the Secondary Distribution statement.*

3. *This information may be subject to privately owned rights.*

4. *The officer in possession of this document is responsible for its safe custody. When no longer required this document should be destroyed and notification sent to: Senior Librarian, Defence Science and Technology Organisation Salisbury Research Library.*

Data Diodes

Executive Summary

Data diodes will become increasingly important with any growth in demand for connectivity of classified and open networks. These devices give one way connectivity and allow for the automatic transmission of information from a less secure network to a more secure network without compromising the security of the latter network.

Data diodes using modified RS-232 serial lines have been in use for some time, but have several flaws in their design. This paper shows how data diodes can be constructed using optical fibre and optical components. Several ways to implement an optical data diode are described and implications of the alternatives are discussed. Optical data diodes could be evaluated to very high levels of assurance, thus potentially could be accredited to allow one way connectivity between unclassified hostile networks and Top Secret codeword networks.

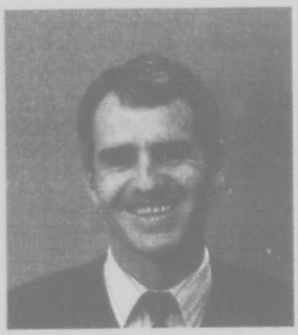
The main aim of this paper is to show that it is relatively easy to construct a data diode, with high assurance, out of commercial off the shelf products. It is also demonstrated that electronic mail and news services can be implemented through the data diode.

This paper demonstrates that even though data diodes prevent communication in one direction, it is still possible to have protocols which require bidirectional handshaking appear to be transmitted through the data diode. This is achieved by having software, which is cognizant of the data diode, watch valid protocol transactions occur and then reconstruct the events on the high side of the data diode. For such communication methods to succeed, it is critical that the gateway machine, on the high side of the data diode, be able to keep up with the flow of data from both its own native network and those arriving from the data diode.

Further investigation and testing is required to improve the reliability of service through the experimental data diode which has been constructed.

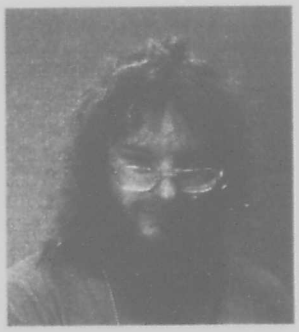
THIS PAGE IS INTENTIONALLY LEFT BLANK.

Authors



Malcolm W. Stevens
Information Technology Division

Malcolm Stevens graduated from the University of Adelaide with a Bachelor of Science (Computing and Applied Mathematics) in 1981, and a Bachelor of Science with First Class Honours (Applied Mathematics) in 1982. He then worked as the computing tutor in the Applied Mathematics Department while studying for a Ph. D. (Numerical Modelling of Tides), which was awarded in 1991. Malcolm joined Trusted Computer Systems Group at DSTO in 1990 and is currently supporting the Head of Group as Manager TCS Group. His main research interests are computer and network security.



Michael Pope
Information Technology Division

Michael Pope graduated from University of Adelaide with a B.E., B.Sc., and Ph.D. (1992) in Electrical Engineering in the field of integrated circuit design and simulation. At DSTO he initially worked on fine-grained parallel computer architectures for Computer Architectures Group, and then joined Trusted Computer Systems Group in 1993 to work on computer security.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Contents

Figures

THIS PAGE IS INTENTIONALLY LEFT BLANK.

1. INTRODUCTION

1.1 Purpose of a Data Diode

A data diode is a computer security device that restricts the communication along a network connection between two points so that data can only be transmitted in one direction. The data diode is configured to guarantee that no data can be passed, either explicitly or covertly, in the opposite direction.

The data diode can be a permanent connection and can eliminate the need for an air gap or the need for tape transfer of data being moved from a network classified at a lower level to a network classified at a higher level.

A typical situation where a data diode is useful has a connection between two systems of different classification levels, where data from the lower classified system is to be sent to the higher classified system. This is depicted in Figure 1. Under security restrictions, these networks cannot normally be connected due to the threat of highly classified data being observed by users on the lower classified network.

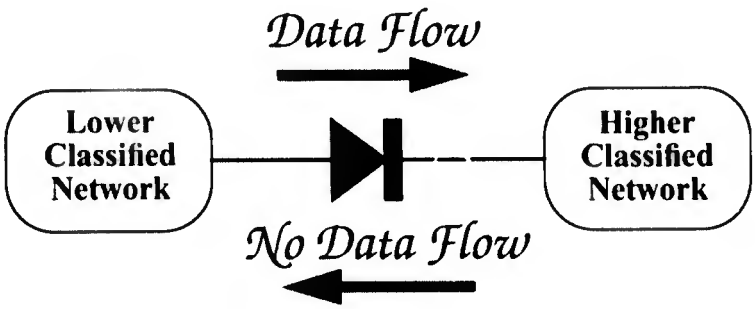


Figure 1 Depiction of a Data Diode

1.2 Assurance of a Data Diode

The assurance of a data diode measures the strength of guarantee that the data diode will behave in the expected manner and can be trusted to do so. The assurance levels E0 to E6 of the Information Technology Security Evaluation Criteria (ITSEC) [1] can be used to measure the assurance of a data diode. Mechanisms to restrict covert channels are generally imposed at levels above the E3 evaluation level. This implies that it is possible for an E3 data diode to leak data from the higher classified network through covert means without failing the accreditation. In some situations this would not be acceptable and higher assurance levels would be required.

1.3 Physical Protection

Since a data diode is essentially a one way path between two networks and it is assumed that the two networks have differing security requirements, the data diode may need to be physically protected to avoid the threat of reconfiguration or bypass.

2. ELECTRONIC CABLE DATA DIODES

A number of computer networks currently use a data diode in the form of an RS232 communication line with one of the transmit lines physically cut to ensure no transmission along that particular line. This is depicted in Figure 2.

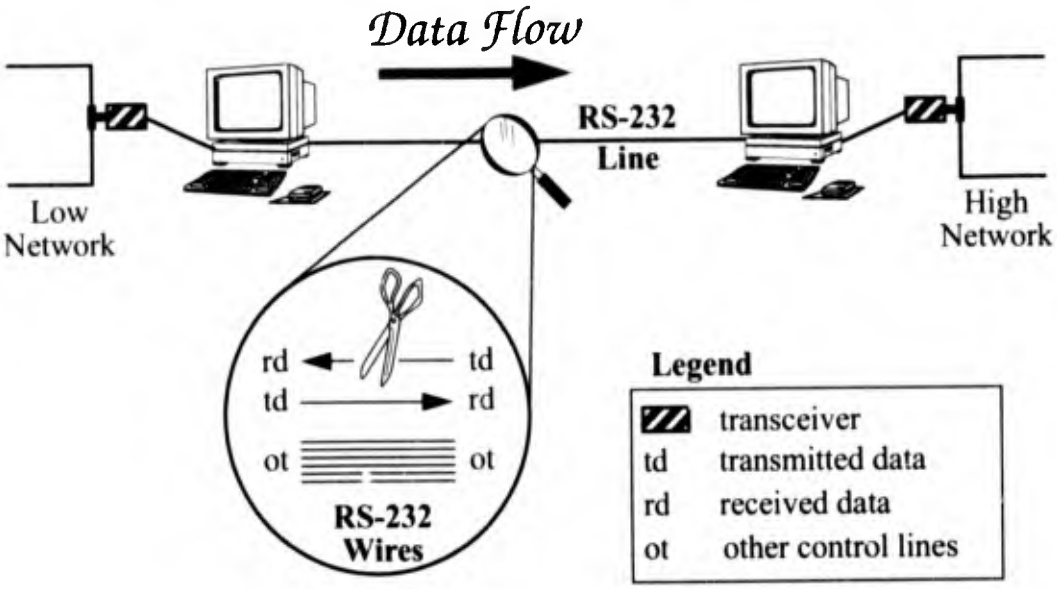


Figure 2 Using a modified RS232 Line as a Data Diode

2.1 *Disadvantages of this (RS-232) approach*

The main disadvantage with this configuration for a data diode is that although no data can be transmitted along the cut wire (that is, no data can be sent along the wire from the RS232 transmit port on the high side of the line to the receive port on the low side of the wire), it is possible for data to be communicated from the high network to the low network along the other wires of the RS232 line. This could be exploited by co-operating processes on each of the machines connected to the RS232 line, that is, the two processes could transmit data in a covert manner. This would suggest that a data diode of this configuration would be most useful in situations requiring evaluation levels less than or equal to E3.

Another disadvantage of this design is that the bandwidth of the data diode link is restricted to the bandwidth of an RS232 line, which is relatively low.

2.2 *Increasing the assurance of this Data Diode*

In order to increase the assurance that covert channels in this type of data diode cannot be exploited, something must be done to stop cooperating processes communicating the "wrong" way through the data diode. One way that this can be done is by enforcing strict administrative, procedural, and physical control over the two machines on either end of the data diode. Such measures might include the following rules:

1. Both gateway machines should have no user accounts and may be accessed only by network security managers.
2. Auditing of the activity on both machines should be conducted.

3. Only cleared personnel should have physical access to the machines and the data diode.

Thus the collective assurance of the cut RS232 line and the computers connected to it, if they are controlled with appropriate measures, could conceivably be accredited for use in situations normally requiring assurance levels greater than an E3.

2.3 *Physical protection*

Since the design and correct operation of the data diode relies on the modified RS232 cable and its configuration to the two computers, it is necessary to prevent reconfiguration of both the cables and the computers. This could be achieved by locating the data diode and the two computers in a room with controlled access. Server rooms often have such controlled access.

3. OPTICAL DATA DIODES

3.1 Background

Trusted Computer Systems group has constructed an optical data diode from "commercial off the shelf" hardware products and special purpose software. It is possible to construct numerous different variations of the design. The following description is specific to the particular way in which the data diode is constructed and to the particular workstations to which it is connected. The objective of this paper is to establish "proof of concept" and not to exhaustively discover all aspects of the concept.

3.2 Principles of Design

The basic principle, that this design relies on, is the fact that fibre optic transceivers transmit data along optical fibre in one direction. For normal two way communication there are two single fibres, each carrying data in one direction. This is shown in Figure 3, which depicts a fibre optic repeater and a fibre optic receiver used in a gateway configuration between two Local Area Networks (LANs). If one of the optical fibres is physically removed then clearly no data can flow in that direction. The assurance of this scheme can be physically guaranteed to an extremely high level.

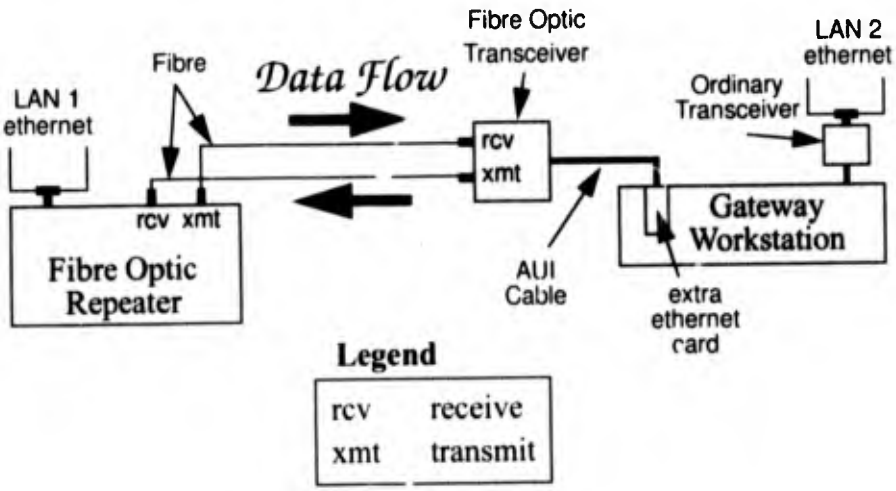


Figure 3 Using a fibre optic repeater and transceiver in a gateway configuration

3.3 A design that works

The following data diode design is a "proof of concept" system, thus there may be better or more cost effective ways of constructing a system with such functionality. This specific design allows the connection of two Ethernet networks.

The components that were used in the data diode are listed below:

- 2 Transceivers – Netcor NC 31F (Fibre Optic Transceiver).
- 1 Repeater – Netcor UCR 507 (Universal Repeater).
- 1 Ethernet card to suit the workstation.

- Appropriate fibre optic and coaxial cables and connectors for ethernet.
- Gateway software on the high side workstation.

The design of the optical data diode is depicted in Figure 4.

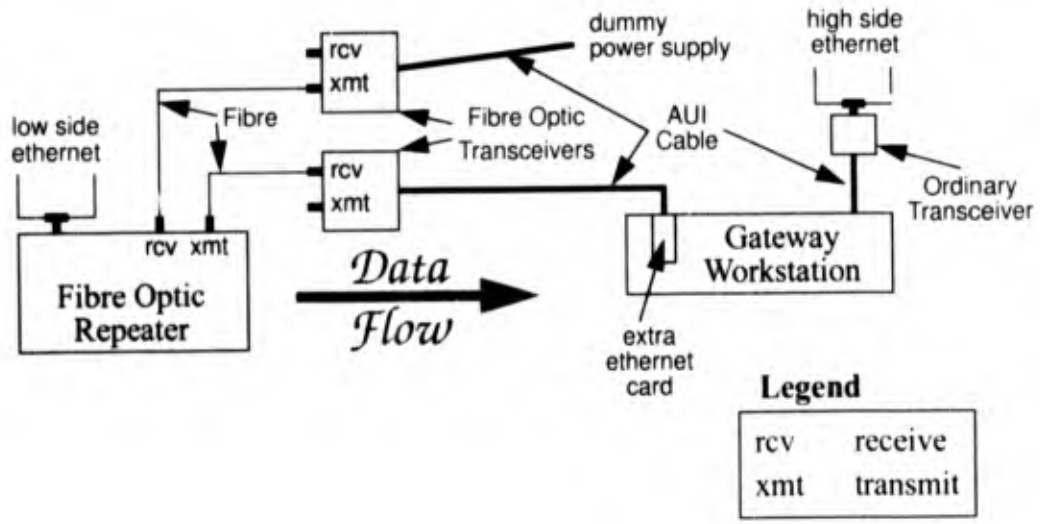


Figure 4 Fibre Optic Data Diode

Some points that should be noted about this design are listed below:

1. It was not possible to simply remove the appropriate optical fibre from the configuration shown in Figure 3. The second transceiver and power supply were required to convince the repeater to work. If this second transceiver was not connected the repeater would detect a failure and would not transmit data to the other transceiver. The second transceiver cannot supply data but does supply a carrier signal which is required by the repeater.
2. The UCR-507 repeater manual states that the repeater "is fully compliant with Ethernet and IEEE 802.3 specifications for a network utilizing the CSMA/CD protocol" and "the repeater operates at the network physical layer, receiving ethernet frames on any of it's receiving ports and regenerating and retransmitting to all other ports which have been installed into the unit". Thus the fibre optic transceiver receives data asynchronously and is not dependant on the repeater or other transceiver for timing signals.
3. Therefore, the repeater copies all ethernet packets that it sees on the low side network through the fibre optic receiver to the extra ethernet card in the workstation. That is all activity on the low side network can be seen on the high side network.
4. The workstation with the extra ethernet card is configured as a gateway machine. Thus this machine will need to monitor all the data that it receives from the data diode and decide if any of the packets need to be transferred to the high network.
5. The fibre optic repeater could be replaced by a fibre optic bridge, which could then assist the gateway workstation in filtering packets.

3.4 *Assurance of the Data Diode*

The assurance of this data diode relies on the following two facts:

1. There is no fibre optic link between the transmit port of the transceiver on the receiving side of the data diode and the receiving port of the transceiver on the transmitting side of the data diode. This can be verified visually.
2. The transceiver on the receiving side of the data diode has not been tampered with. Or more specifically, the detecting diode of the receiving port of this transceiver has not been replaced with a component that can both transmit and receive. This should be easily verifiable.

If both the above facts can be verified then the correct operation of the data diode is assured to a very high level. This means that you do not have to rely on the correct operation or assurance of any of the other components used in the data diode, as is the case with the RS-232 data diode.

3.5 *Quality of Service Through the Data Diode*

The major inherent flaw in this scheme is that the majority of protocols operating over ethernet networks require significant amounts of handshaking between sender and receiver to ensure reliable transmission, which is impossible without a bidirectional data path. At first sight, this would appear to totally eliminate the possibility of providing bidirectional services like those based on TCP/IP, across the data diode link. Fortunately this is not entirely true. Certainly any service that naturally relies on a bidirectional flow of data cannot be initiated from the high side, but appropriate monitoring daemons may react to transactions occurring on the low side and pass the relevant data to the appropriate high side counterparts.

For example (see Figure 5): consider the case of electronic mail. In our configuration, this is transmitted using the TCP/IP based Simple Mail

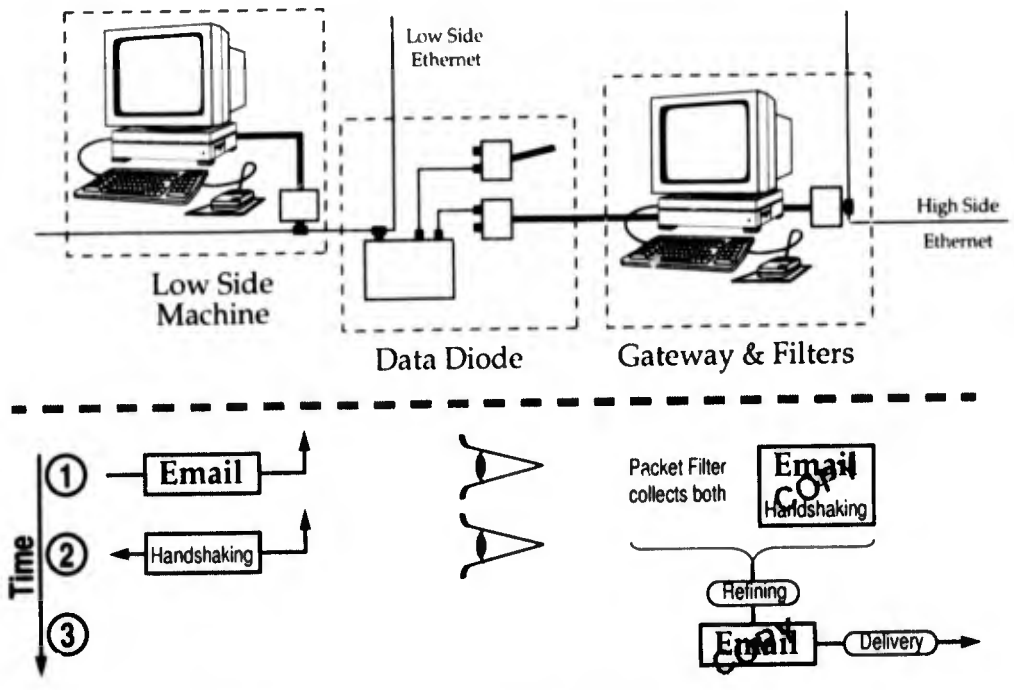


Figure 5 Time line of email delivery through a data diode

Transmission Protocol (SMTP). As noted in the previous section, the high side network sees all the packets that are transmitted on the low side network. When mail arrives, via the low side ethernet, to a machine connected to the low side ethernet (number ① in Figure 5), all the SMTP packets can be collected by a packet filter on the high side. The mail has been addressed to the low side machine and this machine responds appropriately according to the bidirectional protocols used (number ②). The high side gateway simply observes the mail transaction taking place (numbers ① and ②). It can then strip off, layer by layer, the overlying ethernet, IP, TCP and SMTP protocol information, leaving the raw e-mail message (number ③). If the mail delivery transaction between low side sender and receiver machines appears to be valid, the message can be checked to see if the intended recipient is a user with access to the high side network, and if so, it can be forwarded through the conventional mail delivery agent on the high side network. This arrangement has proved useful to the authors, who while having access to two such networks, typically spend more time on the higher secured network and thus were less able to respond in a timely fashion to messages originating on the less secure net. Note though that this configuration results in duplication of messages. If this is a problem the low side mail system could be configured to discard mail for a high side recipient. The mail would still be received on the high side as long as a the low side performs a valid SMTP transaction on first receipt of the message before discarding the message. Indeed the recipient need only be known to the low side system as an alias in the mail system database.

3.6 Low Side Choke

Thus, is has been demonstrated that even though data diodes prevent communication in one direction, it is still possible to have protocols which require bidirectional handshaking appear to be transmitted through the data diode. This is achieved by having software, which is cognizant of the data diode, watch valid protocol transactions occur and then reconstruct the events on the high side of the data diode. However the sending process still does not know if the sent message has been received on the high side of the data diode and the receiving process does not know if it has received everything that was sent. For such communication methods to succeed, it is critical that the gateway machine, on the high side of the data diode, be able to keep up with the flow of ethernet packets from both its own native network and those arriving from the data diode.

Providing a SMTP service is thus a relatively easy case as SMTP is a simple, verbose protocol and most messages are short (typically less than one kilobyte). These conditions rarely stress the packet filtering software. Nevertheless, cases have been noted of large documents (containing images or other binary encoded data) encapsulated as e-mail and successfully mailed on the low side network, which were not completely reconstructed on the high side due to loss of packets through buffer overrun as the filtering software and I/O drivers struggled to keep up.

In order to prevent packet lossage it is necessary for the packets to be processed on the high side gateway faster than they are generated on the low side. This either means that the high side has sufficient processing speed or alternatively the packet emanation on the low side can be artificially slowed to create a low side "choke". One way to assure that the gateway workstation on the high side network has sufficient processing speed is by having it powerful enough and making it a system dedicated to its gateway function.

3.7 *Tamperproofing or physical protection*

Since the design and correct operation of the data diode relies on the absence of a fibre optic cable, it is necessary to stop the threat of reconfiguring or bypassing of the data diode. This is the case with any data diode and the threat could typically be minimised by locating the data diode in a room with controlled access. Often a server room has such controlled access.

Depending on the risks involved and the situation in which the data diode is used, the data diode could require some sort of tamperproofing mechanism in order to detect any malicious reconfiguration.

4. ANOTHER POSSIBLE DESIGN

Another possible design for the data diode is where two machines communicate directly with each other through their ethernet cards connected to fibre optic transceivers. This is depicted in Figure 6. The communication from the high side of the network to the low side of the network is cut by removing the appropriate fibre optic cable between the two optical transceivers.

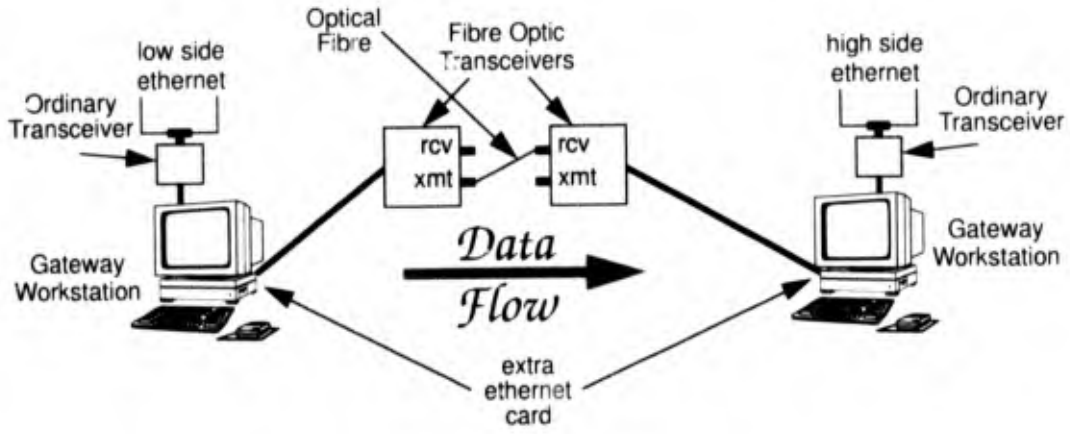


Figure 6 Alternate design for Fibre Optic Data Diode

The major difference of this design to that depicted in Figure 4 is that the fibre optic repeater is not required and another computer with extra ethernet card is connected to the second transceiver.

Some points that should be noted about the design are listed below:

1. As yet, this configuration has not been tested to check for implementation difficulties, but in principle this design should be viable.
2. Both of the gateway workstations require extra ethernet cards and need to be configured to act as gateways to filter and forward data packets that they see on each of their own ethernet cards.
3. As with the previous data diode design, true bidirectional protocols, cannot be used over this configuration.

One advantage of this design is that if the two computers are already required for other network connections, such as integrity filters (for example, a STUBS gateway [2], [3]), then the only components needed to construct the data diode are the two fibre optic transceivers, two extra ethernet cards and appropriate cabling.

5. SUMMARY

5.1 Current Achievement

Trusted Computer Systems Group has shown that it is relatively easy to construct a data diode, with high assurance, out of commercial off the shelf products.

The group has also been able to implement electronic mail and news services through the data diode.

5.2 Future Work

Further investigation and testing is required to improve the reliability of service through the data diode. Experimentation would be needed to discover what configurations are most suitable for the various services required and under which circumstances these configurations are most appropriate. This may depend on the frequency and size of the data to be transmitted or on the protocols that deliver the data to the gateway machine on the low security side of the data diode.

6. REFERENCES

[1] European Communities - Commission. *Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria*, Version 1.2, ISBN 92-826-3004-8, Catalogue number CD-71-91-502-EN-C, June 1991.

[2] Anderson M., Hayman K., Marriott D., Nayda L., Yesberg J. and Beahan B. *P1 Prototype Stubs: an Overview.* Electronics Research Laboratory (DSTO), Research Report - ERL-0668-RR, 1992.

[3] AWA Defence Industries (AWADI) - *"Stubs Operational Concept Document (OCD)"* Issue 2, 489A00000001.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Data Diodes

M. Stevens and M. Pope

(DSTO-TR-0209)

DISTRIBUTION

Copy No.

DEPARTMENT OF DEFENCE

Defence Science and Technology Organisation

Chief Defence Scientist and members of the) DSTO Central Office Executive)	1 shared copy
Counsellor, Defence Science, London	Doc Cont Data Sht
Counsellor, Defence Science, Washington	Doc Cont Data Sht
Scientific Advisor, POLCOM	1 Copy
Senior Defence Scientific Adviser	1 Copy
Assistant Secretary Scientific Analysis	1 Copy
Director, Aeronautical and Maritime Research Laboratory	1 Copy
Chief, Air Operations Division	Doc Cont Data Sht
Chief, Maritime Operations Division	Doc Cont Data Sht
Chief, Weapons System Division	Doc Cont Data Sht
Navy Scientific Adviser	1 Copy
Air Force Scientific Adviser	1 Copy
Scientific Adviser, Army	1 Copy

Electronic and Surveillance Research Laboratory

Director, Electronic and Surveillance Research Laboratory	1 Copy
Chief, Information Technology Division	1 Copy
Chief, Communications Division	Doc Cont Data Sht
Chief, Electronic Warfare Division	Doc Cont Data Sht
Chief, Land, Space and Optoelectronics Division	Doc Cont Data Sht
Chief, High Frequency Radar Division	Doc Cont Data Sht
Chief, Microwave Radar Division	Doc Cont Data Sht
Research Leader, Command & Control and Intelligence Systems	1 Copy
Research Leader, Military Computing Systems	1 Copy
Manager, Human Computer Interaction Laboratory	Doc Cont Data Sht
Executive Officer, Information Technology Division	Doc Cont Data Sht
Head, Software Engineering Group	Doc Cont Data Sht
Head, Trusted Computer Systems Group	1 Copy
Head, Command Support Systems Group	1 Copy
Head, Intelligence Systems Group	1 Copy
Head, Systems Simulation and Assessment Group	Doc Cont Data Sht
Head, Exercise Analysis Group	Doc Cont Data Sht
Head, C3I Systems Engineering Group	Doc Cont Data Sht
Head, Computer Systems Architectures Group	Doc Cont Data Sht

Head, Information Management Group	Doc Cont Data Sht
Head, Information Acquisition and Processing Group	Doc Cont Data Sht
Malcolm Stevens (TCS) (Author)	1 Copy
Michael Pope (TCS) (Author)	1 Copy
Publications and Publicity Officer ITD	1 Copy
Derek Cassells (HFRD)	1 Copy
Doug Carey (HFRD)	1 Copy
Other Department of Defence	
AS, Information Security, DSD	2 Copies
Director General, Force Development (Joint), HQADF	1 Copy
Director General of JCE, HQADF	1 Copy
Director, Intelligence Development and Systems, DIO	1 Copy
Director General, IMCE, Defence Materiel	1 Copy
Project Director, AUSTACCS	1 Copy
Project Director, ADFDIS	1 Copy
Andrew Jordan, Assistant Project Director, ADFDIS	1 Copy
Project Director, JP2030	1 Copy
Deputy Secretary - Technical (DSEC-TECH), Defence Security Branch	1 Copy
Glen Avery (Defence Security Branch)	1 Copy
DSEC-A (Defence Security Branch)	1 Copy
WGCDR Julie Hammer (ARDU-EWSQD)	1 Copy
Libraries and Information Services	
Defence Central Library, Technical Reports Centre	1 Copy
Manager, Document Exchange Centre, (for retention)	1 Copy
National Technical Information Services, United States	2 Copies
Defence Research Information Centre, United Kingdom	2 Copies
Director, Scientific Information Services, Canada	1 Copy
Ministry of Defence, New Zealand	1 Copy
DSTO Salisbury, Research Library	2 Copies
Spares	
DSTO Salisbury, Research Library	6 Copies

Department of Defence

DOCUMENT CONTROL DATA SHEET

1. Page Classification	
UNCLASSIFIED	
2. Privacy Marking/Caveat	
N/A	

3a. AR Number	3b. Establishment Number	3c. Type of Report	4. Task Number	
AR-009-336	DSTO-TR-0209	TECHNICALREPORT	ADF 94/031	
5. Document Date	6. Cost Code	7. Security Classification	8. No. of Pages	22
JULY 1995	840740	R U U (Document Title Abstract)	9. No. of Refs.	3

10. Title
DATA DIODES

S (Secret C (Confi) R (Rest) U (Unclass)
* For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

11. Author(s)
M. Stevens and M. Pope

12. Downgrading/ Delimiting Instructions
No limitation

13a. Corporate Author and Address
Information Technology Division
Electronics and Surveillance Research Laboratory
PO Box 1500 SALISBURY SA 5108

13b. Task Sponsor N/A

14. Officer/Position responsible for

Security	SOESRL
Downgrading	CITD
Approval for release	CITD

15. Secondary Release Statement of this Document

Access additional to the initial distribution list is limited to the Defence Community of Australia, UK, USA, CAN and NZ. Others MUST be referred to the Chief Information Technology Division, Electronics & Surveillance Research Laboratory.

Any enquiries outside stated limitations should be referred through DSTIC, Defence Information Services, Department of Defence, Anzac Park West, Canberra, ACT 2600.

16a. Deliberate Announcement

No limitation

16b. Casual Announcement (for citation in other documents)

[√] No Limitation [ ] Ref. by Author, Doc No and date only

17. DEFTEST Descriptors

Computer security
Secure communication
Diodes

18. DISCAT Subject Codes N/A

19. Abstract

A data diode is a computer security device that restricts the communication along a network connection between two computers so that data can only be transmitted in one direction. This enables more sensitive or highly classified computer networks to receive data directly from a less secure source while prohibiting the transmission of data in the opposite direction. This paper discusses several ways to implement a data diode and some implications of the alternatives