DEEP SECURE

Discussion Paper

How Does a Data Diode Work?

February 2017

Introduction

Data diodes work by using a one-way link to pass information from one network to another. They are a combination of hardware, firmware and software, specially designed to make data transfers fast and reliable and guaranteed one-way.

Applications interface to a data diode in one of three ways: using a network communications protocol, by passing files through a file store or with an Application Programming Interface (API).

The one-way link is typically constructed from fibre optic interface components, which are joined using a fibre optic cable (**Figure 1**), though it is possible to design electronic circuits to do a similar job. A separate computer is used at each end of the one-way link to run the software that provides the interface to applications (though in simple cases hardware logic can take the place of these computers and the software).

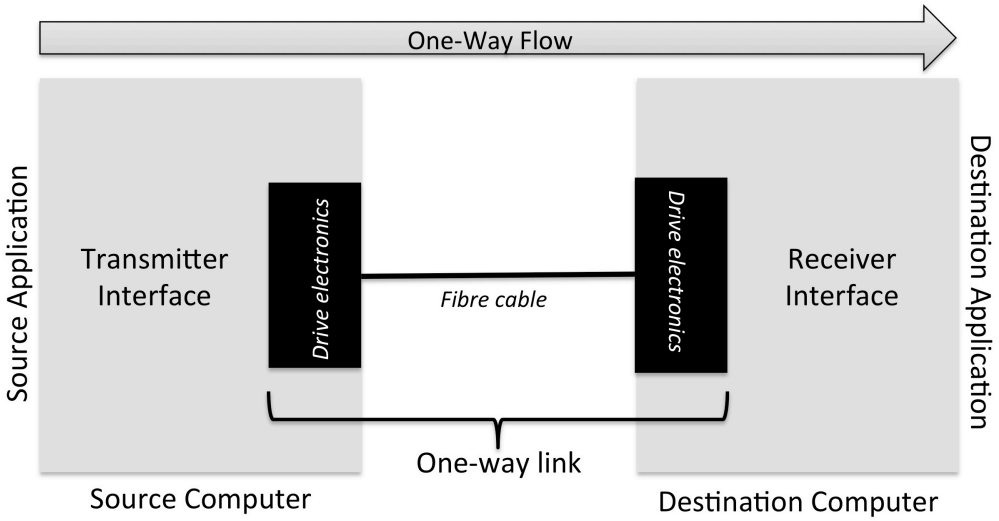

Figure 1: A data diode works by using two one-way fibre optic interfaces

The application that is the source of the data uses the transmitter interface on the source computer to pass data to the data diode. The transmitter interface sends this data to the drive electronics, which transmit it across the fibre. The drive electronics in the destination computer receive the data and deliver it to the destination application using the receiver interface.

The One-Way Link

The one-way link in a data diode works by using circuitry that only transmits at the

source end and circuitry that only receives at the destination end. Typical fibre optic one-way links use a light emitting diode (LED) at the source end to convert electrical pulses into light pulses. The light pulses travel along a fibre optic cable to the receiving end that uses a photo diode to convert the light pulses into electrical pulses (**Figure 2**).

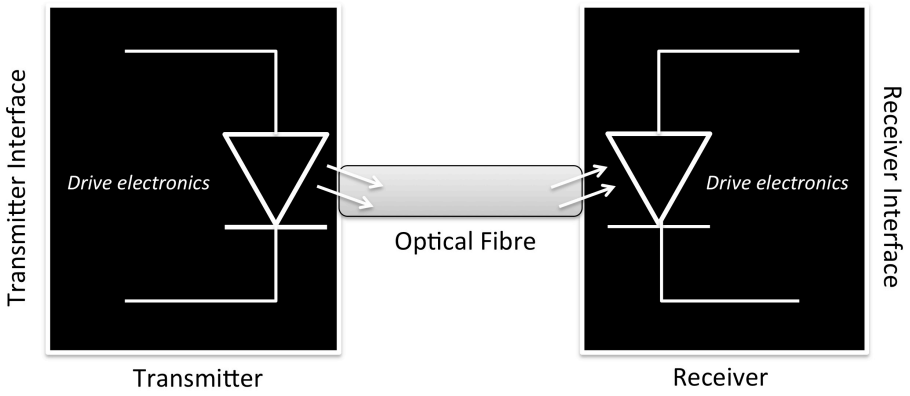

Figure 2: A fibre optic one-way link

Modern fibre optic networking links are bi-directional and use two fibres, each carrying data in a different direction (**Figure 3**). They can be converted into a one-way link by disconnecting one of the fibres. However, network interface controllers often use a bi-directional protocol to agree the data transfer mode they will use to communicate, and disconnecting a fibre breaks this so they fail to operate. Also, modern networking components include features that detect the disconnection of a fibre and treat this as a fault that prevents all communication. As a result, data diodes are generally built from special fibre optic networking components that are designed to operate in a one-way mode.

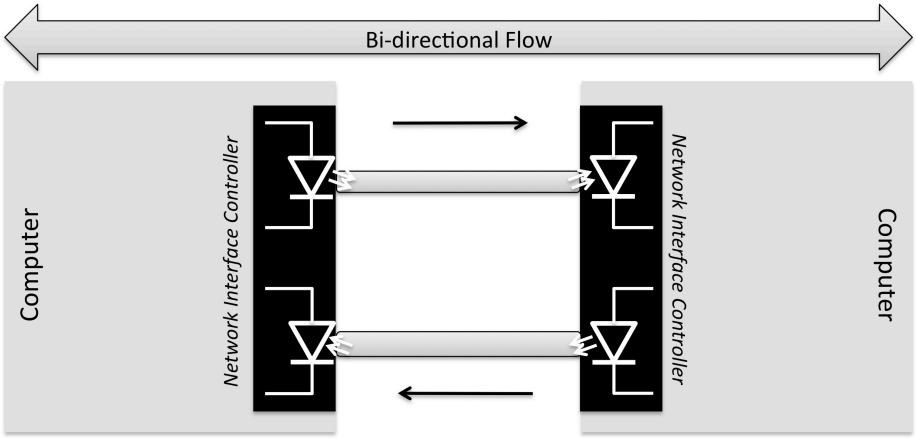

Figure 3: Fibre optic networking uses two fibres to make a connection

Protocol Interfaces

Most data diodes provide external network interfaces of some sort, but there is wide variety in the protocols that are supported.

Perhaps the simplest protocol interface is one that passes UDP datagrams received from the source network to the destination network. This can be used for application level protocols built on UDP, such as syslog and simple video streaming.

More complex protocols use TCP, which is a bi-directional protocol. TCP is used even when data flows are one way because acknowledgements and flow control information need to be passed in the opposite direction to make the data transfer reliable. TCP cannot be used across the one-way link, so the data diode interface on the source computer works by acting as an application level proxy that terminates the TCP connection, extracts the payload data and pushes it across the one-way link and returns the necessary acknowledgements. The interface on the destination computer gets data from the one-way link and uses TCP to deliver it to the destination.

Some data diodes provide TCP interfaces that allow data to be delivered using SMTP email or pushed using HTTP (**Figure 4**).

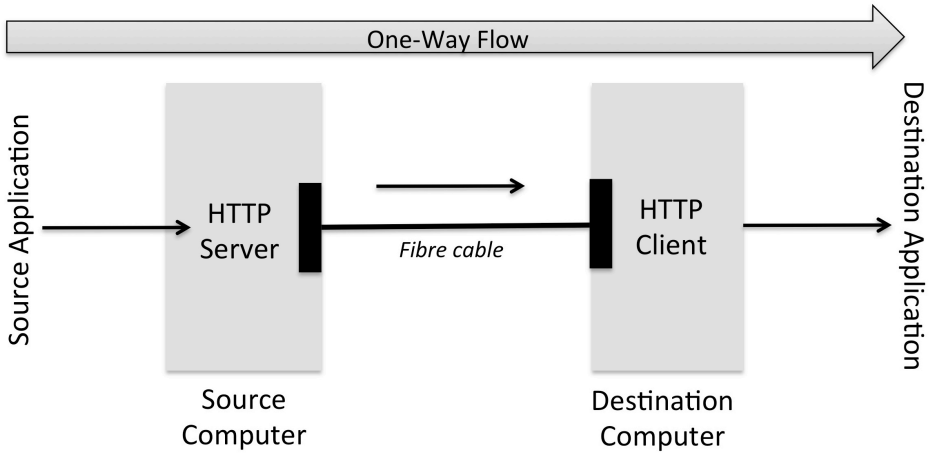

Figure 4: A data diode with an HTTP interface

Some data diode vendors support TCP protocols such as HTTP by using proxies that run on external servers (**Figure 5**). These use some proprietary protocol to move the data payload across the source network from the source proxy to the data diode's source computer and from the destination computer to the destination proxy. The benefit here is that the diode component is simpler, but the overall solution footprint is larger than if the diode directly supported HTTP etc.

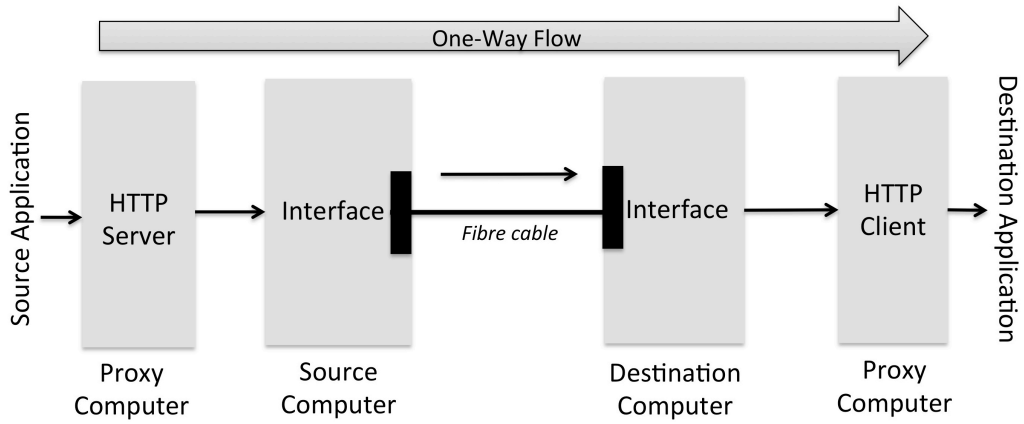

Figure 5: A data diode using external HTTP proxies

File Store Interfaces

Many data diodes provide a file store interface that moves or copies files from a file store on the source computer to a file store on the destination computer (**Figure 6**).

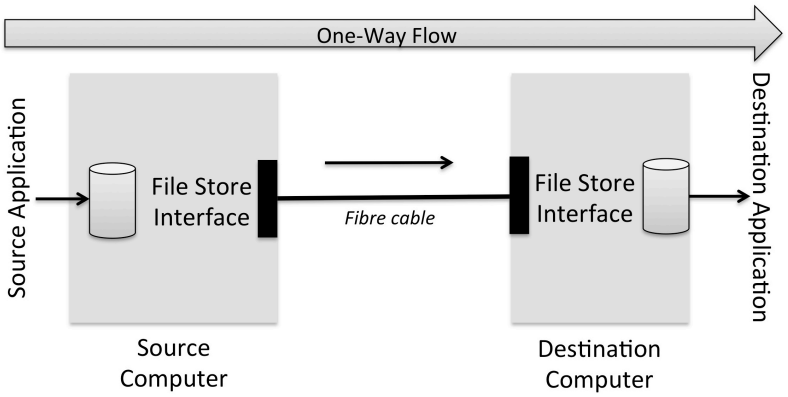

Figure 6: A data diode with a file store interface

The source application accesses the file store on the data diode's source computer using some network file store protocol, such as SMB or NFS. Any files it writes into the store are moved or copied across the one-way link to the interface on the destination computer, which writes the file into its file store. The destination application then accesses the store to read the file.

Some data diodes support file store interfaces using agents that run on external servers (**Figure 7**). The file store agent on the external server on the source network moves or copies files that appear in the file store to the source computer using some proprietary protocol. The file is pushed across the one-way link to the destination computer, which passes it to the agent on the external server on the destination network. The agent stores the data in a file that is fetched by the destination application. This approach generally provides more flexibility than having the file store implemented in the data diode, by supporting a range of file store solutions, but does require a larger footprint.

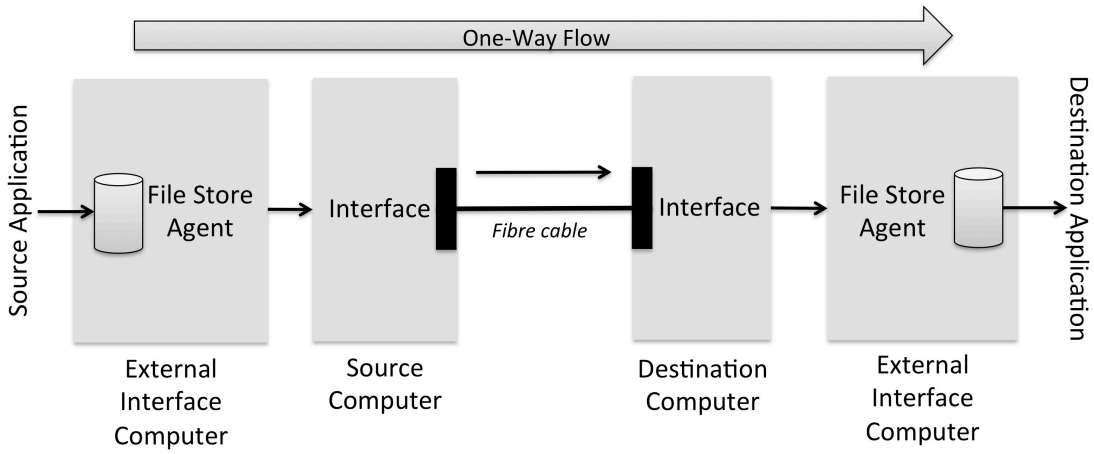

Figure 7: A data diode using external file store interface computers

Application Programming Interfaces

Some data diodes allow custom software to be installed on the source and destination computers. They provide an Application Programming Interface (API) that the software can use to pass data to the data diode's transmitter interface and receive data from its receiver interface. This allows the data diode to be customised to support application specific protocols directly, rather than requiring the use of external interface computers that perform protocol conversion.

Minerva Data Diode

Deep-Secure's Minerva data diode works by providing a link based on special purpose fibre optics that guarantees transfers are one-way, protocol interfaces that allow applications to interface directly to the data diode and utilities that run on external computers to provide additional interfaces. Minerva is supplied as an appliance, which comprises two servers, that is managed through a web interface.