CDAC INTERNSHIP PROJECT REPORT

Topic: Data Diode

Submitted By			Guidance of:
Name	ID	College	Hareesh Reddi
Aman Ranjan Verma	3011	IIIT Manipur	
Anand Kumar Jha	3275	NIT Silchar	
Megha Sharma	3069	NIT Silchar	
S. Pravin	3055	NIT Silchar	
Sumit Bothra	3188	NIT Sikkim	

Table of Content

Acknowledgments

I would like to express our sincere gratitude to CDAC and its coordinators at NIT Silchar and Bangalore. Also, I would like to thank to our guide Harish Sir for providing his invaluable guidance, comments and suggestions throughout the course of the project. Through this internship program we got so many new topics to learn. Industrial visits and guest lectures were the highlights of the program which we enjoyed a lot. This internship provided a great network of people.

Introduction

A unidirectional network (also referred to as a unidirectional security gateway or data diode) is a network appliance or device allowing data to travel only in one direction as shown in figure 1, used in guaranteeing information security. They are most commonly found in high security environments such as defense, where they serve as connections between two or more networks of differing security classification – also known as a "cross domain solution." This technology is also found at the industrial control level for such facilities as nuclear power plants, electric power generation/distribution, oil and gas production, water/wastewater, airplanes (between flight control units and in-flight entertainment systems), and manufacturing.

The majority of unidirectional network applications in this category are in defense, and defense contractors. These organizations traditionally have applied air-gaps to keep classified data physically separate from any Internet connection. With the introduction of unidirectional networks in some of these environments, a degree of connectivity can safely exist between a network with classified data, and a network with an Internet connection.
Examples of this use of unidirectional technology include:

- Government organization
- Commercial companies

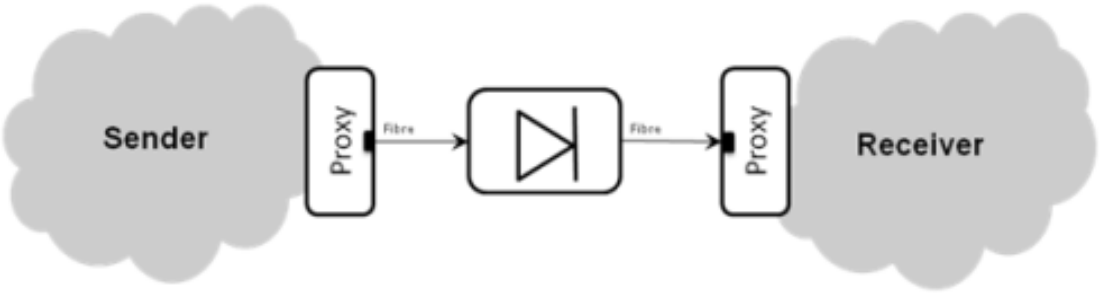


Figure: 1

This means that data diodes can ensure the following:

- Exploited network access is not possible from outside the network
- 100% data leak prevention since no data can leave the network

Why do we need Data Diode?

There are many reasons to use a data diode. Have a look at our top 5.

- A data diode guarantees the only secure segregation of networks

  Network segregation is one of the most effective ways to secure your network. It makes it much more difficult for hackers to get from exposed parts of your network to the more secure parts. This way, access to sensitive information or critical systems can effectively be limited. Methods to achieve network segregation include physical isolation, traffic flow filters, creating VLANs, using proxies, and most widely known, firewalls. All these methods can and should be part of a secure network architecture. But none can provide absolute certainty that the network can't be hacked and that data will flow in only one direction.

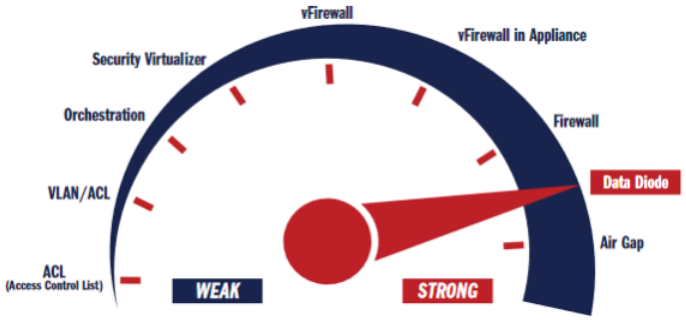


Figure: 2

A data diode is the only security solution that *can* guarantee a one-way data flow as shown in figure 2. The physical data diode device is simple and only consists of fiber ports and a power connection. The physical path for the fiber and electronic signals (which make up the data) only permits one direction. The diode doesn't contain any software or other kind of logic which makes it impossible to reconfigure or hack.

- A data diode lowers costs and reduces complexity

  Compared to firewalls and other software solutions, a data diode is a simple solution that ensures low (maintenance) costs.

- The configuration of a diode is relatively simple. No in-house expertise is needed.
- By using a diode, no matter what configuration errors are made, you can be absolutely certain that data can only flow in the correct direction.

- A data diode allows you to transfer real-time data in highly secure environments

  The solution for network segregation in highly secure environments (for instance nuclear power plants or secret service agencies and such) has long been that of physical network isolation. But this is no longer viable. Data volumes have been increasing steadily and nowadays you need to be able to process and respond to data much faster. Because of these trends it is no longer workable to bring data from one network to another on a CD or USB stick. These types of critical environments are now able to safely transfer big volumes of live data at high rates through a data diode.

- A data diode is able to prevent physical damage or loss of life

  In case of industrial networks, digital systems are connected to physical processes. These are so-called cyber-physical systems. When these systems are connected to insecure networks (i.e. networks connected to the internet), they open up a path for hackers to take over control. If this happens, data leakage or loss may be the best outcome. By using a data diode, you can share data from the OT to the office network and have the peace of mind that no hacker will be able to get into your cyber-physical systems via this path.

- Local regulation recommends or enforce you to implement data diodes

  Some countries recommend or even obligate particular organizations (mainly organizations in the government or critical infrastructure sectors) to implement a data diode in their networks. Be sure to check with your local authority to find out what their recommendations are.

Different forms of Data Diode

As a part of literature Survey our group came across different configuration of Data Diode. The resources which we looked includes IEEE research Paper, Video Lectures from NPTEL and OWL Cyber Defense. The different configurations are as follows:

1. Data Diode Using ATM Protocol
2. Optical Data Diode
3. UDP Proxy Based Data-diode with Modbus

1. Data Diode Using ATM Protocol

A piece of hardware that physically enforces a one-way flow of data. As one-way data transfer systems, data diodes are used as Cybersecurity tools to isolate and protect networks from external Cyber threats and prevent penetration from any external sources as shown in figure 3. A data diode sits at the edge of the network security perimeter; relying on its physical hardware components to mitigate all network Cyber threats against the network while simultaneously allowing the transfer of data out of the network in a highly controlled, deterministic manner.

- Hardware based Cyber security (Dual Diode).
- Hardware designed to only be one-way.
- Impervious to software changes or attacks.
- Either it will work as intended to work or will not work at all.
- Deploy non-routable ATM protocol break between the two segmented networks.

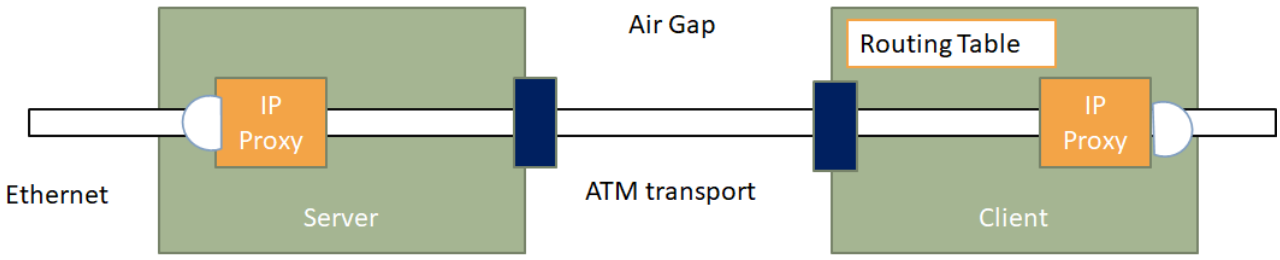


Figure: 3

Why ATM Protocol?

It was designed to move large amount of data asynchronously.

- Large data rates.
- High quality.
- No packet loss.

➢ As a result, we get quality of service, non-routable protocol break which maintains 100% confidentiality and it's all forced in hardware so it can't change.

➢ The optic cable doesn't have any security and if any attacker wants to intercept data through cable, ATM protocol doesn't allow.

About ATM Protocol.

- Driven by the integration of services and performance requirements of both telephony and data networking.
- Transmit all information in small fixed size packets called cells (allowed fast h/w switching).
- Cells are transmitted asynchronously. (unlike SDH).
- The Network is connection oriented. (statistical multiplexing)
- Each cell is 53 bytes long – 5 bytes header and 48 bytes payload.
- Making an ATM call requires first sending a message to setup a connection. Subsequently all cells follow the same path to the destination.
- ATM is independent of transmission medium. They may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems.

ATM Vs Telephony:

- Phone networks are synchronous(periodic).
- Phone network uses circuit switching whereas ATM network uses “Packet” or “Cell” switching with virtual circuits.
- In phone networks, all rates are multiple of 64 kbps. With ATM we can get any rate, and we can vary our rate with time.

ATM Vs Data Networks:

- ATM cell – Fixed/small Size
  IP Packets: Variable size
- ATM uses 20 Byte global addresses for signaling and 32-bit locally-assigned labels in cells. Whereas IP uses 32-bit global addresses in all packets.
- ATM offers sophisticated traffic management whereas TCP/IP: congestion control is packet loss-based.

ATM: Fixed size Packets

- Simpler Buffer Hardware
- Packet arrival and departure requires us to manage fixed buffer sizes.
- Simpler scheduling
- Each cell takes a constant chunk of bandwidth to transmit.
- Overhead for sending small amount of data. Segmentation and reassembly cost.

ATM Layers:

- Convergence sub-layer. Shown in figure 5.
- SAR: Segmentation and reassembly sub-layer
- ATM Layer
- Transmission Convergence sub-layer
- PMD: Physical Medium Dependent sub-layer

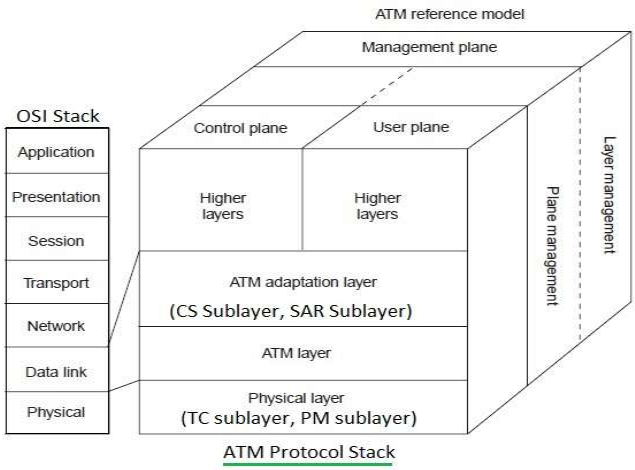


Figure: 4

2. Optical Data Diode

An optical data diode is a computer security device that restricts the wire-line communication along a network connection between two points so that data can only be transmitted in one direction. Since the data diode has a single fiber-optic cable, it is impossible to reverse transmissions due to the basic laws of physics. Shown in figure 5.

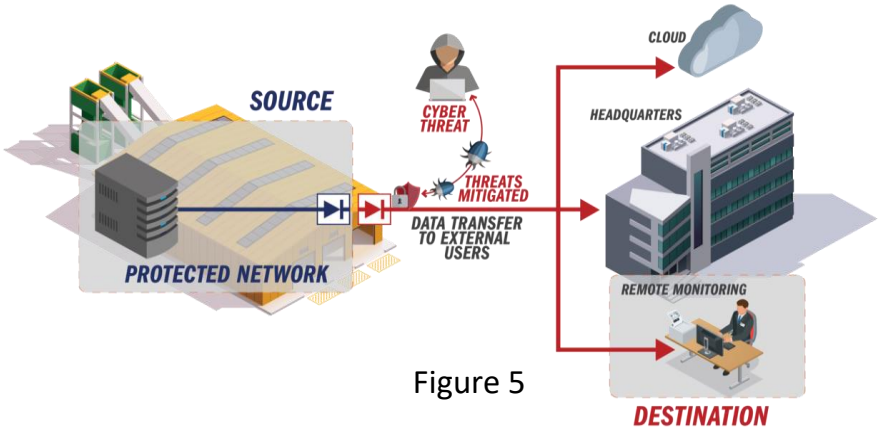


Figure 5

Requirements:

- Three fiber optic transceivers, the third fiber optic transceiver is required simply to supply a carrier signal to the lower side transceiver which will not work if it does not see the appropriate carrier signal.

- Two Ethernet cards. One Ethernet card is put in each of the gateway workstations so that the two workstations are linked by a dedicated sub-network in order to avoid the possibility of packet collision with another network traffic

- A power supply for the third fiber optic transceiver. The power for this could be tapped from the cable that connects the other fiber optic transceiver to the low side Ethernet card, if this card can supply enough power for two cards.

- Appropriate fiber optic and copper cable to make connections as in Figure 6.

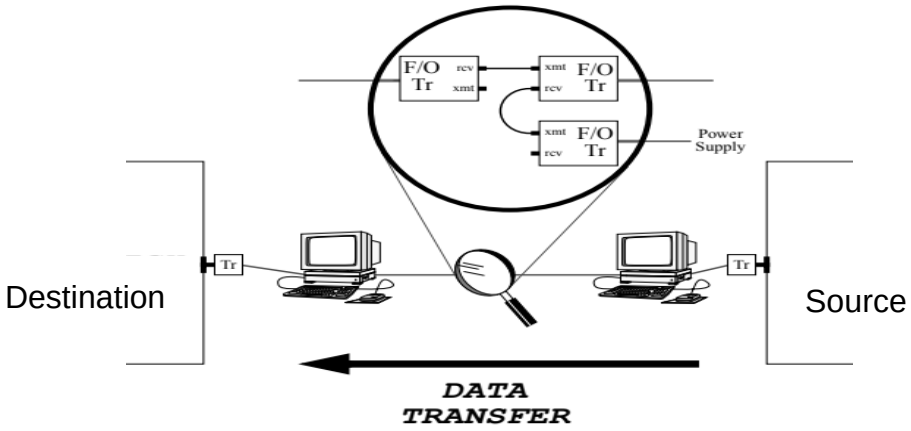


Figure 2 A simple design for an Optical Data Diode

Figure: 6

An optical data diode neatly separates into a hardware component and a software component. The configuration of the hardware is entirely responsible for providing confidentiality security. The software is responsible for providing the functionality or services through the one-way link. Software like virus checkers can be added to provide integrity protection, although this is not at the same high level of assurance as the confidentiality assurance provided by the optical data diode.

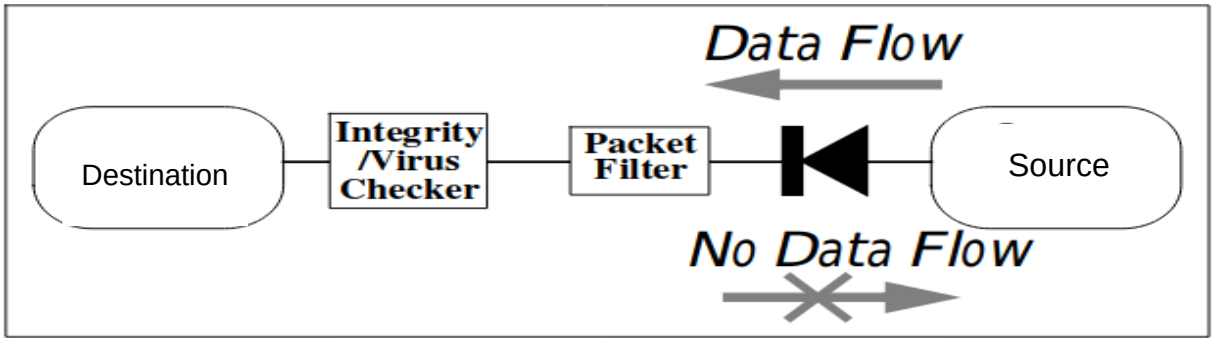


Figure: 7

Advantage

- All the hardware components are commercial “off the shelf” products.
- The design of the optical data diode is very simple. Assurance that it is prohibiting communication in the reverse direction is confirmed by visual inspection of the configuration.
- The simple design should also enable easy accreditation by the local accrediting authority.
- Such a data diode can be built today without waiting for a product to be developed.

Disadvantage

- The main disadvantage of this design is the fact that the delivery of data from the low side to the high side is in theory unreliable.
- In practice it can be very reliable but there is no absolute guarantee that delivery will always occur.

3. UDP Proxy Based Data-diode with Modbus

In data diodes, there is one device which only sends data to the network and the other device which only receives data through the network.

Typical Modbus TCP Communication

- The Modbus UDP Communication is based on Client / Server Request-Response Communication
- In this Protocol, the Client (MTU) requests for data. Based on the request received by the Server (RTU), the response is provided to the Client.

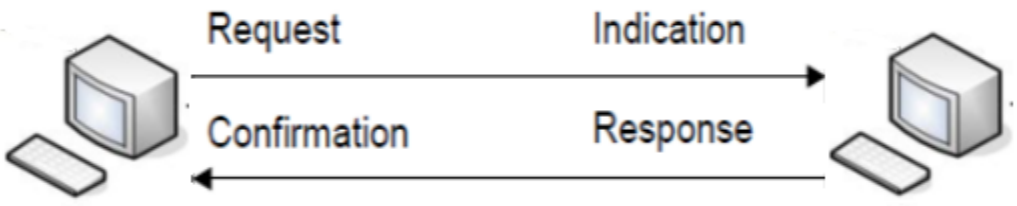


Figure: 8

Data Diode Model for Modbus Protocol

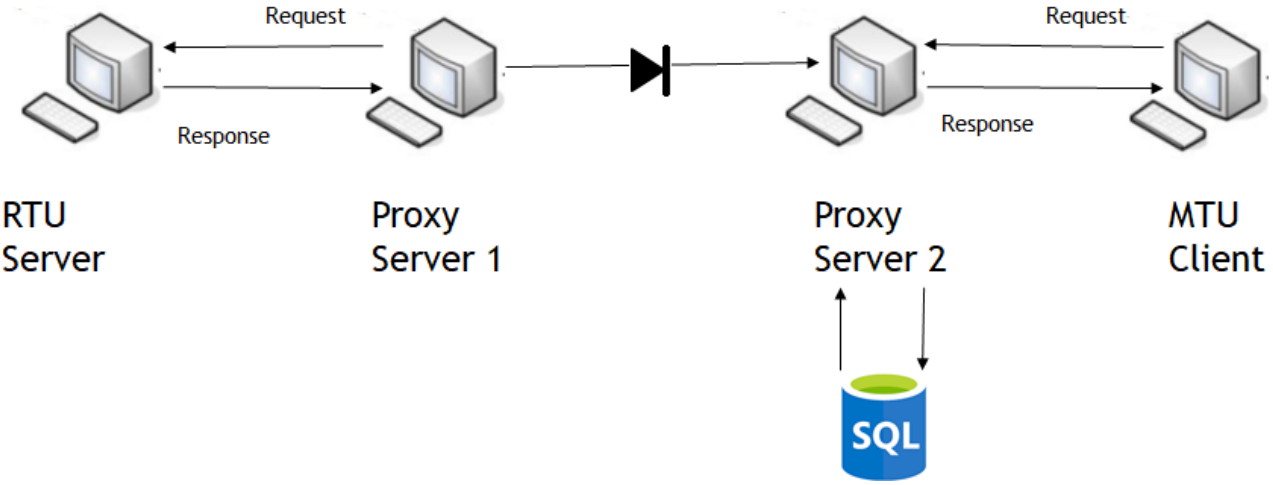


Figure: 9

- The RTU Server and UDP Proxy 1 Server communicates at Modbus Port no 502. The Proxy 1 acts like a Client with respect to RTU and sends request to the RTU. The RTU checks the request, and based on the request, sends a response to the UDP Proxy 1.
- The UDP Proxy 1 acquires the data, the forwards the data to the UDP Proxy 2. Here the data transfer is unidirectional and hence the data transfer cannot take place from UDP Proxy 2 to UDP Proxy 1. Hence the data diode is implemented between UDP Proxy 1 and UDP Proxy 2. Here is transferred from any port other than 1 to 1023 port.
- The MTU requests data from UDP Proxy 2 form the same Port 502. Here the proxy acts like the RTU Server and thus provides data to the MTU. The MTU then forwards the data to the database as well as to the HMI.

Data Transfer in Data Diodes

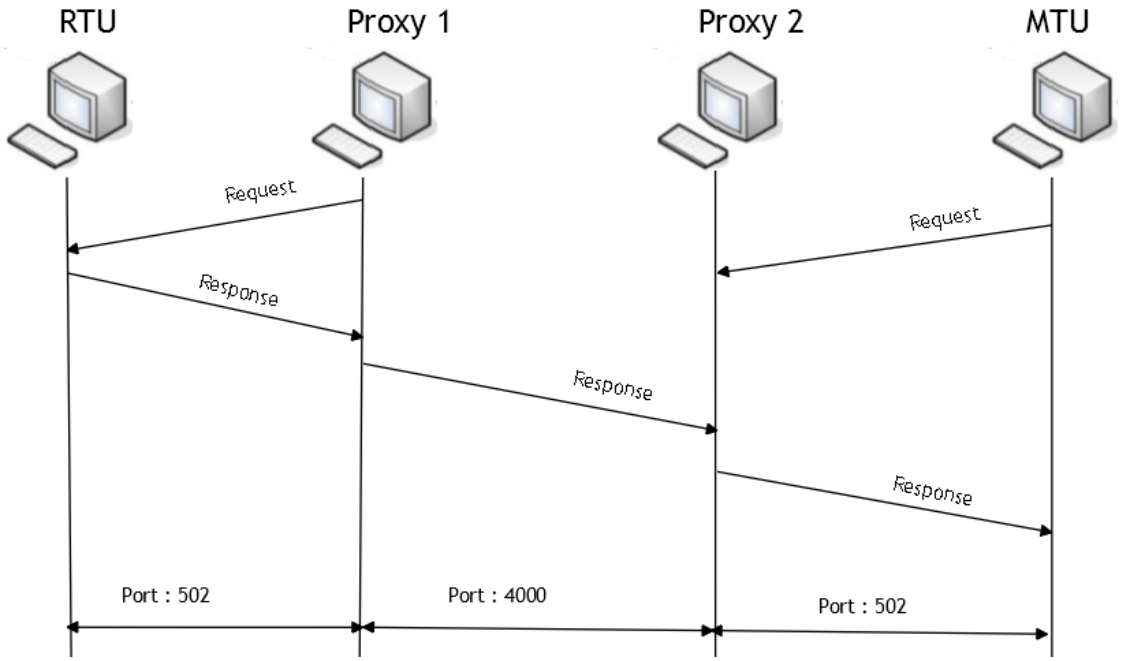
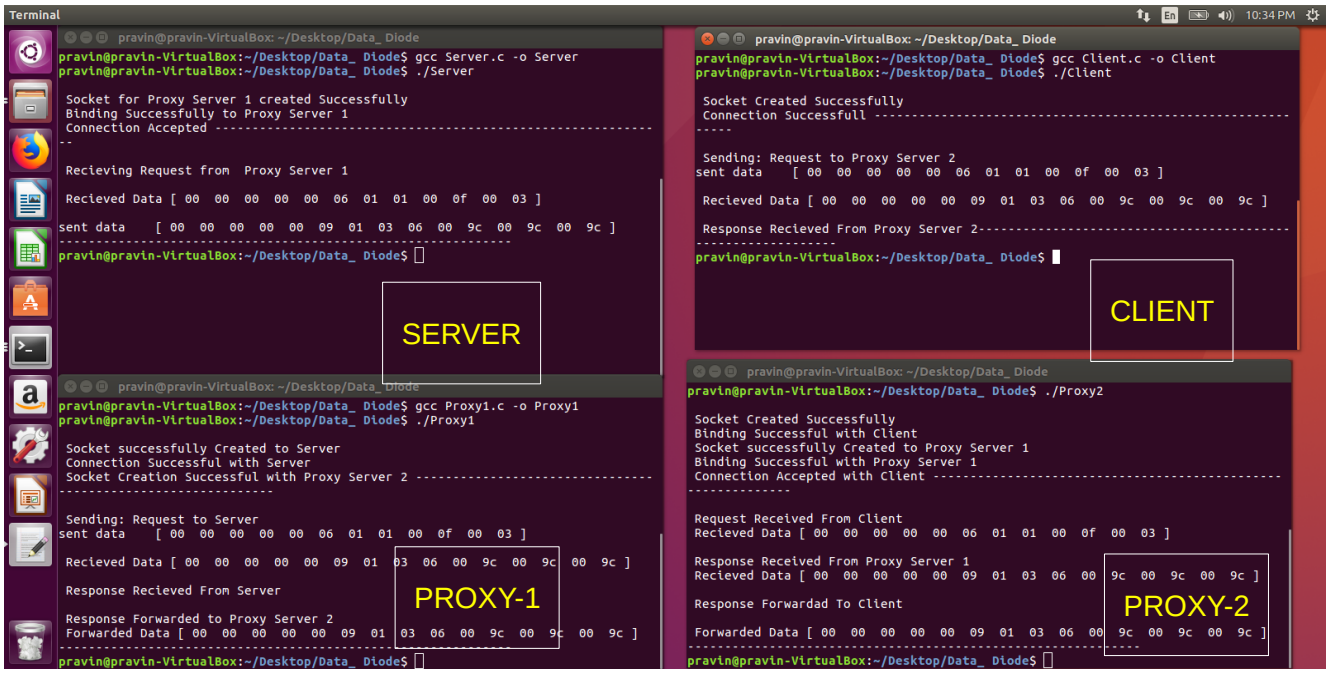


Figure: 10

Result



Advantages of Data Diode

- Since the data transfer is unidirectional, it is very much secure and it is very much difficult to conduct an attack at the RTU/Server
- It can be applicable on various other protocols and is not only bound to Modbus.
- Even is any attack is successfully conducted at the MTU, the attacker cannot perform any attack at the RTU as the UDP Proxies only communicate in unidirectional mode.

Disadvantages

- Since the data transfer is unidirectional in nature, actuators cannot be used in the above model. Hence it limits our usage to only to sensors and the control signals cannot be sent through it.

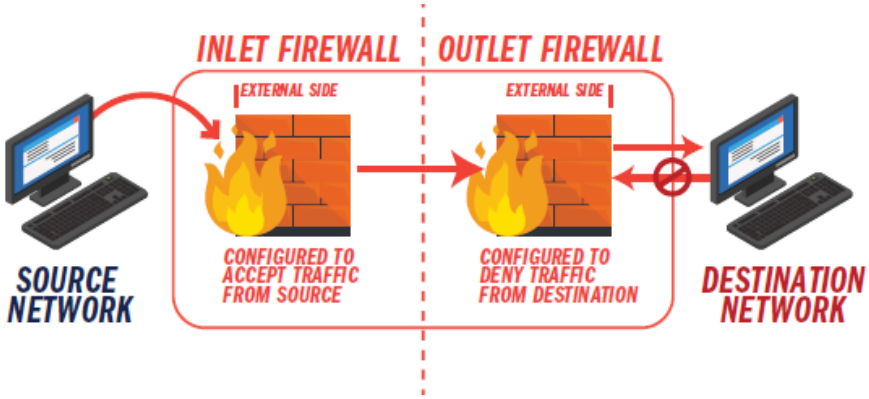
Applications

- SCADA System
- IoT
- In Isolating a Server from the Corporate Network

Code for this Implementation: GitHub Repo

Download Here

Firewall Based Mechanism



- Relies on Software Configuration
- They communicate through Ethernet cables.
- A pair of firewalls configured back-to-back provide a more secure implementation
- Firewall on source side is configured to filter traffic from source side
- Firewall on destination side is configured to deny the traffic from destination side.
- Prone to Malware attacks due to vulnerabilities of software-based solutions.

Common applications

Common deployments of data diode technology include:

- Remote monitoring of equipment or historical data and human-machine interfaces
- Secure printing from a less secure network to a high secure network (reducing print costs)
- Transferring application and operating system updates from a less secure network to a high secure network
- Monitoring multiple networks in a SOC
- Time synchronization in highly secure networks
- File transfer (High to low/Low to high)
- Streaming video (High to low/Low to high)
- Sending/receiving alerts or alarms
- Sending/receiving emails

How can users benefit from a data diode?

By allowing for limited and safe connectivity, users are able to complete their tasks more efficiently, including:

Forwarding email

Users on secure or even air-gaped networks often have several mail addresses referring to different networks. In order to receive mails, users are forced to log in to multiple networks to check their mail accounts. By installing a Data Diode, you will be able to forward all emails to one account on the most secure network and thereby significantly improving efficiency.

User initiated file transfers

Even working within a secure network, users often need graphs, images, and other information for the completion of reports. By using Data Diode technology, users can transfer the information they need by simply dragging and dropping the files to a dedicated transfer folder which is forwarded to the secure network.

Mirror web sites

Permitting full web access to the Internet is always a huge security issue, and with air-gaped networks, full access is simply impossible. Nevertheless, if you or the organization needs online access to pinpointed websites, there is the option to mirror the needed sites using Data Diode technology. The website will have the information sent through the data diode, creating a mirror of it for employee use.

RSS feeds

Employees often rely on RSS feeds to get the latest updates on topics in their industry or profession. High-security organizations can now allow the use of RSS feeds by having the information travel through a data diode, much like the email and website mirroring.

Streaming (video, audio)

Streaming of video and audio is now possible for high-security organizations. Since even video files can contain malware, taking precaution on the use of streaming media such as news feeds, surveillance, or video seminars is important. Using a data diode provides all of the necessary precautions, while not hindering the use of these media types at all.

Centralized print solution

Without the use of unidirectional networking, organizations will have more separated networks and more printer pools. Every separated network would need its own set of printers to allow employees to print information from that network. With Data Diode, it is possible to set up a centralized print solution that covers more networks and even support "follow the print".

Comparative Assessment:

Specifications	Optical Data Diode	Proxy Based Data Diode	ATM Based Data Diode	Firewall Based Mechanism
Connection	One- Way with optical fiber	One-way with proxy servers	One –Way with optical fiber	One-way with Software Configured
Protocol	UDP	MODBUS – UDP	ATM	TCP-IP
Routability	Routable	Routable	Non-Routable	Routable
Reliability	Unreliable	Unreliable	Highly Reliable	Reliable
Throughput	Low	Low	High	Moderate

Conclusion

Data Diode has expanded domain in Govt, Military, Critical Infrastructure, Financial Services and Telecommunications. The Cybersecurity goal of any organization to minimize risks while preserving data availability seems achievable with the advent of ATM Based Data Diode. Advanced Technology will enable network segments to get smaller, providing better security. As IoT expands, Security becomes prime concern & Data Diodes provide promising solution. The Unhackable nature of Hardware based solutions with new innovations for greater efficiency, flexibility & performance presents a bright future ahead.

References

1. https://www.owlcyberdefense.com/about-data-diodes/
2. https://www.ops wat.com/blog/why-data-diodes-are-essential-isolated-and-classified-networks
3. owlcyberdefense-ebook_the-definitive-guide-to-data-diode-technologies.pdf
4. https://en.wikipedia.org/wiki/Unidirectional_network
5. https://www.advenica.com/en/cds/data-diodes
6. https://www.baesystems.com/en/product/data-diode-solution
7. owlcyberdefense-ebook_the-definitive-guide-to-data-diode-technologies.pdf
8. https://www.owlcyberdefense.com/about-data-diodes/
9. A study of cyber security policy in industrial control system using data diodes, IEEE Paper
10. https://www.opswat.com/blog/why-data-diodes-are-essential-isolated-and-classified-networks
11. https://www.baesystems.com/en/product/data-diode-solution
12. The Technique of Network Diode, IEEE Paper
13. https://www.advenica.com/en/cds/data-diodes
14. The application of data diodes for securely connecting nuclear power plant safety systems to the corporate IT network, IEEE Paper
15. https://en.wikipedia.org/wiki/Unidirectional_network