Data Diode for Cyber-security: A Review

Ismail Ahmed Almaazmi
Information Security and Engineering
Technology, Abu Dhabi Polytechnic
United Arab Emirates;
A00043850@adpoly.ac.ae

Mohammed Saeed Al Shehhi
Information Security and Engineering
Technology, Abu Dhabi Polytechnic
United Arab Emirates;
A00053125@adpoly.ac.ae

Omar Ahmed Alkhoori
Information Security and Engineering
Technology, Abu Dhabi Polytechnic
United Arab Emirates;
A00053146@adpoly.ac.ae

Salem Jumah Al Shehhi
Information Security and Engineering
Technology, Abu Dhabi Polytechnic
United Arab Emirates;
A00056096@adpoly.ac

Yasir Hamid
Information Security and Engineering
Technology, Abu Dhabi Polytechnic
United Arab Emirates;
yasir.hamid@adpoly.ac.ae

2022 International Conference on Artificial Intelligence of Things (ICAIoT) | 979-8-3503-9676-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAIoT57170.2022.10121887

ABSTRACT: The rapid growth in network usage and availability has exposed this field to denser and more sophisticated attacks. Sensitive and critical data has been transported over those network nodes and devices, which made them an attack vector to be exploited to gain information or data. To uphold the advantages of the networked systems some data need to be sent out over the highly secure channel. Previous technologies like Firewalls and ACLs being used to pass the data from a highly secure logical area to a lower logical area due to their software nature are proving to be fighting a losing battle with the attackers. Therefore, in the recent past physical security device Aka. Data Diodes which are secure by design and have no documented evidence of flow being reversed are gaining more attention. Unlike software, parameters can tamper, and that leads it to be implemented for those situations in which data need to be secured and protected, while still ensuring full separation between the outside world and the inside world, as data diode can be ranged depending on their complexity from EVL 1 up to EVL 3 in terms of their security strength. In this paper, we provide a comprehensive review of the recent research efforts spared for the data-diodes ranging from their manufacturing to their applications. Furthermore, the paper presents a comparison of data-diodes from options offered by reputed vendors, highlighting the strengths and weekness of each of them.

Keywords—Cyber Security, Data-diode, Hardware-Security, One way communication

I. Introduction

From the first ever network to be created back in 1961, to the birth of the worldwide internet in 1969.[1] Networks served as an important aspect of exchanging data and information throughout destinations and organizations, and the network which did cover a much wider aspect and range of exchanging data in a worldwide fashion rather than a limited area. The same main elements are yet to be done, as the need of maintaining the equilibrium between ease of access and security over the network.

At the core of information, security is the CIA triad of confidentiality, integrity, and availability used to manage the strategies for securing the data in a system.[2] The components of the triad are thought to be the most significant components of security. This guideline is relevant to the entire subject of security analysis, from access to a client's web history to the security of encrypted information over the web.

As networks and the internet started to advance over time, network and internet attacks have become more frequent and complex which even target critical data and infrastructure, and so did the defenses and security mechanism did improve to defend those systems and data.[3] Which did give birth to new technologies and implementation to ensure the security of the information system networks and devices, most common and widely used are firewalls, Intrusion detection systems (IDS), intrusion prevention systems (IPS), and many other devices to be used. [4]

Those devices to be implemented in securing networks from intrusions and unauthorized access do suffer from vulnerabilities and are yet not as secure as the "Data Diode" hardware device, which does implement the saying of "secured by design rather than secured by technology". As it implements a one-way method of communication as it cannot be reversed by any means, because of its design as one side do send and the other receive, a part with a sender and the other with a receiver, therefore, achieving a complete one-way transmission, that acts as a gateway. The objective of this work is to present a comparison of the data diodes with other security mechanisms, present a working design of the data diodes, list the commonly found data diodes in the market, and finally present a comprehensive literature review of the data-diode research works.

II. Background

Utilizing both software and hardware technologies, network security is an activity encompassing a set of rules to safeguard the usability, integrity, confidentiality, and accessibility of your network and data. The goal of network security is to identify the various dangers and contain them after they have entered our network. These features are coordinated to analyze and mitigate traffic before it reaches your protected resources. A network security stack may include components that perform one or more of four different functions (the list below is not exhaustive): (Network Security Monitoring Systems, Firewalls, Proxies, IDS/IPS). A proxy is when a device acts as an intermediary for communication between endpoints (mostly other host-based clients and servers). IPS/IDS – Intrusion Prevention Systems/Intrusion Detection Systems are designed to detect malicious content in traffic passing through inspection points. The main difference between the two types of systems is that they both detect targeted activity, but IDS only issue alerts and IPS can both

979-8-3503-9676-8/22/$31.00 ©2022 IEEE

alert and block detected traffic. A firewall is an appliance or application that runs on a system and is used to filter/restrict access to endpoints or services across bottlenecks between one security domain and another.

Because a firewall depends on configuring code and policies set by admin it has an inherent vulnerability that they cannot get rid of which are zero-day attacks and unknown new attacks. Some types of firewalls just depended on the head of the packet to permit or deny it, even firewalls could not monitor the internal network. [8]. The limitation that the access control list has is that if the admin happens to make a mistake while he is making the policy the access control list will suffer from misconfiguration which literally cannot happen in data diodes. The shortcomings of one or more of the following three qualities of a perfect security model can be summed up as limitations in each model[9]: Invisible seamless user and administrative interaction with the model and Feasible cost-effective and practical to implement the model.

For the network attack classification, a lot of schemes have been proposed in the literature, classifying attacks into seven broad groups Infection: This attack is aimed at installing harmful files or tampering the valid files thereby infecting the files. These attacks can be further sub-categorized as viruses, worms, trojans, etc. Exploding: This attack is aimed at overflowing the victim with bugs, the prominent attack of this type is buffer-overflow. Probe: This attack is aimed at collecting vital information about the network to identify the potential entry points that can be compromised. Some information of interest for an attacker can be to check which services are running, and what IP (Internet Protocols) addresses are working currently. Some attacks falling in this class are PortScan, IPscan, and Nmap. Cheat: These attacks are aimed at gaining access to the network by impersonation i.e, by providing a fake identity to access secured files of the system. Some of the attacks falling in this class are IP Spoofing, Session Hijacking, etc. Traverse: Attacks of this type attempt to break into the system by performing a password match against all the possible passwords. Dictionary attacks and brute force attacks are a few examples of this type. Concurrency: Attacks of this type capitalize on one or more weaknesses of the system to carry out some disastrous actions. A prominent attack of this system is DDoS wherein system resources are exhausted, to deny it from serving legitimate users.

To protect against the above listed and many other attacks a variety of defense mechanisms have been proposed and used over time like Routers, ACLs, Firewalls, and Intrusion Detection and Prevention Systems. A common thing with all of the listed defense mechanisms is the presence of software modules that needs complex configuration. Because a firewall depends on configuring code and policies set by admin it has an inherent vulnerability that they cannot get rid of which are zero-day attacks and unknown new attacks [5]. The limitation that the access control list has is that if the admin happens to make a mistake while he is making the policy the access control list will suffer from misconfiguration which literally cannot happen in the data diode [6]. Routers suffer from a lot of both ACL and firewall limitations because it is not built inherently for Security kinds like a jack of all trades master of none it has some firewall capabilities and some switch and some ACL (Access Control Lists) but because of that, it has all their vulnerability it can suffer of misconfigurations and zero-day attacks. Most of the limitations of the above security tools stem from their software-based nature and which has required hardware-based security that doesn't run into configuration issues. [6]

A. Data Diodes

A data diode is made of three parts. It's thought of it as the source side and receiving side, while in between an airgap which is meant to fully isolate the two parts of each other, acts to a similar matter of a full proxy architecture.

The source side would be on your protected side, and the receiving side where is the destination which is the open network or a less protected network, so the protected side is your internal network and the less protected side will be your external network.

A diode is comprised of two sides, one has an LED that sends a light signal across the fiber optic cable to the destination side, and the destination side is based on the receiver, its job is to receive that light that's coming over the fiber optic channel. The destination side does have a receiver and a converter which would convert fiber optic signals source do have an emitter only, while in between is the Airgap which is most of the work is done there, which data gets stripped down back to the physical layer of an OSI (Open Systems Interconnection model) layer, to ensure no extra data or information to be carried to the other side of a network as an example of an IP Header. The sender in essence can only send light in my direction, which means it's completely unreversible, while it's hardware-based and not able to have tampered with.

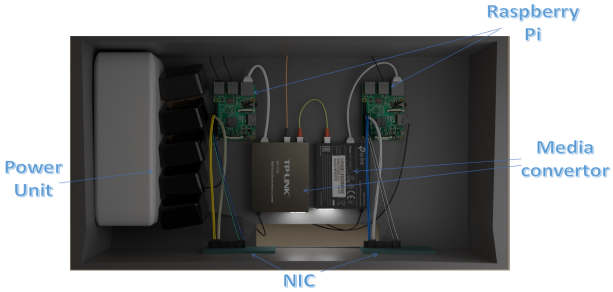


Figure 1. Working design of data diode

B. Characteristics of Data Diodes

Data diode ranges from a scale of one megabit of data throughput between the domains and scales up to ten gigabits of performance, which makes them unmatched by any other networking device in the world, while data diode does also allow control over the flow and speed through rate key change. One of the advantages of data diodes is they provide a complete network separation between the source network and the destination network. And the separation between those networks is a physical air gap to ensure that the networks never connect, they never touch, they never communicate. And we do that through the electric separation of the networks. We do that through photo optics in terms of light transmission, mission, and receiving, through optic connectors.[7] *Data d*iode can support the transfer of multiple protocols protecting your investment on your device. Whether you're passing TCP, UDP file transfer, or even OPC (Open Platform Communications) data Modbus. All of this can be achieved simultaneously across the single data diode. This results in a lower cost, per supported application, Let's say, for example, that you want to send Syslog data from many, many machines across a source network to a destination network. This can be supported by a single data diode solution, adding again, more value to your all advantage.[8] *The Data d*iode has an additional layer of security measurements like role-based access control that does support long passwords with the menu-based interface. it’s also had internal logs and alarms that are stored on the system to track and audit all activities. it also supports security against tampering by having system checks that audit the system for any software modifications and automatically shut down the system if tampering occurs.

A data diode is made of three parts. It’s thought of it as the source side and receiving side, while in between an airgap which is meant to fully isolate the two parts of each other, acts to a similar matter of a full proxy architecture. The source side would be on your protected side, and the receiving side where is the destination which is the open network or a less protected network, so the protected side is your internal network and the less protected side will be your external network. A diode is comprised of two sides, one has an LED that sends a light signal across the fiber optic cable to the destination side, the destination side is based on the receiver, its job is to receive that light that's coming over the fiber optic channel. The destination side does have a receiver and a converter which would convert fiber optic signals source do have an emitter only, while in between is the Airgap which is most of the work is done there, which data gets stripped down back to the physical layer of an OSI layer, to ensure no extra data or information to be carried to the other side of a network as an example of an IP Header. The sender, in essence, can only send light in my direction, which means it's completely unreversible, while it's hardware-based and not able to have tampered with.

There are pinholes in this software-based mechanism that allows data to go back and forth, and the software module is managing those pinholes. But we all know that if I have a pinhole, it becomes a point of entry into my network. Any one of these pinholes can open a vulnerability and allow traffic to get into the network that we don't intend or people that we don't intend to get into. In the data diode, we got the hardware, there is a Led and photo receiver, and therefore absolutely no way to get back into a network. Your network is protected, with no way for an intruder to get through this, and no reverse of path or exploits, Data diodes are hardware-enforced. [8]In that Table 1. given below we present a neat comparison of data diodes with other security mechanisms.

The mechanisms are characterized by their nature i.e., Hardware or Software, Flow of Data i.e.,—way or Two-Way, if they have to send and receive alerts, if they need software configuration and if they provide defense against zero-day attacks.

The only disadvantage arising from the nature of the data diode and their very tight security mechanism is that they don’t seem to be ideal for every network architecture, and they do fill the role of a situational device that do excel in certain parameters than a universal hardware security device as a firewall. Therefore in architecture that requires a lot of connections going back and forth, from a lower secure network to a higher secure network, a data diode would hamper the efficiency of the network, due data diodes are single way only devices, that act like gateway.

Several vendors are already selling a huge collection of data diodes. Table. 2. given below, lists the popular products and provides a comparison to guide the readers about selecting the appropriate product.

III. Literature Review

With the wide geographical expansion of IoT and its scatteration around the globe, they have been a high-priority target due to their vulnerable environment. According to a Report effort done by Nokia, IoT devices do make up 32.72% of infected devices detected in the year of 2020, while in the year of 2019 it did the makeup of only 16.17%, as stated in its “Threat Intelligence Report 2020”, which concluded the report that “Cybercriminals are focusing their effort on IoT and mobile devices.” most uses of data diode are to replicate data and move data from higher secure infrastructure to lower secure infrastructure, with the primary usage of data diode is to backup and disaster recovery repositories, replication of database and other application data, and traffic flow control from different level of security architecture. Data diodes are now supporting multiple IoT at each endpoint, which influential cooperation should utilize various endpoints, or won't be able to achieve a full air gapping measure of IoTs and infrastructure.[9] As also per another study, In 2016 cyberattacks had a large financial impact. U.S. healthcare systems, so owl manufactures data diode cybersecurity products for hardware-enforced one-way data transfer and assured network security against malware, ransomware, and control override. designed with two separate circuits – one send-only, and one receive-only. that also provide certain services like Managed File Transfer, now it's used by the U.S. intelligence, military, and government communities. The result of implementing a data diode is supporting DHS(U.S. Department of Homeland Security), HHS(U.S. Department of Health & Human Services) , and FDA (U.S Food and Drug Administration) best practices in network management, intrusion prevention, and device security and working within standard healthcare protocols. [10] A data diode is a network device allowing data to travel only in one direction to guarantee information security. most found in high-security environments where there are connections between two or more networks of different security levels only allow data to pass from the ‘low’ side of a network connection to the ‘high’ side, and not the other way around There is no shared circuitry beyond the one-way connection, so data diodes are considered by many regulatory bodies to effectively create a physical separation between networks. Once implemented, a data diode cannot be changed in any way.[11] The strength of a data diode is its hardware composition, in which its made with no memory, settings, or configuration that can be remotely changed or altered, in which software-based systems do inherently this issue due to their composition, while some data diodes do implement both software and hardware configuration for further capabilities, but are not as secure as hardware-based data diode. A Data diode is a well-known device to be used when there are legacy systems that do need protection and cannot be protected by themselves, therefore we would use a data diode for this situation. On the other hand, high-standard data diodes are expensive, which makes data diodes less seen in our world, while also some others do not use them due to their lower reliability due to their lacking of acknowledgment of sent data.[12] Further analysis by Boo-Sun Jeon & Jung-Chan Na both about Cyber Security Policy in Industrial Control System using Data Diodes in 2016, data diode is a hardware and software that work on TCP and UDP that provide various services by applied in the industrial application arena to efficiently monitor and control the distributed systems. it uses optical fiber; optical; electrical and electromagnetic technology and for material, it uses nodes, datalink, unidirectional security gateway “TX (Transmitter) only”, and unidirectional security gateway “RX (Receiver) only”. Problems tried to fix the sending node generates Repair Symbols and sends them. When an error occurs, the receiving node can fix it via FEC (Forward Error Correction) decoding with the use of extra data like the Repair Symbol and Source Symbol. The result of that physically allows for one-way communication. We also examine the present commercial products on the market and the many methods that can be used with genuine ICS (Industrial Control Systems).[18] Data diodes are used to standardize network data assembly and streaming of the device diagnostic and instruments reading to a private cloud to perform further analysis and diagnosis over the data, which is implemented in a way got fault recognition and identification. In the 3-layer architecture, the edge tier is the place where data from DCS (Distributed Control System) endpoints and nodes are collected. The edge gateway is what do send the data from the DCS to the main network, and the gateway could be implemented to segregate data and process some data depending on roles. The data is then sent to the platform tier from the edge tier, which is meant where the data is stored, and processed in this tier. UDP & AMQP (Advanced Message Queuing Protocol) Gateways are responsible for handling and sending instrumental data, measurements, and diagnostic data from the field and OTs (Operational Technologies) to the private cloud infrastructure, therefore these types of gateways can be provided through the use of a data diode. As for the layered approach, most IoT systems do follow, it is best to fully airgap the highest critical parts of the system. With the use of initial data diode concepts, and having an upgrade over it, the University of Illinois at Urbana-Champaign designed a data diode in 2007, that was placed on (Temporal Point Cloud Networks) TPCN, to provide a one-way communication which had unidirectional protocols. On both sides of a data diode, gateways translate unidirectional protocols to standard bidirectional protocols to connect the diode to the rest of the network also within high speed such as 3 Gbit/s, there are a study by Wool shows that 80% of firewall rule sets allow any service on inbound traffic and insecure access to firewalls.

Moreover, data diode information flow from low to high, but there is no backflow of data, for that, it uses a fiber optic system with TX capability on only one side and RX capability on the other side, the limitation for data diode is that does not work with the standard TCP/IP protocols, which resulted to accept TCP or UDP packets as input. Which made data diodes to be used by organizations and large cooperations in 2020, governments applied data diodes to various organizations to provide one-way communication by flowing data in one direction only through physical means with high speed, such as optical isolators for example data can be securely transferred from an unclassified NIPR (Non-Classified Internet Protocol Router Network) or HTN (High-Threat Network) to a Secret one, or from unclassified to Top Secret. It is applied on the high network within the organization, and it works like the layered approach to physical security at an airport, but Diodes alone do not provide deep content inspection, sufficient status, control, or even basic availability notifications. To avoid that, the organization must Implement other security mechanisms on the data diode.[14] When implementing data diodes correctly, it provides real-time plant data from the OT network to the IT (Information Technology) network, while also achieving a defense that is impervious to any network-based attacks. With many networks architecture to deploy the data diode, all depending on the need, as we could either deploy a data diode to protect a whole network of control systems, we could deploy a data diode for each control in the network, or even deploy a network level data diode and a data diode for the critical control system. All those choices are meant to satisfy a certain requirement of security depending on how critical the control system is, as data diodes are only a target of physical attacks rather than network-based attacks. The best practice is to have a data diode for each control system itself, which ensures 100% unidirectional operation for each separate data diode.[17] As a supporting matter Dr. Ronald Mraz a Senior Member of IEEE, President & CEO did research that says data diode strategies could have prevented 98% of attacks in 2014 and 2015, According to third-party analysts, data diodes provide the highest level of network security next to physical separation, for the services that provide by data diode Build a Defendable Environment, Reduce Attack Surface Area, Implement Secure Remote Access. data diode should separate into two halves with one diode on each side working together to create a Dual Diode, it supports multiple protocols like Email Alerts and Events, FTP/SFTP (Secure / File Transfer Protocol), Modbus, SQL (Structured Query Language) Database Replication, SNMP (Simple Network Management Protocol) Traps.[15] due to their very high-security feature, The regulator guide, of the Office of Nuclear Regulatory Research, in their Cyber Security Programs of Nuclear Faculties. Data Diodes can be implemented along the communication path to any CDA (Critical Digital Assets) in the nuclear facility, either a direct connection or an indirect connection. As in setting up the defense-in-depth mechanism on the facility, data diodes are mentioned for handling the information flow of logging files [16] The literature review is summarized in Table 3 given below.

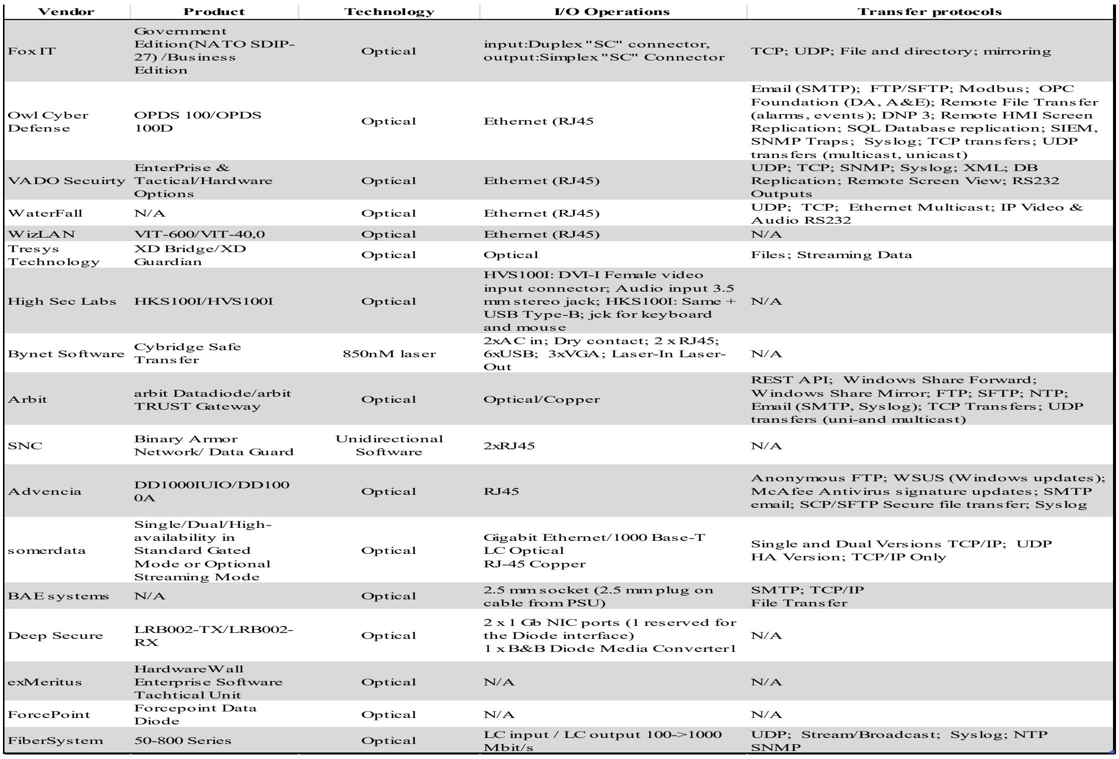
IV. Conclusion

With data diodes are one of the leading security devices, which it is up to date with the current standards and techniques while also implementation techniques. As its implementations allows a secure one-way connection to be established that can be deployed at the convenience of the security team vulnerabilities but are not as secure as the data diode device, which implements the saying "secured by design rather than secured by technology". With this report, we have established a clear engagement and understanding while also clearing up ambiguity about data diodes. While also evaluating the use of data diode and in which sectors it does excel over other security devices, while also revising and understanding future techniques of usage that we can implement data diode in. Its concluded that data diodes are specialized and pricey, it created a barrier to their adoption. Data diode vendors could contribute to addressing the current knowledge gap, improving people's understanding of data diodes' potential, and altering preconceived notions through surveys, reports, and awareness-raising efforts. Businesses lack the expertise and knowledge required to implement data diodes, ensuring that data diode installation is familiar to network security teams, as to be covered in computer science and information technology curricula should be a priority. Although data diodes have been used in networks that require high levels of security, this technology has applications outside of IACS/SCADA and vital infrastructure. The adoption of data diodes would also be advantageous in noncritical industries such as aviation, the auto industry, financial services, health care services, accountancy, legal services, or small manufacturing facilities. Equally crucial is encouraging the use of data diode technology in existing systems.

TABLE I. COMPARING SECURITY MECHANISMS

	Software	Hardware	2 way Connection	Data streaming	Time Sync	NO Physical risk	Sending/receiving alerts	No configuration	Zero day attack
Data Diode	X	√	X	√	√	√	√	√	√
Firewall	√	√	√	√	√	X	√	X	X
ACL	√	X	√	√	√	X	X	X	X
VPN	√	X	√	√	X	X	√	X	X
Encryption / Decryption	√	√	√	√	√	X	√	X	X
Anti - virus	√	X	√	√	√	X	√	X	X
IDS / IPS	√	X	√	√	√	X			

TABLE II. COMPARING DATA DIODE PRODUCTS



Vendor	Product	Technology	I/O Operations	Transfer protocols
Fox IT	Government Edition(NATO SDIP-27) /Business Edition	Optical	input:Duplex "SC" connector, output:Simplex "SC" Connector	TCP; UDP; File and directory; mirroring
Owl Cyber Defense	OPDS 100/OPDS 100D	Optical	Ethernet (RJ45	Email (SMTP); FTP/SFTP; Modbus; OPC Foundation (DA, A&E); Remote File Transfer (alarms, events); DNP 3; Remote HMI Screen Replication; SQL Database replication; SIEM, SNMP Traps; Syslog; TCP transfers; UDP transfers (multicast, unicast)
VADO Secuirty	EnterPrise & Tactical/Hardware Options	Optical	Ethernet (RJ45)	UDP; TCP; SNMP; Syslog; XML; DB Replication; Remote Screen View; RS232 Outputs
WaterFall	N/A	Optical	Ethernet (RJ45)	UDP; TCP; Ethernet Multicast; IP Video & Audio RS232
WizLAN	VIT-600/VIT-40,0	Optical	Ethernet (RJ45)	N/A
Tresys Technology	XD Bridge/XD Guardian	Optical	Optical	Files; Streaming Data
High Sec Labs	HKS100I/HVS100I	Optical	HVS100I: DVI-I Female video input connector; Audio input 3.5 mm stereo jack; HKS100I: Same + USB Type-B; jck for keyboard and mouse	N/A
Bynet Software	Cybridge Safe Transfer	850nM laser	2xAC in; Dry contact; 2 x RJ45; 6xUSB; 3xVGA; Laser-In Laser-Out	N/A
Arbit	arbit Datadiode/arbit TRUST Gateway	Optical	Optical/Copper	REST API; Windows Share Forward; Windows Share Mirror; FTP; SFTP; NTP; Email (SMTP, Syslog); TCP Transfers; UDP transfers (uni-and multicast)
SNC	Binary Armor Network/ Data Guard	Unidirectional Software	2xRJ45	N/A
Advencia	DD1000IUIO/DD1000A	Optical	RJ45	Anonymous FTP; WSUS (Windows updates); McAfee Antivirus signature updates; SMTP email; SCP/SFTP Secure file transfer; Syslog
somerdata	Single/Dual/High-availability in Standard Gated Mode or Optional Streaming Mode	Optical	Gigabit Ethernet/1000 Base-T LC Optical RJ-45 Copper	Single and Dual Versions TCP/IP; UDP HA Version; TCP/IP Only
BAE systems	N/A	Optical	2.5 mm socket (2.5 mm plug on cable from PSU)	SMTP; TCP/IP File Transfer
Deep Secure	LRB002-TX/LRB002-RX	Optical	2 x 1 Gb NIC ports (1 reserved for the Diode interface) 1 x B&B Diode Media Converter1	N/A
exMeritus	HardwareWall Enterprise Software Tachtical Unit	Optical	N/A	N/A
ForcePoint	Forcepoint Data Diode	Optical	N/A	N/A
FiberSystem	50-800 Series	Optical	LC input / LC output 100->1000 Mbit/s	UDP; Stream/Broadcast; Syslog; NTP SNMP

TABLE III. LITERATURE REVIEW SUMMARY

Work	Conceptual or Experimental	Application Area	Bidirectional communication	Material Used	Services provided	Commercial availability
U.S. Nuclear Regulatory Commission, [16]	Experimental	NUCLEAR FACILITIES	Any other bi-directional communication occurs only through a device that enforces all of the security policy y between each level	n/a	Military services	no
T. B. [17]	Conceptual	NUCLEAR FACILITIES	n/a	n/a	Power services	no
Gang Wang [13]	Conceptual	Cloud computing	n/a	n/a	Security services	no
Castagna, R. [9]	Conceptual	IoT	n/a	n/a	Security services	no
K. K. [12]	Experimental	Industry	n/a	LED,sensor, ethernet cable, fiber optic cable	Security services	yes
Forcepoint [14]	Experimental	Industry	bi-directional can be achieved by using additional data diode	LED,sensor, ethernet cable, fiber optic cable	Security services	yes
Jeon [18]	Experimental	Industrial	n/a	n/a	Security services	no
Ronald [15]	Experimental	Business	n/a	LED,sensor, ethernet cable, fiber optic cable	Accreditation Services Configuration Management Services	yes
DeepSecure [11]	Experimental	Industry	n/a	n/a	ZERO TRUST CBR	yes
Owl Security [10]	experimental	Healthcare	n/a	LED,sensor, ethernet cable, fiber optic cable	security services	yes

REFERENCES

[1] E. Andrews, “Who Invented the Internet?,” HISTORY. https://www.history.com/news/who-invented-the-internet (accessed Oct. 31, 2022).

[2] B. Lundgren and N. Möller, “Defining Information Security,” Sci. Eng. Ethics, vol. 25, no. 2, pp. 419–441, 2019, doi: 10.1007/s11948-017-9992-1.

[3] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” Energy Rep., vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[4] “Intrusion detection and prevention system for an IoT environment | Elsevier Enhanced Reader.” https://reader.elsevier.com/reader/sd/pii/S2352864822001201?token=BCA55F3A5BE79BA5F4CCA255AE12E29BCC02535B4E35B2286CB158592A91E4F4CBE2E5254F6D97E7CFFE84996682CF57&originRegion=eu-west-1&originCreation=20221031172333 (accessed Oct. 31, 2022).

[5] “Firewalls vs. Data Diode — Why OT Security Teams Turn to Data Diode TAPs.” https://www.garlandtechnology.com/blog/firewalls-vs.-data-diode-why-ot-security-teams-turn-to-data-diode-taps (accessed Oct. 31, 2022).

[6] H. Okhravi and F. T. Sheldon, “Data diodes in support of trustworthy cyber infrastructure,” in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW ’10, Oak Ridge, Tennessee, 2010, p. 1. doi: 10.1145/1852666.1852692.

[7] D. Pereira, “What is a Data Diode & How Do Data Diodes Work?,” Owl Cyber Defense, Jun. 26, 2018. https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/ (accessed Oct. 31, 2022).

[8] “19-OWL-DataDiodes-Firewalls.pdf.” Accessed: Oct. 31, 2022. [Online]. Available: https://owlcyberdefense.com/wp-content/uploads/2019/05/19-OWL-DataDiodes-Firewalls.pdf

[9] “Why Data Diodes Bolster IoT Security With One-Way Traffic.” https://www.iotworldtoday.com/2021/09/27/why-data-diodes-bolster-iot-security-with-one-way-traffic (accessed Oct. 31, 2022).

[10] “owlcyberdefense-use-case_securing-hospital.pdf.” Accessed: Oct. 31, 2022. [Online]. Available: https://owlcyberdefense.com/wp-content/uploads/2019/05/owlcyberdefense-use-case_securing-hospital.pdf

[11] “Data Diode,” Deep Secure. https://www.deep-secure.com/hsv.php (accessed Oct. 31, 2022).

[12] “HSD-Rapport-Data-Diodes.pdf.” Accessed: Oct. 31, 2022. [Online]. Available: https://hcss.nl/wp-content/uploads/2021/01/HSD-Rapport-Data-Diodes.pdf

[13] G. W. Nixon Mark and M. Boudreaux, “Towards Cloud-assisted Industrial IoT Platform for Large-scale Continuous Condition Monitoring.” Accessed: Oct. 31, 2022. [Online]. Available: https://eprint.iacr.org/undefined/undefined

[14] “datasheet_data_diode_en.pdf.” Accessed: Oct. 31, 2022. [Online]. Available: https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_data_diode_en.pdf

[15] D. R. Mraz, “Data Diode Cybersecurity Implementation Protects SCADA Network and Facilitates Transfer of Operations Information to Business Users,” p. 21, 2015.

[16] “ML090340159.pdf.” Accessed: Oct. 31, 2022. [Online]. Available: https://www.nrc.gov/docs/ML0903/ML090340159.pdf

[17] R. T. Barker and C. J. Cheese, "The application of data diodes for securely connecting nuclear power plant safety systems to the corporate IT network," 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, 2012, pp. 1-6, doi: 10.1049/cp.2012.1514.

[18] B. -S. Jeon and J. -C. Na, "A study of cyber security policy in industrial control system using data diodes," 2016 18th International Conference on Advanced Communication Technology (ICACT), 2016, pp. 314-317, doi: 10.1109/ICACT.2016.7423374.