OWL Cyber Defense

Webinar: "Data Diodes 201"

Q&A Recap

In a recent Energy Central PowerSession - Data Diodes 201: Digging into the Use Cases - we dove into specific use cases, shared examples of data diode deployments, and explained how various data types are supported. If you missed the webinar, you can watch it here.

This document highlights questions from session participants and responses from our panel of cybersecurity experts.

What are the merits of a hardware-based diode approach over a software deployed solution?

Answer – Any software-based solution relies on a CPU for its operation, and a CPU has no built-in restrictions on what it will and will not do— if malicious code reaches the CPU, the CPU will execute it. This remains a fundamental challenge even after decades of effort to develop secure software-based solutions. Hardware-based solutions, on the other hand, can be designed so that it is physically impossible for a component to operate in an unintended way, or to perform any function other than the one it was designed to perform. A data diode, for example, has a one-way transmitter and a one-way receiver that cannot be made to send data in the reverse direction.

Are data diodes used as part of a defense in depth strategy, a stand alone security solution, or both?

Answer – Diodes are best viewed as part of a defense-in-depth strategy. Data diodes can work directly with existing firewalls, with layers of security tools working together for additional security. Some customers use multiple paths for transfer of information into and out of networks, with the addition of defense-in-depth techniques like deep packet inspection, authentication and white-listing to enable the uploading of software patches and the transfer of demand orders.

Is it possible to have multiple servers/applications utilizing a single data diode device as a gateway to corporate servers?

Answer – Data diodes can transfer multiple data types and data flows simultaneously, with multiple sources and destinations. Owl customers commonly route dozens of data flows (or even more) over multiple protocols through a single data diode solution.

Can data diodes be used in conjunction with Emerson Ovation?

Answer – Yes, Owl customers have used data diodes to provide hardware-enforced one-way data flow in conjunction with remote monitoring systems including Emerson Ovation. Owl provides functionality that allows remote personnel to view screen displays and other data in essentially real time, without enabling remote access to systems. Modifications to systems within the plant can be made by onsite personnel in collaboration (typically via phone) with remote engineers.

Can you comment on the recent Colonial Pipeline attack and how data diodes would mitigate similar risks?

Answer – Based on the initial reports, Colonial appears to have shut down its pipeline as a precautionary measure. Once malware was active on their IT network, the company may not have known whether or not the damage could spread to the operational technology (OT) systems that actually control the flow of fuel through the pipeline.

Data diodes provide reliable network segmentation that protects OT systems from malware that exists within IT environments and mitigates the risk that an attack can spread to the operational layer. For example, When Russian hackers attacked the Wolf Creek nuclear facility in 2017, the plant was able to maintain operations with no disruption, because they trusted the diode-enforced isolation between the business network and the OT systems within the facility. The plant's operators knew that even if the IT network was compromised, there was minimal risk that it would find a path from the infected systems into the plant.

How does having a one-way in connection and a one-way out differ from a single two-way connection?

Answer – Owl's ReCon bidirectional data diode solution enables a secure, non-routable bidirectional command and control initiated only on the secure side of the network that meets NERC requirements for eliminating persistent, routable bidirectional data connections. Separate, one-way-in and one-way-out connections can be used when certain data (for example, software patches) needs to be sent into a secure facility. Modification to the bidirectional configuration would require physical access to the facility.

How widespread is the use of data diodes today?

Answer – Data diodes are utilized in power stations and energy production facilities worldwide and can help meet a variety of standards and regulatory requirements.

Data diodes can be deployed virtually anywhere from the edge of the facility network all the way down to individual devices. Typically, we see them deployed at DMZs between various levels of the network, to control data flows from one to the next. More recently, however, we've seen more installations at the micro-segmentation level and have recently released a line of embedded solutions designed to be installed within SCADA/ICS devices themselves.

Can the secure side diode transfer web page data to the unsecure side?

Answer – Yes, Owl provides a protocol adapter for HTTP(S), so this could be achieved by routing HTTP(S) traffic from a computer on the secure (or "send") side through a data diode and to a destination on the "receive" side of the diode. HTTP(S) "PUT" and "POST" commands are able to send data one-way, not requiring a two-way communication channel.

Can data diodes be used to send equipment sensor data from OSI Plant Historian to the cloud?

Answer – Yes. For over 9 years, Owl has partnered with OSIsoft® to protect and replicate PI System historians, with hundreds of implementations around the world, spanning a number of industries. A common data diode use case involves replicating OT historian data in the cloud. Sensor data is streamed to a local historian database, and then the database contents are replicated to the cloud after passing across a data diode. This proven solution, used in conjunction with OSIsoft operational intelligence technology, allows users to meet stricter security requirements for their business practices, through hardware-enforced network segmentation and one-way, deterministic data transfer.

How would the use of data diodes relate to ISA 18.2 and IEC 62682 alarm management standards?

Answer – The use of data diodes would not be likely to affect an organization's compliance with alarm management standards such as ISA 18.2 and IEC 62682. Alarm management systems are generally only expected to receive data from monitored systems, not to send data into a protected system.