Enabling secure browse-down with Oakdoor™ Hardware Security Solutions

There are number of situations in which a device on your high-security side of a network needs to communicate with a lower-security segment, possibly even the internet. Doing this securely by adopting a robust browse-down approach is essential to prevent attackers gaining access to your organisation's trusted environment. The volume and speed of traffic involved can make it challenging to achieve a practical solution.

Typical browse-down infrastructure

The UK National Cyber Security Centre (NCSC) emphasises the importance of protecting devices within high-security systems by not allowing them to natively perform activities such as browsing the internet or opening external email. It recommends browse-down techniques like using a virtual machine or connecting over a remote desktop to ensure that if malware does succeed in compromising the environment, the attacker has not yet compromised the high-security side. While the software-based browse-down approach makes attacks harder, there is still a real possibility of exploits breaking free from remote or virtual systems and exploiting your sensitive high-security systems.

How Oakdoor helps

Oakdoor data diodes, an integral part of a robust cross domain solution, use hardware-enforced verification to minimise the risk of malicious data penetrating your secure systems without compromising the ability of users to interact with other networks when they need to.

Unlike software-based approaches, hardware solutions offer a more reliable alternative and are also able to better handle the high data rates involved in browsing-down.

Data diodes are simple but powerful devices that permit data to move in just one direction. They ensure that during data export, no malicious data can return through the same channel, thus securing the connection. Conversely, when importing data, they prevent any unauthorised exfiltration of data through the same network path, effectively blocking potential security breaches.

Combined with content inspection they prevent transmission of malware across network boundaries in way that is highly resistant to hacking. Our data diodes combine flow control with careful syntactic content inspection and semantic verification to prevent transmission of malware from untrusted to trusted parts of a network. They are one of the first data diodes to implement this hardware-based syntax verification, which allows structured data to enter while ensuring that potentially malicious data will always be identified and handled in a safe way. Our technology enforces segregated browsing, in which only authorised keyboard and mouse commands are allowed to exit your high-security system, and the only data that is allowed to enter is securely verified bitmap images.

Oakdoor Diodes are already established in government and defence environments. By implementing key stages of the UK National Cyber Security Centre's (NCSC) design patterns for Safely Importing Data and Safely Exporting Data, Oakdoor data diodes are accredited for use in even the most secure environments.

Hardware-based security has traditionally been inflexible and hard to deploy in existing network infrastructures. Oakdoor changes that by offering a combined hardware and software solution that is scalable and reliable for organisations to implement data diodes at multiple points across their network.

Features

- Hardware-enforced unidirectional flow control
- CAPS-approved by NCSC for use in the most sensitive operational environments
- Ideal for cross-domain applications that require flexibility and speed
- Data structure inspection ensures that only structured data can pass
- High data throughput
- More secure and lower maintenance than a software firewall alone

Our products

Oakdoor 1G Data Diodes

Strong security with a low capital cost, ideal for a variety of cross-domain applications that require flexibility and speed.

Oakdoor Enterprise Diodes

Designed for data centre needs, a massively parallel internal architecture supports content syntactic verification at a full 10GbE line rate. Flexibility to route data between thousands of virtual machines in source and destination networks.

Oakdoor Gateway

Single-box solution for applications that require bidirectional data transfer. An import diode and export diode with two integrated servers on either side to accommodate the necessary software for your specific application.

About Oakdoor

Developed at PA's Global Innovation and Technology Centre (GITC), Oakdoor Hardware Security Solutions combine innovative thinking and breakthrough technologies to combat modern day cyber threats.

To find out more about our products, visit us at: **LinkedIn** and **oakdoor.io**