OWL Cyber Defense

SSUS
Secure Update Transfers

FEATURES

- Secure transfer of any executable & non-executable files
- Utilizes hardware-enforced data diode security technology
- Multi-factor file validation & scanning
- Separate user interfaces for Send/Receive
- Support for multiple hash code algorithms
- Comprehensive activity monitoring, error logging, and error log management
- Integrity check failure alarms user
- Low-to-high, peer to peer transfers

BENEFITS

- Provides highly controlled means to transfer ONLY files into secure networks
- Secure process for timely updates of software patches & anti-virus programs
- State-of-the-art transfer audit trails
- Scans and verifies file type against extension to prevent "masked" threats
- Two-user authentication helps mitigate insider threats
- Easy configuration and transfer management

Safely Import Software Updates Into Closed Networks

Just like any other network, secured or isolated networks (plants, oil rigs, substations) contain computers, servers, control systems, databases, etc. that require software updates on a recurring basis. In order to update these devices, software updates are typically downloaded from the vendor's website to a local server, copied onto a portable media device (e.g. a USB drive) and hand-carried into the secure network for installation.

According to the DHS, FBI, and NSA, this method is not a good choice. In the process of downloading, saving, copying to portable media and uploading on the secure network, the source file could be intentionally attacked or the portable media device itself could be compromised with malware lurking. In the process of downloading, saving, copying to portable media and uploading on the secure network, the source file could be unwittingly manipulated.

The Owl Solution

The **Owl Secure Software Update Solution (SSUS)** is a data diode-based cybersecurity solution that follows the "Seven Steps to Effectively Defend Industrial Control Systems by providing a highly secure method to validate, scan, and transfer software patch and executable files into secured or isolated networks. SSUS individually validates executable and non-executable files against a manifest of pre-configured hash numbers provided by the software provider or vendor. Files that do not have a matching hash are quarantined.
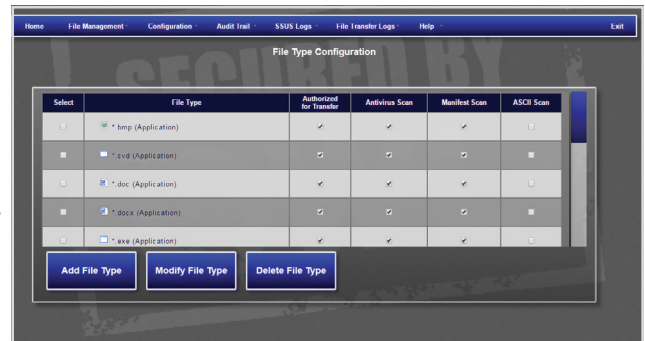
For additional security and information assurance, SSUS provides enhanced controls to enable content inspection, file type/extension checks, antivirus, and ASCII scanning. SSUS also permits implementation of two-person authentication approval and release process. These comprehensive security features allow organizations to establish a security policy which explicitly prohibits the use of portable media devices to transfer data between security levels and only allows low-to-high and peer to peer transfers.

The technician operating for a secure network needed a reliable and secure method to verify and transfer software patches, provided by vendors, into the network. The IT Technician selected SSUS to maintain tight control over the data that can enter the network. Utilizing the SSUS highly secure method for file transfer, the IT Technician requests a hash code from the software vendors that is independently entered into a manifest on SSUS. When a file is copied onto SSUS for transfer, SSUS calculates the hash code of the file, compares it to the hash code in the manifest and if it matches it is transferred to the secure network, otherwise it is quarantined.
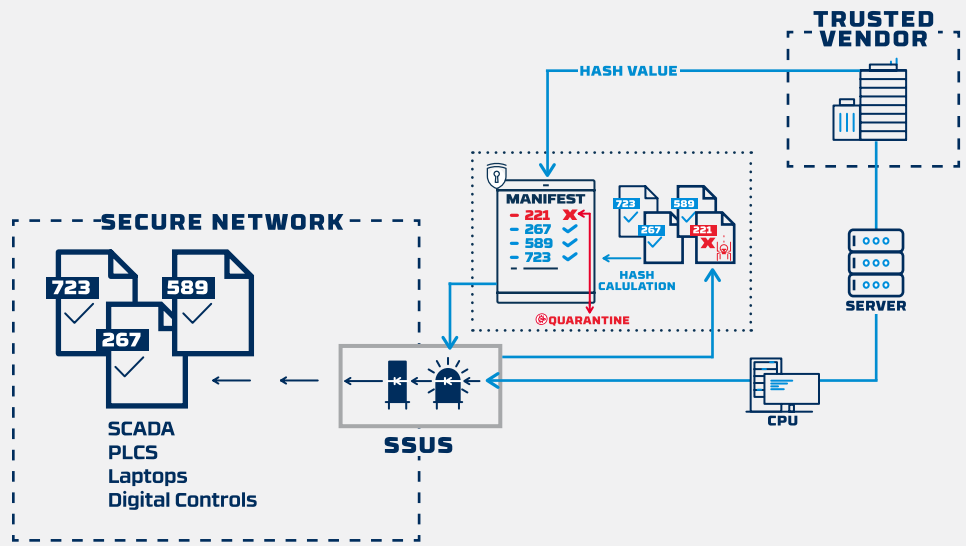
Architecture

SSUS operates on 1U 19" rack mountable platform and leverages Owl's market-leading data diode technology. This all in one cybersecurity solution is designed to create a hardware-enforced cyber perimeter by heavily regulating incoming files through Owl's sophisticated scanning and filtering software.

With an easy-to-use graphical user interface for both Send and Receive sides of the diode, SSUS dramatically simplifies the process of vetting incoming software updates and other files into a secured network. SSUS also includes a comprehensive logging suite, capturing a detailed history of all actions, files, and transfers performed on the platform.

For those business operations that require highly secure methods for updating patches on a routine basis but do not want to create risk by downloading a file or using a potentially attacked portable media device , SSUS is the ideal solution. Its ability to transfer files only by hash codes prevents unknown traffic from passing through, making it completely secure.

Technical Specifications

OPERATING CONDITIONS:
- 32°F to +110°F
- 0°C to +43.33°C
- 5% to 90% humidity non-condensing

POWER SUPPLY:
- Input: 75-230 VAC,
- Estimated Normal operating Usage 10-16 W/side
- Max. 20W per side

STORAGE:
- -40°F to 158°F
- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION:
- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (Operational)
- Vibration 2g(10-500Hz) (Operational and Non-Operational)

CHASSIS SIZE:
- 16.5" W x 1.75" H x 13" D
- 41.91 cm x 4.5 cm x 33 cm

SHOCK:
- Shock: (IEC 60255-21-2)
- Shock 10g 11ms (Operational)
- Shock 30g 11ms (Operational and Non-Operational)

UNIT WEIGHT:
- 7.92 lbs./3.6 kg.

MEAN TIME BETWEEN FAILURE (MTBF):
- 11+ years