The CyberFence Difference

Comprehensive Encryption for Embedded Systems in Industrial Control Networks

Precise processes in most critical-infrastructure networks rely on the undisturbed operation of industrial control systems (ICS). Failures within the ICS can cause critical services to fail, and may result in severe injury to people, property and the environment. In evaluating options for securing vulnerable endpoints within an ICS, encryption and authentication should be thoroughly reviewed. This advanced security thwarts unauthorized devices and malicious interference to critical command and control processes in ICS.

CyberFence offers a fully-certified, high-performance solution that uniquely addresses the ICS cyber security recommendations of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). 3eTI and the CyberFence series surpass alternatives for independent, third-party evaluation and certification. Additionally, CyberFence interoperability, key management and encryption solutions are unmatched in the industry. Validated and easy-to-use key infrastructure solutions can be included as a package with every installation.

Security experts recommend the following CyberFence performance features:

CyberFence Attributes & Applications

Independent Validation

The CyberFence encryption implementation is fully vetted by numerous independent labs and experts to highest standards for assured protection. It is Common Criteria Certified by the National Information Assurance Partnership (NIAP), as well as FIPS 140-2 Validated by the National Institute of Standards and Technology (NIST). As most encryption vulnerabilities result from weak implementations, the fully-validated CyberFence is chosen for defense industrial networks for which efficiently secured machine-to-machine (M2M) communications are essential.

Key Generation

3eTI engineers built a hardware-based entropy source into CyberFence so that all encryption is seeded with truly random numbers. There is no need for weaker computer-generated or pseudo-artificial randomness.

Key Management

Contrary to best practice, purchasers often perform a cursory evaluation then buy encryption based on the algorithms used. Independent experts, including those with DHS, also recommend the purchase and implementation of a key management cryptosystem. Operators often bypass this functionality because it is complex and difficult to implement without compromising ease of use. They too often opt to sacrifice hardened security for convenience. CyberFence solves this challenge by providing a complete key-management solution or by interoperating with any existing PKI (public or private). With the UltraVision key management solution, users generate and control their own keys and certificates that are securely distributed to devices with a single click.

Hardware Implementation

Encryption can be implemented separately in hardware or through a device's software. The hardware option's main advantage is superior latency and throughput performance. From a security standpoint, the preferred approach is to use dedicated hardware to prevent a software encryption bug from compromising applications or causing a denial-of-service failure.

Virtual Private Network (VPN)

CyberFence includes the latest and strongest commercially available algorithm suites, among them DH and ECDH for key exchange, AES 128/192/256 CBC/GCM/CCM for encryption, and SHA-1/256/384/512 for integrity. CyberFence also supports RSA and EC-DSA certificates for end-to-end authentication. All of this affords compatibility with an exceptionally wide range of systems, among them Cisco ASA gateways and Windows 2012 security servers. Moreover, CyberFence supports users installing their own certificates to prevent rogue or default credentials, or third-party key intercepts compromising encryption integrity.

V-LAN Encryption

The CyberFence series provides Layer 2 encryption. It secures Ethernet packets using AES 128/192/256 encryption, with unique keys for each VLAN. The result is very fast local-network encryption that supports distributed mesh, or multi-point to multi-point communications without introducing a single point of failure (such as a VPN server). V-LAN encryption can protect existing control-system deployments without requiring upgraded devices or protocols. In this way, CyberFence can be retrofitted to protect legacy and new-build systems.

Transport Layer Security (TLS)

Operators of industrial control networks often opt to secure communications by tunneling protocols over TLS. While doing so may seem a straightforward solution, it often introduces unanticipated impacts. TLS has a higher overhead relative to VPN or V-LAN encryption, which reduces network performance. Moreover, TLS supports only TCP/IP traffic, leaving critical broadcast or point-multi-point communications unprotected. TLS is implemented at the application level where a software bug will completely expose devices to multiple threats. Each critical device will then have to perform all cryptographic functions at a significant performance and setup cost. CyberFence reduces the impact encryption has on a system and does not expose critical control applications to inherent vulnerabilities.

Interoperability

Overwhelmingly, solution providers claiming use of open standards deliver products that are not interoperable with other systems. Typically users must connect using a vendor's equipment at both ends, use the vendor's proprietary management interface or, worst of all, vendor provided/installed keys. By contrast, 3eTI and CyberFence are fully and universally interoperable with cryptographic and management functions.

Separate Management

Most ICS security solutions perform management in-band and over the same VPN tunnel or network connection used by other ICS data. This practice renders those solutions vulnerable to any malware that has penetrated the data network. 3eTI's CyberFence solution separates data and management across different tunnels and interfaces. In so doing, CyberFence isolates access to the management interface from any malware in the control network, ensuring that those managing the security device cannot interfere with critical-control traffic, or vice versa.