CybrSec

Warfighter Authentication & Secure Communication System (WASC)

2018 Defense TechConnect Innovation Award Winner
https://events.techconnect.org/DTCFall/awards.html#

For over 30 years, the military has relied on Public Key Infrastructure to protect critical communications and data assets. Certificate Authorities have been developed to fill the gaping weakness of PKI of not providing authentication. Certificate Authorities do nothing to solve the problem though, as the trustworthiness of the CA itself is still not guaranteed for any particular individual. It is a form of argument from authority fallacy. For actual trustworthiness, personal verification that the certificate belongs to the CA and establishment of trust in the CA are required. This is usually not possible.

A new security infrastructure has been developed which cracks the age old problem of securely exchanging encryption keys, and which also provides a robust authentication capability. The new technology is called B2 Cryptography. It utilizes portable security tokens to provide the unprecedented new level in data protection while supporting a hierarchal structure so the chain-of-command has control of informational assets.

CybrSec Corporation is the first to deploy products based on B2 Cryptography. The GoldKey security products have been evaluated by the US Navy and are now fully deployed. GoldKeys are FIPS Certified.

The WASC solution offered by CybrSec provides important benefits to the DOD.

1. It is the only hardware based security system to provide intrinsic authentication. It eliminates man-in-the-middle or MITM attacks.
2. Can be used to remotely manage security credentials based on a chain-of-command hierarchy.
3. Makes email, text, telephone and video communications extremely secure even over public networks when necessary.
4. Deploys on top of existing security methods and solutions.
5. Protects sensitive data in Servers even when captured in the field by insurgents.
6. Utilizes nano-latency networking technologies developed under SBIR Army Contract #W31P4Q-12-C-0118, improving network response times by orders of magnitude making it possible for warfighters and leaders to be able to make critical data-driven decisions at “mission-speed”.
7. The ability to make sensitive data available in the battlefield, but then restricting the data decryption capability upon demand from central command.

By combining hierarchal security tokens, secure servers, and nano-latency networking products with built-in security, the company brings the DOD the first completely integrated solution combining extreme security with extreme performance.

While these products have been commercially used by the military for the past few years, these have been proof of concept projects in preparation for the full launch of the product line.

The full commercial launch of these products is set for Defense TechConnect, October 23, 2018 in Tampa, Florida.