NSA-approved two-layer encryption approach slashes cost and development time

By Paul Davis

An industry perspective from Curtiss-Wright Defense Solutions

In today's world, it is becoming increasingly important to be able to protect classified data-at-rest with encryption for critical data, such as that captured and stored during airborne intelligence, surveillance, and reconnaissance (ISR) missions. For some programs with limited budgets and schedule, using National Security Agency (NSA)-approved Type 1 encryption, the highest level of data protection, may prove impractical due to the high cost – typically several millions of dollars for a new development – and long process – typically two to three years that it takes to reach full certification. The cost and schedule required to deliver Type 1 encrypted hardware has meant that industry's ability to provide robust data protection has lagged far behind the demand.

The good news is that, in response to the growing need to protect increasing amounts of sensitive data, the NSA has initiated an alternative approach that provides a route for the use of commercially sourced encryption technologies for applications that do not require the highest levels of protection (for example, Top Secret/Unattended). For these transactions, the NSA/Central Security Service's (NSA/CSS) Information Assurance Directorate (IAD) launched the Commercial Solutions for Classified Program (CSfC).

According to the NSA, the CSfC Program "enables commercial products to be used in layered solutions to protect classified NSS (National Security Systems) information." The goal of the program is to "provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years." This means that commercial off-the-shelf (COTS) vendors can now, for the first time, significantly reduce the cost and time needed to deliver data security solutions that meet NSA approval. CSfC includes a definition in its "Data at Rest Capability Package" for two-layer encryption that incorporates software full disk encryption (SWFDE) combined with hardware full disk encryption (HWFDE).

In one approach to two-layer encryption, the hardware layer protection is handled by an application-specific integrated circuit (ASIC) that provides AES 256-bit encryption. The ASIC has been certified under National Institute of Standards and Technology (NIST) standards to the FIPS140-2 specification. While a software encryption layer can be done in a variety of different ways – using, for example, Linux or Windows – for the CSfC program NSA defines use of a certified version of an operating system, and points to Red Hat Enterprise Linux (RHEL). RHEL includes an encryption layer, dm_crypt, that performs the AES 256-bit encryption in software.

For COTS vendors who to want to use two-layer encryption in a product, the process starts by signing a Memorandum of Agreement (MOA) with the NSA to undergo CSfC certification. After the proposed product is successfully evaluated, it is placed on the CSfC Component List that integrators, such as prime contractors, can use to identify certified products for data protection. The system integrator can then apply to the NSA to use a specific approved product included on the Component List to encrypt the level of data required by their particular program. This approach enables system integrators to begin evaluating their data-security architecture and greatly reduces program risk.

Figure 1 | The Curtiss-Wright Data Transport System 1-Slot (DTS-1) supports the NSA two-layer encryption approach.

A rugged COTS product designed to support the NSA-defined two-layer encryption scenario described above, combining the ASIC and Linux O/S hardware and software encryption methodology in a single device, is Curtiss-Wright's Data Transport System 1-Slot (DTS-1), a rugged network attached storage (NAS) file server that provides high-capacity secure storage. (Figure 1.) The small-form-factor, single-slot NAS data transport system provides 2 TB of storage and supports two-layer encryption.

For aerospace and defense COTS customers, the advantages and benefits of the CSfC-defined two-layer encryption approach are clear. After a product is listed on the Component List, the cost of data protection essentially disappears, dropping from several million dollars to zero, since the COTS vendor has absorbed all the costs of the approval process. Once the system integrator gets the "go-ahead" from the NSA to use a particular Component List product in their program, they can simply purchase the desired product. This approach, using commercial encryption technologies, promises to speed the protection of vast amounts of critical data using COTS hardware.

Paul Davis
Director of Product Development – Data Solutions
Curtiss-Wright
www.cwcdefense.com