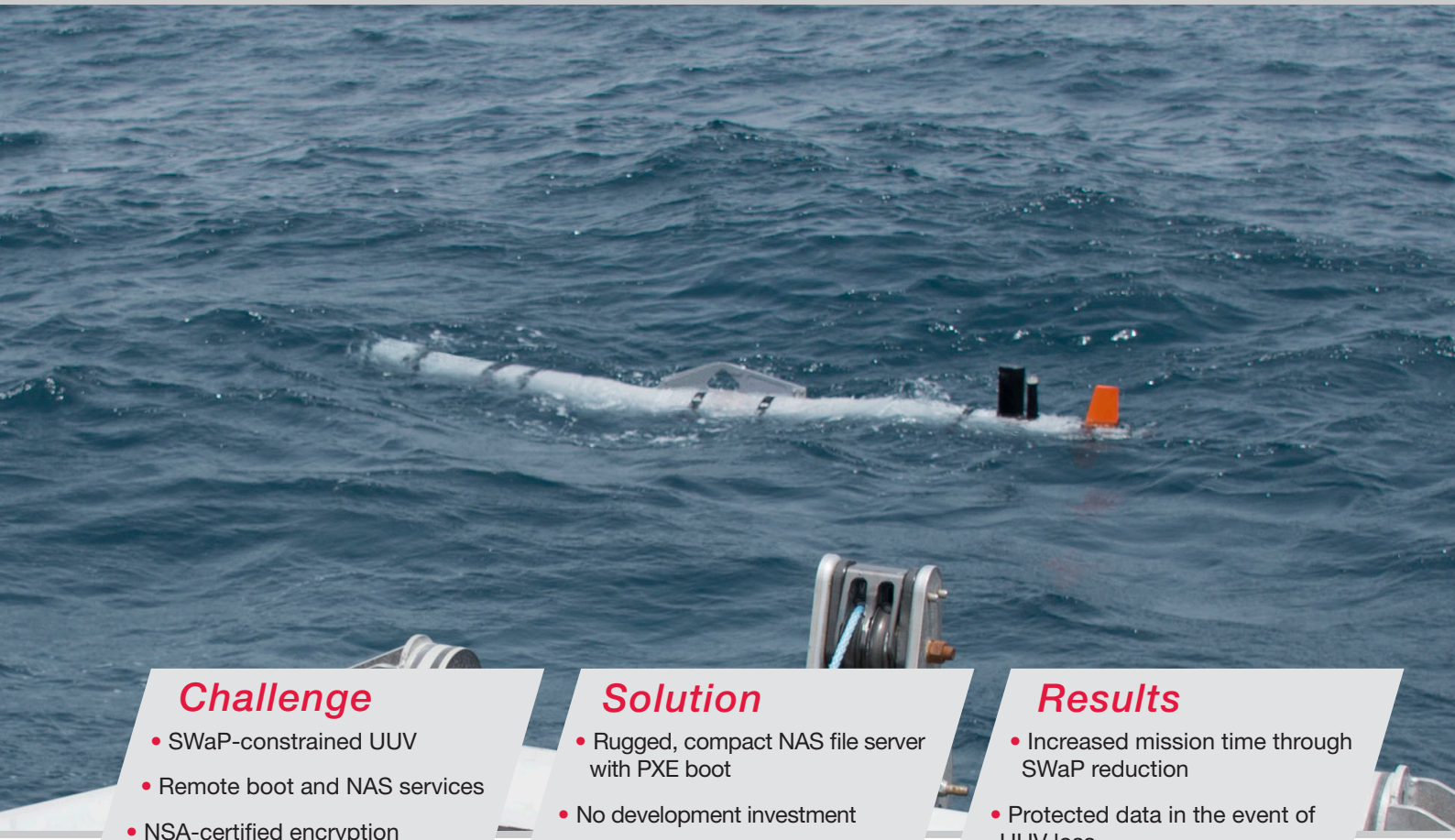
CASE STUDY

A COTS Approach to Data-at-Rest Encryption Onboard an Unmanned Underwater Vehicle (UUV)

CURTISS-WRIGHT



Challenge

- SWaP-constrained UUV
- Remote boot and NAS services
- NSA-certified encryption
- Very tight schedule

Solution

- Rugged, compact NAS file server with PXE boot
- No development investment
- CSfC certification

Results

- Increased mission time through SWaP reduction
- Protected data in the event of UUV loss
- Met aggressive delivery schedule

Challenge

Looking for a network attached storage (NAS) device for an unmanned underwater vehicle (UUV), a system developer contacted Curtiss-Wright. Due to the size, weight and power (SWaP) constraints of the vehicle, the NAS needed to be very small while providing the network services of a larger file server. This aggressive approach to SWaP would extend the UUV mission length by propelling less mass through the water, free up space for other sensing or computing equipment and enable the vehicle's power plant to last longer and go further.

In addition to reducing the physical size and weight of the NAS, implementing remote boot of the network clients would provide an added SWaP optimization opportunity. Successful remote boot would eliminate the need for each network client to have independent storage. With over a dozen network clients on board, each with its own OS and unique application allowing it to perform its system function, the removal of a storage drive from each client could significantly reduce SWaP.

Since the UUV could be lost during deployment (as recent events in the South China Sea have shown), the developer (and their end customer) required that the classified data be protected to national standards. For data encryption, the choices included Type 1 devices or commercial encryption methods, but either solution must meet NSA approval.

With an accelerated deployment schedule, the choices were limited to what could be accomplished without a long RFI/RFP and development process. The program could not afford schedule delays due to an encryptor development schedule and nor could they afford NRE investment.

DTS1: 1-slot Rugged Network Attached File Server

Solution

With support for industry-standard network file services, the DTS1 was chosen, allowing any network client to save a file on the device or retrieve a file from it. In addition to Network File System (NFS), Common Internet File System (CIFS), File Transfer Protocol (FTP), and HTTP protocols, the DTS1 also supports the ability to boot network clients with Pre-boot Execution environment (PXE). This enables the customer to load operating systems (OS) and application code on the DTS1's removable memory cartridge (RMC). Each time the system boots, each network client uses PXE to obtain its OS and application program from the DTS1, thus eliminating separate solid-state storage drives (SSD) in each of the clients.

The data stored on the DTS1 is protected by two different layers of encryption – a hardware and a software layer. The hardware layer is full disk encryption (HWFDE) using an AES256-bit FIPS certified ASIC. The software layer is full disk encryption (SWFDE) and the AES256-bit algorithm is also FIPS certified. This layered encryption approach was a critical requirement needed for National Security Agency (NSA) certification of the storage device.

The DTS1 was developed with the goal to be certified by the NSA under their Commercial Solutions for Classified (CSfC) program. The CSfC process enables commercial components to be used in layered solutions to protect classified National Security Systems (NSS) information. The key word is 'layered'. The NSA defines the approved solutions in their DAR Capability Package (CP). The CSfC process also includes the means for vendors to get their components on the CSfC Components List, making them eligible for use in a CSfC solution.

In order to qualify to be on the CSfC approved component list, the device must first be evaluated by the National Information Assurance Partnership (NIAP) which oversees U.S. evaluations of commercial IT products for use in NSS. The NIAP has implemented the Common Criteria Evaluation and Validation Scheme (CCEVS) to meet the requirements of the internationally supported Common Criteria Recognition Arrangement (CCRA). So NIAP evaluations are mutually recognized in all CCRA member nations.

The NIAP evaluations are conducted by National Voluntary Laboratory Accreditation Program (NVLAP)-accredited commercial testing labs. Working with Gossamer Laboratories (accredited under NVLAP), Curtiss-Wright identified the appropriate two Protection Profiles (PP) which were used to complete the evaluation for such a data-at-rest (DAR) product. A PP is an implementation-independent set of security requirements and test activities for a particular technology that enables achievable, repeatable, and testable evaluations. All products evaluated under NIAP must demonstrate exact compliance to the applicable Protection Profile(s). If successful, NIAP validates the results of the security evaluation conducted by the lab by issuing a Common Criteria certificate. NSA reviews the CC report and (if in agreement) lists the product on the CSfC Component List.

Results

Since Curtiss-Wright had already started the DTS1 IRAD development, the delivery schedule supported the developer's requirement for quick delivery of pre-production units. The early units were delivered and are currently successfully operating on-board the vehicle. Having performed a CC and CSfC Gap Analysis with Gossamer, Curtiss-Wright was able to provide a low risk certification roadmap to the developer, and in turn to their customer. This certified encryption approach enabled the developer to assure their customer that the data-at-rest would be protected in the event of vehicle loss; fulfilling a critical requirement for deployment approval by the end customer.

Curtiss-Wright's investment in not only the DTS1 development but also the CC and CSfC testing allowed both developer and end customer to save money by leveraging the COTS investment. The implementation of remote boot using PXE, allowed them to save SWaP on-board the vehicle resulting in longer missions and a smaller, less detectable vehicle profile. Additionally, the network client software was field updatable, resulting in more vehicle up-time.

INFO: CURTISSWRIGHTDS.COM
EMAIL: DS@CURTISSWRIGHT.COM