Unmanned Surface Vehicle Requires NetBoot and Commercial Encryption

Challenge	Solution	Result
High-capacity removable network attached storage	An 8 TB, removable memory cartridge	Massive sensor data was shared between network clients
NSA-approved encryption	NSA CSfC-approved 2-layer encryption	Protection of top-secret data during transport
Network booting for multiple clients	PXE protocol support	Simplified client software maintenance

Challenge

An Unmanned Surface Vehicle (USV) developer, to meet the mission statement and customer's requirements, planned to connect all the computer and sensor systems using an Ethernet network. These systems (called network clients) would share data during the mission, including map, mission, and sensor data. So, a network-attached storage (NAS) device was required to store and distribute the data.

Since the USV would have no crew on-board to protect it from an adversary, the top-secret-level data had to be protected with National Security Agency (NSA)-approved encryption. The developer decided to follow the NSA's Commercial Solutions for Classified (CSfC) program. Before each mission, the mission plans and map data were to be transported from the base station to the USV. After each mission, any data collected would have to be transported back to the base station for analysis.

With over a dozen network clients, the USV developer decided to use the NAS to not only store and protect the classified data but also to host the operating systems (OS) and applications (APP) for the various clients. Instead of having a solid-state disk (SSD) in each client, the NAS would distribute the OS and APP to each client. To support data transport to and from the USV, the NAS had to include removable storage with high capacity. The removable memory had to be considered unclassified during that transport.

curtisswrightds.com/case-studies
ds@curtisswright.com
1.937.252.5601

Solution

Working to a tight schedule, the USV developer sought a low-risk solution: an existing NAS that did not require development or government approval. They turned to Curtiss-Wright Defense Solutions. With many years of experience protecting data-at-rest (DAR), Curtiss-Wright proposed a low-risk, high-security solution.

Curtiss-Wright proposed the Data Transport System 1-Slot NAS (DTS1), the industry's first commercial off-the-shelf (COTS) NAS solution that supports two layers of full-disk encryption in a single data-at-rest (DAR) device. The DTS1 is a small form-factor file server that weighs just three pounds, occupies less than 50 cubic inches, and provides scalable storage of up to 8 TB on a single removable memory cartridge (RMC). The RMC is easy to transport and small enough to fit into a shirt pocket.

The two full-disk encryption layers (one hardware and one software) have been approved by the NSA as CSfC components. CSfC is an NSA-approved COTS approach for protecting classified National Security Systems (NSS) information. As a requirement for NSA approval, the two DTS1 encryption layers have been certified by the National Information Assurance Partnership (NIAP) under the Common Criteria (CC) program. With the DTS1, the developer could securely store top-secret data on-board the USV and then safely transport the data to and from the USV. The RMC is considered unclassified when removed and unpowered.

In addition to standard protocols like CIFS, NFS, iSCSI, and FTP, the DTS1 also includes the Preboot eXecution Environment (PXE) protocol. PXE (commonly pronounced 'pixie') protocol allows the clients to ping the DTS1 upon startup. Each client is identified before being sent their OS and APP. The clients do not require a local SSD, just a startup ROM and operating RAM.

Result

An obvious benefit of the DTS1 NAS was the ability to share data between all the network clients: the mission plans and maps loaded before the mission were available to all clients. The 8 TB RMC provided plenty of room to collect and store massive amounts of sensor data.

Given the capricious nature of battlefields, it was expected that some USVs would be captured. Many deployed vehicles, especially unmanned ones, have been lost recently. With CSfC-approved encryption, the developer's end customer was assured that the top-secret data was protected from adversaries in such an event.

During transport to and from the USV, the RMC is subject to capture by adversaries or misplacement by personnel. Because the two NSA-approved encryption layers protect the data on the RMC, the RMC is considered unclassified when unplugged and unpowered.

Prior to a mission at the base station, the RMC would be loaded with the latest OS and APP for the various clients. Upon startup, these updated files would be distributed to each client. Thus, each client was loaded with the latest software before each mission. The USV also had more up-time and was ready for missions more frequently. Risks were eliminated, and time to update software was reduced. Fewer personnel were required at the depot.

DTS1 - Data Transport System

curtisswrightds.com/case-studies
ds@curtisswright.com
1.937.252.5601