Choosing the Best Location for Your Data-At-Rest Encryption Technology

CURTISS-WRIGHT
DEFENSE SOLUTIONS

Read About

- Data-at-rest (DAR) encryption
- DAR vulnerabilities
- GOTS vs COTS Encryption
- NSA CSfC
- NSA Type 1
- Removable Media

Introduction

Data protection and encryption is a basic data storage requirement on-board nearly all military vehicles because they are routinely deployed into contested areas. Though encryption method options such as government off-the-shelf (GOTS) vs. commercial off-the-shelf (COTS) are well understood, as are the encryption algorithms (AES-128 vs AES-256), currently the guidance and understanding of where the encryption should be located in deployed storage systems, is unclear.

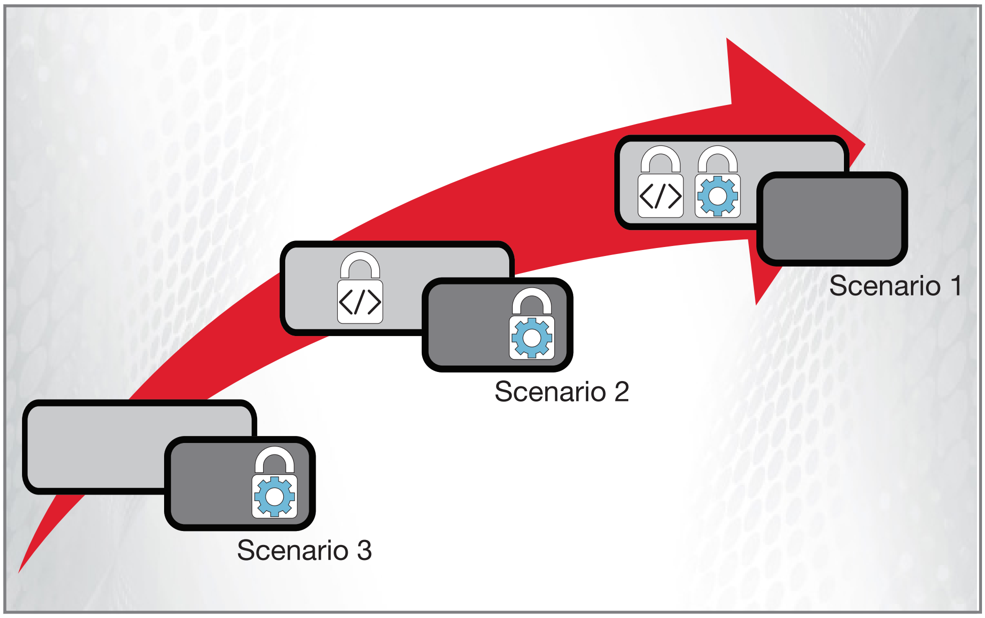

Figure 1: Relative Scenario Strength

The choice of encryption location can make the difference in the concept of operations (CONOPS). This decision determines how difficult it is for adversaries to decrypt sensitive data and use it to their advantage. This paper discusses the different places the encryption technology can be located on a data storage solution and aims to help you chose a solution that is best for your application.

Threats of Loss or Capture

For context of this paper and to frame the argument, a short list of vehicle losses are mentioned. While loss of the data is the focus of this paper, it is not intended to ignore the loss of life in many of these incidents.

Manned Vehicle Loss Events

Jet fighters are, by definition, designed to go into dangerous environments. While there have been few fighter vs. fighter engagements like in World War II, Korea or Vietnam, there have been many accidents and losses to surface-to-air missiles (SAM) and anti-aircraft artillery (AAA). Numerous aircraft were lost during the 1991 Gulf War due to SAM and AAA fire and a few were lost in the Balkans operations. An F-111 was lost in Libya in 1986 and Navy aircraft in Lebanon in 1983. While not attributed to SAM or AAA, an F-16 aircraft crashed near Bagram Airfield in Afghanistan as recently as 2016. In each case, the adversaries certainly tried to obtain as much information and wreckage as possible.

Intelligence, surveillance, and reconnaissance (ISR) and command and control aircraft are usually located well back of the direct battle area. These aircraft include examples like the Lockheed P-3 Orion, Boeing E-3 Sentry (AWACS), or the Boeing P-8 Poseidon. In 2001, the Chinese forced a U.S. Navy signals intelligence P-3 aircraft to land on China's Hainan Island. The crew certainly did their best to destroy sensitive equipment and data, but it is also certain the Chinese did their best to obtain any information possible.

Tanker and cargo have been lost in operations as well as ISR aircraft. Numerous crashes of each occurred in both the Iraq and Afghanistan conflicts.

The loss of helicopters is unfortunately a much more frequent occurrence than fighters, tankers, cargo, or ISR aircraft. Dozens of helicopters have been lost in Iraq and Afghanistan operations. These losses often occurred in very remote, mountainous areas.

Unmanned Vehicle Loss Events

With the advancement in unmanned technology in the last decade, today there are unmanned fixed-wing aircraft, rotorcraft, underwater vehicles, surface vehicles, and ground vehicles that are subject to loss or capture, maybe more so than manned vehicles. Remember the unmanned aerial vehicle (UAV) that landed in Iran in December 2011 and the Global Hawk RQ-4 that was lost in routine training missions in the U.S. in 2017. More recently, a Global Hawk was downed by an Iranian missile over the Strait of Hormuz amid increasing tensions in the area. The data gathered by aircraft such as the RQ-4 or P-3 is very valuable and worth protecting. As a result of these vehicle losses, increasing effort has been spent on encryption type and strength development, but little has been published on where to locate the encryption technology.

Such loss incidents are viewed as inevitable in a random and often dangerous world. Losses of unmanned vehicles are actually expected to increase with the concept of 'swarms'. Unclassified videos can be viewed of unmanned surface vehicles (USV) guiding a swarm of small UUVs, enabling missions like mine hunting or other similar dangerous tasks to be performed without the need for direct human involvement. Now with the advent of artificial intelligence (AI) in deployed platforms, such missions are well within the capabilities of unmanned systems.

Post Mission Loss Events

Non-documented, but theoretical threats include capture of data storage devices while in transport from the base station to the deployed vehicle. Nation states and 'non-state actors' could benefit from the capture and analysis of data (for example map, mission plan, target, or sensor data). Non-state actors might include terrorists, trans-national criminal organizations, cyber hackers, and other malicious people with a contrary agenda. Some of these non-state actors are obvious external groups while perhaps the largest security risk is actually from the people inside the organization with ready access.

Simple negligence may also present a threat to data security. It was reported in 2012 that 1,500 boxes of classified documents had gone missing in the Washington National Records Center. Over 80 of those boxes were labelled Top Secret. Some of the files were from the Office of the Secretary of Defense, the National Imagery and Mapping Agency, and the Navy. While espionage was not believed to be a causal factor, you can be sure that adversaries would have liked to get their hands on such data. With data being more and more available digitally, hackers can now gain access to more and more data.

Mission Data and Classifications

While a vehicle could be a fixed-wing or rotary-wing aircraft, an unmanned underwater vehicle, a land vehicle, or anything inbetween, going forward this paper will use the general term *vehicle* for the purposes of discussion.

Mission Data

Manned and unmanned military vehicles require access to certain data prior to the mission. Map data, for example, is required to understand the terrain and mission area, and is therefore critical in mission planning and execution. Similarly, the mission plan must be pre-loaded on the mission computer prior to takeoff, and can be just as valuable as the data collected during the mission.

The data collected during the mission primarily comes from on-board sensors such as traditional radars, ISR, electro-optical (EO), or synthetic aperture radar (SAR). Targets of interest may be identified during the mission such as ground radar sites or SAM sites, and this information is critical for future mission planning, identifying what areas need to be avoided to reduce the chance of detection or interception.

Post Mission Data Analysis

Data that is collected on board a vehicle during the mission is analyzed post mission in a location remote from the vehicle.

Classification Levels

Military systems may be asked to handle or collect different levels of secure data. In the U.S., there are three basic levels of sensitive data – Confidential, Secret, and Top Secret. Similarly, in the U.K., there are three levels of sensitive data – Official, Secret, and Top secret. Generally speaking, Confidential or Official applies to information whose release could “damage” national security, whereas Secret carries with it the potential for “serious damage” and Top Secret “grave damage.” In practice, the definitions are flexible and each agency has adapted the terminology for its own use[1].

Modern Data Storage and Recording

Most modern deployed vehicles have been, and are being designed with Ethernet networks as the backbone for data transfer. Though MIL-STD-1553 is still used, Ethernet is clearly predominant in data collection and storage.

Originally, deployed Ethernet networks supported data rates of 10 Mbps and then 100 Mbps. Though exciting at the time, these data rates seem extraordinarily slow by comparison today. Then the leap was made to gigabit networks (1 GbE) which are now widely supported and deployed, and are still being designed into new systems today. This fact can be explained by the wide industry and technology support available to designers. Now 10 Gbps networks are being deployed with 40 Gbps and 100 Gbps networks expected soon.

[1] Slate.com - What’s the Difference Between “Top Secret” and “Confidential”?

The data storage device in an Ethernet network is the network file server or network attached storage (NAS). NAS systems not only store data but also enable sharing of files and data between network clients. A small number of clients can connect to the NAS directly but as Ethernet networks in deployed systems are becoming more and more complex and Ethernet switches are added, more clients can now connect with each other and more importantly with the central NAS in the system. Any of these numerous clients can store data on the NAS or retrieve data from the NAS from any part of the vehicle.

Deployed NAS protocols are not vendor proprietary, due to the use of widely supported industry standards for file serving, net booting, packet capture, and block transfer.

+ For file serving, the standard protocols are NFS, CIFS, FTP, and HTTP. In deployed applications, NFS is used a majority of the time with CIFS a distant second.
+ For net booting, the two basic protocols supported are PXE and DHCP.
+ For packet capture, the basic protocol is PCAP.
+ For block transfer, the basic protocol is iSCSI.

An example of such a modern NAS is shown in Figure 1. Used for ISR applications on larger vehicles, this NAS has 8 x 1 GbE ports, 4 x 10 GbE, a Xeon® D processor, 2 x Type 1 encryptors, and a sustained throughput of 2 GB/s. The NAS in Figure 1 is a larger device at 17.8 x 7.1 x 18.95” with one removable media (RM) module.

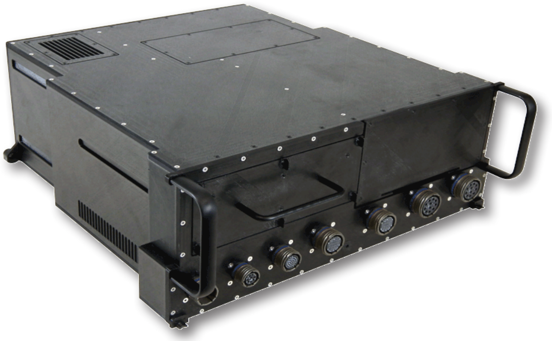

Figure 1: Unattended Network Storage (UNS) from Curtiss-Wright

Today’s vehicles are using a variety of RM to transport data to and from the vehicle. Large ISR vehicles require massive storage modules with 32 TB to 64 TB or higher capacities. The RM module for the NAS in Figure 1 can be seen in Figure 2. It supports 32 TB capacity today, but can increase as requirements change. This RM is a larger device (2.5 x 5.0 x 6.5”) and could not fit into a shirt pocket or thigh pocket. It would be carried by the handle or in a protective case during transport.

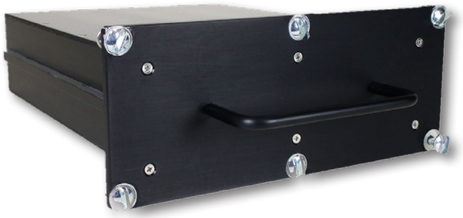

Figure 2: Removable Storage Module (RSM) from Curtiss-Wright

The NSA Commercial Solutions for Classified (CSfC) program defines Removable Media (RM) in its Data at Rest Capability Package as: device(s) which have the primary purpose of providing external storage of data protected by DAR through implementing two layers of encryption. Removable media can include: a USB drive, a microSD card, or a removable drive. Removable media does not include other portable computing devices such as smartphones and tablets. This use case allows customers to transfer data using an external storage device between different systems or expand the storage of a single system. For example, this use case can be used to transport data via a removable media device between secured facilities, using a DAR CP compliant solution on both ends. This requires using two approved layers of encryption on the RM device that is provisioned within a secured facility, then transporting the RM under continuous physical control to access data on a DAR CP compliant workstation or device.

Smaller vehicles can have RM (and associated NAS) that are more easily handled like the 4 TB removable memory cartridge shown in Figure 3. This RM can fit into a shirt or thigh pocket. The RM in Figure 3 is used with the NAS in Figure 4. Both are much smaller than the NAS and RM shown previously in Figure 1 and Figure 2, respectively.

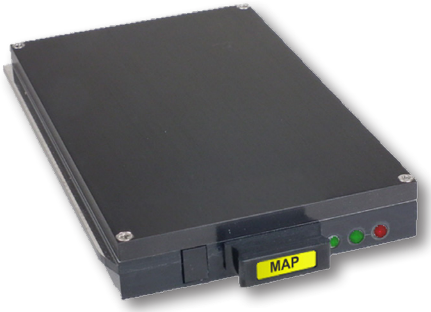

Figure 3: Removable Memory Cartridge (RMC) from Curtiss-Wright

This small RM size (0.66 x 3.0 x 5.0”) can be alternately viewed as a blessing or a vulnerability. The small size is easy for the pilot or flight engineer to carry, fitting into a shirt or thigh pocket. However, that same small size could make theft during transport and, concealment, easier to accomplish. This paper will discuss the issues with theft or loss and possible choices to reduce such vulnerability.

While some RM in the past used rotating drives, almost all RM today are based on solid-state drives (SSD). The data residing or stored on the RM is known as data-at-rest (DAR), as opposed to data on the move in a network. While 128 GB cartridges cost a small fortune 10 years ago, todays cartridges hold SSDs with capacities of 4 TB and well beyond. An RM may house only one SSD like Figure 3. Or the RM may house multiple SSDs like Figure 2. SSDs have a very high mean time between failure (MTBF) value and high shock and vibration characteristics. Industrial SSD versions support wide operating temperature ranges, key for any deployed NAS. The RM like those shown in Figure 2 and Figure 3 have a high technology readiness level (TRL) and are routinely deployed on UAVs, UUVs, USVs, fighters, helicopters, and ISR aircraft.

Mission Data Vulnerability

Pre-mission, the RM carrying map and mission data (loaded at the ground station) must be transported to the vehicle. Sometimes the NAS is called upon to boot network clients, in which case the RM will also be loaded with the operating systems and software applications needed for those network clients. Read more about NetBoot in the white paper: Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems. Post mission, the same RM is transported from the vehicle with the same map and mission data back to the ground station, but now also carries the data gathered during the mission, making it even more valuable and attractive to an adversary.

If captured, the pre-mission data can tell an adversary where and how the vehicle will (or did) travel; valuable planning insights could be gained from that data. For example, this mission and map data could be used to redeploy anti-aircraft batteries used to intercept or deter incoming flights. Post-mission, this same data would be supplemented by actual ISR data and possibly maintenance data about the vehicle, if collected. This data could prove invaluable to an adversary when looking for weaknesses.

Types of Encryption

The logical solution to protect valuable DAR is to encrypt the data. Some military systems require the use of National Security Agency (NSA) approved Type 1 encrypting devices. These GOTS devices must be approved by the NSA and certified for certain situations or environments. They are usually International Traffic in Arms Regulations (ITAR) restricted and available only to U.S. Department of Defense (DoD) entities or possibly to the other countries making up the 'Five Eyes'. These DAR encryptors may employ Suite A or [2]Suite B algorithms. The Type 1 certification process is necessarily detailed. Top Secret Type 1 DAR encryptors will usually be designated with a 'KG' in the part number.

Other military systems may be able to use COTS devices approved by the NSA under its Commercial Solutions for Classified (CSfC) program. CSfC is an important part of the NSA's commercial cybersecurity strategy to deliver secure solutions that leverage commercial technologies and products in order to deliver cybersecurity solutions more quickly. The CSfC program is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications. The NSA has developed, approved, and published solution-level specifications called Capability Packages (CPs), and works with technical communities from across industry, governments, and academia to develop and publish product-level requirements in U.S. Government Protection Profiles (PPs). For CSfC approval, a DAR component must complete Common Criteria (CC) certification. In the U.S., the CC certification process is managed by NIAP and the resulting certifications are recognized by 30 other Common Criteria Recognition Agreement (CCRA) member countries. The CCRA was formed to produce a set of stringent standards for IT products and to allow certification in one country, to apply in another country without re-validation.

Thanks to CSfC, system designers can now deploy a COTS solution with encrypted data protection in a matter of months and at a fraction of the cost typically required to achieve certification for more sensitive Type 1 products.

As an alternative, CSfC defines an approach for protecting critical data using two-layer commercial encryption technologies. In many cases, system integrators considering a Type 1 approach may be pleasantly surprised to find that their application can instead use the pre-approved and less-costly CSfC approach.

This paper will focus on the COTS approaches only. The GOTS approach with an NSA approved Type 1 encryptor is a well known process to a closed group. If you need Type 1 encryption, your Authorizing Official (AO) or Designated Approving Authority (DAA) will identify that need.

Common Criteria and the CSfC Program Resources

- Learn more about the Commercial Solutions for Classified Program (CSfC)
- Learn more about Common Criteria Recognition Arrangement (CCRA) and which countries are certificate authorizing and which are consuming
- Get a better understanding of how products get listed on the NSA's CSfC Components list
- Read more about the Curtiss-Wright products listed on the NIAP Product Compliant List
- Download the DTS1 Hardware Encryption Common Criteria Certificate
- Download the DTS1 Software Encryption Common Criteria Certificate

[2]Suite B algorithms are also now known as Commercial National Security Algorithms (CNSA)

Encryption Locations

In a file server or data recorder with RM, the encryption mechanism can be located in the stationary chassis, which does not move out of the vehicle, or the mechanism could be located in the RM. A deployable file server with a removable cartridge is shown in Figure 4. This particular file server has one RM.

Figure 4: DTS1 File Server from Curtiss-Wright

Scenario 1 – Two Layers of Encryption in the Stationary Chassis

The encryption in the NAS in Figure 4 takes place in the stationary chassis. This NAS device has two layers of encryption, one hardware layer and one software layer. Other file serving devices may only have one layer, but the concept is the same.

The data received by the example NAS via the Ethernet ports is first encrypted by the software layer using AES 256-bit encryption. Because all of the data going to the disk storage is encrypted, this process is known as full disk encryption (FDE). Because the FDE is performed by software, it is known simply as SWFDE.

After being converted to SATA protocol, the data is encrypted a second time by a FIPS 140-2 certified ASIC that also uses AES 256-bit encryption. As noted with the software layer, all data going to the disk is encrypted a second time so this is also considered FDE. Since this encryption is performed by hardware, it is known simply as HWFDE.

Once the data has been double encrypted, it is sent to the RM and is then considered 'at rest'. This scenario is depicted in Figure 5. The smaller NAS in Figure 4 supports only two 1 GbE ports while the larger NAS in Figure 1 supports multiple 10 GbE and 1 GbE ports. The NAS shown in Figure 4 employs two layers of COTS encryption as depicted, while the NAS in Figure 1 supports one HWFDE layer which employs Type 1 encryption. In both Figures 1 and 4, the encryption mechanism remains in the respective, stationary chassis not in the RM.

The removable cartridge or RM has no encryption mechanism in it. It simply houses an SSD that can be a single or multi-level cell (SLC or MLC) type NAND Flash and can be any type of SSD, as long as neither the cartridge nor SSD has an encryption mechanism.

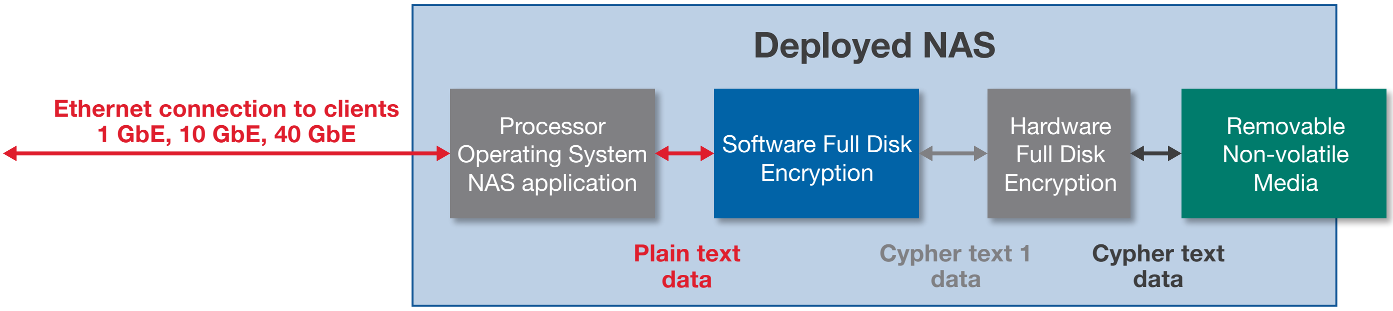

Figure 5: SWFDE and HWFDE COTS Encryption in Stationary Chassis

As previously mentioned, prior to a mission, the RM is loaded with map and mission planning data at a base station. During that loading process, the same double encryption process takes place, ensuring the data is well protected and, per the NSA CSfC definition, is considered to be unclassified when no power is applied. The RM is then transported from the base station to the vehicle. During that transport, the RM may be vulnerable to loss or capture by an adversary. That level of vulnerability is of course dependent on the distance from the base station to the vehicle, and on the nature of the location.

- If the data is transported from a base station located on an Air Force (AF) base to a vehicle on the same AF base, then the vulnerability may be quite low from an external adversary. However, the vulnerability may still be high for someone who has an agenda contrary to the military or government and such a person may try to copy the map and mission data to sell or leak it to outside agencies.
- If the data is transported from a base station located on an AF base, to a vehicle located external to the base, then the vulnerability to adversary interception may be higher. The person transporting the RM may be intercepted and the RM captured.
- While less likely in most well run organizations, the RM may simply be lost or misplaced by the person transporting it. Some tasks are given to very junior, young personnel who may not take the necessary care with the RM and its valuable data. Once lost or misplaced, the adversary or person with a conflicting agenda may have a chance to locate the RM and try to extract the data.

NOTE: Ultimately, the vehicle is going to be deployed into what may be a hostile area. As history shows, these deployed vehicles can be lost or captured despite the best intentions and plans. This paper only addresses the vulnerabilities to the RM and not the entire vehicle.

Benefit of Stationary Chassis Approach

Because the COTS encryption mechanism is located in the stationary chassis, the RM does not contain any of the mechanisms that perform the encryption. The software encryption is performed using an AES 256-bit algorithm running in the operating system (OS), which is not available in the RM, and the hardware encryption is performed by the ASIC in the stationary chassis, as previously described, and therefore the ASIC is also not present in the RM.

This encryption location configuration requires the adversary wishing to decrypt the data to begin with the same OS and ASIC, and then determine both the passphrase for the SWFDE layer and the password for the HWFDE layer. Gaining access to the double encrypted RM without access to the encryption mechanism makes the task of decrypting the RM incredibly difficult. It may be possible but it would certainly be very time consuming.

Data always has a length of time over which it is valuable or critical. The value of the data often reduces as time passes. So the object is to delay access to the data for as long as possible. The double layers of encryption and abstraction from the mechanism make the time to defeat impossible if not at least very lengthy.

Scenario 2 - SWFDE in the Stationary Chassis and HWFDE in the Removable Media

An alternative to locating both layers of encryption in the stationary chassis is containing the software layer in the chassis and the hardware layer in the RM. This type of encryption location configuration is depicted in Figure 6. Again, this device has two layers of encryption – one hardware layer and one software layer. The data received via the Ethernet ports is first encrypted by the software layer using AES 256-bit encryption. After converting to SATA protocol, the data is encrypted a second time by a FIPS 140-2 certified ASIC (HWFDE) also using AES 256-bit encryption, but in this scenario the ASIC is located in the RM. The double encrypted data is then routed to the NAND Flash memory where it rests.

The same steps and assumptions noted in Scenario 1 apply for Scenario 2 as well.

Pitfalls of Removable Media Encryption Approach

In this scenario, the SWFDE layer is still applied by the OS as before. The software encryption is performed using an AES 256-bit algorithm running in the operating system (OS). The OS is not available in the RM. That SWFDE mechanism remains in the stationary chassis. So that is still in place and a benefit.

However, the HWFDE layer is now located in the SSD (which is inside the RM), not in the stationary chassis. The SATA data received by the RM (and SSD) is encrypted using AES 256-bit encryption as before. There is no degradation in the type of COTS encryption. However, the difference is that the actual mechanism (ASIC, FPGA, controller) is transported along with the data in the RM.

This means the adversary would have access to the actual hardware mechanism for encryption. With enough time and resources applied, this encryption in the RM can be more easily defeated or compromised than if no encryption mechanism were present. The adversary would still have to determine the passphrase for the SWFDE layer and would not have that exact mechanism in their hands. With SWFDE in the stationary chassis and the HWFDE mechanism in the RM, the adversary's job just got easier than in Scenario 1. It may still be a very time consuming process but it would be significantly easier to defeat Scenario 2 than Scenario 1, and thus the time sensitive data may be more accessible in Scenario 2 than in Scenario 1.

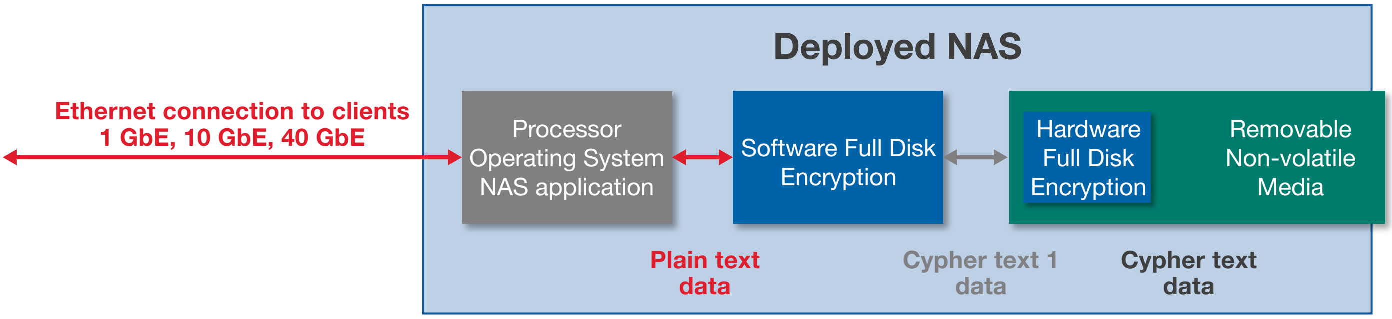

Figure 6: SWFDE in Stationary Chassis and HWFDE in Removable Media

Scenario 3 – HWFDE in the Removable Media, No SWFDE

The HWFDE encryption in the file server in Figure 7 takes place in the RM. This device has only one layer of encryption - the hardware layer, and no software layer. The data received via the Ethernet ports is converted to SATA data for transport to the RM (and its SSD). After receipt by the SSD, the data is encrypted with a hardware mechanism (ASIC, FPGA, controller) using AES 256-bit encryption. The encrypted data then resides on the NAND Flash memory in the RM.

In this scenario, the removable cartridge has the encryption mechanism in it. It houses an SSD that can be SLC or MLC type. The type of SSD does not matter, it only matters that the RM, and embedded SSD, has the encryption mechanism inside it.

Example SSD with SED

Samsung makes a variety of SSDs, both SATA and NVMe types. This example scenario describes only a SATA drive, but the idea is the same for an NVMe approach. Figure 8 shows a Samsung® 860 EVO SATA SSD. Our extensive testing has shown these SSDs to be very good performers. This particular disk is only rated 0 to 70°C and so would be a good choice for a lab, but not a deployed vehicles with temperature extremes.

The 860 EVO includes AES 256-bit encryption capability which the user controls whether the encryption is employed. SSD manufacturers will often note the existence of the self-encrypting drive (SED) feature with the phrase TCG/Opal. TCG stands for Trusted Computing Group and they have formed a Storage Workgroup which developed the Opal Storage Specification.

Prior to a mission, the RM is loaded with map and mission planning data. During that loading process, the SED encryption is performed on the data. The RM is then transported from the base station to the vehicle. During that transport, the RM may be vulnerable to loss or capture by an adversary same as in Scenarios 1 and 2. As explained previously, that level of vulnerability is of course dependent on the distance from base to vehicle and on the nature of the location.

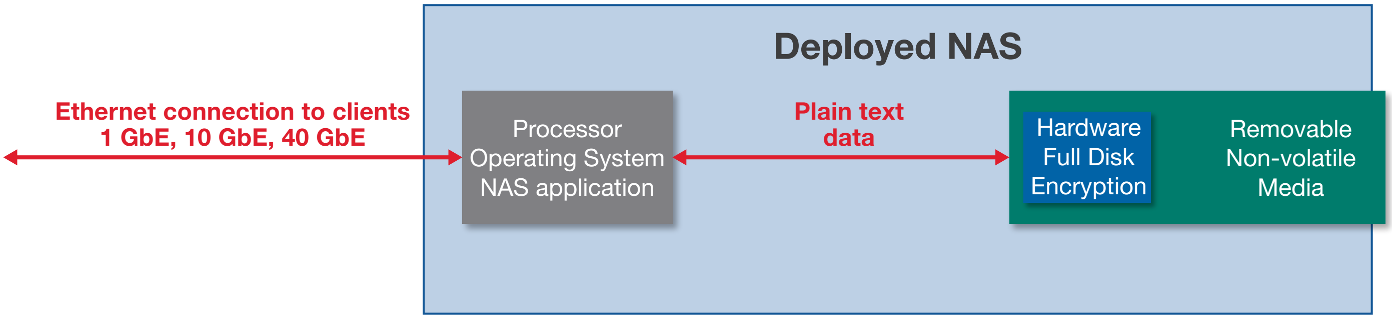

Figure 7: HWFDE only in the Removable Cartridge

Figure 8: Samsung 860 EVO SATA SSD

Why locating the COTS Encryption only in the Removable Media is not preferred

In this scenario, the SWFDE layer does not exist. However, the HWFDE (and only) layer is now located in the SSD (inside the RM), not in the stationary chassis. The SATA data received by RM and SSD is encrypted using AES 256-bit encryption as before. There is no degradation in the type of COTS encryption. The difference is that the actual mechanism (ASIC, FPGA, controller) is transported along with the data in the RM.

If the adversary were to capture the RM in transport, then they have the actual HWFDE encryption mechanism. With time and resources, this singular encryption layer may be more easily defeated than in Scenarios 1 and 2. With no additional SWFDE layer, the adversary now has access to the critical DAR. Their job just got easier and as previously mentioned, data is time sensitive so the knowledge gained may be exploited to their advantage quicker than the other Scenarios.

Conclusion

Encryption of DAR in deployed applications is being required and specified by military personnel planning systems and the integrators developing those systems. A choice can be made about what type of encryption to use and where to locate that encryption.

This paper suggests that a simple, prudent choice is to locate the encryption in the stationary NAS, not in the RM because the RM is vulnerable to a number of threats during transport or storage.

There are adversaries who are easy to identify. These nation states have many resources and are highly motivated to obtain and decrypt classified data. They will go to great lengths to obtain sensitive data.

There are also people that exist in any organization with conflicting agendas. These people are motivated by a variety of ideals or money, and often believe they know best what should happen.

In either case, locating the encryption in the NAS and not in the transportable RM is the best choice. Without the physical encryption mechanism, the decryption of, and access to, the data is much more difficult for adversaries. If COTS encryption can be used, then the two layer encryption approach (SWFDE and HWFDE) makes the tasks for adversaries and foes even more difficult yet.

As mentioned, data always has a ‘shelf life’. So do not make it easier for motivated opponents. While you may not be able to avoid any vulnerability, you can make a simple choice to make it more difficult.

How would you rate this white paper?

1 (low)	2	3	4	5 (high)
☆	☆	☆	☆	☆

Authors

Paul Davis (Retired)
Director, Product Management
Data Solutions
Curtiss-Wright Defense Solutions

Steven Petric
Senior Product Manager
Data Solutions
Curtiss-Wright Defense Solutions

Elisabeth O'Brien
Manager, Product Marketing
Curtiss-Wright Defense Solutions

Learn More

Encryption Information

- National Security Agency (NSA) Type 1
- NSA Commercial Solutions for Classified (CSfC)
- Common Criteria (CC)
- FIPS 140-2
- United States NIAP Product Compliant List
- NSA's CSfC Components List
- International Common Criteria Certified Products List

Curtiss-Wright White Papers

- Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions
- Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems
- COTS Encryption for Data-at-Rest
- The Root of Trust: A Foundation for Trusted Computing
- TrustedCOTS: Leading the Way to Secure Systems

Curtiss-Wright Case Studies

- Protecting Data-at-Rest with NSA CSfC Approved Encryption on a UAV
- A COTS Approach to Data-at-Rest Encryption Onboard an Unmanned Underwater Vehicle (UUV)
- Aircraft Looks to Modernize Storage of Sensitive Data

Curtiss-Wright Products

- DTS1 1- Slot Network Attached Storage
- DTS3 3-Slot Network Attached Storage
- CNS4 4-Slot Network File Server
- UNS Unattended Network Storage