RAMPART™ Distributed End-to-End Embedded Cyber Security

End-to-End Encryption

For Military Applications

Why does BiTMICRO® RAMPART matter?

Over the next several years, the US DoD and other global military organizations will face regular and complex decisions regarding the complete protection of all digital data. Data must be protected regardless of how and where it is created, processed, stored or transferred – physically and across networks. Existing solutions may be exposed as inadequate. Innovative and determined nation states, terrorist groups and criminals will combine with technology to threaten even the strongest, currently impermeable environments. Stored data, and more importantly, data being transmitted, may be intercepted and compromised.

The Proven Standard for Data Encryption

The Advanced Encryption Standard (AES) is a standard ratified by the National Institute of Standards and Technology (NIST). The AES specification is approved by Federal Information Processing Standards (FIPS 197) used to protect electronic data. AES is the only publicly available cipher approved by the US NSA and other global associations for storage and communication of top-secret data.

Currently, no significant weaknesses have been found in AES. This means brute force is the only existing form of attack that can decrypt AES encrypted data. Brute force can also be described as the method of trial and error: every possible key is tried until the correct one is found. It would take the world's fastest supercomputer with ~ 100 petaFLOPs, thousands of centuries to characterize a single AES-256 deployment.

What does BiTMICRO RAMPART do?

The RAMPART solution delivers end-to-end AES-256 encryption. RAMPART creates the most advanced, distributed, and seamless, secure data storage and data transmission environment for remote military/US DoD systems. Regardless of how or where military and defense data is created, stored, processed, enriched or sent, it can be safeguarded by RAMPART AES-256 encryption, while it is stored and while it is being transmitted.

With RAMPART, data can be created and securely stored on a drone, satellite, submarine, fighter jet, launch vehicle, or surveillance aircraft. The data can then be transmitted across any

network to another location, while remaining fully encrypted. Even if the data falls into the wrong hands while stored or during transmission, it will be encrypted and unusable. Once the data is received at the other location, it will remain encrypted. Only with a properly configured system, and authenticated user, can the encrypted data at the receiving location be decrypted and used.

Why is BiTMICRO RAMPART better?

RAMPART is comprised of RAMPART Cyber Secure Management Software and RAMPART Cyber Secure Solid State Storage Modules or “CS4 Modules.”

RAMPART CS4 Modules encrypt, decrypt, and store data. They are compact and efficient hardware-based systems designed for remote and mobile applications.

RAMPART CS4 Modules include embedded hardware-based encryption. Unlike software-based encryption which is generally slow, resource hungry, and prone to attacks, the RAMPART hardware-based solution is extremely fast, resource frugal, and fully hardened. RAMPART CS4 Modules encrypt data automatically and in real-time as the data is written and stored.

Data stored on a remote RAMPART CS4 Module cannot be decrypted. Unless otherwise configured, there is never a key encryption key (KEK) present on the remote system. The data remains encrypted while it is stored, being read, and transmitted from the remote CS4 Module to a local CS4 Module. Once it arrives, it remains encrypted while it is written and stored on the local CS4 Module. The data remains encrypted through the entire data path. Only an authenticated user, with a properly configured system and the correct AES-256 key can access the local CS4 Module so the data can be decrypted and used.

RAMPART is unique because it is true end-to-end AES-256 encryption. Other solutions encrypt data at the OS, link, or network level. But system levels like the memory, CPU, OS and network interfaces can be suseptable to attacks and malware. Network gateways, routers, switches, and transmission signals can also be compromised. Finding and protecting against attacks at all these levels is challenging.

RAMPART encrypts data at the flash chip/NAND level. As data is written to RAMPART it is immediately encrypted and stored on the internal flash chips within the solid state storage. The data remains encrypted as it is read from the solid state storage within RAMPART. The CS4 encryption remains inforce as the data passes through the device controller, bus, memory, CPU, OS, and network interface on the remote system. And remains encrypted through the network and transmission links. Even if the physical flash chips are removed from the RAMPART solid state storage and probed, the data will still be encrypted and unuseable.

Not only does RAMPART provide seamless end-to-end AES-256 encryption, it can also securely erase RAMPART stored data if needed or completely wipe the RAMPART solid-state

storage using military/DoD grade sanitization. Data can be erased and sanitized on any remote or local CS4 Module.

How is BiTMICRO RAMPART deployed and managed?

RAMPART assures that data is encrypted and cyber secure.

- When stored on any CS4 Module
- When transmitted between any two CS4 Modules

With RAMPART, encryption is seamless and unbroken

- Through air and space
- Through any network link
- Through any NIC, bus, memory, controller, or host bus adapter

RAMPART CS4 Modules are NVMe devices that are available in a variety of storage capacities. They can be installed into any remote system that uses the NVMe protocol. CS4 Modules retain data in a fully AES-256 encrypted state while data is stored, transmitted, or transported between any two CS4 Modules.

RAMPART CS4 Modules do not necessarily require an operating system. They can be deployed on a larger variety of systems. All that is needed from the connected system is the ability to receive a command and send that command to the NVMe connected RAMPART CS4 Module. CS4 Modules are not only compact, secure, and energy efficient, they also verified rugged. They resist shock, vibration, wide temperature ranges, altitude, humidity, power outages, and power degradation.

Future versions of RAMPART will include RAMPART CS4 Modules that can be configured in many to one, one to many or many to many topologies and can be configured or combined into RAMPART CS4 Module groups in a distributed manner. CS4 Modules will be able to support third-party NVMe storage devices such as SSDs and can also be partitioned to provide encrypted and unencrypted zones.

RAMPART CS4 Modules are managed by RAMPART Cyber Secure Management Software via a lite CS4 Module management application running on the CS4 Module host system. RAMPART management software provides an informative user interface to manage all the aspects of the RAMPART CS4 Module architecture. It provides a software-configurable framework that is language/platform-neutral and extensible, simplifying and lowering the high cost of implementation typically required to protect the entire ecosystem – from the host, network, to storage. A CLI is also available for simpler integration into existing management and host systems. CS4 Modules can also be managed via basic commands to support a wide variety of environments that do not have an operating system.

RAMPART - Cyber Secure Management Software:

- Finds and manages all RAMPART CS4 Modules with one interface
- Displays module health, performance, and usage information
- Supports multiple users, hosts, and modules
- Manages AES-256 encryption, key management, and topology configurations
- Manages “secure-erase” and military sanitization of the RAMPART CS4 Module stored data.

RAMPART Conclusion

Military and defense data must be protected regardless of how and where the data is created, processed, stored or transferred – physically and across networks. Stored data, and more importantly, data being transmitted, may be intercepted and compromised.

The Advanced Encryption Standard (AES) is a standard ratified by the National Institute of Standards and Technology (NIST), is approved by Federal Information Processing Standards (FIPS 197), and by the US NSA and other global associations for storage and communication of top-secret data.

The RAMPART solution delivers end-to-end AES-256 encryption. RAMPART creates the most advanced, distributed, and seamless, secure data storage and data transmission environment for remote military/US DoD systems. Regardless of how or where military and defense data is created, stored, processed, enriched or sent, it can be safeguarded by RAMPART AES-256 encryption, while it is stored and while it is being transmitted.

NOTES:

Artificial Intelligence
RAMPART with BiTMICRO ACUMEN™ for AI on the EDGE

RAMPART distributed cyber security can be used in conjunction with BITMICRO ACUMEN™ – AI on the Edge. ACUMEN is a low SWaP, compact, portable and rugged platform for remote AI, supercomputing, or data recording applications. BiTMICRO ACUMEN and BiTMICRO RAMPART can be combined to provide a secure and powerful military-grade solution delivering security and intelligence to the edge of your infrastructure.

Solid State Storage
RAMPART with BiTMICRO ALTIMA™ Solid State Storage

RAMPART utilizes up to 16TBs of BiTMICRO Altima™, verified rugged, solid state storage. Altima solid state storage supports all popular SSD NAND types and includes features to ensure durability and reliability.