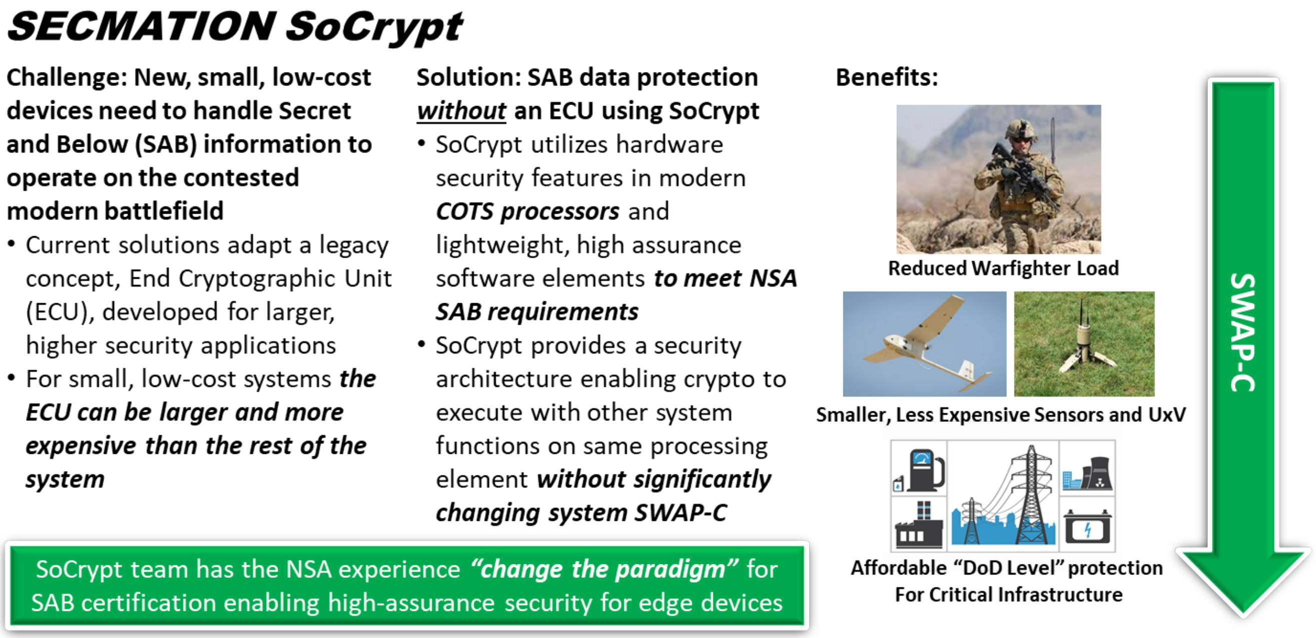
SECMATION

SoCrypt – Enabling Secret and Below Data Protection in Small, Low-Cost Devices

POC: Hal Aldridge, Ph.D., CEO Secmation, hal@secmation.com, 919 887 2560

Sponsor: Air Force Research Laboratory, Contract #FA9453-19-P-0549

Modern computing and communications devices mix both “secure” functions which use cryptography (e.g. banking application) and “non-secure” functions on the same small, low-cost device. While the isolation and other security features in these devices that enable hosting of secure/non-secure functions is adequate for some applications, their security is not adequate to meet NSA requirements to protect classified data. Current solutions to handle even lower data classifications, such as Secret and Below (SAB), can significantly affect the Size, Weight, Power, and Cost (SWAP-C) of the protected device. In some cases, the available SAB protection solutions can be larger, heavier, consume more power, and cost more than the protected device. Addressing this SWAP-C issue is essential to enabling wide deployment of small, low-cost, low-power devices (e.g. sensors, unmanned systems) on the battlefield without compromising security. By lowering SWAP-C, applications such as critical infrastructure can benefit from “DoD Level” security protections.



SECMATION SoCrypt

Challenge: New, small, low-cost devices need to handle Secret and Below (SAB) information to operate on the contested modern battlefield

- Current solutions adapt a legacy concept, End Cryptographic Unit (ECU), developed for larger, higher security applications
- For small, low-cost systems ***the ECU can be larger and more expensive than the rest of the system***

Solution: SAB data protection *without* an ECU using SoCrypt

- SoCrypt utilizes hardware security features in modern ***COTS processors*** and lightweight, high assurance software elements ***to meet NSA SAB requirements***
- SoCrypt provides a security architecture enabling crypto to execute with other system functions on same processing element ***without significantly changing system SWAP-C***

Benefits:

Reduced Warfighter Load

Smaller, Less Expensive Sensors and UxV

Affordable “DoD Level” protection For Critical Infrastructure

SWAP-C

SoCrypt team has the NSA experience ***“change the paradigm”*** for SAB certification enabling high-assurance security for edge devices

Developed to meet the security and SWAP-C challenges of small DoD satellites (e.g. CubeSats), SoCrypt provides an advanced security architecture for small devices enabling SAB data protection. Different from previous attempts to address NSA certification requirements without use of dedicated hardware elements such as Field Programmable Gate Arrays (FPGA), SoCrypt’s innovative architecture targets ARM-based COTS processors maximizing hardware protections and implementing an easily verifiable software architecture. The purpose-built

SoCrypt software architecture is significantly simpler and more robust than Trusted Execution Environments, hypervisors, secure OS, or other traditional security solutions through its innovative use of hardware-based protections in modern processors. A key challenge for any NSA certification process, especially one for SoCrypt that will push some established preconceptions, is knowledge of NSA challenges and how the certification requirements originated. The Secmation team has experience with NSA policy development, security architecture, NSA certification processes, and Type-1 equipment design enabling low-risk, rapid certification and transition of SoCrypt-enabled capabilities to the warfighter.

Program Status: During the Phase I SBIR program, the architecture for SoCrypt was developed and a detailed analysis performed on how SoCrypt would address the NSA IASRD requirements for SAB. Secmation received a Phase II SBIR award for SoCrypt in November 2019 from the Air Force Research Laboratory (AFRL POC: Robert Vick, Program Manager, Space Protection And Response Program, AFRL/RVSW robert.vick.2@us.af.mil). Due to organizational changes, AFRL lost funding for this and several other awarded Phase II programs before contracts were completed. **Funding/sponsorship is needed to continue this important program.**