A compact End Cryptographic Unit for tactical unmanned systems

Hoa G. Nguyen*[a], Ben Nahill†[b], Narek Pezeshkian[a], David A. Wilson[b], John Yen‡[a],
Jacob Leemaster[b], Brian Telle[a], Rafael Suero[a], Joseph Sobchuk[b], Daniil Utin[b],
Joseph D. Neff[a], Roger Khazan[b]
[a]Naval Information Warfare Center Pacific, 53560 Hull Street, San Diego, CA USA 92152-5001;
[b]Massachusetts Institute of Technology Lincoln Laboratory, 244 Wood Street, Lexington, MA 02421-6426

ABSTRACT

Under the Navy's Flexible Cyber-Secure Radio (FlexCSR) program, the Naval Information Warfare Center Pacific and the Massachusetts Institute of Technology's Lincoln Laboratory are jointly developing a unique cybersecurity solution for tactical unmanned systems (UxS): the FlexCSR Security/Cyber Module (SCM) End Cryptographic Unit (ECU). To deal with possible loss of unmanned systems that contain the device, the SCM ECU uses only publicly available Commercial National Security Algorithms and a Tactical Key Management system to generate and distribute onboard mission keys that are destroyed at mission completion or upon compromise. This also significantly reduces the logistic complexity traditionally involved with protection and loading of classified cryptographic keys. The SCM ECU is on track to be certified by the National Security Agency for protecting tactical data-in-transit up to Secret level.

The FlexCSR SCM ECU is the first stand-alone cryptographic module that conforms to the United States Department of Defense (DoD) Joint Communications Architecture for Unmanned Systems, an initiative by the Office of the Secretary of Defense supporting the interoperability pillar of the DoD Unmanned Systems Integrated Roadmap. It is a credit card-sized enclosed unit that provides USB interfaces for plaintext and ciphertext, support for radio controls and management, and a software Application Programming Interface that together allow easy integration into tactical UxS communication systems. This paper gives an overview of the architecture, interfaces, usage, and development and approval schedule of the device.

Keywords: unmanned systems (UxS), cybersecurity, encryption, End Cryptographic Unit (ECU), Tactical Key Management (TKM), Joint Communications Architecture for Unmanned Systems (JCAUS)

1. INTRODUCTION

Cybersecurity is critical for unmanned systems (UxS) performing national security missions, yet there has been little work in developing multipurpose cybersecurity solutions to support unmanned operations. The US Department of Defense (DoD) *Unmanned Systems Integrated Roadmap (2017-2042)* highlights this as a key gap inhibiting growth of UxS in DoD missions. There are several important factors that often make cybersecurity solutions for manned applications unsuitable for unmanned uses, namely: (1) greatly increased expectation of loss of the UxS host, (2) cumbersome delivery process for cryptographic keys, (3) complex human-machine interface for the configuration of cryptographic devices, and (4) demanding size, weight, and power (SWaP) requirements.

To address these challenges, the Naval Information Warfare Center Pacific (NIWC Pacific), formerly the Space and Naval Warfare Systems Center Pacific (SSC Pacific), and the Massachusetts Institute of Technology's Lincoln Laboratory (MITLL), under the Navy's Flexible Cyber-Secure Radio (FlexCSR) program, are jointly developing a unique cybersecurity solution: the FlexCSR Security/Cyber Module (SCM) End Cryptographic Unit (ECU). The SCM ECU is the first stand-alone cryptographic module that conforms to the new DoD Joint Communications Architecture for Unmanned Systems (JCAUS) standard[1], a DoD initiative supporting the interoperability pillar of the *Unmanned Systems Integrated Roadmap*. It is designed to protect *tactical* data at Secret level, that is, data that have no long-term intelligence value.

*hoa.nguyen@navy.mil †bnahill@ll.mit.edu ‡john.yen@navy.mil

Unmanned Systems Technology XXI, edited by Charles M. Shoemaker, Hoa G. Nguyen, Paul L. Muench,
Proc. of SPIE Vol. 11021, 110210F · © 2019 SPIE · CCC code: 0277-786X/19/$18 · doi: 10.1117/12.2520396

At 3.1” x 2.7” x 1” and less than 0.4 lb, the SCM ECU (Figure 1) should meet the SWaP requirements of all but the smallest UxS. To address the issues of possible loss and cumbersome handling of classified equipment and keys, the SCM ECU uses only publicly available Commercial National Security Algorithms (CNSA) and a Tactical Key Management (TKM) system to generate and distribute onboard mission keys that are destroyed at mission completion or upon compromise. There is no required key loader or special handling procedures, and no need to attempt to retrieve the units if lost. Incorporating the Air Force Life Cycle Management Center (AFLCMC)/Viasat *Mini Crypto (MC)* module, the SCM ECU provides 10-mbps throughput (a 20-mbps mode is possible at higher energy consumption), and makes use of the built-in controlled bypass to also allow a pre-approved set of unencrypted messages to pass through for configuration and control of host radio equipment or to pass radio status messages to the operator control unit (OCU).

The rest of this paper will briefly describe the SCM ECU’s embedment within a radio system, its form factor and interfaces, the TKM concept, and steps for provisioning and using the units.

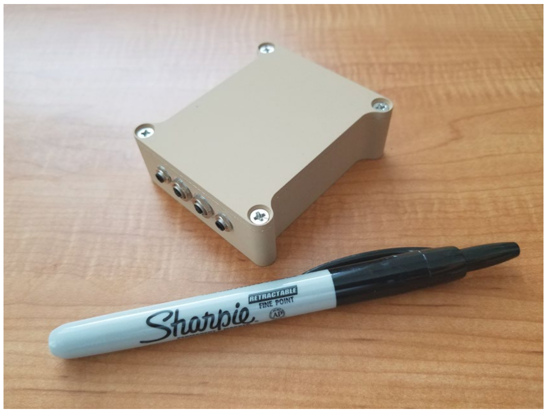

Figure 1. The SCM ECU

2. EMBEDMENT ARCHITECTURE

Figure 2 shows the placement of the SCM ECU within a radio system functional architecture that conforms to the JCAUS standard. Interfaced to the data ports of the SCM ECU are two microprocessors (or microcontrollers) referred to as the red and black processors of the Payload Host Module (PHM). The main role of the red PHM processor is to translate between the communication protocol used on the OCU or the unmanned vehicle (UxV), such as the Joint Architecture for Unmanned Systems (JAUS) protocol[2], and the functions specified in the JCAUS SCM Application Programing Interface (API), implemented by the SCM ECU. The black PHM processor translates between the API functions and the radio-module-specific commands/status messages. These processors call the appropriate API functions to either pass data to be encrypted and receive encrypted data (ciphertext, CT), or to send and receive unencrypted data (plaintext, PT) through the SCM ECU’s controlled bypass.

The API offers a high-level communication interface to the PHM, abstracting away the cryptographic details of key management and distribution. The red processor can use simple API functions to instruct the SCM ECU to set up a secure connection to a remote device, which will cause the SCM ECU to automatically perform all of the necessary cryptographic operations.

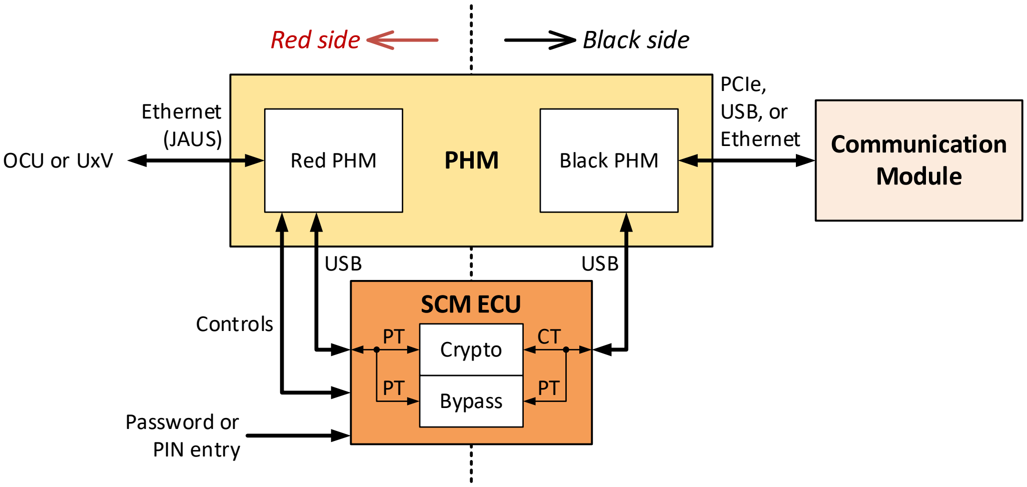

Figure 2. The SCM ECU within a radio system functional architecture

3. FORM-FACTOR AND INTERFACE

The JCAUS SCM specifications are designed to allow a variety of cryptographic modules to be integrated within a defined form-factor while adhering to specified electrical, mechanical, and logical interfaces, resulting in the production of a standardized stand-alone cryptographic product.

The goal of the introductory application of the JCAUS SCM—the FlexCSR SCM ECU—is to provide cybersecurity to radios developed under the FlexCSR program. It must fit within the size, weight, and power (SWaP) constraints of a FlexCSR radio along with all other radio-related hardware. We have taken advantage of the small-form-factor *MC* module to develop an SCM ECU with a minimal SWaP so as to maximize the design flexibility for the remaining hardware of the radio. This has the added benefit of allowing the SCM ECU to be used in a greater number of future SWaP-constrained applications. The sections that follow provide details of the interface ports and the form-factor.

3.1 Data and power ports

Every aspect of the SCM ECU was designed to minimize its SWaP, including the ports and the interfaces. The red- and black-side data/power ports use Universal Serial Bus (USB) 2.0. It only requires four pins for data and power, making it electrically simple to implement and mechanically compact, while providing plenty of bandwidth for future applications. The SCM ECU is designed to accept power from a 5V-30V source for greater flexibility. Furthermore, the SCM ECU can be powered from one or both USB ports. When powered through both ports, it provides the following benefits:

a) When the voltage difference between both ports is under 30 mV, load-sharing takes place.

b) When the voltage difference is greater than 30 mV, the port with the higher voltage will supply all of the current. This may be useful for host systems that support auxiliary power. If the primary power becomes unavailable, the auxiliary power will be used.

The power consumption of the SCM ECU is estimated to be about 1.5W average and 3W max.

3.2 Logic port

Although the SCM ECU is internally protected from unintended use, there may be situations during field operations that necessitate rendering it useless, either automatically through the host-platform or remotely by the operator. Therefore, an external port has been made available to allow logic-level discrete signals to the SCM ECU.

3.3 Serial port

Unlocking the SCM ECU for use requires logging in with proper credentials. For versatility, two methods are available: 1) using the red-side USB interface, or 2) using the Serial Port. The Serial Port accepts 3.3V CMOS-level serial data.

3.4 Connectors

The choice of connector type used for the SCM ECU's external interfaces was driven by the following good-engineering practices and requirements in designing an ECU:

- There must be physical separation between red- and black-side ports to facilitate meeting TEMPEST requirements.
- Connectors must maintain 360 degree shielding contact with enclosure. This allows shielded cables to mitigate electromagnetic interference (EMI) and electrostatic discharge (ESD).
- Connectors must be environmentally sealed to IP67 since future applications may require exposure to the elements.
- Connectors must support high-speed USB 2.0 signaling.
- Connectors must be as small as possible to help minimize SWaP.

The last bullet eliminates using standard USB connectors, including sealed versions, for the data/power ports, in favor of the standard M5-type circular connector. They are cost-effective, widely available, and provide both gender types. To eliminate catastrophic damage due to accidental cable swapping, the power/data ports use male connectors, while the Logic and Serial ports use female connectors.

If the red- and black-side data/power cables are swapped, the SCM ECU will not be damaged, nor will it be rendered useless. The user will simply not be able to log in until the error is corrected. Similarly, the SCM ECU will not be damaged if the Logic and Serial cables are swapped during installation.

3.5 Enclosure

Advanced printed circuit board manufacturing techniques and compact electronic components were used to achieve the absolute minimum footprint possible for the internal electronics, the size of which drove the enclosure design.

The material of the box is aluminum and painted tan with a military-standard paint. The box forms a conductive chassis around the electronics and is grounded. The total weight of the prototype SCM ECU, including all electrical and mechanical components, is approximately 0.4 lb (200 g), although we are currently optimizing the design to drive the size and weight down even further. Current dimensions are given in Figure 3.

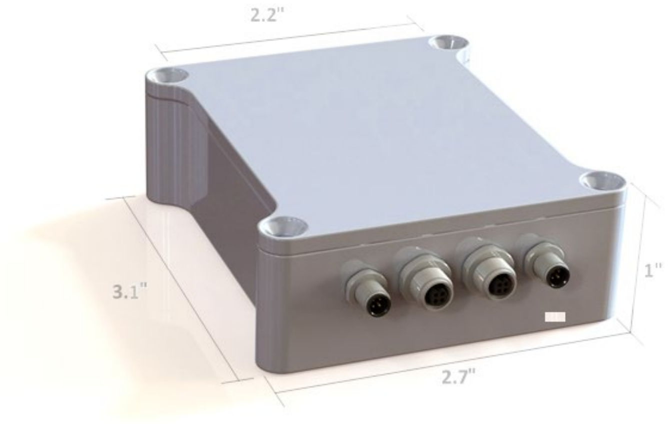

Figure 3. Outside dimensions of the SCM ECU

4. KEY MANAGEMENT

Within the small package of the SCM ECU is a powerful cryptographic key management engine that greatly simplifies pre-mission logistics while allowing for operations that are more dynamic. TKM eliminates manual preloading of classified keys destined for specific ECUs. Instead, one SCM ECU (usually attached to an OCU) is able to generate keys on demand and securely deliver them to any other SCM ECU as they are needed during a mission. The security of this transfer and subsequent communication rests on mutual trust in a Certificate Authority (CA), in this case provided by DoD Public Key Infrastructure (PKI). The application of this technique to small embedded systems was pioneered by MIT Lincoln Laboratory on the Air Force Stand-Alone Crypto program[3], which later transitioned to the production and National Security Agency (NSA) certification of the *Mini Crypto* module by the AFLCMC Cryptologic and Cyber Systems Division through a contract to Viasat.

4.1 The tactical setting

The tactical setting provides several distinct challenges from a general commercial medium such as the internet. On the internet, PKI is generally used to assure integrity and confidentiality when communicating with a web service, and conveniences are afforded by constant access to PKI resources on a client. However, in a tactical environment this infrastructure is unavailable, leading to a different set of security and operational concerns.

For example, Certificate Revocation Lists (CRLs) are used in PKI to provide timely warning of the compromise of a web server's private key material. In the tactical environment, where devices may be disconnected from infrastructure for extended periods of time and located in an environment with a higher probability of loss or compromise of multiple trusted devices, we need mechanisms to update trust dynamically. Thus, TKM employs CRLs for periodic updates but also allows for use of blacklists that identify devices suspected to be compromised during a mission.

Additionally, data throughput can be limited in the tactical environment, which can be strained by the verbose messages used in internet protocols such as Transport Layer Security (TLS) or its datagram equivalent, Datagram TLS (DTLS). With a narrower scope and more limited cryptography suites, TKM simplifies the Cryptographic Message Syntax (CMS) specifications that define its key management messages, greatly reducing the amount of data that needs to be transported to establish secure communication.[4]

Furthermore, devices in a tactical setting—particularly UxS—face a higher probability of loss and/or compromise. As such, the SCM ECU uses only algorithms from the CNSA suite, and does not retain mission keys when powered off. Thus, it avoids many of the security and handling requirements incurred by traditional COMSEC equipment, and in particular is expected to be categorized as a Cryptographic High Value Product (CHVP)[5] and not a Controlled Cryptographic Item (CCI)[6].

4.2 Provisioning and operation

The provisioning process for an SCM ECU is simple, but relies on a brief connection to DoD PKI. When provisioning an SCM ECU, the *device administrator* may export a pair of Certificate Signing Requests (CSRs), one for each type of key used in operation. These contain user-provided information (e.g. common name, organizational unit) about the device, which will become part of the SCM ECU's certified identity. These CSRs are provided to the appropriate DoD PKI administrator for signing, resulting in a pair of certificates to be installed in the device. The device administrator may also create and later manage operational users.

Once provisioned, an SCM ECU may be put into operation. An operational device is unlocked with a password after power up, enabling secure communication with potentially any other provisioned SCM ECU. In many UxS, directly entering a password on the vehicle is impractical. To deal with this, the SCM ECU supports a form of remote unlocking, wherein one unlocked device (e.g., the OCU’s SCM ECU) may unlock others over an otherwise-insecure communication link.

Once unlocked, secure sessions may be created. A session is an encrypted communication net which may have many members, with all members capable of decrypting any message sent within the session. A pair of devices may use more than one session simultaneously in order to enable broader information sharing. For example, an operator controlling a UxS may wish to have a dedicated Command and Control (C2) channel with which no other operator may interfere, while at the same time sharing the video feed coming back from the UxS. In this case, placing the video feed in a separate session allows the operator to include multiple devices in the video session while keeping sole control of the UxS.

The ability to re-key and redefine groups enables fine-grained access control which may be dynamically altered as the mission evolves and participants come and go. New devices may be added at any time. Compromised or otherwise unauthorized devices may be removed quickly through recreation of the session with a new key. This enables, for example, an operator to seamlessly hand over control of a UxS to another remote operator, or access to a UxS video stream to be determined based on the vehicle's location.

4.3 Controlled bypass

As seen in Figure 2, the SCM ECU provides separation of the sensitive robot or OCU and its non-sensitive communication module, controlling what information may be transferred across this red/black boundary. In general, data from the robot or OCU is encrypted as they pass through the SCM ECU to the communication module, and data from the communication module is decrypted before reaching the robot or OCU. However, operation of the communication module requires that certain control and status messages local to the radio (e.g., for changing channels or monitoring received signal strength) must be passed through the SCM ECU unmodified. These data will not be transmitted over-the-air, and must pass through the SCM ECU's controlled bypass via specific API function calls. The fine-grained control is defined in an approved bypass policy.

A bypass policy defines all valid control and status messages (and their parameters) that need to be passed between the robot or OCU and its communication module. Once a bypass policy has been tailored to support a given radio, it will need to be approved by the relevant authorities (NSA, et al.) and compiled into a properly formatted policy file. When an SCM ECU is provisioned, the radio-specific policy file can be installed in a process similar to the one used to install the device's certificates. The bypass logic ensures that sensitive data is not revealed by ensuring that all bypassed messages conform to the installed policy.

5. SCHEDULE AND MILESTONES

The SCM ECU is approaching the final stretch of the development process. An SCM Emulator and a software API are available for radio developers to explore integration and embedment of the SCM ECU before it is available for use. Prototype units will be available for TEMPEST testing in May 2019, depending upon the availability of low-rate initial production *MC* modules, which are due to be NSA certified around that timeframe. NSA certification of the FlexCSR SCM ECU is expected at the end of 2019.

6. CONCLUSIONS

Originally developed for the Man-Transportable Robotic System (MTRS) / Advanced Explosive-Ordnance-Disposal Robotic System (AEODRS) Radio for Cybersecure Operation with Network Integration (MARCONI) radio system[7], the SCM ECU has now been decoupled from the radio, modularized, packaged in tamper-resistant housing, and is being certified by the NSA to protect tactical data up to Secret level. Military communication systems making use of the SCM ECU may not have to be re-certified by the NSA, but only need to be authorized to operate by the individual Services (with assessment and input from the NSA to ensure proper embedment).

We believe that the FlexCSR SCM ECU, by enabling easy integration and reducing the logistic burden involved with protection and handling of classified keys and equipment, will significantly transform the cybersecurity landscape for tactical military systems in general, and UxS specifically, for years to come.

ACKNOWLEDGEMENTS

This project is funded by the Naval Sea Systems Command (NAVSEA), PMS 408. MIT Lincoln Laboratory's material is based upon work supported by the NAVSEA under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Navy. We would also like to express our appreciation for the significant collaboration and assistance we have received from the Johns Hopkins University Applied Physics Laboratory, the NAVSEA Indian Head Explosive Ordnance Disposal Technology Division, and the AFLCMC Cryptologic and Cyber Systems Division.

REFERENCES

[1] Reese, S., and Chang, W., "Joint communications architecture for unmanned systems (JCAUS)," Proc. SPIE 10195, Unmanned Systems Technology XIX, 10195P (2017).

[2] Rowe, S., and Wagner, C., "An Introduction to the Joint Architecture for Unmanned Systems (JAUS)", Technical Report from Cybernet Systems Corporation (2008), available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.489&rep=rep1&type=pdf.

[3] Massachusetts Institute of Technology Lincoln Laboratory, "Lincoln Open Cryptographic Key Management Architecture," TechNotes (2012), available online at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a594037.pdf.

[4] O'Melia, S.R., Khazan, R., and Utin, D., "Efficient Transmission of DoD PKI Certificates in Tactical Networks," The 2011 IEEE Military Communications Conference, 1739-1747 (2011).

[5] Committee on National Security Systems, "Cryptographic High Value Products", CNSS Instruction No. 4031, 16 February 2012.

[6] Committee on National Security Systems, "Controlled Cryptographic Items", CNSS Instruction No. 4001, 7 May 2013.

[7] Nguyen, H.G., Pezeshkian, N., Yen, J., and Hart, A., "Development of an advanced cybersecure radio for small unmanned ground vehicles," Proc. SPIE 10195, Unmanned Systems Technology XIX, 10195Q (2017).