ModuleOT: A Hardware Security Module for Operational Technology

Preprint

William Hupp, Adarsh Hasandka,
Ricardo Siqueria de Carvalho, and Danish Saleem

National Renewable Energy Laboratory

Presented at the IEEE Texas Power and Energy Conference (TPEC)
College Station, Texas
February 6–7, 2020

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-74697
February 2020

ModuleOT: A Hardware Security Module for Operational Technology

Preprint

William Hupp, Adarsh Hasandka,
Ricardo Siqueria de Carvalho, and Danish Saleem

National Renewable Energy Laboratory

Suggested Citation
Hupp, William, Adarsh Hasandka, Ricardo Siqueria de Carvalho, and Danish Saleem. 2020. *ModuleOT: A Hardware Security Module for Operational Technology: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-74697. nrel.gov/docs/fy20osti/74697.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-74697
February 2020

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Module-OT: A Hardware Security Module for Operational Technology

William Hupp, Adarsh Hasandka, Ricardo Siqueira de Carvalho, and Danish Saleem
National Renewable Energy Laboratory
Golden, CO, USA
Email: [william.hupp, adarsh.hasandka, ricardo.siqueiradecarvalho, danish.saleem]@nrel.gov

***Abstract*—Increased penetration levels of renewable energy and other types of distributed energy resources (DERs) on the modern electric grid—combined with technological advancements for electric system monitoring and control—introduce new cyberattack vectors and increase the cyberattack surface of energy systems. According to the IEEE Std. 1547-2018, DERs must use Modbus, Distributed Network Protocol 3 (DNP3), or Smart Energy Profile 2.0 (SEP2) as their communication protocol. Previous research identified several vulnerabilities and security breaches in each one of these communication protocols; despite this, existing standards for DERs do not recommend cybersecurity measures. In order to reduce vulnerabilities in power distribution systems, this paper presents a novel open-source hardware security module that improves both information and operational security to better protect data and communications on the distribution grid. The security hardware is called "module for operational technology," or simply Module-OT, and it has been validated and tested in an emulated distribution system application. Module-OT is integrated within a communication system in the transport layer of the Open Systems Interconnection (OSI) model. It improves system security through encryption, authentication, authorization, certificate management, and user access control. The main advancement of Module-OT is the addition of hardware encryption acceleration that improves the overall communication performance in terms of end-to-end latency.**

I. Introduction

The modern power distribution grid is constantly and rapidly changing, and this includes an increasing deployment of distributed energy resources (DERs) [1]. Increased DER penetration has some benefits, such as enabling a more efficient and more sustainable electric system, but this also increases the use of information and communication technology (ICT) devices, which has drawbacks. Most notably, increased ICT use in electric systems means higher cyberphysical interdependency and a larger surface for potential cyberattacks [2]–[4].

Cyberattacks targeting the electric grid could clearly have serious impacts, including asset damage, cascade failures, or even energy blackouts [5]–[7]. A major example of this is the recent blackout in the Ukrainian electric grid resulting from a cyberattack [2]. Cyberattacks targeting DERs have the potential to propagate outside the devices themselves and affect the whole grid, even up to the transmission level [8]. Therefore, improving the cybersecurity of DERs is an urgent problem, but the recently modified IEEE Std. 1547-2018 (which regulates the interconnection of DERs within distribution systems) still does not yet enforce cybersecurity measures for such systems [9].

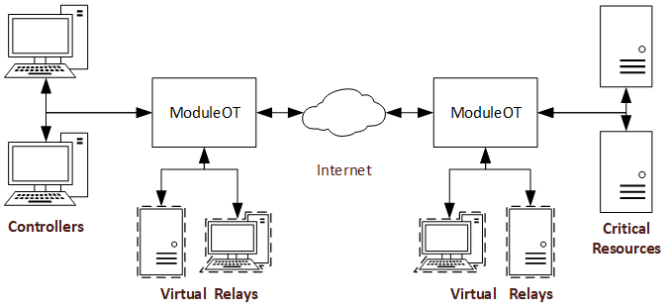

Fig. 1. Typical application network topology

Some electric utilities invest in cybersecurity already, and several research efforts are currently underway in academia as well [10]. Recent work related specifically to DER cybersecurity includes the research published in [8] and [11]–[13]. Cryptography is one potential solution for securing DERs against cyberthreats; however, researchers found that adding this functionally to the existing ICT system increases the end-to-end communication latency because of the necessary time for encryption and decryption [14], [15]. The monitoring and control of DERs is a delay-sensitive application, and the addition of data cryptography for such application could potentially impact the DER operation in a negative way [14], [16].

The main contribution of Module-OT compared to related encryption solutions for DERs is the use and leverage of low overhead encryption based on the advanced encryption standard (AES) [17]–[19], together with support for legacy DERs that use serial Modbus. Besides end-to-end encryption, Module-OT also provides authentication and authorization to secure communications to a remote DER site in order

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Cybersecurity for Energy Delivery Systems Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

to improve cybersecurity of DERs in a holistic way. An additional contribution of this paper is to provide a detailed description of Module-OT design so other utilities and the research community might implement and/or integrate Module-OT's cybersecurity functionalities with their own cybersecurity solutions and needs.

II. Module Overview

The purpose of Module-OT is to provide a single device that provides features of end-to-end encryption, authentication, and authorization to secure communications to a DER site. To facilitate this, we implemented the following core features: the application allows for communications to DERs using serial or Ethernet connections, performs key management, and provides data security through white-listing IP addresses and ports, blocking unauthorized connections and controlling user access.

A. End-to-End Encryption

This module leverages OpenSSL to perform encryption and decryption for all in-flight data. The device uses the ECDH_ECDSA_AES_128_CCM cipher suite; however, it could be configured to use any cipher suite supported by OpenSSL. The end-to-end encryption is enabled by using TLS to allow for communication with networked and legacy DERs and supports any Transmission Control Protocol/Internet Protocol.

B. Hardware Cryptographic Acceleration

To handle large numbers of devices at one DER site, the module leverages hardware cryptographic acceleration in the form of a processor that supports Intel's Advanced Encryption Standard New Instructions (AES-NI) x86 advanced instruction set. This instruction set allows software packages (such as OpenSSL) to use the processor directly to compute the Advanced Encryption Standard (AES) cryptographic algorithm and to show marked improvement over pure software implementations of AES [18]. The use of AES-NI implies that using more expensive and faster processors can provide significant speedup in throughput, as demonstrated in reports comparing the results of OpenSSL speed tests across a variety of x86 processors that support AES-NI [19].

C. IP White-listing

Module-OT uses a preconfigured white list to determine which hosts are allowed to connect to it. The IPs in this white list can be edited by users by making changes to a Java Script Object Notation file. If the device sees a successful connection attempt from a non-white-listed IP address, it immediately closes the connection and shows a warning message. This behaviour is allowed to repeat a preconfigured amount of times before more drastic measures are taken, such as using a firewall for blocking. In the test bed used to validate this module, 10 such connection attempts were allowed before the connection was explicitly blocked. After the preconfigured number of times, the connection is blocked from sending any packets to the device using an iptables-based firewall. The application adds a rule to automatically block connections from the malicious IP. In this manner, Modules-OT provides denial-of-service (DoS) attack protection. This behaviour can also be configured to protect the device from distributed DoS attempts.

D. Key Management

We designed this module to use certificates to perform key management and authentication. It requires a valid X.509 certificate to connect to other modules using TLS. To test the communications locally, it can use self-signed certificates; however, this is not recommended for devices deployed outside a laboratory environment. The device's home and certificate folders are encrypted to prevent unauthorized access and protect data at rest.

E. Serial Device Support

One of the most commonly overlooked areas in existing secure-gateway or endpoint solutions is the ability to support legacy grid devices. Because the technologies on the electric grid are designed to last many years, a significant number of these devices use legacy or serial RS485 connections for communications. Many researchers recommend a bump-in-the-wire solution to address these problems [20], and one of Module-OT's core functions is to provide this support. To achieve that, the module performs conversion between TCP and serial protocols and relays serial commands to the DERs. It automatically virtualizes a TCP-based device that clients could target for communication with the legacy device.

F. Role-Based Access Control

To allow for remote control and monitoring, Module-OT supports the Secure Shell (SSH) protocol. To limit the potential for abuse of this connection (as well as the device in general), the module allows outside SSH connections only through its least-privileged user. This user account has read-only access to many of the configuration files and can be used to monitor the device or view its settings. To change any settings, the active user must be switched to a more privileged account that has the ability to request administrative privileges using the "sudo" command. By requiring a pass phrase and hardening the SSH server, the device aims to be protected from least-privileged violations that lead to unwanted intrusion and alteration of its configuration.

III. Module Design

A. Software

The Module-OT application is written in the Go programming language and therefore is operating-system independent. For our implementation, the application was run on an Ubuntu 18.04 LTS Desktop with the x86-64 instruction set architecture. The software leverages many open-source packages and software tools to function, including Python, Nmap, OpenSSL, OpenSSH, and the PyModbus library; however, because these are the only external software requirements and they are

Fig. 2. OpenSSL speed test on the Raspberry Pi

all open source, the overall application is hardware-platform independent. We generally recommend running the application on hardware with AES-NI support, however, in order to take advantage of hardware acceleration for improved performance. Ultimately, because Module-OT is a hardware- and operating-system-agnostic solution, the security application can be easily imaged or containerized for virtual or cloud deployments. This ease of deployment and flexibility allows the module to be a low-cost and easily implementable solution for securing valuable assets.

B. Communications

All networked DER communication protocols, such as Distributed Network Protocol 3 and Modbus, encapsulate TCP at the transport layer of the Open Systems Interconnection model. Therefore, all the protocols can be relayed using TCP clients and servers. By operating only at the transport layer and below, Module-OT is protocol- and data-model-agnostic. For a new protocol to function correctly, it needs to use TCP, and because nearly all client-server protocols support TCP, the module supports nearly all client-server protocols. In this manner, Module-OT supports all protocols recommended by IEEE 1547-2018 [9]. The module also supports simultaneous connections using these various protocols on all open and enabled ports in DERs. Because the device is designed to connect to an untrusted network along one interface, the application does not open any ports on that interface other than the one used for TLS by the application.

C. Intended Operation

Two security modules are needed to secure end-to-end communications to a remote DER site. One device is needed on the grid site—the server module. Another device is required at the control center site—the client module. The security application is configured to automatically start upon boot. Therefore, once the server module starts and sees a connection from a client module, it automatically scans the local network to see what DER connections are available. The IP information of any white-listed DERs that the server module can see are automatically communicated to the client module. The client then creates a virtual interface to relay communications intended for that device. This process requires a few seconds to complete once the device has been plugged into the network. Once this process is completed, the communications pathway to the remote DER is available through the modules, and clients at the control center can freely connect to the device.

D. Hardware Requirements

Module-OT was deployed on two different hardware platforms during development to compare performance and determine the minimum hardware requirements necessary to meet the application's goals of authentication, authorization, and encryption for large DER sites.

1) Raspberry Pi 3B+: The Raspberry Pi is a low-cost, single-board computer that allows for expansion of the motherboard with serial peripherals. One such peripheral is the ATECC608A integrated circuit made by Microchip, which provides low-cost hardware acceleration for the Raspberry Pi. This chip provides the functions of key verification for encryption/decryption, secure hardware-based key storage, and support for a variety of cipher suites; however, the CryptoAuthLib library for the ATECC608A chip does not support AES-128-CCM. AES-128-CCM must be used to meet the recommendations for DER standards [11]. Because CryptoAuthLib does not support AES-128-CCM, the integrated circuit is unable to perform hardware acceleration for our desired encryption scheme. However, as the driver currently supports Cipher Block Chaining (CBC), Counter, and Galois/Counter modes of AES, support for this driver may added if support for Counter with CBC-Message Authentication Code (CCM) mode or support for other AES modes is added in a future version. Figure 2 shows the result of an OpenSSL speed test of the AES-128-CCM cipher on this hardware. Note that approximately 23,500,000 bytes are processed in 16,384 byte blocks with AES-128-CCM in 3 seconds. This result could be improved with further development of the integrated circuit driver, or support for another integrated circuit that provides hardware acceleration for the Raspberry Pi. For individual or small DER sites, however, this level of performance is quite acceptable, and this can be considered the minimum recommended hardware platform.

2) Protectli Vault: Intel has developed a subset of the x86 instruction set, known as AES-NI, which supports low-level processor routines for individual AES functions. This allows high-performance hardware AES computation to be performed on the processor [18]. Most modern processors have incorporated the AES-NI instruction set, and it is enabled by default on all processors that support it. One such CPU is the Intel Quad Core Celeron J3160, which is incorporated into the Protectli Vault Network Appliance. The Protectli Vault is a fanless microfirewall solution that is able to implement Module-OT and serve larger DER sites than the low-cost

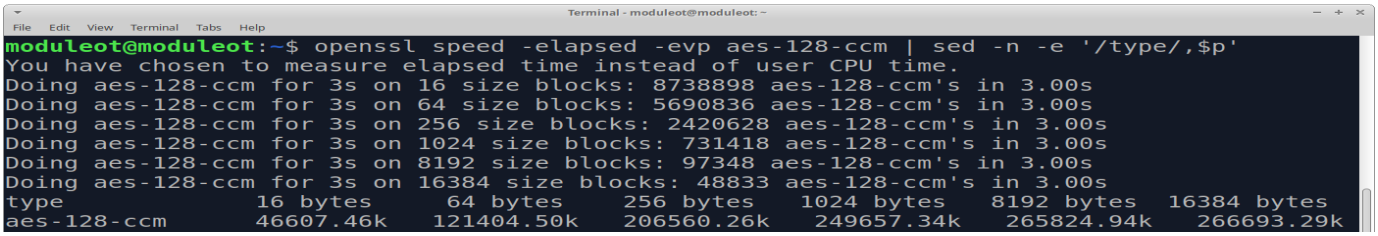

Fig. 3. OpenSSL speed test with AES-NI

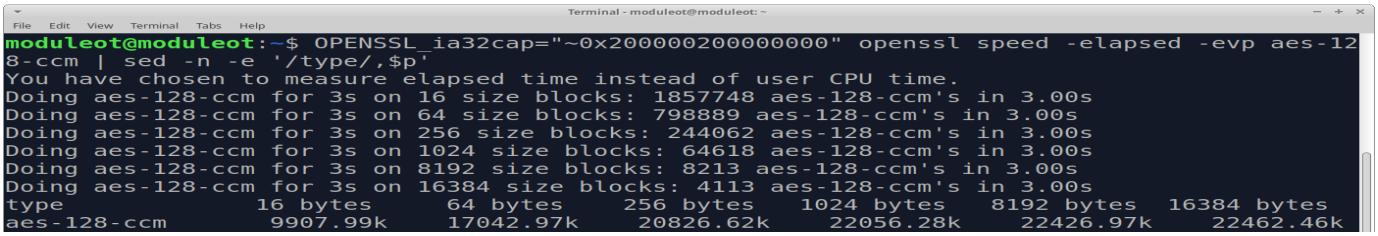

Fig. 4. OpenSSL speed test without AES-NI

platform. Figure 3 shows the result of an OpenSSL speed test of the AES-128-CCM cipher on this hardware. Approximately 267,000,000 bytes are processed in 16,384-byte blocks with AES-128-CCM AES-NI in 3 seconds. This is approximately a 10x increase in speed compared to the low-cost platform, Raspberry Pi. This improved throughput as a result of the hardware acceleration naturally decreases encryption overhead and hence can be expected to reduce latency and increase the number of supported DERs in the system. For comparison on the same hardware, Figure 4 shows the result of an OpenSSL speed test of the AES-128-CCM cipher on this hardware when AES-NI is disabled. Approximately 22,500,000 bytes are processed in 16,384-byte blocks with AES-128-CCM AES-NI in 3 seconds.

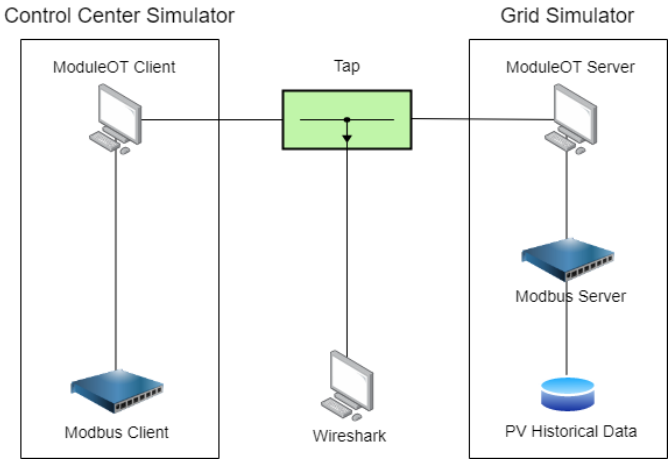

Fig. 5. Module test bed

IV. Test Bed

To validate Module-OT, we developed a proof-of-concept test bed. Figure 5 depicts the design of the test bed.

The edges of the test bed consist of two distribution system device emulators running on local computers, one on each side. One is emulating the inverter and its communication features by using historical photovoltaic generation data from a data set from the Electric Power Research Institute [22]. The other emulator is on the utility side and emulates DER reading requests from the control center. Figure 8 shows the physical data input for the test bed. Two security modules built using the Protectli Vault hardware are used to encrypt and decrypt data between the distribution system data emulation devices. The specifications of these devices contain an Intel Quad Core Celeron J3160 2.2-GHz processor, 8GB DDR3L RAM, 120GB mSATA SSD, 4 Intel i210 Ethernet, 2 USB 3.0, an RJ-45 COM, and 2 HDMI ports. Each device has the capability of acting as a server or a client, depending on its configuration as defined in the application configuration file. In this test bed, Ethernet cables were used to connect all the devices, as shown in Figure 5. A network data tap was connected in between the two modules to observe the encrypted data.

V. Results

In the initial test, the system was connected directly by connecting the Modbus client and server to the tap, without security modules in between. Figure 6 shows the output of the Wireshark session on the man-in-the-middle system. In Wireshark, the computer in between is easily able to decode the Modbus packets and see in plain text data, such as the request type “Read Input Registers.” Similar, command and control signals can easily be intercepted in this scenario.

The next test is performing the same communications using security modules between the Modbus server and client. Figure 7 shows that after connecting the devices in between, the malicious system is unable to see the Modbus traffic. The Wireshark session simply sees TLS packets with encrypted (and

```
55944 → 504 [ACK] Seq=4621 Ack=4236 Win=29312 Len=0 TSval=3529471230 TSecr=2614890873
 unknown: Trans: 26168; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
 unknown: Trans: 26168; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
55944 → 504 [ACK] Seq=4633 Ack=4247 Win=29312 Len=0 TSval=3529472233 TSecr=2614891876
 unknown: Trans: 33293; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
 unknown: Trans: 33293; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
55944 → 504 [ACK] Seq=4645 Ack=4258 Win=29312 Len=0 TSval=3529473235 TSecr=2614892879
 unknown: Trans: 53487; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
 unknown: Trans: 53487; Unit:   1, Func:   4: Read Input Registers. Unable to classify as query or response.
55944 → 504 [ACK] Seq=4657 Ack=4269 Win=29312 Len=0 TSval=3529474238 TSecr=2614893882
```

Fig. 6. Unencrypted traffic visible on Wireshark

261	82.103476	10.10.49.49	10.10.49.45	TLSv1.2
262	82.105951	10.10.49.45	10.10.49.49	TLSv1.2
263	82.106297	10.10.49.49	10.10.49.45	TCP
264	83.109733	10.10.49.49	10.10.49.45	TLSv1.2
265	83.112241	10.10.49.45	10.10.49.49	TLSv1.2
266	83.112638	10.10.49.49	10.10.49.45	TCP
267	83.669146	0.0.0.0	255.255.255.255	DHCP
268	83.678591	169.254.146.185	239.255.255.250	SSDP
269	84.116309	10.10.49.49	10.10.49.45	TLSv1.2

Fig. 7. Encrypted traffic only visible as TLS packets

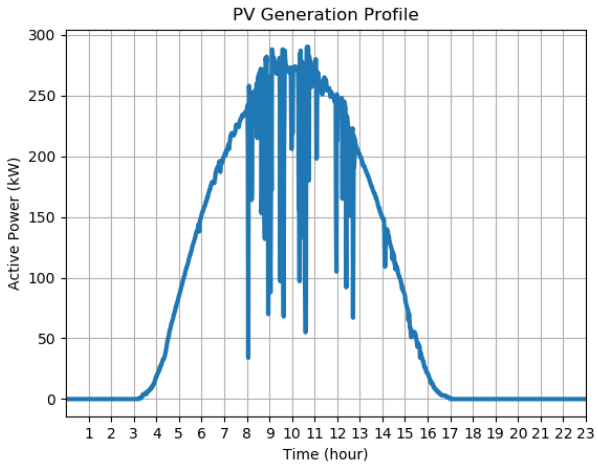

Fig. 8. Photovoltaic generation values initialized on the device

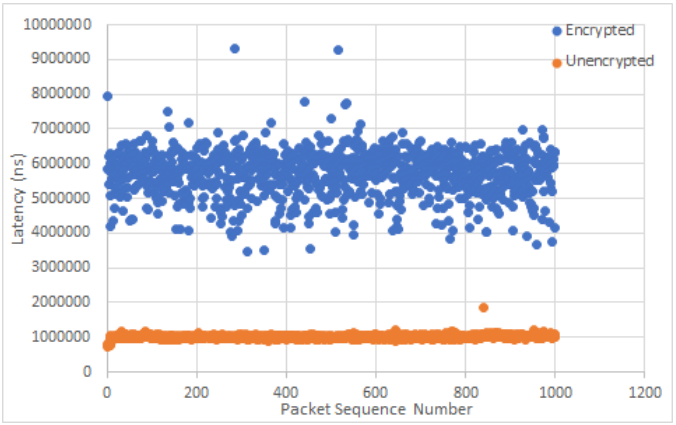

Fig. 9. Round-trip latency measurement for 1,000 packets

thus unreadable) data, thereby demonstrating that Module-OT effectively masks the data as well as the true source and destination.

While this encryption adds latency to the connection, the latency is still in the order of tens of milliseconds as seen in the measured latency for 1,000 packets shown in Figure 9. This level of latency is acceptable for DERs [13]. With continuing improvements to the application, this latency can be improved in the future. Connection requests from modules that are not white-listed are unable to establish a connection to the TLS server. The server immediately breaks any attempted connections, and after multiple consecutive attempts, the IP is blocked by adding a rule to the server module's firewall.

VI. Future Work

Several future avenues of development are currently planned for Module-OT.

A. Penetration Testing

Thorough testing, red-teaming, and third-party security evaluation of the device's communications, software, and hardware is necessary to ensure that the device is able to provide a reliable level of security for important assets. Third-party security evaluation is planned to establish a solid initial baseline of security for the module.

B. SunSpec Certificate Authority

We plan to move from using a self-signed or test certificate authority to contracting SunSpec as the root certificate authority and public key infrastructure management. If a compromised client is able to access the system services with a valid certificate, the compromised client could launch a cyberattack. To prevent this, the module will use a trusted

certificate authority, such as the one maintained by SunSpec. A trusted certificate authority maintains an updated certificate revocation list and helps ensure that only valid clients are given certificates and allowed to connect. This is important to prevent legacy clients from having access to a system beyond their allocated time.

C. Custom Hardware Platform

Although the Vault is a suitable hardware platform for the module, it is an off-the-shelf, third-party device. Going forward, a custom hardware platform could be designed specifically to run Module-OT with optimal performance, throughput, and latency. The design should incorporate a high-performance CPU with AES-NI hardware acceleration support. A Trusted Platform Module would also aid the hardware security of our module by securely storing RSA keys.

D. Vendor Hardware Integration

Because of the open nature of the module, vendors are free to take elements of the system design and manufacture the hardware requirements directly into their power system devices. This would greatly improve the physical security of the module through direct integration and remove the need for a separate bump-in-the-wire solution in an already complex smart grid.

VII. Conclusion

Module-OT's functionality improves on the current end-to-end security applications for DERs by providing not only encryption, authentication, and authorization from a control center to DERs on a distribution grid, but also support for legacy hardware in an open-source security module. Module-OT has been tested and verified to operate successfully on a physical networking test bed with emulated distribution system devices and data. With an operating-system-independent design, the module can cohesively (and with minimal configuration from the system administrator) improve security of communications from malicious adversaries on the smart grid. In our testing, Module-OT demonstrated its ability to secure power system communications to minimize attacks such as man-in-the middle, eavesdropping, and replay attacks, preventing negative impacts on the grid and other critical systems. Experimental results show that the use of hardware cryptographic acceleration for DER data encryption significantly improves the end-to-end communication latency.

References

[1] Y. Xue, M. Starke, J. Dong, M. Olama, T. Kuruganti, J. Taft, and M. Shankar, "On a Future for Smart Inverters with Integrated System Functions," 2018 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Charlotte, North Carolina, United States, pp. 1–8, 2018.

[2] [2] R. Siqueira de Carvalho and S. Mohagheghi, "Analyzing Impact of Communication Network Topologies on Reconfiguration of Networked Microgrids, Impact of Communication System on Smart Grid Reliability, Security and Operation," 2016 North American Power Symposium (NAPS), Denver, Colorado, United States, pp. 1–6, 2016.

[3] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security," Energies, vol. 11, pp. 1996–1073, 2018.

[4] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," in Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012.

[5] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[6] P. Kaster and P. K. Sen, "Cybersecurity and Rural Electric Power Systems: Considering Competing Requirements for Implementing a Protection Plan," in IEEE Industry Applications Magazine, vol. 23, no. 5, pp. 14–20, Sept.-Oct. 2017.

[7] D. J. Sebastian and A. Hahn, "Exploring Emerging Cybersecurity Risks from Network-Connected DER Devices," 2017 North American Power Symposium (NAPS), Morgantown, West Virginia, United States, pp. 1–6, 2017.

[8] R. Siqueira-de-Carvalho and D. Saleem, "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," in IEEE 2019 Resilience Week, San Antonio, USA, 2019.

[9] IEEE, "IEEE Std. 1547-2018—IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," 2018.

[10] J. Ausmus, R. Siqueira de Carvalho, A. Chen, Y. N. Velaga, and Y. Zhang, "Snapshot of Big Data Analytics in Power Systems," in The First IEEE International Conference on Smart Grid Synchronized Measurements and Analytics – SGSMA, Texas AM University, College Station, Texas, USA, May 20-23, 2019.

[11] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, R. Ih, "Recommendations for Trust and Encryption in DER Interoperability Standards," Tech. Report, Sandia National Laboratories, Albuquerque, USA, SAND2019-1490, 2019.

[12] D. Saleem, and C. Carter, "Certification Procedures for Data and Communication Security of Distributed Energy Resources," National Renewable Energy Laboratory, Golden, USA, Tech. Report, NREL/TP-5R00-73628, 2019.

[13] C. Lai et al., "Cryptography Considerations for Distributed Energy Resource Systems," 2019 IEEE Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 2019, pp. 1-7.

[14] R. Siqueira-de-Carvalho, "Integrating Big Data Analytics and Cybersecurity for Power Distribution Networks with Distributed Energy Resources," Ph.D. Dissertation, Colorado School of Mines, Golden, USA, 2019.

[15] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources," 2019 IEEE Power and Energy Conference at Illinois (PECI), Champaign, Illinois, United States, 2019, pp. 1–8.

[16] R. Siqueira-de-Carvalho, P. K. Sen, Y. N. Velaga, L. F. Ramos, and L. N. Canha, "Communication System Design for an Advanced Metering Infrastructure," Sensors, Vol. 18, 2018.

[17] N. Andreea, P. Victor, M. Lautentiu, and K. Andrei, "Comparative Study on AES Hardware Implementations," Proceedings of the 8th International Conference on Telecommunications and Informatics (TELE-INFO '14), Kuta, Indonesia, 2014.

[18] K. D. Akdemir, et al. "Breakthrough AES performance with intel AES new instructions," white paper, Jun. 2010.

[19] "AES-NI SSL Performance: a study of AES-NI acceleration using LibreSSL, OpenSSL" https://calomel.org/aesnisslperformance.html

[20] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," in IEEE Security Privacy, vol. 8, no. 1, pp 81-85, Jan.-Feb. 2010. doi 10.1109/MSP.2010.49

[21] V. Perelman and M. Ersue, "TLS with PSK for constrained devices," Tech. Report, Citeseer, Feb. 2012.

[22] Electric Power Research Institute (EPRI), "Measurement Data from Field Monitoring Sites: Single Modules on Poles and PV Plants" Available online: https://dpv.epri.com/measurementdata.html (accessed on 13 August 2019).