Design Considerations of a Cryptographic Module for Distributed Energy Resources

Danish Saleem*, Adarsh Hasandka*, Christine Lai†, Deepu Jose†, Christopher Howerter†

*National Renewable Energy Laboratory
Golden, CO USA
{Danish.Saleem,Adarsh.Hasandka}@nrel.gov

†Sandia National Laboratories
Albuquerque, NM USA
{Cflai, Djose, Cmhower}@sandia.gov

Abstract—The digitization of distributed generation has prompted utilities to deploy distributed energy resources (DERs) with ubiquitous communications that potentially widen the attack surface. To protect critical infrastructure on digital networks, appropriate security controls need to be placed using either purpose-built cybersecurity technologies or embedded security controls in command and control center protocols. Few vendors offer devices that use cryptography to secure the communications from DERs to command and control centers or to distribution substations. There is a need to research and develop a suitable cryptographic module that is capable of mitigating the risk of unforeseeable threats, specifically to DERs and bulk power systems. This paper presents research to improve the security of an electric grid that employs millions of DERs with the goal of securing DER communications with a robust and inexpensive cryptographic module.

Keywords—Cryptography, distributed energy resources, distributed generation, hardware security module.

I. INTRODUCTION

The electric sector is witnessing a rapid global transformation because of environmental concerns about generation from fossil fuels and increasing demand from consumers for clean energy choices and deregulation. At the same time, advanced digital technologies are entering the electric sector to improve energy efficiency, integrate increasing amounts of variable renewable energy, and improve command and control functions farther out on the electric grid. These changes come at a cost because a more intelligent and networked grid opens new surfaces that can be exploited by cyberattacks from a variety of hackers with different motivations [1], [2]. Utilities have traditionally relied on intrusion detection and prevention systems, firewalls, and other tools to protect the bulk of their resources, but such tools are limited to signature-based malware detection and fail to protect against data fuzzing, stealthy attacks, and insider threats [3]. Further, analysts have poor cybersecurity business processes to follow while integrating new products into their trusted networks [2], [4]. In other words, utilities have been relying on information technology-focused defense, but there is need for defense mechanisms that are focused on distributed energy resources (DERs). For DER security, approaches such as defense in depth and defense in breadth are needed to create a robust and secure architecture [5], [7]. Although the overall security of distributed generation has been well researched [7]–[9], there is still a need to perform research on how to secure the communications of DERs to command and control centers of utilities effectively, efficiently, and specifically with the focus on developing a robust and inexpensive cryptographic module.

This paper presents research performed by the National Renewable Energy Laboratory (NREL) and Sandia National Laboratories (Sandia), along with industry partners, on the design considerations that are required to develop an innovative and low-cost cryptographic module that would be lightweight in terms of power, memory, and networking requirements but flexible enough to provide end-to-end encryption, authentication, and authorization to secure command and control messages and communications sent to and from DERs. This research primarily focuses on the security of communications over a wide-area network (WAN) between a site where DERs are installed [e.g., photovoltaics (PV)] to the control center or between a DER site and a distribution substation. The cryptographic considerations for designing the module for DER systems and the module’s system and interoperability impact are studied in [10], [11].

NREL has developed the first prototype of this cryptographic module. It is able to address vulnerabilities to attacks, such as man-in-the-middle, replay, reconnaissance, and unauthorized access for DER communications. This module is vendor and technology agnostic. Its key features are to:

- Perform authentication and authorization using its white-listing capability and encrypt the communications to provide data integrity;
- Perform key management and provide data security and compliance;
- Provide an added layer of security that will require a master key each time the user tries to perform reconfiguration of the default settings;
- Provide ease of use to reduce the total cost of implementing an adequate level of security;
- Provide capabilities to communicate using serial, Ethernet, and wireless connections.

II. PRACTICAL CONSIDERATIONS OF IMPLEMENTING CRYPTOGRAPHY IN DER SYSTEMS

To implement cryptography in DER systems, many practical considerations must be addressed. These include reliability, timing needs, and anti-tamper techniques. These crucial
concepts need to be considered when deploying a cryptographic module in DER systems.

Reliability: Traditional reliability for bulk generation is a standard-based prediction that employs empirical methods based on test data to estimate the failure rate. The results are well recognized by the industry [12]. Although DERs are not considered in traditional reliability calculations for bulk generation, rapid and consistent growth in DERs has already changed how grid operators sustain system reliability. DER devices and technologies impact not only distributed generation, but also demand response, load, and transmission [13]; however, data required to characterize and create requirements specific to the DER space are currently lacking [14]. It is increasingly apparent that the proliferation of smart devices is driving the electricity grid to have faster, sub-second response times that are beyond the capabilities of a human operator. Timing discrepancies can have a severe impact on the operation of advanced grid components. Meanwhile, these smart grid devices are passing increasingly large quantities of data across networks, often using unprotected, best-effort, multicast techniques that prioritize reliability over security. A primary concern with implementing encryption on a communications system is increased latency and potential data loss, so timing requirements are crucial to these efforts.

Timing: Time accuracy and synchronization requirements vary widely among sections of the power grid and depend on the types of communications or actions being performed, including those operating over WANs and wireless networks. For example, sampling values for frequency event detection require sub-microsecond time accuracy whereas the requirement for time accuracy and latency for DER performance information is milliseconds.

Anti-tamper Techniques: Anti-tamper protection can take many forms and will depend highly on the design of the device itself. In fact, many anti-tamper protections must be part of the module design from the beginning. Depending on the overall architecture of the device—including memory, integrated circuits, data storage, and others—many techniques might be necessary [15]. In addition, tamper prevention, detection, response, and evidence techniques should be considered as part of the overall anti-tamper design. Because no security measures can ever truly defeat all attackers, having the ability to detect a tampered item is crucial. Many hardware-related anti-tamper techniques exist, such as making the enclosure difficult to open, applying coatings, and designing specialized switches and circuitry; however, hardware attacks are not the only avenue of attack. Networking and software attacks are also used. Standard protections should be applied to ensure that the network protocol stack is minimal and contains only protocols that are necessary to the function of the system. The National Institute for Standards and Technology recommends a set of controls for anti-tamper techniques for federal information systems that protects against threats like modification, reverse engineering, and substitution. Some of these controls are notification of physical attack, resistance to physical attack, passive detection of physical attack, and security architecture description [16]. These recommended controls can be considered when deploying a cryptographic module in DER systems.

III. DESIGN CONSIDERATIONS FOR THE PROTOTYPE CRYPTOGRAPHIC MODULE

A. Design Requirements of Hardware Platform

There are many ways to develop a cryptographic security module that provides the required security features. For the optimal design of the module, however, some considerations are required to be addressed. These are primarily related to the capabilities of the module, such as the location of the device within the system and in the network topology overall, the devices with which the module needs to communicate, mode of communication, software or hardware security measures, and which additional security features it should provide. These elements determine much of the requirements for the hardware platform. For example, a module placed next to a single power system device, such as a PV inverter, will require less powerful hardware than a module placed next to a device operating at the aggregator level. At the aggregator level, the security module would be responsible for all DERs within the local area network (LAN) of a distributed generation site.

These important considerations determine the necessary performance and hence the required specifications for a hardware development platform. Table 1 lists the different design aspects that were considered in the research for developing the prototype along with the planned solution to achieve each design aspect.

<table>
<thead>
<tr>
<th>Design Considerations</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module location in network topology</td>
<td>Gateway for WAN uplink/downlink</td>
</tr>
<tr>
<td>Expected communications agents in network</td>
<td>Controller via WAN at one end and LAN controller at another</td>
</tr>
<tr>
<td>Communications protocol</td>
<td>Secured TCP/IP communications via SSL</td>
</tr>
<tr>
<td>User authentication method</td>
<td>Using X.509 certificates</td>
</tr>
<tr>
<td>Required hardware interfaces</td>
<td>RJ45, RS485</td>
</tr>
<tr>
<td>Selected cryptographic cipher suite</td>
<td>AES_128_CCM_8</td>
</tr>
<tr>
<td>Cryptographic key protocol</td>
<td>ECDH_ECDSA</td>
</tr>
<tr>
<td>Key management method</td>
<td>Managing certificates through a selected certificate authority</td>
</tr>
<tr>
<td>Management software interface</td>
<td>Hardening SSH server</td>
</tr>
<tr>
<td>White-listing capability</td>
<td>Implementing firewall policies on local OS</td>
</tr>
<tr>
<td>Device-hardening method</td>
<td>Encrypting system file and hardening SSH policies</td>
</tr>
<tr>
<td>Management interface-hardening method</td>
<td>Using access logs, user authentication lockout, and user account access control</td>
</tr>
</tbody>
</table>

B. Form Factors of the Module

It is important to consider a few options for hardware implementation before finalizing a better and more suitable cryptography module that can be physically implemented into DER systems. Some hardware implementation options that were considered when developing a suitable cryptography module to mitigate the risk of foreseeable threats to DERs were:

1) Bolt-on solution: This is a plug-and-play solution that is used to provide cost effectiveness in securing existing legacy systems. It is a low-cost option with little disruption to existing DER systems; however,
considering a cryptography application would require additional computing resources, and existing DER hardware is unlikely to support a bolt-on solution.

2) Embedded solution: This is like a Trusted Platform Module (TPM). TPMs are typically used in high-end servers that have large computing capacity. Usually DERs do not have large computing capacities. In addition, different DERs have different ways of operating; therefore, this route would require module customization for each inverter, which would be nearly impossible.

3) Bump-in-the-wire (BITW) solution: This is usually used to provide ease of use because there is no need to have additional computing resources in the DERs to implement and validate such types of solutions in the system. BITW implementation inserts devices into the communication lines of existing systems so that no legacy DER hardware needs to be manipulated; however, it also creates latency in the system. This latency issue can be addressed by careful design of the BITW device so that it minimizes the increase in latency in the overall DER communications system so that it is negligible. Therefore, this solution seemed most appropriate for the research and development of a cryptography module for DER systems.

C. Selected Hardware Platform for Module

A single-board computer running Linux was the low-cost option selected to support the prototype test and provide sufficient platform flexibility. Four commercially available development boards were evaluated on the basis of performance and cost. Performance parameters were defined as memory, processing speeds, number of ethernet interfaces, number of wireless interfaces like Bluetooth and WiFi, and number of audio or video interfaces like High Definition Multimedia Interface (HDMI) and Universal Serial Bus (USB) ports. Raspberry Pi was selected for its performance and cost. The specifications for Raspberry Pi are as follows:

- **Raspberry Pi 3B rev 1.2**: This device runs on a quad-core 1.2-GHz Broadcom BCM2837 CPU with 1 GB of RAM. It provides a single 100BASE Ethernet interface as well as Wi-Fi and Bluetooth for network connectivity. Among the many provided interfaces are HDMI, USB, Inter-Integrated Circuit (I2C), Serial Peripheral Interface (SPI), and General Purpose Input Output (GPIO). This board has four USB 2.0 ports available for peripherals.

In addition, the following two hardware cryptographic accelerators were selected to implement cryptography:

- **ZYMBIT Zymkey 4i**: This device provides advanced encryption standard (AES) and secure hash algorithm (SHA) encryption functions with elliptic-curve Diffie-Hellman (ECDH) and elliptic curve digital signature algorithm (ECDSA) key generation and authentication. It has an onboard real-time clock for timing accuracy and an onboard TPM that acts as tamper-resistant memory for secure key storage. It was clear from the specification that this device provides many important security features and is close to an all-in-one solution. The drivers for this device are maintained by the manufacturer.

- **Microchip Technology AT88CK590**: This device directly interfaces with the ATSHA204A, ATAES132A, and ATECC508A via USB to the main board using an AVR AT90USB1287 microcontroller. These crypto chips provide hardware solutions for SHA, AES, and ECDH functions, respectively. Because this device is an evaluation module from the manufacturer of these chips, custom drivers are necessary to integrate it with the main board of the module.

D. Initial Design of the Module

The initial design of the developed prototype module is shown in Fig. 1.

![Design of the module](image)

E. Interfaces of the Module

The module has the following physical and networking interfaces:

- **Ethernet**: The RJ45 port is used for TCP or User Datagram Protocol communications. One port is used for upstream and downstream communications. This allows the user to connect to the system using a secure shell (SSH). The other Ethernet interface, either direct or using an adapter, is connected to the DER and is used to communicate using Modbus over TCP. This interface also hosts a hardened SSH server. The regular communications are secured using a secure socket layer (SSL) with signed certificates. This interface is protected by a firewall with white-list capability. Unused ports on this interface are closed, and traffic is monitored and configured to minimize denial-of-service attacks.

- **USB**: This is used to connect peripherals and adapters and is secured by controlling physical access and disabling unused ports.

- **SSH**: This is used to harden the software interface for remote monitoring and controlling the module. It uses logs and certificates to implement access controls and user tracking. It is
also configured to require users to enter either a valid certificate or a passkey in case the certificate management is not possible.

**RS-485:** This is used to provide a twisted-pair wire interface for Modbus systems. It is also used to control physical access to the port.

**Micro-SD:** This is used to provide local flash storage to house the operating system and firmware.

**Wi-Fi and Bluetooth:** These two wireless interfaces are available by default in the hardware platform (Raspberry Pi), but they are disabled for security purposes.

### F. Key Features and Assumptions

Table II lists the key features and available options to implement those key features in the hardware security module. To limit the scope of what the cryptographic module can do, the following assumptions were made while designing the cryptographic module for DER systems.

- The module provides security against attacks that originate on the inverter side and attempt to migrate upstream of the utility’s command and control centers and other DERs. This is to ensure that if one device is compromised, the adversary is not capable of impacting other devices on the network.
- The module performs authentication and data integrity checks of the data traffic between DERs and the command and control center.
- The module requires a master key for any reconfiguration of the settings or setting them to default. This provides an extra layer of security if someone obtains the module and tries to change the configuration. When deployed in the field, the master key will be provided only to specific personnel, and it will require two-factor authentication.
- The module has a built-in white list that allows access to the module only to those devices or Internet Protocol (IP) addresses or personnel that are already identified as legitimate.
- The module has a Web interface through which utilities can manage the module. The utilities can directly access the module using this interface through a secure link. The IP address of the connection is added to the module’s white list before field testing, so that the module can process that it is an authentic connection.
- The module also has data logging capability (such as Syslog). Any changes in configuration, default setting changes, and log-in/log-out information will be sent to a Syslog server of the utility or equivalent.
- The module uses AES_128_CCM_8 as the encryption standard.

### IV. Laboratory Testing of the Cryptographic Module

Fig. 2 shows the lab testing setup at NREL. This setup includes using two different virtual machines acting as a grid controller and a third-party controller. The third-party controller might be owned by a vendor or stakeholder who needs to be able to monitor and/or control the devices. To do this, the third party will need to be provided with the secure keys by the operator. Both controllers will use a module to encrypt and decrypt all communications going across the WAN to each other and the DER site. Another module connected to the DER facility’s LAN passes messages to the relevant DER controllers. The test scenario will implement a communication path using each supported communications protocol to the DER.

To test the performance of this system as part of this planned initial lab testing, a LAN network will be used in place of the WAN emulator within the test bed. For more accurate results, a WAN emulator is recommended to model the delays and drops associated with WAN connections. From a performance perspective, the LAN test scenario will represent an ideal test case. The attack cases planned to be tested are denial-of-service and man-in-the-middle, which are two of the more common types of cyberattacks on remote systems, and the resilience of the module to these types of disruptions will be evaluated.
V. FIELD-TESTING THE CRYPTOGRAPHIC MODULE

A. Use Case 1: Field-Testing at PV Site in Albuquerque

The Prosperity site, which is owned and operated by Public Service Company of New Mexico, features combined battery storage and PV energy, commonly referred to as solar energy. The goal of the Prosperity project is to learn and address how to safely integrate a variable power source (e.g., solar energy) with a grid designed to handle steady, one-way power flows and make solar power available when the customer most wants it. The goal is also to develop a way to manage solar energy and other renewable resources so they can be accessed and used when they are most needed. The project is part of a nationwide effort to help the economy, develop reliable renewable energy, and research battery energy storage technology. The PV array contains 2,158 panels producing up to 500 kW on a 4.9-acre site in south Albuquerque, New Mexico. The site uses advanced lead-acid batteries with an energy rating of 1 MWh.

In this use case, the project team will first test the module by placing it adjacent to the plant controller via Ethernet cable, where it will encrypt the Distributed Network Protocol (DNP3) traffic going to the WAN, as shown in Fig. 3. This will enable a check of the feasibility of placing the module next to the plant controller. Once the testing next to the controller is done, the project team will test the module again by placing it adjacent to the inverter. This will enable study of any effects of placing the module next to the inverter.

B. Use Case 2: Field-Testing at PV Site in Toledo, Ohio

The system configuration shown in Fig. 4 is the direction that large solar projects are rapidly taking: incorporating dc-coupled storage with the PV system to enable dispatching renewable energy resources. Rated at 500 kWac, the system comprises high-power Series 6 PV modules from First Solar and XGI 1500 inverters rated at 166 kWac from Yaskawa Solectria Solar. The system is a scalable building block that can be replicated to create multimegawatt PV-plus-storage systems. The PV array will potentially be rated at approximately 1 MWdc, leading to a dc/ac ratio of approximately 2, which might be necessary in certain dc-coupled storage systems. dc-coupled storage introduces additional components into the system, including the storage element itself, a dc/dc controller that regulates the charging and discharging to the storage element, and a plant controller. The plant controller communicates with the dc/dc converter and the inverters to control the power flow. The plant controller is also the communications hub. This configuration is proposed for the test site in Toledo, Ohio, with the aim to achieve operational status, pending the agreement with all parties involved, in the first quarter of 2020.

In this use case, the project team will first test the module by placing it adjacent to the plant controller via Ethernet cable, where it will encrypt the DNP3 traffic going to the WAN, as shown in Fig. 4. This will enable a check of the feasibility of placing the module next to the plant controller. Once the testing next to the controller is done, the project team will test the module again by placing it adjacent to the first inverter via Ethernet. This will enable study of any effects of placing the module next to the inverter.
VI. CONCLUSIONS AND FUTURE WORK

This paper presents the design considerations to develop a cryptographic module for DERs. It also presents the schematics explaining how the module can be tested in both the laboratory environment and as well as in the grid-connected DER sites. It describes the requirements for selecting the hardware platform, key features, and interfaces of the module and presents the initial design of the module. As a next step, we will develop and test the module.

ACKNOWLEDGMENTS

This work was authored in part 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

This work was also authored by Sandia National Laboratories, operated by National Technology and Engineering Solutions of Sandia, LLC, for the DOE under Contract No. DE-V00028308

Funding was provided by the DOE Cybersecurity, Energy Security and Emergency Response (CESER) Cybersecurity for Energy Delivery Systems (CEDS) R&D program. 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.

REFERENCES


