Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem[1] and Cedric Carter[2]

[1] *National Renewable Energy Laboratory*
[2] *The MITRE Corporation*

National Electrical Manufacturers Association

Technical Report
NREL/TP-5R00-73628
July 2019

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

Contract No. DE-AC36-08GO28308

Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem[1] and Cedric Carter[2]

[1] *National Renewable Energy Laboratory*
[2] *The MITRE Corporation*

Suggested Citation
Saleem, Danish and Cedric Carter. 2019. *Certification Procedures for Data and Communications Security of Distributed Energy Resources*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-73628. https://www.nrel.gov/docs/fy19osti/73628.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

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-73628
July 2019

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

NOTICE

This work was authored in part 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. Funding provided by the National Electrical Manufacturers Association and the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office.

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

Preface

This document is intended for distributed energy resource (DER) vendors, utilities, certification laboratories, and government organizations. The document provides cases that can be used to test the cybersecurity posture of the data and communications of DERs. Currently, vendors and utilities are communicating with DERs that use poor cybersecurity practices. Additionally, there is a significant gap and lack of consistency in the adoption of basic cybersecurity requirements for DER information systems. As the electric power system infrastructure has evolved, the industry has increasingly relied on the availability of modern DER information systems to operate power system controls. This document provides a draft certification procedure for DER cybersecurity, and it is intended to be used as input to national and international certification test standards for DER equipment.

Acknowledgments

This work was initially funded by the National Electrical Manufacturers Association (NEMA) and subsequently by the U.S. Department of Energy Solar Energy Technologies Office.

We thank all the contributors from the SunSpec Alliance Distributed Energy Resource Cybersecurity Working Group and from NEMA who provided their valuable comments and feedback to this document, including, but not limited to, Jörg Brakensiek (Wivity), Jay Johnson (Sandia National Laboratories [Sandia]), Tom Tansy (SunSpec), Aditya Sundararajan (Florida International University), Andrew Michalski (National Renewable Energy Laboratory [NREL]), Alfred Tom (Wivity), Taylor McKenzie (Sandia), Frances Cleveland (Xanthus Consulting International), Gordon Lum (Kitu Systems), Steve Griffith (NEMA), Patrick Hughes (NEMA), Candace Suh-Lee (Electric Power Research Institute), Vladimir Bronstein (Enphase Energy), Thomas (Blue Oak Energy), Frank Tarzanin (ABB), Qiang Fu (Eaton Corporation), John Berdner (Enphase Energy), Nate Diamond (Doosan), Ralph Mackiewicz (SISCO), Anuj Sanghvi (NREL), Maurice Martin (NREL), Jonathan White (NREL), Bob Fox (SunSpec), and all others.

List of Acronyms

CRL	Certificate Revocation List
CSIP	Common Smart Inverter Profile
DER	distributed energy resource
DHE	Ephemeral Diffie-Hellman
DNP	Distributed Network Protocol
DTLS	Datagram Transport Layer Security
DUT	device under test
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
HTTPS	Secure Hypertext Transfer Protocol
ICCP	Inter-Control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	industrial control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LDAP	Lightweight Directory Access Profile
MAC	message authentication code
MITM	man-in-the-middle
NEMA	National Electrical Manufacturers Association
NIC	network interface controller
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSI	open systems interconnect
RSA	Rivest–Shamir–Adleman
Sandia	Sandia National Laboratories
SCADA	supervisory control and data acquisition
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

Executive Summary

This document contains 11 test cases that can be used to verify authentication, authorization, confidentiality, and data integrity for data and communications for distributed energy resources (DERs) that use Transmission Control Protocol/Internet Protocol (TCP/IP) for communications with the electric grid. These security requirements can also help vendors improve the overall cybersecurity posture of their products (i.e., DERs).

In this report, we compare high-level business use cases that are essential for DER security to the specifications mentioned in the International Electrotechnical Commission (IEC) 62351 standards, and we convert them into 11 test cases. Next, we distill a detailed test plan for test case with action and review items so that they are easy to test and validate on DERs in a lab environment. Once validated, the 11 test cases can serve as certification procedures for vendors, utilities, and certification labs. These test cases are applicable to all communications flowing from DERs to the grid over TCP/IP. These 11 test cases protect DER communications from cyberattacks, such as:

- Eavesdropping
- Replay
- Man-in-the-middle
- Denial of service
- Spoofing through security certificates
- Least-privilege violation
- Brute-force credentials.

This document provides a set of security procedures, categorized into 11 test cases, for DERs that can be used by vendors, utilities, certification labs, government organizations, and industry partners. These test cases can also be used to add adequate security to some of the most commonly used communications standards for information exchange of electric power systems, including IEC 60870-5, Distributed Network Protocol, Inter-Control Center Communications Protocol, Institute of Electrical and Electronics Engineers 2030.5, and IEC 61850. In addition to providing a set of security procedures, this document serves as a starting point for ongoing efforts to secure DERs and their communications infrastructure. This document also provides a starting point for multiple national or international standards development organization committees. These committees might continue refining it until it becomes a standard document for DER security that vendors, utilities, aggregators, government institutions, and other industry partners can follow and adopt.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The infrastructure of distributed energy resources (DERs) was originally designed with the primary intention of harnessing the potential of renewable energy resources. Hence, security at the device, network, or application levels of DERs was of little to no concern. The lack of in-place security controls for critical infrastructures led to many cyber-physical attacks during the past 5 years.

In December 2015, hackers successfully compromised the information systems of three energy distribution companies in Ukraine by using spear-phishing emails with BlackEnergy malware. The hackers temporarily disrupted the electricity supply to end consumers by gaining control of the supervisory control and data acquisition system (SCADA) and remotely switching off 30 substations. As a result, about 230,000 people were left without power for almost 6 hours (SANS Industrial Control Systems 2017). In April 2000, the Maroochy Shire sewage treatment plant SCADA system was compromised and forced by the attackers to dump 264,000 gallons of raw sewage into the environment (Oman, Schweitzer, and Frincke 2000; U.S. Department of Energy, Office of Energy Assurance 2002). Other examples of recent cyber-physical attacks are listed in Table 1. Figure 1 shows that data theft is also a problem for other sectors—more than 9 billion data records were lost or stolen between 2013 and mid-2018, averaging nearly 5 million records per day (Breach Level Index 2019).

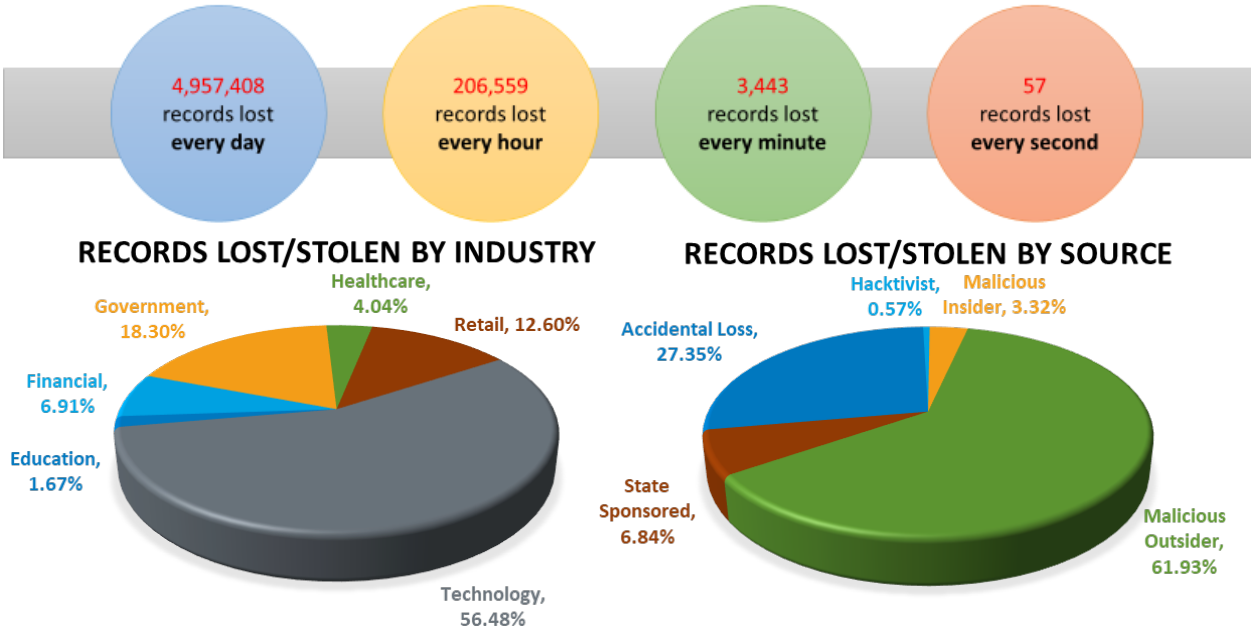

Figure 1. Past data breaches

Table 1. Summary of Recent Cyber-Physical Attacks[a]

Year	Source of Attack	Target	Attack Specifics
2014	Spear phishing, Havex malware for watering hole attack (SANS Industrial Control Systems 2016)	Industrial control system (ICS)/SCADA	Espionage using OPC protocol to map devices on ICS network
2015	Trojan.Laziok reconnaissance malware (Amerding 2018)	Energy companies	Attackers gathered information from compromised devices
2015	BlackEnergy 3 malware (Lee, Assante, and Conway 2016)	Ukraine's grid control centers	Power outage to 220,000+ customers
2016	Industroyer or Crash Override malware (SANS Industrial Control Systems 2017)	Pivnichna substation ICS, Ukraine	Power outage to one-fifth of Kiev
2017	WannaCry ransomware cryptoworm (Langde 2017)	Computers running Microsoft Windows operating system	Exploited EternalBlue, a vulnerability in older Windows systems
2015, 2017	Dragonfly 2.0 (U.S. Computer Energy Readiness Team 2018)	Western energy sector	Spear-phishing, Trojan-ware, watering hole attacks
2018	VPNFilter malware (Higgins 2018) (prevented successfully)	Ukraine's chlorine plant	Data exfiltration, espionage
2019	Denial of service	U.S. western electric utility	Temporary loss of visibility in some parts of SCADA system

[a] Source: (Sobczak 2019)

These recent cyber-physical attacks speak to the urgency of securing all aspects of critical infrastructure. Despite improvements in communications security capabilities, however, strong security controls and preventive measures have yet to find their way to DERs (SANS Industrial Control Systems 2017; Langde 2017). Existing security controls and preventive measures might also be ineffective against well-funded attacks sponsored by nation states, including advanced persistent threats and social engineering (U.S. Computer Energy Readiness Team 2018; Higgins 2018; Federal Trade Commission 2017; Semantec Blogs 2017).

Several industry standards and guidelines have been developed and established. For example, the North American Electric Reliability Corporation developed cybersecurity requirements for critical infrastructure protection, but these requirements apply to security issues of the bulk power system and are not applicable to cybersecurity issues of DERs. Similarly, the National Institute of Standards and Technology (NIST) has developed a cybersecurity framework that tells organizations how to develop processes to manage cyber risk to a system. The cybersecurity framework, however, does not address the cybersecurity risks of DERs and their communications with the grid. NIST also developed many other standards, including:

- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- NISTIR 7628: Guidelines for Smart Grid Cybersecurity
- NIST SP 800-82: Guide to Industrial Control Systems Security.

In addition to the North American Electric Reliability Corporation and NIST, other organizations have developed security standards and guidelines for power systems, including, but not limited to:

- The International Electrotechnical Commission (IEC) 62351 standards provide security for information exchange in power systems.
- The U.S. Department of Energy developed the Cybersecurity Capability Maturity Model to provide cybersecurity benchmarks and guidance for utilities on effective risk-management processes with consideration of specific organizational requirements and constraints.
- The Institute of Electrical and Electronics Engineers (IEEE) C37.240 standards provide cybersecurity requirements for substation automation, protection, and control systems.

Existing cybersecurity frameworks address cybersecurity issues related to the distribution grid as whole, but there are not sufficient guidelines and procedures that can help vendors, utilities, aggregators, government institutions, and other industry partners adopt and implement the procedures to secure the data and communications of DERs that are connected to the distribution grid. Therefore, to create an effective and efficient way of securing next-generation DERs that will be connected to the distribution grid, there should be a standard that industry can follow.

1.2 Scope

This document serves as a starting point for ongoing efforts to secure DERs and their communications infrastructure. Standards committees of organizations such as IEEE and UL may refine this work into standard documents for DER security that vendors, utilities, aggregators, government institutions, and other industry partners can adopt. In this document, 11 test cases provide procedures that vendors and manufacturers can use to check that the respective security features are up to the mark; if not, they can add basic missing security features as embedded functions in their DERs.

Note that most smart grid devices, including DERs, use application-layer protocols that work on the Transmission Control Protocol (TCP)/Internet Protocol (IP) stack that extends from the established open systems interconnect (OSI) basic reference model. The network interface, Internet, and transport layers of the TCP/IP stack correspond to the physical and data link, network, and transport layers of the OSI model. The session, presentation, and application layers of the OSI model come cumulatively under the application layer of the TCP/IP stack. (Sans Institute 2004) In addition to this logical mapping between the two models, it is noteworthy that the vulnerabilities within the scope of this document (V1–V7) described in Section 3 target one or more layers from 1–6 of the OSI model. This document illustrates a mapping between the protocols of layers 1–6 and the vulnerabilities that are related to DERs and to which they are vulnerable. A mapping between test cases and the vulnerabilities is also included. The 11 test cases in the document cover only up to Layer 6 of the OSI model.

The application-layer protocols considered within the scope of this document are IEC 60870-5, IEC 60870-6 (ICCP), IEEE 1815 (DNP3), IEC 61850, and IEEE 2030.5 (SEP2)/Common Smart Inverter Profile (CSIP). As mentioned in the previous paragraph, these protocols run on top of the TCP/IP stack. Because the vulnerabilities discussed in Section 3 are mapped to OSI layers 1–6 (see Table 3) and the test cases outlined in Section 4 are mapped to the communications protocols (see Table 4), any DER device employing any of these application-layer protocols will, by default, be secured against the vulnerabilities V1–V7 because these vulnerabilities exist in only some of or all the OSI layers 1–6.

Out of scope of this document are the following:

- Actual testing and validation of the test cases (mentioned in Section 4) in the lab environment
- Application-to-application security (OSI Layer 7)
- Criteria and selection of certificate authority
- The process of how to revoke a certificate using a Certificate Revocation List (CRL) and/or how to check the revocation state of the certificate using the Online Certificate Status Protocol (OCSP).

1.3 Objectives

1. **To accelerate the adoption of basic and advanced security controls for DERs**. DERs are now capable of performing granular monitoring and have the option to enable advanced control functions with broad access. This increases device-level vulnerabilities. Therefore, by accelerating the adoption of basic and advanced security controls for the security of the data and communications of DERs, the probability of a cyberattack can be significantly reduced.
2. **To standardize certification procedures for DER security.** For a multi-vendor environment, minimal variation in DER security and interoperability controls improve the industry's security posture. Standardizing the certification procedure will help vendors, utilities, aggregators, and end users move toward a common set of effective security practices.

2 Improving Security

Improving security for DERs requires a change in how the electricity industry currently develops and integrates DERs. Some basic and advanced security controls could be adopted as best practices. Security controls could also help better protect vendor devices from future cyberattacks. The attacks listed in Table 1 could have been prevented with the implementation of a few basic controls, such as periodically updating software security patches and firmware; proper network segmentation to create a logical air gap between information technology, operational technology, and management networks; and selective encryption (Dragos 2018). Figure 2 provides a high-level overview of the basic (Johnson 2017) and advanced (Cleveland 2012) security controls that can be used to effectively secure the DER infrastructure.

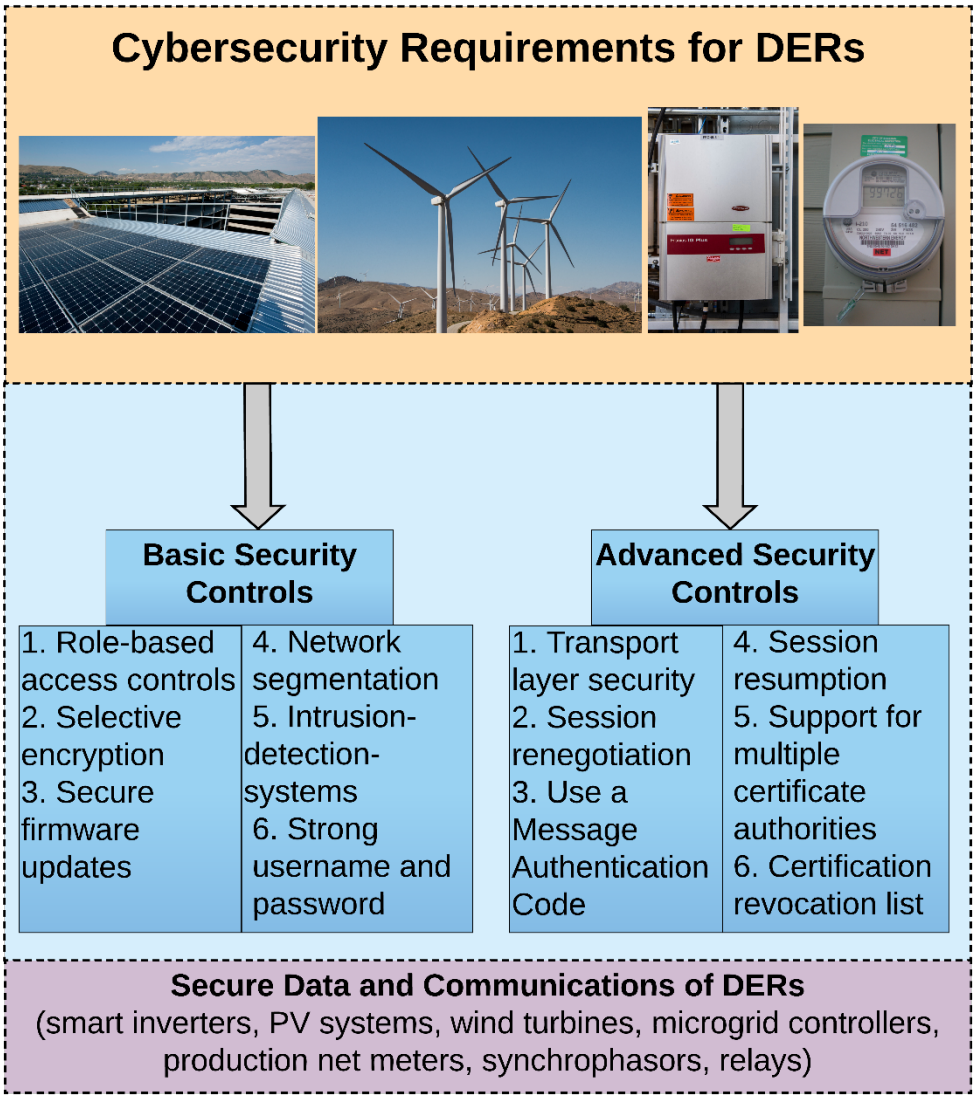

Figure 2. Strengthening the security posture of distributed energy resources.
Photos by (left to right): NREL 21299; Dennis Schroeder, NREL 50709; Dennis Schroeder, NREL 45576; Susan Bilo, NREL 21394

2.1 Basic Security Controls

Basic security controls are best practices for DER networks (National Electrical Manufacturers Association 2015; National Electrical Manufacturers Association 2018), but they are not specific to DER equipment, and they will not be tested using this certification protocol. These should be considered necessary but not sufficient for DER cybersecurity. Some basic security controls include, but are not limited to:

- Using role-based access controls on network equipment, firewalls, and DER devices
- Using network segmentation with different virtual local area networks to create logical segmentation between operational technology, information technology, and management networks
- Periodically updating software security patches and firmware
- Creating strong passwords and not using default factory passwords
- Selectively encrypting to minimize processing overhead and communications latency
- Systemically securing the network using context-based and signature-based intrusion-detection systems and by using in-line blocking tools
- Disabling all unused ports and processes to eliminate unauthorized access.

2.2 Advanced Security Controls

Stringent security controls are required by a given communications or interconnection standard for DER equipment. Recommended stringent security controls include:

- **R1**: Support the use of the NIST *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (SP 800-52) Revision 2, Version 1.2 or Version 1.3, if applicable (NIST, Computer Security Resource Center 2018a). (See Table 2.)
- **R2**: Support the use of the following TLS implementations. Table 2 shows the recommended certificate implementations and cipher suites (NIST, Computer Security Resource Center 2018a).
- **R3**: Session resumption should occur if the session is severed for the time shorter than the TLS session resumption time using the secret session key.
- **R4**: Session negotiation should occur if the session is severed for the time longer than the TLS session renegotiation time.
- **R5**: Support the use of a message authentication code (MAC).
- **R6**: Support the use of authorized multiple certificate authorities for the device under test (DUT) and server.
- **R7**: Determine a capability for terminating a session if a revoked certificate is used to establish the connection. This is accomplished by using a CRL or OCSP.
- **R8**: Determine a capability for identifying and terminating a session if an expired certificate is used to establish the connection.
- **R9**: Disable all unused physical ports, e.g., Universal Serial Bus ports, ethernet ports.

Table 2. Recommended Cipher Suites[a]

Cryptographic Algorithms	Cipher Suites	TLS Version
Elliptic Curve Digital Signature Algorithm (ECDSA)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C) TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xC0, 0xAC) TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xC0, 0xAD) TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xC0, 0xAE) TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xC0, 0xAF) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x23) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x24)	TLS 1.2
Rivest–Shamir–Adleman (RSA)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x00, 0x9E) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x00, 0x9F) TLS_DHE_RSA_WITH_AES_128_CCM (0xC0, 0x9E) TLS_DHE_RSA_WITH_AES_256_CCM (0xC0, 0x9F) TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xC0, 0xA2) TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xC0, 0xA3) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x27) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x00, 0x67) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x00, 0x6B)	TLS 1.2
Ephemeral Diffie-Hellman (DHE)	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00, 0xA2) TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00, 0xA3) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x00, 0x40) TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x00, 0x6A)	TLS 1.2
Diffie-Hellman (DH)	TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00, 0xA4) TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00, 0xA5) TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x00, 0x3E) TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x00, 0x68)	TLS 1.2
Elliptic Curve Diffie-Hellman (ECDH)	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2D) TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2E) TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x25) TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x26)	TLS 1.2
Advanced Encryption Exchange	TLS_AES_128_GCM_SHA256 (013x, 0x01) TLS_AES_256_GCM_SHA384 (0x13, 0x02) TLS_AES_128_CCM_SHA256 (0x13, 0x04) TLS_AES_128_CCM_8_SHA256 (0x13, 0x05)	TLS 1.3

[a] Source: (NIST 2018a)

3 Vulnerabilities Addressed

By implementing the recommendations discussed here and validating them to the test cases that are discussed in Section 4, some of the vulnerabilities related to DERs can be addressed and mitigated. The following vulnerabilities, however, are not the only ones; many others exist (The MITRE Corporation 2018a; 2018b). These are a few among many that the authors believe to be most common based on familiarity with equipment and discussions with industry. Each vulnerability references one or more test cases; Section 4 explains these test cases and provides procedures for each.

3.1 Man-in-the-Middle (V1)

A man-in-the-middle (MITM) attack occurs when a third party secretly replays and possibly alters the communications between two parties. This attack can drop, modify, or add data transmissions while in transit to a destination (Cedric et al. 2017).

The following test cases can be used to check whether the device is vulnerable to a MITM attack:

- Test case 2: TLS activation
- Test case 3: Session resumption/renegotiation.

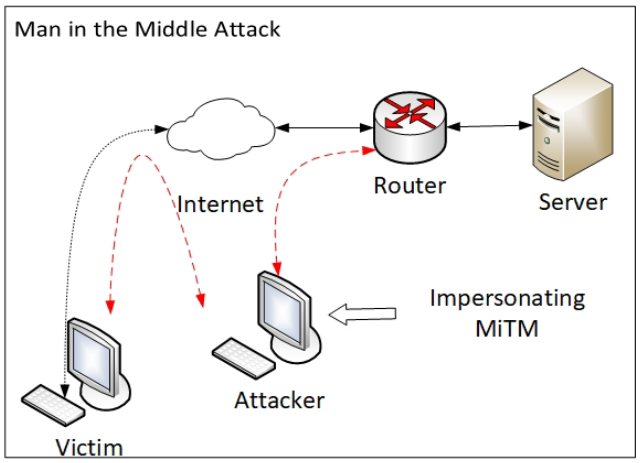

Figure 3. Illustration of man-in-the-middle attack

3.2 Replay (V2)

Packet replay (also known as a playback attack) is an attack wherein a third party maliciously captures and repeats, or delays, valid data transmissions. This threat is countered using specialized processing state machines specified by the normative references of this document (Cedric et al. 2017).

The following test cases can be used to check whether the device is vulnerable to a replay attack:

- Test case 2: TLS activation
- Test case 5: MAC activation.

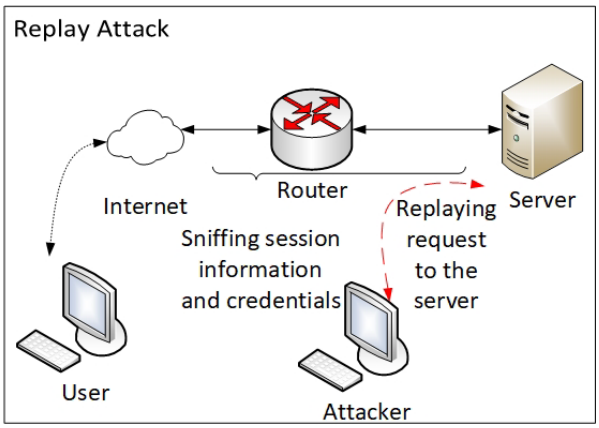

Figure 4. Illustration of replay attack

3.3 Eavesdropping (V3)

This is a reconnaissance attempt from a third party to view valid data transmissions from legitimate sources to gain information about the system of interest (Cedric et al. 2017)

The following test cases can be used to check whether the device is vulnerable to an eavesdropping attack:

- Test case 2: TLS activation
- Test Case 3: Session resumption/renegotiation.

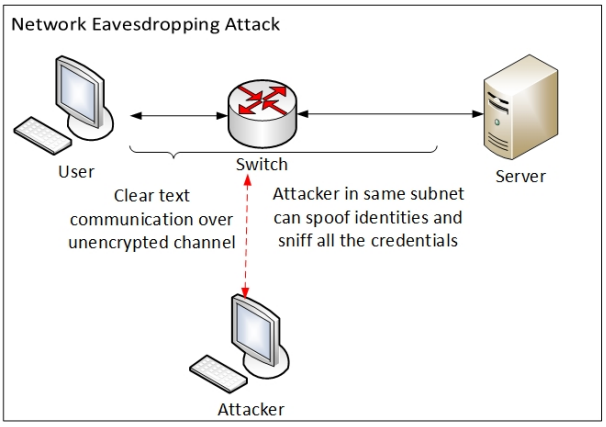

Figure 5. Illustration of eavesdropping

3.4 Spoofing through Security Certificates (V4)

Security certificates are used to authenticate the DER device and the DER server. A CRL can be issued in the event of a compromised certificate to ensure that connections occur only between an authenticated DER device and DER server (Peifer n.d.).

The following test cases can be used to check whether the device is vulnerable to attacks based on spoofing security certificates:

- Test Case 2: CRL activation
- Test Case 3: Session resumption/renegotiation.

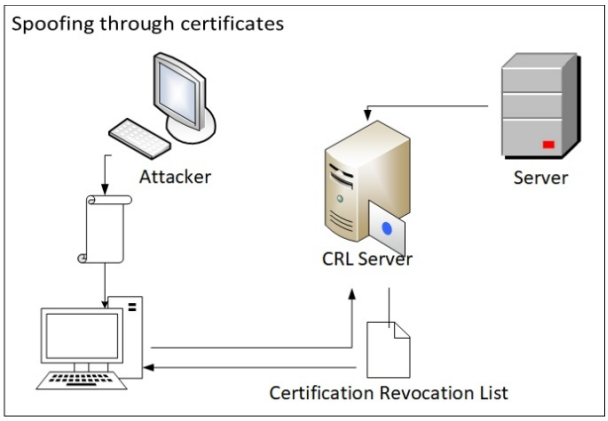

Figure 6. Illustration of spoofing through certificates

3.5 Denial of Service (V5)

Denial of service is an availability interruption to an authorized user's access. The purpose of the attack is to render a machine or network service unavailable to its intended users. The attack can temporarily or indefinitely disrupt services to authorized users on a computing network (Cedric et al. 2017). Examples include, but are not limited to:

- Attempts to "flood" a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, i.e., DER device and DER server
- Attempts to prevent an authorized DER device from accessing a service
- Attempts to disrupt service to a specific system or authorized user.

Note: The attack can be caused by intentional or unintentional means.

The following test case can be used to check whether the device is vulnerable to attacks based on denial of service:

- Test Case 9: Hardening operating system and service version.

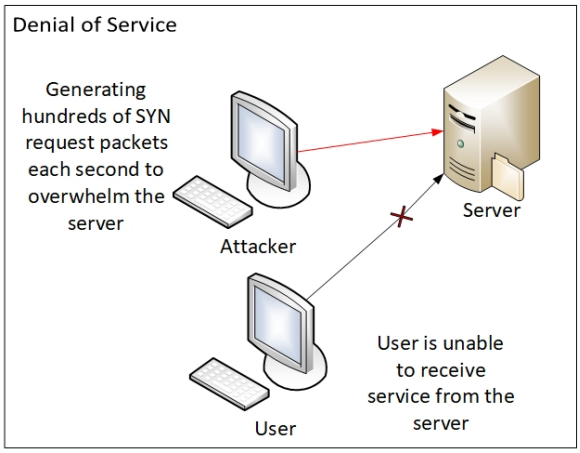

Figure 7. Illustration of denial of service

3.6 Least-Privilege Violation (V6)

The principle of least privilege states that in a computing environment, the user must be able to access only the information and resources that are necessary for the user's legitimate purpose. Services that are unintentionally installed or unpatched in the computing environment can be hijacked or accessed by third parties. This threat can be mitigated by limiting the number of services needed to perform the computing environment's functions (Cedric et al. 2017).

The following test cases can be used to check whether the device is vulnerable to attacks based on least-privilege violation:

- Test Case 9: Hardening operating system and service version.

3.7 Brute-Force Credentials (V7)

Enforcing weak passwords on a computing environment can expose the system to password vulnerabilities and guessing. In a brute-force attack, automated software is used to generate many consecutive guesses about the value of the desired data. This attack can be easily achieved if the system of interest enforces weak credentials and does not restrict access because of failed consecutive authentication attempts (NIST 2015).

The following test cases can be used to check whether the device is vulnerable to attacks based on brute-force credentials:

- Test Case 10: Use of authentication and password management.

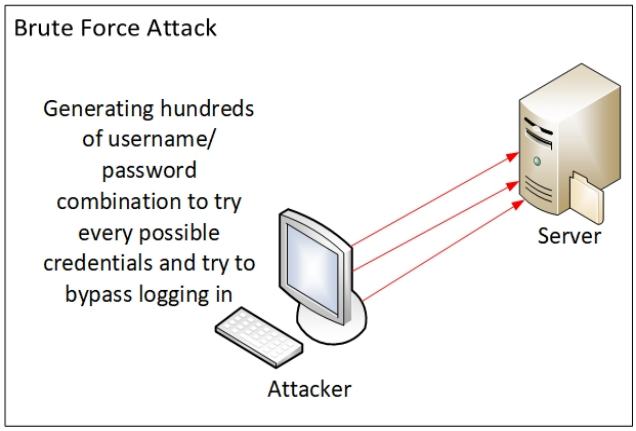

Figure 8. Illustration of a brute-force attack

As mentioned in Section 1.2, Table 3 depicts the mapping between layers 1–6 of the OSI model and the common vulnerabilities associated with DERs.

Table 3. Mapping of Vulnerabilities to OSI Model

	RS232 (Physical Layer)	Ethernet (Data Link Layer)	IPv4/IPv6 (Network Layer)	TCP, UDP (Transport Layer)	Session Layer	Presentation Layer
V1			x	x	x	x
V2			x	x	x	x
V3	x	x	x	x	x	x
V4					x	x
V5			x	x	x	x
V6	x	x	x	x	x	x
V7					x	x

4 Test Cases

The test architecture used to execute the test cases involves the following components:

- Device under test: The DUT is the DER device, which undergoes testing.
- Lower tester: The lower tester is a test system that emulates a DER server and can receive and send messages to and from the DUT. The lower tester might include an active DER management system.
- Upper tester: The upper tester is an optional test component (required for some test cases) that allows triggering the DUT to execute certain operations and that receives a result about the success of the requested operation.

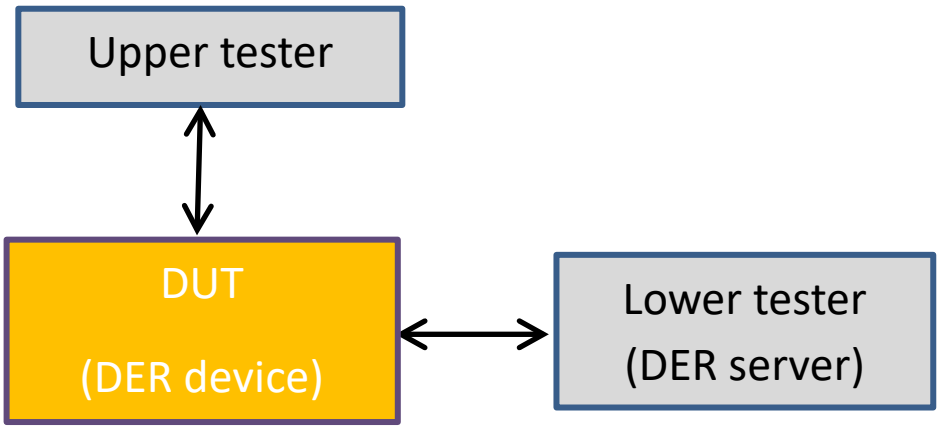

Figure 9. Simplified test architecture

The interface between the upper tester and the DUT is proprietary and outside the scope of the test cases. Vendors are required to provide upper tester functionality, which allows the test engineer to execute all test cases. The upper tester might be part of the DUT device (e.g., a management interface).

The DUT and the lower tester are connected to a single switch or wireless network, configured with an addressable IP address, and connected on an isolated IP network. The switch should have a mirror port to which a laptop can be plugged into to capture traffic between the DUT and the lower tester. Prior to all tests, connectivity between the DUT and lower tester should be tested. The lower tester should host its own OCSP responder on its loop-back interface and capture loop-back traffic to observe requests that will be sent to the OCSP. Between each test, the DUT and the lower tester should be rebooted to ensure that there are no active connections.

The 11 test cases in this section test the security posture of the DERs. Any experiment will require verifying the functionality prior to running the cybersecurity tests. In addition to verifying the functionality, the following assumptions must be considered before starting the test:

1. The DER vendor is responsible for enabling all default cybersecurity features of the DER prior to experimentation.
2. The DUT is certified to the respective interoperability standard(s) listed in Table 4.
3. The DUT can be one device or system of devices.

4. All the respective security features are enabled.
5. The testing network should be IP-based and shall support either IPv4 or IPv6.
6. Use TLS (1.2 or greater) for TCP and Datagram Transport Layer Security (DTLS) for User Datagram Protocol (UDP).
7. The security strength for TLS should be greater than or equal to 128 bits.
8. The Network Time Protocol (NTP) time server is set up.
9. The DUT has been pre-provisioned with the certificates for setting up the TLS session.
10. In case of multiple certificate authorities, the actual number of certificate authorities will be decided by the implementor.
11. The exchange and validation of the certificates is bidirectional so that authentication from both ends can be achieved.
12. The owner of the DER will have the ability and authority to revoke the certificate regardless of who is managing the certificate authorities.
13. OCSP can be used to check the revocation state of certificates if the user does not want to use the CRL.
14. There is already an established management process through which the security certificate renewal takes place. The renewal frequency of certificates will be decided by the implementor. Ideally, the frequency should be 1 month.
15. Default factory passwords, if available, shall be disabled.

Table 4 indicates which experiments must be conducted for each communications protocol to meet the basic security requirements of the five communications protocols/interoperability standards.

Table 4. Required Test for Each Communications Protocol/Interoperability Standard

Tests	IEC 60870-5	IEC 60870-6 (ICCP)	IEEE 1815 (DNP3)	IEC 61850	IEEE 2030.5 (SEP2)/CSIP
T1	x	x		x	
T2		x		x	
T3		x		x	
T4			x		x
T5		x			
T6		x			
T7		x			x
T8		x			x
T9	x	x			x
T10	x	x		x	x
T11	x	x		x	

4.1 Two-Party Application Association (T1)

Background: Two-party application association maintains the session states and provides an active connection and virtual view of the DER to the client resource. When needed, the DUT can close the association with the DER server and verify that no interactions can take place.

Purpose: The purpose of this test case is to verify whether there is an active connection using TCP/IP between the DER and the source. This test case does not check or validate any security requirements in the DER; thus, there is no attack method that can be countered with implementation of this test case.

Vulnerabilities addressed: N/A

Requirements: A DER (such as photovoltaic inverter) and software/hardware through which the communications to the DER can be controlled and monitored.

Table 5. Test Procedure to Verify Two-Party Application Association

No.	Action
1	Test engineer connects the DUT and the lower tester on an isolated network.
2	Test engineer assigns a static IP address (optional) to the DUT and the lower tester.
3	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
4	Test engineer verifies the connection between the DUT and the lower tester via Internet Control Message Protocol (ICMP) or ping.
5	Upper tester requests the DUT to initiate a two-party application association using TCP/IP with the lower tester.
6	Test engineer keeps the session active for 10 minutes.
7	Upper tester requests the DUT to close the session and documents the time.
8	Test engineer leaves the session closed for at least 10 minutes and then stops the packet capture.
9	Test engineer reviews the packet capture log file to verify success.
No.	**Review**
1	DUT initiates the TCP/IP connection to the lower tester.
2	Lower tester accepts the TCP/IP connection.
3	The properties of the established TLS session (e.g., TLS version, cipher suite) meet the requirements of the respective application layer protocols shown in Table 4.
4	No communications between the DUT and lower tester took place after session termination.

4.2 Transport Layer Security (T2)

Background: TLS uses encryption to ensure that the communications between two devices or applications are secure. TLS is the successor version of the secure socket layer and is considered a more secure and efficient protocol because it uses key generation and message authentication with supported encryption algorithms and cryptographic keys.

Purpose: This test case ensures that the established connection between the DUT and the DER server has TLS enabled.

Vulnerabilities addressed: MITM (V1), eavesdropping (V3)

Requirements: TLS for the network should be activated at both the DUT and the DER server end using the mandatory T-profile cipher suite (Rahm 2017). The public key infrastructure (Gautam and Upadhyay 2014) technology is used to establish secret keys and initiate the creation and use of session keys. For recommended cipher suites, refer to Table 2.

Table 6. Test Procedure to Verify Transport Layer Security

No.	Action
1	Test engineer connects the DUT and the lower tester.
2	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
3	Lower tester initiates TLS with the DUT with TLS, and two-party application association is activated.
4	Test engineer verifies the TLS version within the packet using Wireshark (see Table 2).
No.	**Review**
1	TLS is established with mutual (two-party) authentication.
2	The properties of the established TLS session (e.g., TLS version, cipher suite) meet the requirements of the respective application layer protocols shown in Table 2.

4.3 Session Resumption/Renegotiation (T3)

Background: Session resumption is a way to avoid a full handshake, thereby reducing the latency and processor usage in the TLS-enabled connections. This is done by storing the secret information of previous sessions and then reusing that information to connect to the host (or DER) the next time. On the other hand, session renegotiation requires a full handshake, with a new negotiated master key and session key required at the time of the connection.

Purpose: This test case ensures that the lower tester renegotiates a TLS session with the DUT when the TLS session has been active for longer than defined in one of the following conditions:

- Predefined maximum resumption time, as defined by the respective application layer protocols in Table 4
- CRL refresh time (if CRL use is defined)
- OCSP cache time (if OCSP use is defined).

It also ensures that the lower tester is performing session resumption with the DUT.

Vulnerabilities addressed: MITM (V1), eavesdropping (V3)

Requirements: For active connections, the lower tester should initiate the session renegotiation after the defined interval—e.g., every 24 or 48 hours. This is to ensure that the certificate that was used to establish the connection is still valid. In addition, the lower tester shall perform session resumption with the DUT if the connection is disturbed before the maximum TLS session resumption time and perform session renegotiation if the connection is disrupted after the maximum TLS session resumption time.

Table 7. Test Procedure to Verify Session Resumption/Renegotiation

No.	Action
1	Test engineer connects the DUT and the lower tester.
2	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
3	Upper tester requests the DUT to establish a TLS session with the lower tester.
4	Lower tester maintains an active TLS session with data exchange.
5	Test engineer disables the DUT network interface controller (NIC) after 15 or more minutes and records the time.
6	Test engineer re-enables the DUT NIC, before the TLS session expires, and records the time.
7	Test engineer records when the TLS session resumption occurred.
8	Lower tester maintains an active TLS session with the data exchange.
9	Test engineer disables the DUT NIC after 15 or more minutes.
10	Test engineer re-enables the DUT NIC after a duration longer than the session resumption time.
11	Test engineer records the time when the TLS session renegotiation occurred.
No.	**Review**
1	Review the packet capture to ensure that the DUT/lower tester successfully exchanged data.
2	Review the packet capture to ensure that communications stopped after the DUT's NIC was disabled.
3	Verify in the packet capture that session resumption occurred when the NIC was disabled for a shorter time than the session resumption time.
3	Verify in the packet capture that a session was renegotiated when the NIC was disabled longer than the session resumption time.
4	Verify that the properties of the renegotiated session meet the requirements of the respective application layer protocols shown in Table 4.

4.4 Master Secret Key Update (T4)

Background: When a DER is deployed in the field, it is usually there for about 20 years. During this time period, there are not enough instances when the operator tries to ensure that the master key that was

assigned to the DER is still valid and did not get compromised. There is a need to set fixed time intervals during which the DER server sends the new master key to the DUT. In this way, even if the master key of the DER is compromised, it will be renewed by the DER server after the predetermined interval, thereby securing the connection.

Purpose: This test case ensures that the connection between the DUT and DER server is secured by sending updated master secret keys to the DUT if the connection has been active for more than the master secret key update time. This test case also verifies that if a session has changed, the master key has also changed.

Vulnerabilities addressed: MITM (V1)

Requirements: In the DER server settings, the configuration of the predefined update time of the master secret key is required. In addition, there is a need to ensure that the DUT and DER server are communicating with each other before the DER server sends the updated key.

Table 8. Test Procedure to Verify Master Secret Key Update

No.	Action
1	Test engineer connects the DUT and the lower tester.
2	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
3	Upper tester requests the DUT to establish a TLS session with the lower tester.
4	Lower tester maintains an active TLS session with the data exchange.
5	Lower tester provides the DUT with a new master secret key.
6	DUT reestablishes the TLS session using the new master secret key.
7	Lower tester maintains an active TLS session with the data exchange.
No.	**Review**
1	Review packet capture and identify when the master secret keys are updated.

4.5 Message Authentication Code (T5)

Background: A MAC is a snippet of information used to authenticate or validate if a message originated from its intended sender or source. Additionally, MACs are used to confirm that the original message or data has not been modified before it is delivered to its intended destination or receiver.

Purpose: This test case ensures that there is enough protection for both the message data integrity and its authenticity (Goldreich 2004). Although there are multiple implementations of MACs, three are approved general-purpose MAC algorithms stated by NIST (NIST, Computer Security Resource Center 2018b):

- Keyed-hash MAC
- Keccak MAC
- Cipher-based MAC.

Vulnerabilities addressed: Replay (V2), MITM (V1)

Requirements: An approved cipher suite with a MAC implementation.

Table 9. Test Procedure to Verify MAC

No.	Action
1	Test engineer connects the DUT and the lower tester.
2	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
3	Upper tester requests the DUT to establish a TLS session with the lower tester.
4	Lower tester maintains an active TLS session with the data exchange.
5	Upper tester requests the DUT to terminate the connection to the lower tester.
No.	**Review**
1	Verify if MAC is used while transporting data between the DUT and lower tester. The MAC implementation is usually indicated in the last section of the cipher suite, named as follows: Cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

To check for invalid behavior testing, repeat action items 1–4 from Table 9 and then execute the following steps:

- From the lower tester, send packet with invalid MAC to DUT.
- Resend the already sent packet (replay attack).
- Remove a packet.
- The DUT terminates the TLS session to the lower tester and reports an error condition to the upper tester.
- To verify, check whether the DUT discovers the invalid behavior and informs the upper tester.

4.6 Multiple Certification Authorities (T6)—Optional

Background: A certificate authority is an entity that issues a digital certificate**.** Support for multiple certificate authorities is always a good option to secure the DER's communications with the DER server.

Purpose: This test verifies that before launching a secure connection, the DUT uses the certificate of one of the approved certificate authorities to authenticate the connection on the DER server side. This test also satisfies the authorization part of the connection because the DER server will not entertain the request from the DUT for initiation of a connection until there is a secure connection with a valid certificate from one of the approved and valid certificate authorities. In this test case, support for multiple certificate authorities is verified, including with secret keys and public keys.

Vulnerabilities addressed: Replay (V2), MITM (V1), spoofing through security certificates (V4)

Requirements: It is expected that error conditions will be handled correctly, and they will be used to send notifications to a centralized DER server. If any error occurs, the connection needs to be terminated. In addition, the DUT should have a root certificate from multiple certificate authorities. The exchange and validation of the certificates must be bidirectional so that mutual authentication from both ends can be achieved. The connection shall be terminated if any entity (either the DUT or the DER server) cannot validate the received certificate chain.

Table 10. Test Procedure to Verify Multiple Certificate Authorities

No.	Action
1	DUT is provisioned with a set of approved root certificates.
2	Test engineer connects the DUT and the lower tester.
3	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
4	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses one of the approved root certificates for the server trust chain.
5	Lower tester maintains an active TLS session with the data exchange.
6	DUT maintains the TLS session to the lower tester and reports no error condition to upper tester.
7	Upper tester requests the DUT to terminate the connection to the lower tester
8	Repeat steps 4–7 for each approved root certificate.
9	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses an unapproved root certificate for the server trust chain.
10	DUT terminates the TLS session to the lower tester and reports an error condition to upper tester.
No.	**Review**
1	Review packet capture for error conditions and notifications generated.
2	Verify that the certificate issued by the certificate authority matches the root certificate.

4.7 Certificate Revocation List (CRL) (T7)

Background: A CRL is used to identify the DER server as having a revoked certificate. It is a list of digital certificates that have been revoked by the issuing certificate authority before their scheduled expiration date and should no longer be trusted. CRLs contain certificates that have been either irreversibly revoked (revoked) or marked as temporarily invalid (hold). The DUT takes the appropriate action and terminates the session based on that certificate. Once all certificates are revoked, the connection is terminated, and a notification is issued.

Digital certificates can be revoked for many reasons. For example, if a certificate authority discovers that the certificate was issued improperly, it will revoke the original certificate and issue a new one. Another example is if a certificate is discovered to be counterfeit, the certificate authority will revoke it and add it to the CRL. The most common reason for revocation occurs when a certificate's private key has been compromised. Other reasons for revoking a certificate include the compromise of the issuing

certificate authority, the owner of the certificate ceasing operations entirely, or the original certificate being replaced with a different certificate from a different issuer.

Purpose: This test case verifies whether a digital certificate, which is issued by the certificate authority, is valid and trustworthy.

Vulnerabilities addressed: Spoofing through security certificates (V4)

Requirements: x.509 standard. If vendors are using CRLs locally on the DUT and if vendors are using a third-party certificate authority, the DUT should check the CRL list for validity. If a CRL did not accompany a certificate from the approved certificate authority (does not match) and/or it is not installed on the DUT, then the DUT should make an attempt to install it automatically from a distribution access point (certificate authority server) with some form of authenticity. Applicable protocols include Lightweight Directory Access Profile (LDAP) and Secure Hypertext Transfer Protocol (HTTPS). If a certificate authority cannot be used, manually installing the CRL should be a solution.

Table 11. Test Procedure to Verify CRL

No.	Action
1	DUT is provisioned with an initial CRL.
2	Test engineer connects the DUT and the lower tester.
3	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester and the CRL provider.
4	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses a certificate placed on the initial CRL.
5	DUT terminates TLS session handshake and informs the upper tester about the revoked certificate.
6	Upper tester requests the DUT to retrieve a CRL update.
7	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses a certificate placed on the updated CRL.
8	DUT terminates TLS session handshake and informs the upper tester about the revoked certificate.
No.	**Review**
1	Review packet capture for notifications and verify that the connection is terminated.

4.8 Expired Certificate (T8)

Background: Once the DER is deployed in the field and the connection is established with the DER from the control center, it is very rare for the original certificate using the initial connection to be renewed. This opens a major vulnerability in which the DER is not able to catch an expired certificate and continues to respond to the requests generated from the source using an expired certificate. Therefore, a requirement is needed to prevent the establishment or renegotiation of the session if an expired certificate is used.

Purpose: This test case ensures that if the DUT receives an expired certificate, it refuses the request to establish, terminate, or renegotiate a connection using that expired certificate.

Vulnerabilities addressed: Replay, MITM (V1), eavesdropping (V3)

Requirements: The lower tester rejects the connection with the DUT if the DUT is attempting to establish a connection with the lower tester using an expired certificate. The same applies to the scenario when the lower tester tries to establish the connection with the DUT using an expired certificate. The connection should not be established, and a notification to the upper tester should be issued.

Table 12. Test Procedure to Verify Expired Certificate

No.	Action
1	Test engineer connects the DUT and the lower tester.
2	Test engineer initiates a packet capture with TcpDump or Wireshark on the DUT's configured networked interface to verify communications to and from the lower tester.
3	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses an expired server certificate.
4	DUT terminates TLS session handshake and informs the upper tester about the expired certificate.
5	Upper tester requests the DUT to establish a TLS session with the lower tester. Lower tester uses an expired intermediate certificate authority certificate.
6	DUT terminates TLS session handshake and informs the upper tester about the expired certificate.
No.	**Review**
1	The packet capture will show that the session was attempted but did not complete.

4.9 Operating System and Service Version (T9)

Background: Industries have traditionally struggled to maintain an accurate asset inventory. Outdated software, firmware, and service versions can contain vulnerabilities that can be leveraged into an exploitable cyberattack. With the increasing risk of cyber threats, many DER vendors are looking to secure their products. Without fully understanding the asset of interest, however, it is tedious to provide proper patching and remediation.

Purpose: This procedure hardens the overall security of the DER host by ensuring that the operating system, firmware, and networked services are patched with the latest secured version available. In addition, this test case grants the opportunity to make necessary patches to the DER host before it is released to the public. The principle of least privilege states that in a computing environment, the user must be able to access only the information and resources that are necessary for legitimate purposes. Networked services that are unpatched or not implemented with the DER's functionality should be uninstalled or disabled in the DER's operating environment.

Vulnerabilities addressed: Denial of service (V5), least-privilege violation (V6)

Requirements: These steps should be implemented in a controlled testing networked environment. The use of Nmap, Nessus Professional, or any approved network host vulnerability scanner is recommended.

Table 13. Test Procedure to Verify Operating System and Service Version

No.	Action
1	Test engineer connects the DUT and the lower tester on an isolated network.
2	Test engineer obtains the operating system version, list of applications, and network service versions operating on the DUT.
3	Test engineer runs the network service version scanner on the DUT to retrieve the DER's network service information. (Nmap, Nessus Professional, or any approved host scanner is recommended.) Nmap example: nmap -v -p <1-65535> -sV -O [-sS | -sU] -T<0-5> <DER host ip addr> *-v: Verbose mode* *-p <1-65535>: Port identification* *-sV: Probe open ports to determine service/version info* *-O: Enable OS detection* *[-sS | -sU]: TCP SYN/Connect()/ACK/Window/Maimon or UDP port scans* *-T<0-5>: Set timing template (higher is faster)*
4	Test engineer ensures that all operating systems, firmware, and network services operating on the DUT are updated and patched with the latest versions.
5	Test engineer disables or uninstalls any network services that are not intended to be operational or used on the DUT.
No.	**Review**
1	Define a scheduled routine for this procedure to ensure that the DUT's operating system, firmware, and networked services are patched and up to date. This includes, but is not limited to: • Updating manually or physically • Updating remotely (4G or higher cellular, Wi-Fi, or wired networks) • Updating via process-controlled script. *Ensure that these options are performed on a secure medium.*

4.10 Authentication and Password Management (T10)

Background: With the increasing need for support for more interoperable DER devices, some industries can enable this functionality on DER devices that have little to no password hygiene management. Without securing the first line of defense of accessing a critical asset, adversaries can easily bypass networked services to carry out their agenda. Authentication and password management is critical for securing a DER device.

Purpose: This procedure prevents successful brute-force attempts and enforces strong passwords for authenticating to the DER software and DER server. In a brute-force attack, automated software is used to generate many consecutive guesses about the value of the desired data. This attack can be easily achieved if the DER's functionality contains one or more of the following:

- Poor password management on local and network services
- User accounts enforce weak credentials for access
- Does not limit access because of failed consecutive log-in attempts.

Vulnerabilities addressed: Brute-force credentials (V7)

Requirements: NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST 2017).

Table 14. Test Procedure to Verify Authentication and Password Management

No.	Action
1	Test engineer obtains all user access levels on the operating system and services on the DUT, i.e., usernames and network services.
2	Test engineer defines lockout cycle period (e.g., 30 seconds).
3	Test engineer configures the DUT's local and network services to lock out after three failed consecutive authentication attempts.
4	DUT enforces strong password complexity requirements for authenticating to either the DUT or DER server's access levels and network services. Refer to the guidelines in NIST SP 800-63-3. Password complexity example: • Use a minimum of eight characters. • Allow all printable ASCII characters. • Require capital case (A–Z), lowercase (a–z), and special characters (!,@,#,$,%,^,&,*, ~,`). • Do not use consecutive and repeatable characters. • Do not use common dictionary words.
5	If DUT uses default passwords to authenticate the DUT forces users to change the default passwords immediately upon use!
No.	**Review**
1	The DUT forces a lockout period and denies unauthorized access after three unsuccessful log-in attempts. Additionally, the DER should not allow the user to retry for at least 5 minutes.

4.11 Physical Security (T11)

Background: Physical security is a hardening methodology for protecting hardware and data from malicious physical actions and events that could cause serious data loss or damage to an enterprise or institution. This includes protection from man-made or natural events. Impediments and the actual location should be considered in an effort to secure the DER locally and to prevent unauthorized access or natural disasters from affecting the DER's control processes. Impediments should be in place to increase the time it takes to cause a cyberattack or physical attack. The physical location of the DER should be considered thoroughly to prevent ease of unauthorized access, and testing should be done in a secure place to ensure safe regulation of the DER (NIST n.d.).

Purpose: This test verifies if any physical security techniques are embedded on the DER.

Vulnerabilities addressed: Denial of service (V5), least-privilege violation (V6)

Requirements: Knowledge of physical controls that can be maliciously accessed on the DER.

Table 15. Test Procedure to Verify Physical Security

No.	Action
1	Test engineer identifies form factors and mediums that are embedded on the DUT that can be easily accessed by adversarial or open means. Examples include the following: • Open interfaceable physical ports • No use of locks or anti-tamper seal • Open-source intelligence.
2	Test engineer obtains the level of real-world risk if mediums are accessed.
No.	**Review**
1	Develop a guide or test procedure to regularly test the physical security of the DUT.
2	No physical security issues identified, embedded on the DUT.

5 Next Steps

To ensure that DERs have minimum cybersecurity policies, controls, and procedures that ensure the authentication, authorization, and integrity of the data, communications, and exchange of information, the scope of this project will be extended by collaborating with government and industry partners—including SunSpec Alliance, UL, National Electrical Manufacturers Association, IEEE 1547 standard working group, IEEE P2030 standard working group, IEC Technical Committee 57 Working Group 15, Smart Electric Power Alliance Smart Grid Cybersecurity Committee, and NIST Smart Grid Program—to support the development of a national/international standard. Once standard test procedures are established, laboratory testing of 11 cases on a photovoltaic inverter will be performed. Based on the results and observations from testing, these procedures will be refined. Finally, the refined test procedures will be submitted to a standards development body to improve and formalize the developed standard.

References

Armerding, T. 2018. "The 18 Biggest Data Breaches of the 21st Century." *CSO*, December 20, 2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

Breach Level Index. 2019. "Data Breach Statistics: Data Records Lost or Stolen Since 2013." https://breachlevelindex.com/.

Cedric, C., P. Cordeiro, I. Onunkwo, and J. Johnson. 2017. "Cyber Security Assessments of DERs." Presented at the 2017 IEEE Photovoltaic Specialists Conference, June 2017. https://www.osti.gov/servlets/purl/1431871.

Cleveland, F. 2012. *IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure*. Geneva, Switzerland: International Electrotechnical Commission. http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf.

Dragos. 2018. *Crashoverride: Analysis of the Threat to Electric Grid Operations*. Hanover, MD. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Federal Trade Commission. 2017. "The Equifax Data Breach." https://www.ftc.gov/equifax-data-breach.

Gautam, K., and D. Upadhyay. 2014. "Implementing Dynamic Certificates for Securing Database." Presented at Confluence: The Next Generation Information Technology Summit, 5th International Conference, 2014. https://ieeexplore.ieee.org/document/4604595/citations#citations.

Goldreich, O. 2004. *Foundations of Cryptography II: Basic Applications*. Cambridge, UK: Cambridge University Press.

Higgins, K. 2018. "Ukraine Security Service Stops VPNFilter Attack at Chlorine Station." *DARKReading*, July 12, 2018. https://www.darkreading.com/attacks-breaches/ukraine-security-service-stops-vpnfilter-attack-at-chlorine-station/d/d-id/1332282.

Johnson, Jay. 2017. "Roadmap for Photovoltaic Cyber Security." Sandia National Laboratories. https://doi.org/10.13140/RG.2.2.25829.91361

Langde, R. 2017. "WannaCry Ransomware: A Detailed Analysis of the Attack." *Techperspective*, September 26, 2017. https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/.

Lee, R.M., M.J. Assante, and T. Conway. 2016. *Crash Override: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos.

National Electrical Manufacturers Association. 2015. "Supply Chain Best Practice." https://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

———. 2018. “Cyber Hygiene Best Practice.” https://www.nema.org/Standards/Pages/Cyber-Hygiene-Best-Practices.aspx.

National Institute of Standards and Technology (NIST), Computer Security Resource Center. 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management* (SP 800-63B). Gaithersburg, MD.

———. 2018a. *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (SP 800-52). Gaithersburg, MD. https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/draft.

———. 2018b. “Message Authentication Codes.” https://csrc.nist.gov/Projects/Message-Authentication-Codes.

———. 2015. *De-Identification of Personal Information* (NISTIR 80530). Gaithersburg, MD. https://simson.net/ref/2016/2016-10-26%20De-Identification%20and%20NISTIR%208053%2015%20Minutes.pdf.

———. n.d. *Physical and Environmental Protection Control Family* (Special Publication 800-53, Rev. IV). Gaithersburg, MD. https://nvd.nist.gov/800-53/Rev4/control/PE-1.

The MITRE Corporation. 2018a. “Common Vulnerabilities and Exposures (CVE).” https://cve.mitre.org/.

———. 2018b. “CVE Details.” https://www.cvedetails.com/.

Oman, P., E. Schweitzer, and D. Frincke. 2000. “Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems.” *Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference*.

Peifer, D. n.d. “SSL Spoofing: Man in the Middle Attack on SSL.” https://www.owasp.org/images/7/7a/SSL_Spoofing.pdf.

Rahm, J. 2017. “SSL Profiles Part 4: Cipher Suites.” *DevCentral*. March 13, 2017. https://devcentral.f5.com/articles/ssl-profiles-part-4-cipher-suites.

SANS Industrial Control Systems. 2016. *The Impact of Dragonfly Malware on Industrial Control Systems*. North Bethesda, MD.

———. 2017. *Analysis of the Cyber-Attack on the Ukrainian Power Grid*. North Bethesda, MD.

Sans Institute. 2004. *Global Information Assurance Certification Paper*. Westminster, CO. https://www.giac.org/paper/gsec/3908/layered-security-model-osi-information-security/106272.

Semantec Blogs. 2017. “What You Need to Know About the WannaCry Ransomware.” October 23, 2017. https://www.symantec.com/blogs/threatintelligence/wannacry-ransomware-attack.

Sobczak, B. “Experts assess damage after first cyberattack on U.S. grid.” *E&E News*. May 6, 2019 https://www.eenews.net/stories/1060281821

U.S. Computer Energy Readiness Team. 2018. “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors: Alert (TA18-074A).” https://www.us-cert.gov/ncas/alerts/TA18-074A.

U.S. Department of Energy, Office of Energy Assurance. 2002. *21 Steps to Improve Cyber Security of SCADA Networks*. Washington, D.C.