Identification and Testing of Electric Vehicle Fast Charger Cybersecurity Mitigations

For Project: 1.3.4.402 Consequence-Driven Cybersecurity for High-Power Charging Infrastructure

Anuj Sanghvi, Tony Markel, Steve Granda, Adarsh Hasandka, and Myungsoo Jun

National Renewable Energy Laboratory

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

Technical Report
NREL/TP-5R00-80799
November 2021

Identification and Testing of Electric Vehicle Fast Charger Cybersecurity Mitigations

For Project: 1.3.4.402 Consequence-Driven Cybersecurity for High-Power Charging Infrastructure

Anuj Sanghvi, Tony Markel, Steve Granda,
Adarsh Hasandka, and Myungsoo Jun

National Renewable Energy Laboratory

Suggested Citation
Sanghvi, Anuj, Tony Markel, Steve Granda, Adarsh Hasandka, and Myungsoo Jun. 2021. *Identification and Testing of Electric Vehicle Fast Charger Cybersecurity Mitigations*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-80799. https://www.nrel.gov/docs/fy22osti/80799.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

Technical Report
NREL/TP-5R00-80799
November 2021

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 Energy Efficiency and Renewable Energy Vehicle Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

List of Acronyms

ARP	Address Resolution Protocol
API	application programming interface
CEEP	Cyber-Energy Emulation Platform
DER	distributed energy resource
DHCP	Dynamic Host Configuration Protocol
ESS	energy storage system
EV	electric vehicle
EVSE	electric vehicle supply equipment
HCE	high-consequence events
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
MITM	man in the middle
MQTT	MQ Telemetry Transport
NREL	National Renewable Energy Laboratory
OCPP	Open Charge Point Protocol
PV	photovoltaics
TCP	Transmission Control Protocol
VM	virtual machine

Table of Contents

List of Figures

Introduction

Fast charging infrastructure for electric vehicles (EVs) is needed to enable and achieve the national goals of transitioning the vehicle fleet toward increased electrification. The Biden-Harris Administration has set a goal for more than 500,000 charging stations to be deployed in the United States by 2035 (The White House 2021). Although we are still in the early stages of this rapid deployment, there is a need to identify and address potential cybersecurity risk and mitigation pathways for EV charging infrastructure.

In 2019, Idaho National Laboratory, Oak Ridge National Laboratory, and the National Renewable Energy Laboratory (NREL) were awarded a scope of work called Consequence-Driven Cybersecurity for High-Power Charging Infrastructure, and the laboratories have jointly worked to identify, evaluate, and mitigate potential cyber-related consequences associated with high-power fast chargers.

NREL has contributed by considering cyberattack scenarios and consequences associated with integrating distributed energy resources (DERs) at fast charging stations. The dynamic nature of fast charger load profiles would encourage site operators to incorporate solar generation for energy cost reduction and energy storage for peak demand cost management at future charging facilities with multiple fast chargers at a site. These energy resources would be monitored and coordinated via a site energy management controller with data exchange between devices and local power metering infrastructure; thus, networking between devices and the design of the system becomes important in the overall cybersecurity posture. In addition, component vendors and system operators likely will have remote interfaces to any of these systems. It is therefore important to understand the breadth of the cyberattack surface and potential strategies to mitigate impacts.

Figure 1 was developed and incorporated into a publication at the 2021 Institute of Electrical and Electronics Engineers (IEEE) Transportation Electrification Conference to document the potential landscape of consideration. The diagram details the spectrum of stakeholders and components within the system and indicates some of the likely communication protocols that are or will be in use. This project has focused on the contents shown within the blue envelope that would be components and protocols expected to be found within a local charging site that includes multiple chargers and DER resources. Laboratory research and testing have explored the security challenges and opportunities with Open Charge Point Protocol (OCPP) and Modbus. Each can be used to coordinate the operations of EV charging systems at a refueling facility. Many additional paths for cyberattack might exist for impacting this system, and they could be the focus of future efforts to monitor, defend, and enhance the resilience of future charging infrastructure.

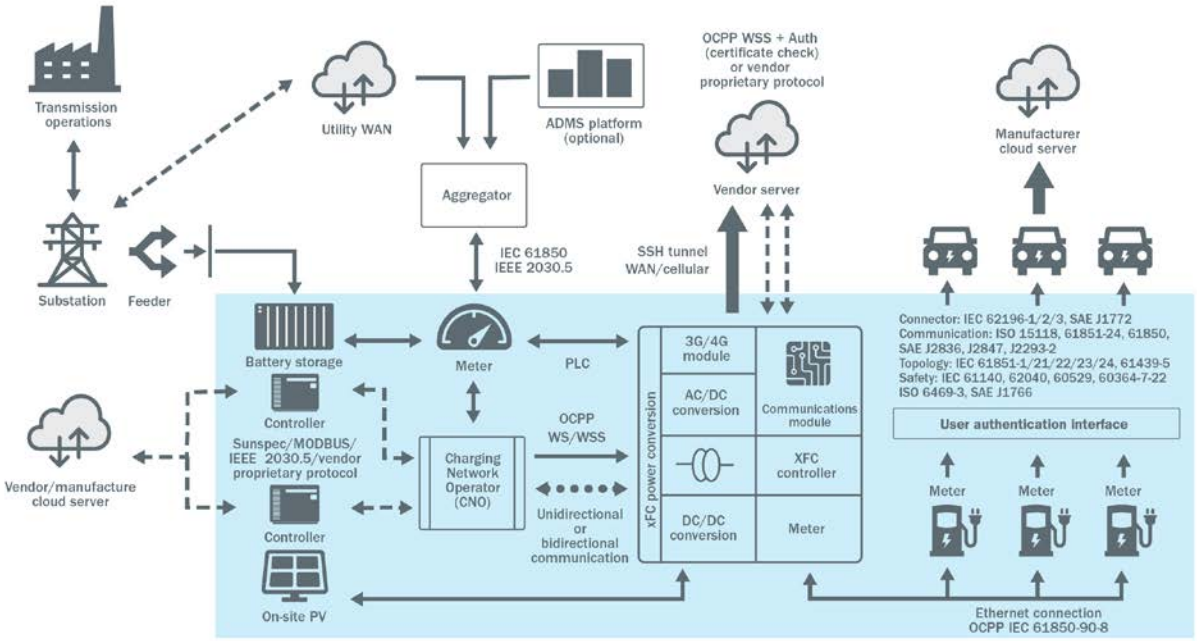

Figure 1. EV fast charging ecosystem communication architecture developed to identify communication standards, interconnections, and control elements to consider within the high-consequence event analysis

Given EV fueling system dependencies on networking, controls, and power systems, NREL's work benefited from the use of the Cyber-Energy Emulation Platform (CEEP) for creating repeatable system-level scenarios and interactions between virtual and hardware components (Hasandka, Rivera, and Van Natta 2020). In 2020, the research team successfully completed a hardware-in-the-loop integration between a power system model running in CEEP and a Tritium 50-kW Veefil fast charger located in the Optimization and Control Laboratory in NREL's Energy Systems Integration Facility. Research activities since that connectivity milestone have explored attack and mitigation scenarios that are the focus of this final report. The team also completed the integration of an energy storage system (ESS) model and a site energy management controller within the CEEP environment and maintained the interface with a physical charger. Our most recent progress provides results of test scenarios that compare a baseline implementation under attack on both unprotected systems and systems with potential mitigations implemented. Our methods and results are summarized in this final report.

1 Distributed Energy Resource-Related High-Consequence Events

High-consequence events (HCE) are situations that lead to significant outcomes, such as the loss of system control, equipment damage, and/or financial loss. NREL collaborated with the multi-laboratory team during the initial phases of this project to identify and define a broad spectrum of these component and system scenarios that could result in HCEs. Approximately 50 concepts were created and refined, at which point the team categorized the concepts into the following types of outcomes (with examples):

- Grid impacts (power flow dynamics, generator or substation operation change)
- Safety (fire, electrocution)
- Loss of service (exceeding circuit limits or forcing mis-operation)
- Hardware damage (blown fuses, overloaded components, bricked communications)
- Data theft/alteration (credit card data, personal information).

NREL focused on the HCEs that were associated with either the components—e.g., fast charger, photovoltaics (PV), battery storage, site controller—or the communications surrounding the site-level fast charger coordination with local DERs. These HCEs are included in both the grid impacts and the safety categories.

An example of an action leading to an HCE includes the manipulation of a power meter reading that when provided to a system-level site controller results in an incorrect operational decision. For DERs, these decisions may lead to a grid impact via a significant load change, more dynamic conditions, or other disturbance. Or they can lead to a financially detrimental situation for the owner/operator, such as paying much higher charges for the energy and power than normally would be required for the services delivered.

DERs integrated with an EV fast charging station have the primary purpose of managing the energy delivery costs for the EV charging function. PV generates electricity locally from renewable resources and offsets the grid energy consumed. Energy storage can be integrated to improve the value proposition of the solar generation by storing and using excess solar energy locally versus reselling excess energy at wholesale utility rates, or it can be used to mitigate momentary spikes in load caused by coincident charging events that could result in high monthly costs from excessive peak power demand. We also assume that a site energy management controller is used to monitor the collection of facility power meters and make control decisions on how energy storage should be used to enable cost-effective fast charging. Cyberattacks on any of these components at a local level or across multiple sites can result in a high-consequence cyber event that could lead to excessive operational costs, site or equipment outages, and potential distribution grid disturbances.

2 Cyber Emulation Environment for Fast Charging Scenarios

This project uses CEEP to host component models in the virtual environment while being able to link to physical resources. The basic architecture includes an EV fast charging unit, an OCPP client/server system, a site controller, a site meter, an ESS, and a PV system interconnected with both power and communications. An interconnection diagram showing how these components are networked is provided in Figure 2.

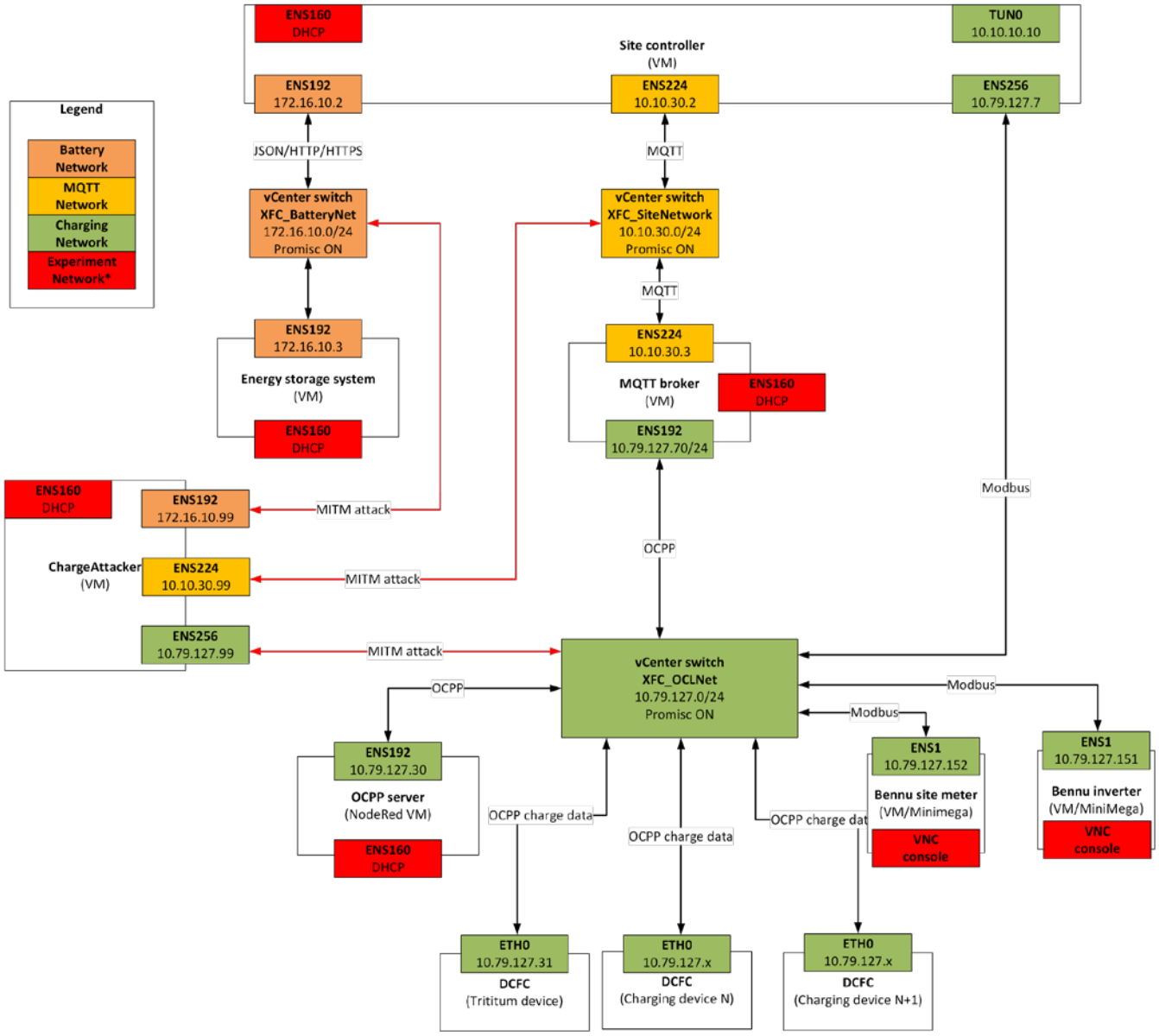

Figure 2. Detailed fast charger station interconnection diagram for testing cyberattack mitigations

Starting at the top of Figure 2, the site controller virtual machine (VM) is shown with network connections to the ESS virtual machine and the MQ Telemetry Transport (MQTT) broker virtual machine. The site controller also has connections to the vCenter switch, which provides connections to

the physical fast charger, the OCPP server virtual machine, and the site meter and PV inverter as emulated devices. Finally, shown on the left of the diagram, a charge attacker virtual machine is included as an adversary device with assumed network access and the ability to perform reconnaissance. With this information and access they can perform man-in-the-middle (MITM) attacks on message transfers within the various segments. The core components are described in the following sections.

2.1 Site Controller

The site controller is a crucial element of the experiment. It collects the status from interconnected components across various networks and makes decisions based on system demands and the battery state. The site controller also monitors the net load for the building/site on a separate interface using Modbus. The site controller can drive battery charge or discharge functions, modify the ESS thresholds, and can enable full or restricted fast charger power delivery. Additionally, the site controller makes the appropriate decision to provide power either through the grid connection or the local storage system. This component includes NREL-developed logic based on prior work representing basic decisions of operating a station. The site controller decision points are depicted in the following flowchart (Figure 3), and the possible manipulations are discussed later.

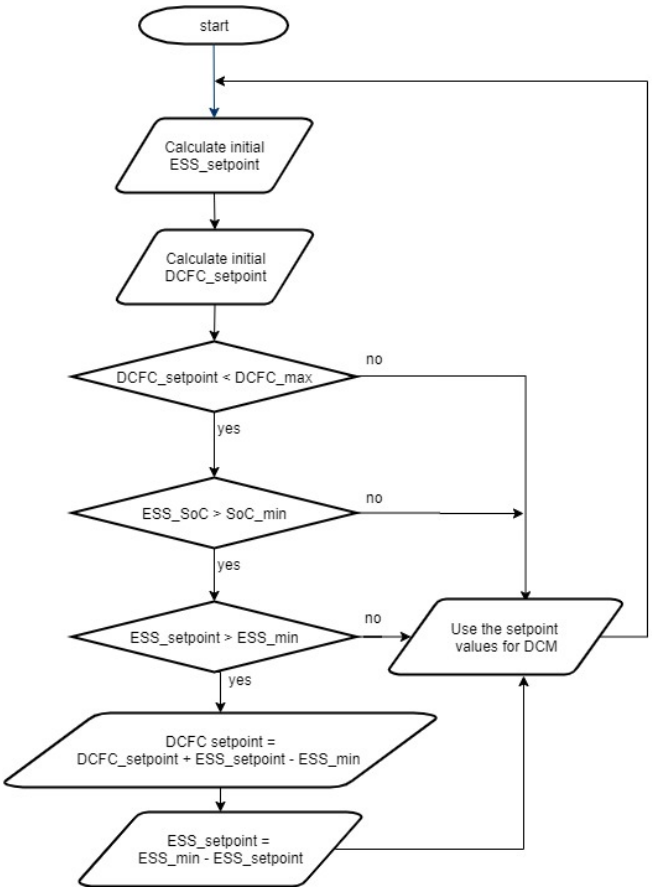

Figure 3. Logic diagram of the site controller at a fast charging station

This logic is embedded within the site controller virtual machine shown in Figure 2.

2.2 OCPP Server and Client

The OCPP server is used to coordinate the fast charger operational point with the site controller. OCPP is used by charge network operators to enable and monitor charging operations across all chargers at a site or across a broad region. Within the context of these experiments and as depicted in the center of Figure 2, the OCPP server, upon receiving information from the fast charger, transmits the information to the MQTT broker, which is then consumed by the site controller upstream. The OCPP server communicates with the client on the fast charger for authorizing, initiating, and stopping the charging sessions with the EV. The OCPP server also provides the operator an ability to configure and control the fast charger functions. Several versions of OCPP are in use today. OCPP 1.6J is common and can be implemented via web sockets and secure web sockets. The OCPP exchange is a primary target for these experiments to sniff and manipulate plaintext communications between the server and the client. The capture of the *transaction_ID* parameter on accessing the network enables a rogue agent to inject disruptive OCPP commands. OCPP 2.0 was recently introduced and enables additional functionalities of certificate management and secure web sockets that could mitigate some message integrity risks. OCPP 1.6J, is the commonly used version today and was used for nearly all the experiments conducted.

2.3 Battery System Model

The experiment includes a software model emulating a locally installed commercial ESS. The storage system is emulated with its own virtual machine that communicates with the site controller over a RESTful API and provides status values, such as target state of charge and system limits. The software implementation also included a Modbus TCP/IP server for control and Public Key Infrastructure (PKI) capability to test various attack and mitigation strategies. The mis-operation of the battery system would be influential to the site controller decisions and could lead to potential failed fast charger operations.

2.4 Power System and Photovoltaic Implementation

The power system and PV in this experiment consist of elements sufficient to represent a single EV charging site (Figure 4). A commercial building is included, with its load partially provided by on-site solar PV. All the remaining load is supported by the grid substation and the local battery. A smart site meter is connected to the breakers and metering sensors at the substation for monitoring and controlling the loads and load breakers. The power system components are modeled using OpenDSS, and the electrical state information is made available using Modbus TCP/IP to the interconnected virtual machines representing these nodes via the CEEP framework.

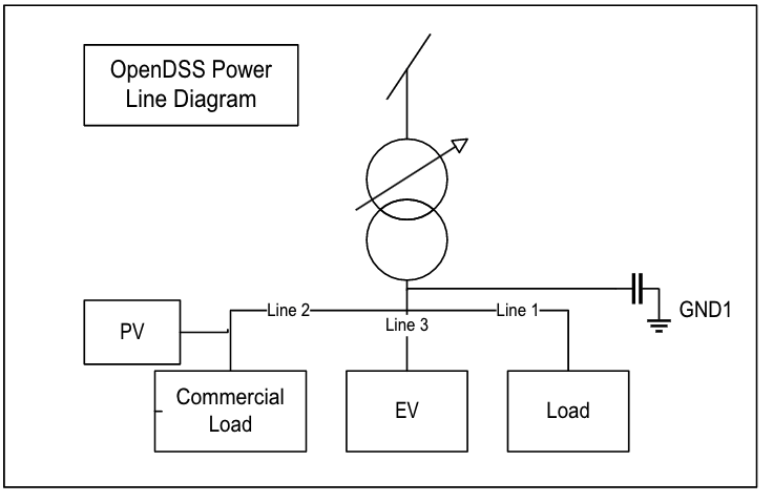

Figure 4. Power system configuration represented using OpenDSS

2.5 Electric Vehicle Fast Charger (Hardware-in-the-Loop and Simulated)

A 50-kW Tritium Veefil fast charger is located in the Optimization and Control Laboratory in NREL's Energy Systems Integration Facility. This specific fast charger was used primarily as a message generation device and our use is not intended to suggest that there are any cyber vulnerabilities associated with the unit. For these experiments, the communications and control interface was directly patched to the CEEP models via a dedicated network switch. This enables the OCPP server within the emulation to interface with the fast charger OCPP client to access the status and manage the charger operations. Prior work in this project successfully implemented the hardware-in-the-loop connection between the fast charger and the CEEP model.

3 Attacks and Mitigations

Aligning with the HCEs introduced previously, the next stage of work focused on creating attacks that can result in an HCE and specifically in HCEs that could be associated with the DER components. Potential mitigations that could prevent the attacks were planned and later demonstrated. The three attack and mitigation scenarios associated with DER systems and fast chargers that were tested are described as follows.

3.1 Scenario 1—Energy Storage System Man-in-the-Middle Attack

In the ESS MITM attack scenario, a site controller aggregated power data from various sources and implemented the logic depicted in Figure 3. One of these data sources, the ESS, was assumed to not be properly configured and was deployed without protections (i.e., authentication, access control, encryption). Figure 5 shows the site controller updating the set points for the ESS using a RESTful API.

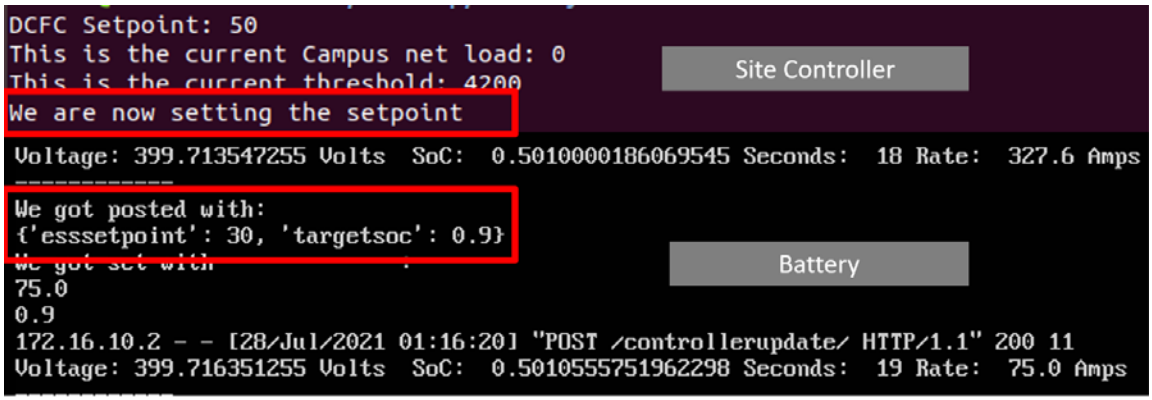

Figure 5. Site controller updating the ESS

From the architecture in Figure 2 there is an attacker with existing network access, who has pivoted into the XFC_BatteryNet network segment and started enumerating assets and protocols. In Figure 6, in the red box, the attacker sees the JavaScript Object Notation (JSON) data being sent via POST and GET requests over Hypertext Transfer Protocol (HTTP) between site controller (172.16.10.2) and the ESS (172.16.10.3). In this scenario, the Site Controller sets the energy storage set point (*esssetpoint*) to 30 and the target state of charge (*targetsoc*) to 0.9 (90% state of charge).

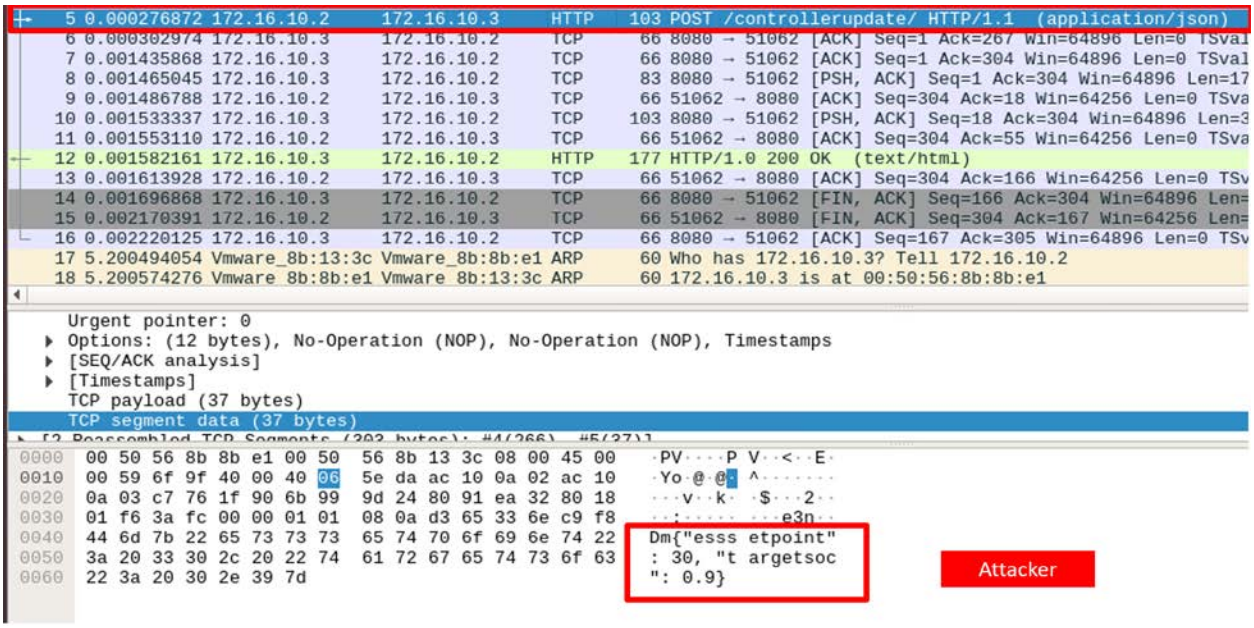

Figure 6. Attacker conducts asset enumeration via unencrypted data exchange using Wireshark

Without important cyber protections in place, the attacker can easily manipulate data from the site controller to the battery using an MITM attack. A network-based attack—i.e., Address Resolution Protocol (ARP) spoofing, Dynamic Host Configuration Protocol (DHCP) race— could then be performed to MITM the battery and the site controller. The attacker can now manipulate the data being sent between the components using publicly available tools such as MITMProxy or Ettercap. The original packet with the *esssetpoint* and *targetsoc* is shown in Figure 7.

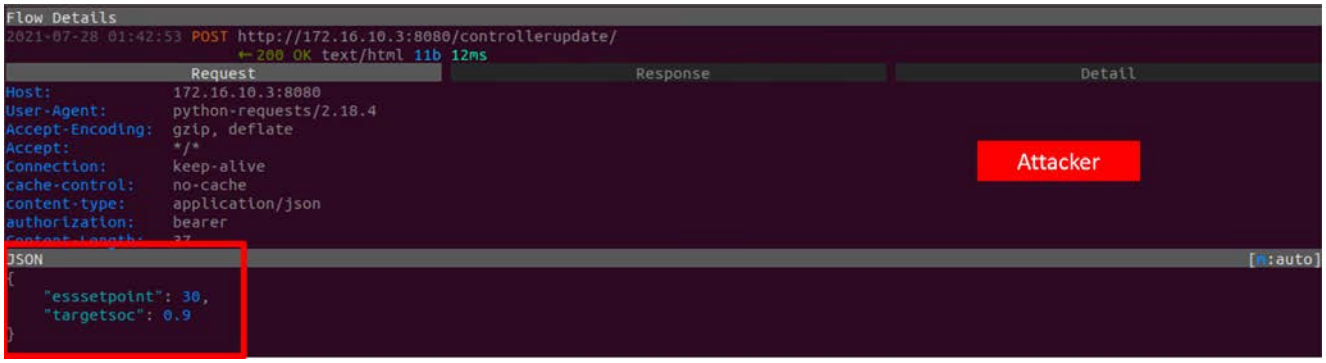

Figure 7. MITMProxy successfully capturing the packet from the site controller to be manipulated

The attacker then manipulated these values and replayed the malicious packet back to the network, where the battery then accepted it. Figure 8 shows the change in the energy storage set point (charging value) from 30 to 5000 and the change in the overall target state of charge from .9 (90% charge) to .1 (10% charge). As a result, we demonstrated manipulation of the system (Figure 8), and we expected the battery to substantially increase charge rate and site load.

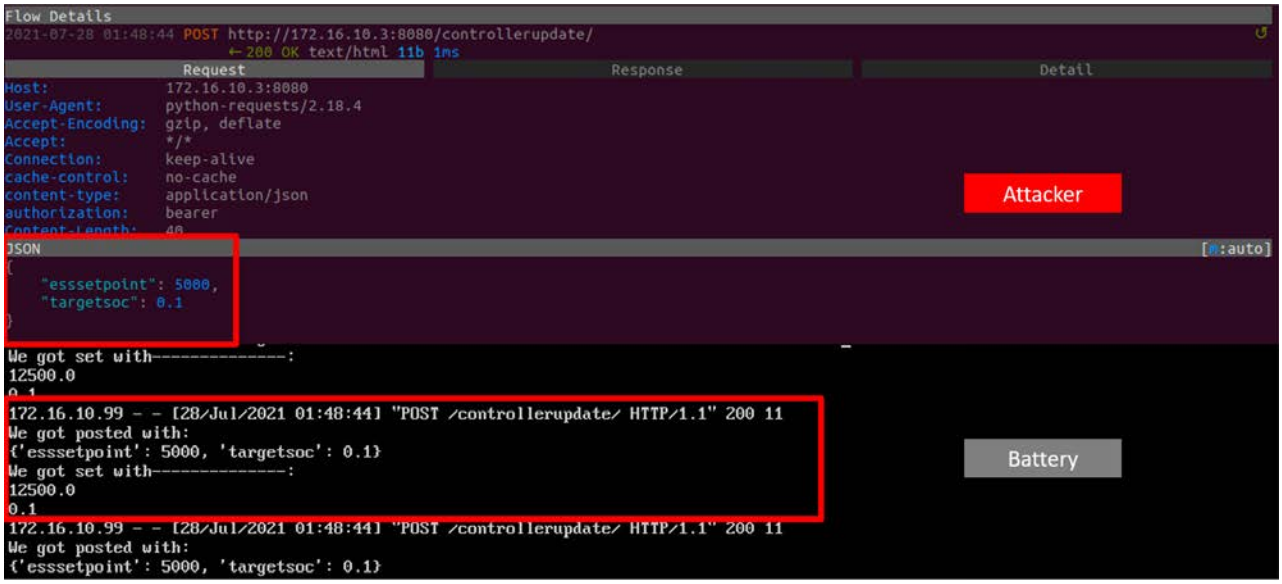

Figure 8. Manipulated values from the attacker successfully sent to the local ESS

To mitigate against these attacks, our ESS was reconfigured to use authentication and encryption. Figure 9 shows the security actions implemented and is completely transparent to the operation between devices.

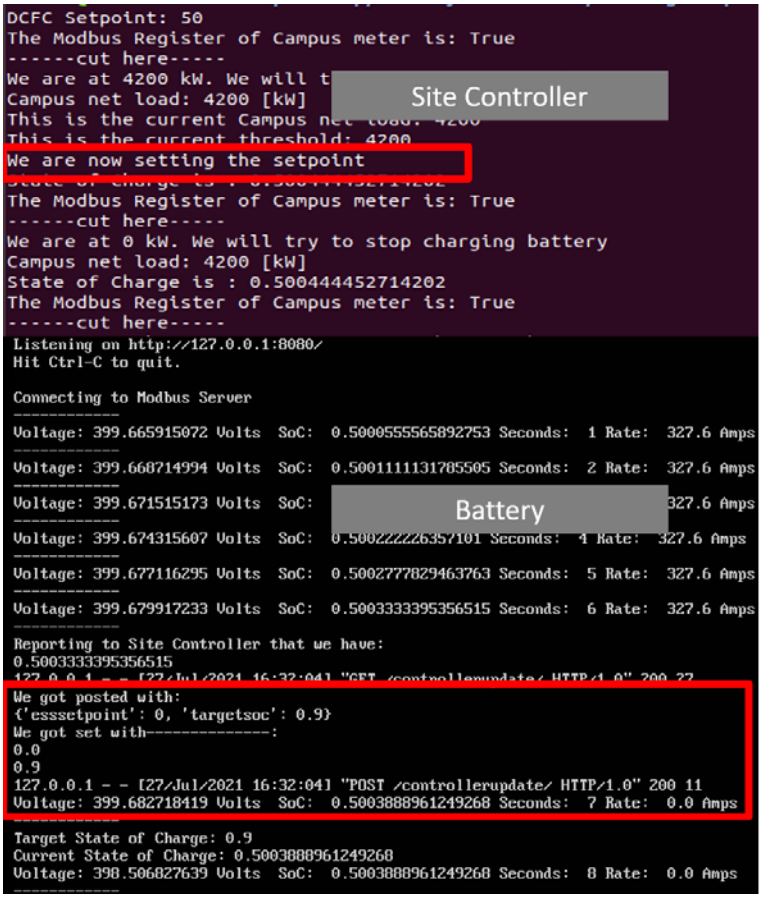

Figure 9. Site controller updating the ESS using HTTPS

With the encryption in place, the attacker cannot readily read or manipulate the traffic between the site controller or the ESS because the messaging is now encrypted using Hypertext Transfer Protocol Secure (HTTPS) (Figure 10).

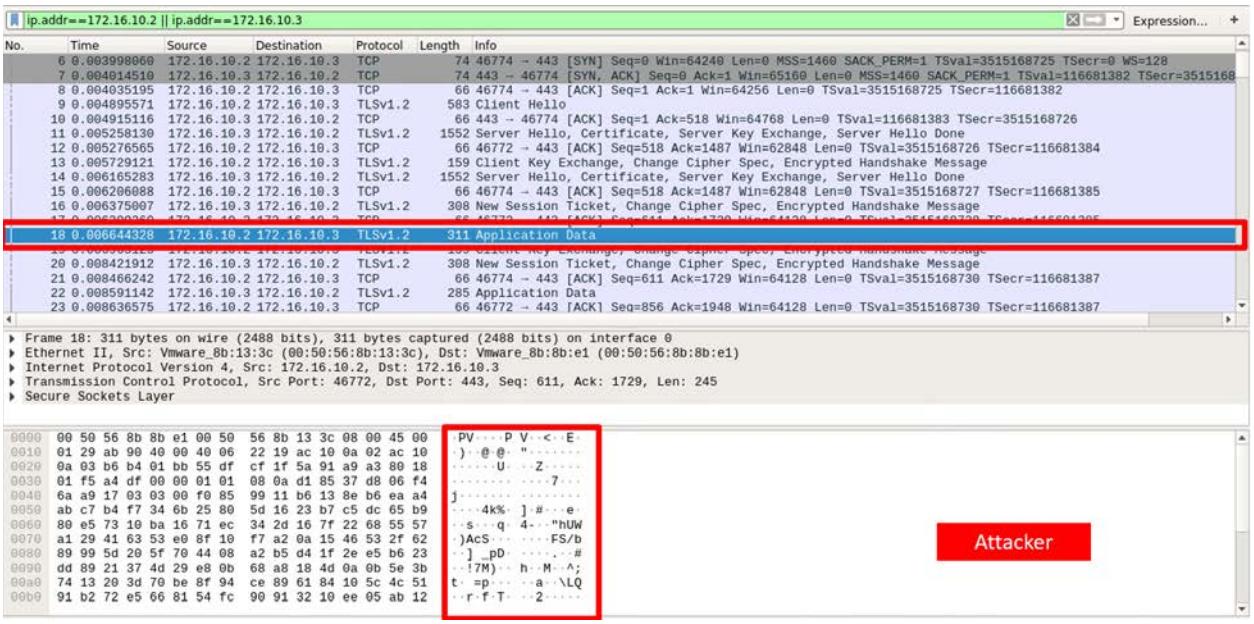

Figure 10. Encrypted communications between the ESS and the site controller as seen by the attacker node via Wireshark

Although the mitigation in this scenario was successful, unfortunately, many existing legacy and embedded devices deployed today might not have the capability to perform modern cryptographic functions. Mitigations for legacy devices communicating over various ICS protocols such as Modbus are explored in a later scenario using Module-OT, which is a bump-in-the-wire (a device added to legacy communications network links to provide enhanced functionality) encryption solution developed by NREL and funded by the U.S. Department of Energy Cybersecurity for Energy Distributions Systems program (Hupp et al. 2020). Alternatives to encryption for legacy systems could include introducing Intrusion Detection or Protection Systems (IDS/IPS) that would analyze traffic behavior for anomalous activity.

3.2 Scenario 2—Site Meter Malicious Command Injection

This scenario focused on testing and securing the Modbus communications between the site controller and the site meter instances in the experiment and leveraged the site controller's dependencies on the site meter's load information. Modbus TCP/IP is a commonly used protocol, and the solutions presented here have broad applicability to commercial systems. In our scenario, the site controller balanced the energy supply from the ESS or grid power based on the site's overall load conditions relative to thresholds. In the experiment, the attack manipulated these communications and injected a malicious Modbus write command providing inaccurate information to the site controller and causing manipulated operation of the battery controller and the power provided to the fast charger. The control operations being altered caused the battery system and the charging operations to disturb the overall power flow at the site which may impact the system dynamics under certain conditions.

Figure 11 depicts the plaintext communications between the site meter and the site controller, which the attacker then sniffed and manipulated the output of the site controller's logic. Based on the load profiles, the attacker targeted the site meter using the Modbus client module within Metasploit and injecting a WRITE_COIL command. Without proper authentication services running on the site meter, the attacker is able to write to internal registers and thus forced the meter to provide an incorrect Modbus register value to the site controller, as shown in Figure 12.

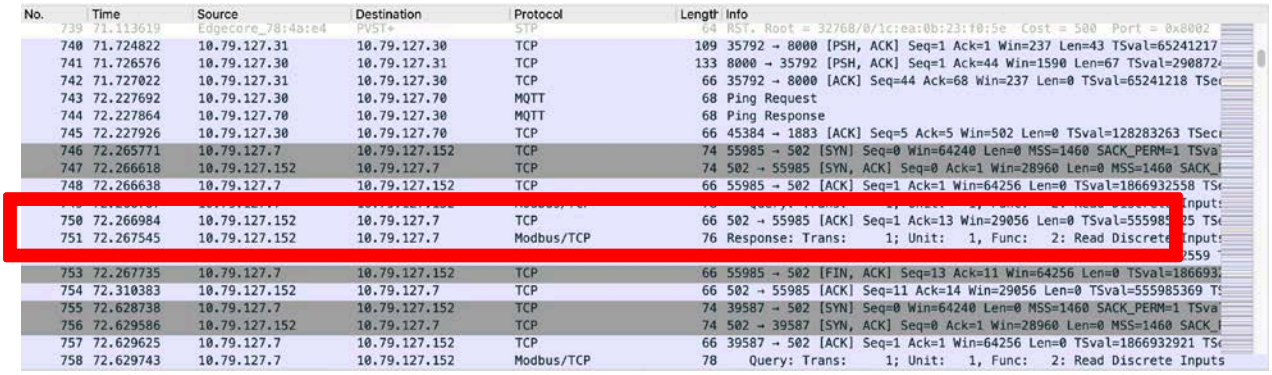

Figure 11. Normal communications between the site meter and the site controller via Modbus (baseline)

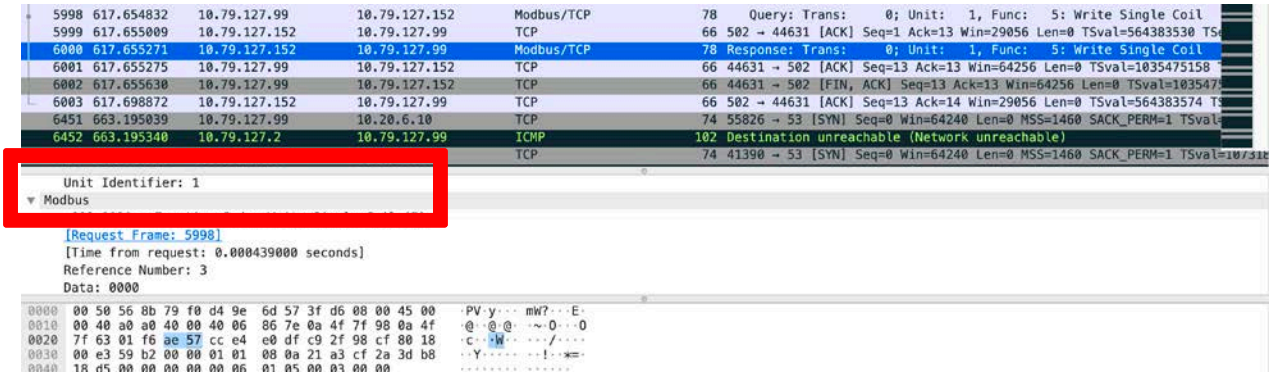

Figure 12. Malicious Modbus command injection

The Modbus write command changed the value of a Modbus status register in the site meter which was then read by the site controller. This malicious update informs that the field device—in this case, the virtual charging station—is not "charging" even though it might have been charging. This information coming from the site meter disturbed the logic of the site controller to make critical decisions about switching load allocations between the ESS or grid power. Potential mitigations include adding encryption to the data transfer or giving the site controller a means to validate the data integrity.

To mitigate this attack and prevent data interception and modification, a bump-in-the-wire solution, Module-OT, was considered and tested. This virtual instance of a device acted as a client/server and was placed at each site meter and site controller location. The Modbus communications between these two critical assets was then encrypted, as shown in Figure 13.

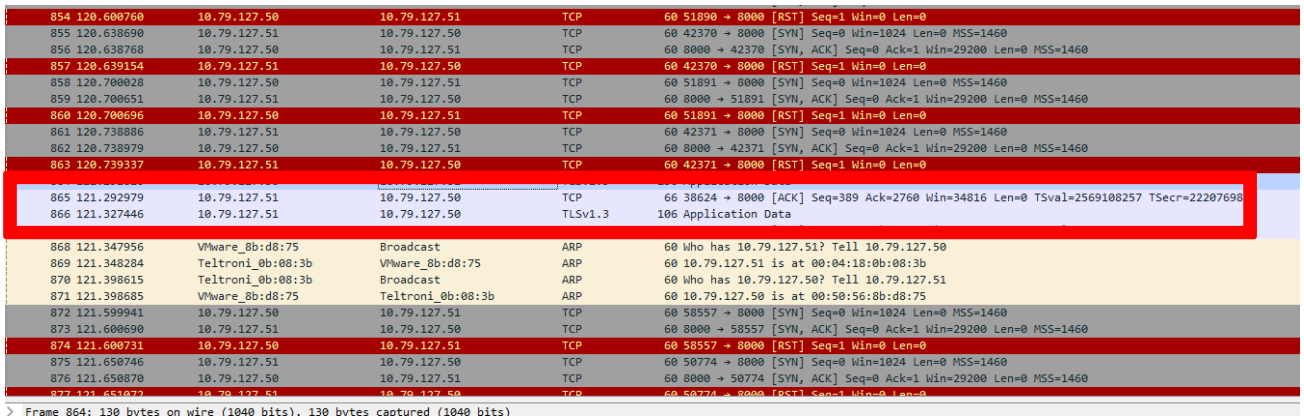

Figure 13. Communications encrypted using TLS enabled by Module-OT

The implementation of Module-OT as a mitigating solution is an option for protecting one of the many protocols associated with a fast charging station. Our work will continue to test this as a way of advancing and maturing the fast charging infrastructure as whole to prevent malicious activities within DER systems from impacting station operation. Figure 14 represents a section of the architecture in Figure 2 showing the application of Module-OT to protect these communication pathways from attack.

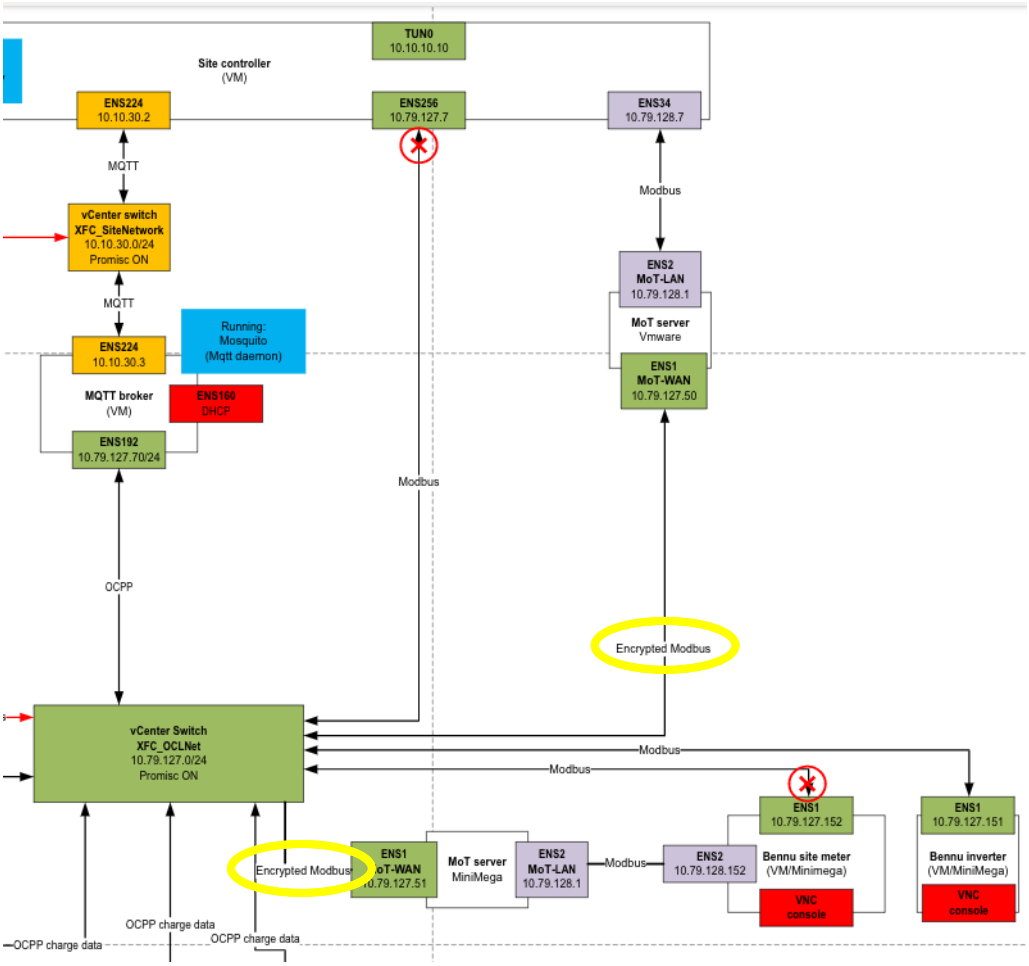

Figure 14. Emulation environment diagram with Module-OT mitigations applied (purple) enabling Modbus encryption

The experiments thus far have explored attacks across multiple components at a fast charging site and suggest that mitigations including message encryption on various protocols in use offer enhancements. Additionally, improvements to the site controller logic that emphasize resilience to attacks on data linkages could be of significant benefit.

3.3 Scenario 3—Message Translation Exchange Hijacking

This scenario focused on a unique aspect of protocol conversion happening within the demonstrated experiment. The OCPP server not only connects to the charging station but also sends and reports live values to the site controller via an instance of the MQTT broker. The purpose of this agent is to translate the OCPP messages from the server and have it sent upstream to be consumed by the site controller or other services as necessary. Protocol translations like this are common across infrastructures, and they offer the attacker another avenue to hijack information exchanges. In our case, the communications between the MQTT broker and the site controller present a pathway of feeding incorrect values to the site controller. As we learned from the previous scenarios about the crucial functions of the site controller, conducting this proof-of-concept attack demonstrates that the site controller can be poisoned with malicious messages.

Figure 15 shows a series of MQTT messages being exchanged from the view of the attacker virtual machine on the local network. Without encryption and authentication, the attacker collected sufficient insights to then initiate a hijacking script that allowed for manipulating the values on the wire for the site controller to ingest.

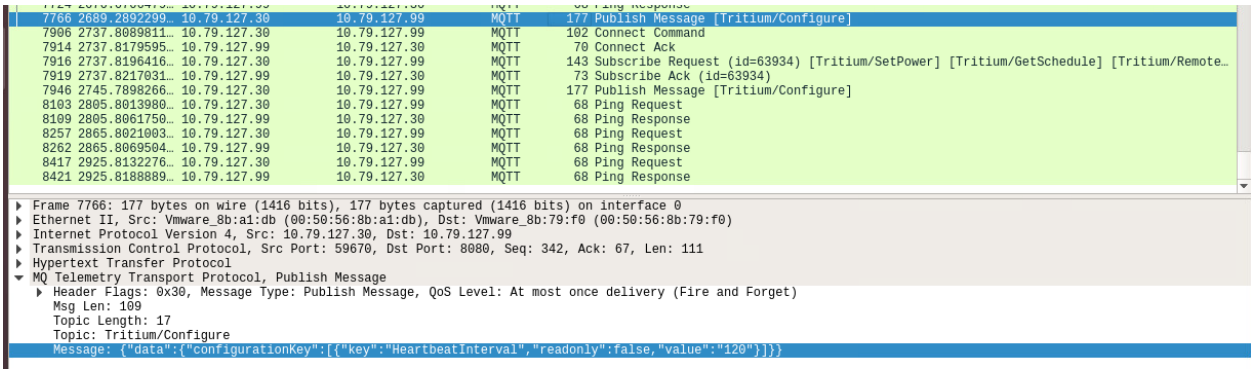

Figure 15. OCPP server gets heartbeat message from fast charger of 120, sniffed by the attacker

Figure 16 shows an approach for manipulating the heartbeat value in an OCPP message, and Figure 17 shows the receipt of a manipulated value. Again, the emphasis for the mitigation approach for this scenario is proper PKI with attribution by using certificates along with session encryption using TLS 1.3 and secure web sockets to prevent the attacker from understanding the communications contents. The use of secure web sockets is an option available for OCPP message exchange but may not always be enabled. This attack and mitigation exercise highlights the importance of enabling optional security features when available.

```
import re
from mitmproxy import ctx, http, tcp
from mitmproxy.utils import strutils

def websocket_message(flow: http.HTTPFlow):
    ctx.log.info(f"Flow Attack")
    #assert flow.websocket is not
    message = flow.websocket.messages[-1]

    if message.from_client:
        ctx.log.info(f"client sent a message: {message.content!r}")
    else:
        ctx.log.info(f"server sent a message: {message.content!r}")

def tcp_message(flow: tcp.TCPFlow):
    message = flow.messages[-1]
    #message.content = message.content.replace(b"true", b"false")
    #ctx.log.info(f"tcp_message[from_client={message.from_client}), content={strutils.bytes_to_escaped_str(message.content)}]")
    message.content = message.content.replace(b"120", b"199")
    ctx.log.info(f"tcp_message[from_client={message.from_client}), content={strutils.bytes_to_escaped_str(message.content)}]")
```

Figure 16. Modification of heartbeat values (proof of concept)

Figure 17. Manipulated value of heartbeat 199 injected with MITMProxy

To mitigate this protocol translation intrusion risk, a token-based authentication server was instituted so that each device can confirm the source and integrity of the messages exchanged on both sides of the translation. Once the token-based authentication occurred between the MQTT broker and the OCPP server, the mode of communication was secured with the TLS, which encrypted the traffic sent by the OCPP server. This prevented a rogue agent on the wire from using the information for any manipulation within the time constraints of a transport layer session. A simple implementation of the X.509 standard certificate definition was used for the creation of the certificate that enables public key exchange.

4 Conclusions

The research conducted lays a foundation for further exploration and collaboration with industry to mitigate cyber risks associated with EV fast charging infrastructure and to potentially design these mitigations into future implementations. Through thoughtful discussion among national laboratory partners, a long list of potential HCEs that could be relevant to fast charging systems were documented and ranked based on complexity and impact. NREL's responsibility was to dig deeper into the HCEs that could be influenced and/or impacted by a compromise of the DER components. The approach was to leverage the CEEP for modeling power flow and communications and to use the cyber analytics of the platform to provide further insights. The CEEP also provided a critical linkage to physical hardware in the laboratory for data and message collection and manipulation experiments.

The project successfully constructed an emulation environment that represents a fast charging station with integrated DERs. Scenarios were implemented that demonstrate the attack outcomes on both an unprotected baseline and systems that leverage mitigation scenarios that include encryption and authentication. Based on the attack and mitigation results to date for a station design that includes DERs, the following recommendations can be offered:

1. Security best practices, such as the use of a virtual private network for remote connections and the use of TLS for internal networks, that provide encryption between critical assets responsible for site energy management would reduce the MITM attack surface.
2. The deployment of a certificate authority would enable message authentication between site equipment.
3. Use of network design practices including segmentation and switch configuration specifically for the most critical components (site controller and fast charger in this analysis) would limit attacker mobility and the introduction of intrusion detection and protection tools might provide better alerts.
4. Given the range of protocols used at a fast charging station with integrated DERs, thorough analysis using emulation will help ensure that weak linkages can be strengthened and that translations do not open systems for further attack.

The cyber assessments and mitigations that have been developed by the multi-laboratory team will be most effective when further refined with industry leaders and adopted. The following section discusses recommended next steps that could build upon these efforts and contribute to the U.S. Department of Energy and industry success.

5 Recommended Next Steps

The EV charging infrastructure ecosystem can be complex, with multiple chargers integrated at a site with PV, energy storage, and overarching site controls. External systems likely also interface for maintenance and operations. It will be important to devise and share valuable strategies.

Creating a layered network architecture for EV charging infrastructure, like that shown in Figure 18, would provide opportunities for incorporating appropriate types of cyber controls throughout. Network segmentation at the lowest hardware levels helps protect compromised devices from affecting other devices and allows for better zone management with traditional IDS/IPS endpoint solutions. TLS is shown within the controls layer to provide encryption between internal devices. In the upper layers, firewalls control the types of acceptable traffic, and the introduction of certificate authorities provide authentication and attribution capabilities. Finally, external connections are hosted in demilitarized zone protected data servers or enabled via virtual private networks. The business layer featuring Enterprise IT systems are segmented within higher levels of Purdue model to limit exposure of the ICS network. Further refinement of this proposed layered cybersecurity architecture for EV charging stations should be pursued and shared with industry.

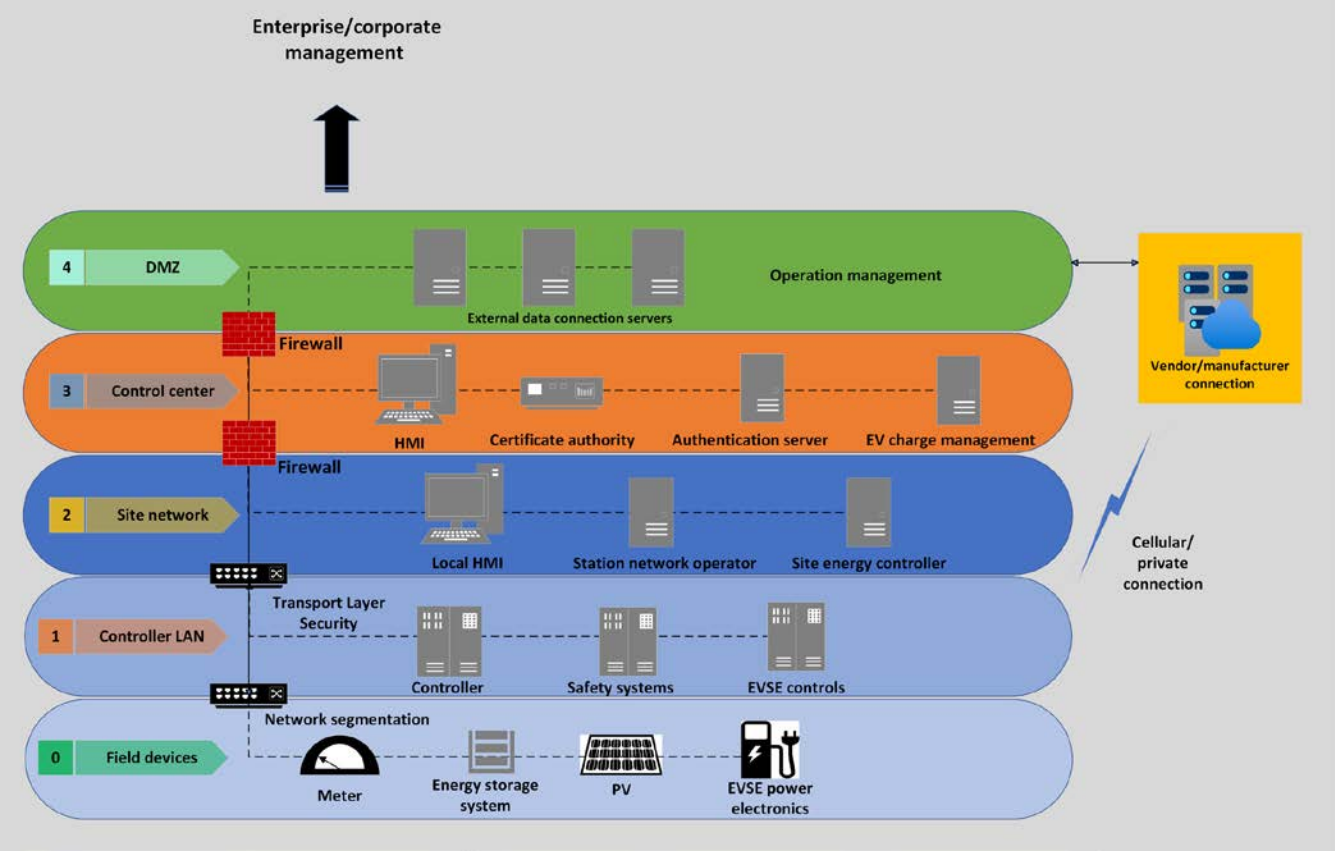

Figure 18. A layered security architecture for EV charging stations

The U.S. Department of Energy Vehicle Technologies Office has made significant progress toward understanding the risks in EV charging infrastructure through a portfolio of projects, including this one. The industry could benefit from the roll-up of project outcomes into a guidance document. A potential approach is for NREL to engage with industry and standards community stakeholders—which could

include the Electric Power Research Institute, SAE, and the National Institute of Standards and Technology—to produce a document that formalizes best-practice security architectures and defense methods that would apply to electric vehicle supply equipment (EVSE) and EV charging facilities.

In the U.S. Department of Energy Vehicle Technologies Office's recent request for information, NREL highlighted that the common protocols (e.g., OCPP, IEEE 2030.5, J1772, and OpenADR) need continued research to evaluate against potential threat activities. Our current project included work that addressed OCPP and Modbus; however, several others remain unassessed. Further research and a guidance document are needed to summarize how to implement available security features for these protocols when used for EVSE systems.

Through this project, the team began to understand the implementation approach and complexity of EVSE and their surrounding systems; however, a more thorough dissection of component hardware and software that identifies areas for purpose-built approaches to eliminate many future vulnerabilities could be valuable. A supply of commodity components that are EVSE-specific shared across vendors in addition to the simplification of system and component designs with a focus on eliminating potential vulnerabilities while reducing costs would be impactful. This effort would emphasize security by design for EV fast chargers. We see this effort also informing cyber response playbook development and workforce skills enhancement.

Through our simulations of a local ESS for site-level load control, we identified the dependencies of site control on sensor data, the importance of rate limits, and the opportunity to prepare the system for resilience. The local ESS and site controller should be designed such that the multiple objectives of financial benefit and security and resilience are balanced based on the current risks. Other work highlighted that synchronizing the emergency stop of many chargers across a power network might cause instability. The local ESS should then be further evaluated as a tool to mitigate rapid power fluctuations via intelligent control linked to charger operating state.

This project did not explore the software dependencies within EV ecosystem components. Other related work (e.g., the Grid Modernization Laboratory Consortium "Firmware Command and Control" project) is studying these aspects for other energy system components. More research is needed on how to properly maintain and share access to an EVSE-specific software bill of materials to avoid inadvertently introducing potentially damaging software during development and production. In addition, the software bill of materials could improve the response efficiency and speed when new threats arise.

References

Hasandka, Adarsh, Joshua Rivera, Joshua Van Natta. 2020. "NREL's Cyber-Energy Emulation Platform for Research and System Visualization." Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-74142. https://www.nrel.gov/docs/fy20osti/74142.pdf.

Hupp, William, Adarsh Hasandka, Ricardo Siqueria de Carvalho, and Danish Saleem. 2020. "ModuleOT: A Hardware Security Module for Operational Technology—Preprint." Presented at the IEEE Texas Power and Energy Conference (TPEC), College Station, Texas, February 6−7, 2020. NREL/CP-5R00-74697. https://www.nrel.gov/docs/fy20osti/74697.pdf.

The White House. "Fact Sheet: Biden Administration Advances Electric Vehicle Charging Infrastructure." April 22, 2021. Washington, D.C. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-biden-administration-advances-electric-vehicle-charging-infrastructure/.

Bibliography

Sanghvi, Anuj, and Tony Markel. 2021. "Cybersecurity for Electric Vehicle Fast-Charging Infrastructure: Preprint." Presented at the IEEE Transportation Electrification Conference and Expo (ITEC), June 21–25, 2021. NREL/CP-5R00-75236. https://www.nrel.gov/docs/fy21osti/75236.pdf.