

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

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

Contract No. DE-AC36-08GO28308



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. <u>https://www.nrel.gov/docs/fy22osti/80799.pdf</u>.

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

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

Contract No. DE-AC36-08GO28308

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.

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

U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via www.OSTI.gov.

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

NREL prints on paper that contains recycled content.

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

Intr	oduc	tion	.1
1	Distr	ibuted Energy Resource-Related High-Consequence Events	. 3
2	Cybe	er Emulation Environment for Fast Charging Scenarios	. 4
	2.1	Site Controller	. 5
	2.2	OCPP Server and Client	. 6
	2.3	Battery System Model	. 6
	2.4	Power System and Photovoltaic Implementation	.6
	2.5	Electric Vehicle Fast Charger (Hardware-in-the-Loop and Simulated)	. 7
3	Atta	cks and Mitigations	. 8
	3.1	Scenario 1—Energy Storage System Man-in-the-Middle Attack	. 8
	3.2	Scenario 2—Site Meter Malicious Command Injection	11
	3.3	Scenario 3—Message Translation Exchange Hijacking	14
4	Cond	clusions	16
5	Reco	ommended Next Steps	17
Ref	erend	Ces	19
Bib	liogra	aphy	20

List of Figures

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	on e 2
	∠
Figure 2. Detailed fast charger station interconnection diagram for testing cyberattack mitigations	4
Figure 3. Logic diagram of the site controller at a fast charging station	5
Figure 4. Power system configuration represented using OpenDSS	7
Figure 5. Site controller updating the ESS	8
Figure 6. Attacker conducts asset enumeration via unencrypted data exchange using Wireshark	9
Figure 7. MITMProxy successfully capturing the packet from the site controller to be manipulated	9
Figure 8. Manipulated values from the attacker successfully sent to the local ESS	10
Figure 9. Site controller updating the ESS using HTTPS	10
Figure 10. Encrypted communications between the ESS and the site controller as seen by the attacker	
node via Wireshark	11
Figure 11. Normal communications between the site meter and the site controller via Modbus (baseline	e)
	. 12
Figure 12. Malicious Modbus command injection	12
Figure 13. Communications encrypted using TLS enabled by Module-OT	13
Figure 14. Emulation environment diagram with Module-OT mitigations applied (purple) enabling	
Modbus encryption	13
Figure 15. OCPP server gets heartbeat message from fast charger of 120, sniffed by the attacker	14
Figure 16. Modification of heartbeat values (proof of concept)	15
Figure 17. Manipulated value of heartbeat 199 injected with MITMProxy	15
Figure 18. A layered security architecture for EV charging stations	17

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 systemlevel 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 (*essetpoint*) to 30 and the target state of charge (*targetsoc*) to 0.9 (90% state of charge).

H	•	5	0.0	9002	27687	72	172.	.16.	.10	.2	17	2.1	6.10	.3		HTT		L03 F	OST	/co	ntrol	lerup	date.	∕HT	TP/1.	1	(app	olica	tion.	/jsor)
		6	0.0	0003	80297	14	172.	.16.	.10	. 3	17.	2.1	6.10	.2		TCP		66 8	080	→ 5	1062	[ACK]	Seq	=1 A	ck=26	57 V	/in=6	4896	Len	=0 15	val
		7	0.0	9014	13586	58	172.	.16.	.10	.3	17	2.1	6.10	1.2		TCP		66 8	080	→ 5	1062	[ACK]	Seq	=1 A	ck=36)4 V	lin=6	64896	i Len	=0 TS	ival
		8	0.0	9014	16504	15	172.	.16.	.10	.3	17	2.1	6.10	1.2		TCP		83 8	080	→ 5	1062	[PSH,	ACK	Se	q=1 A	Ack=	:304	Win=	6489	6 Ler	1=17
		9	0.0	9014	18678	38	172.	.16.	.10	. 2	17	2.1	6.10	1.3		TCP		66 5	1062		8080	[ACK]	Seq	=304	Ack=	:18	Win=	6425	6 Le	n=0 T	Sva
		10	0.0	9015	53333	37	172.	.16.	.10	. 3	17	2.1	6.10	1.2		TCP		103 8	080	→ 5	1062	[PSH,	ACK	Se	q=18	Ack	(=304	4 Wir	=648	96 Le	en=3
		11	0.0	0015	55311	10	172.	.16.	. 10	. 2	17	2.1	6.10	1.3		TCP		66 5	1062	-	8080	[ACK]	Seq	=304	Ack=	:55	Win=	6425	6 Le	n=0 T	Sva
-	-	12	0.0	9015	58210	51	172.	.16.	.10	.3	17	2.1	6.10	1.2		HTT	P :	L77 H	TTP/	1.0	200	OK (text	htm	1)						
		13	0.0	9016	51392	28	172.	.16.	.10	. 2	17	2.1	6.10	1.3		TCP		66 5	1062	-	8080	[ACK]	Seq:	=304	Ack=	166	6 Wir	1=642	256 L	en=0	TSv
		14	0.0	9016	69686	58	172.	. 16 .	.10	. 3	17	2.1	6.10	1.2		TCP		66 8	080	- 5	1062	[FIN,	ACK	Se	q=166	S Ac	:k=36	94 W	.n=64	896 L	.en=
		15	0.0	9021	17039	91	172.	.16.	. 10	. 2	17	2.1	6.16	1.3		TCP		66 5	1062	-	8080	[FIN,	ACK	Se	q=304	A	:K=16	57 W3	.n=64	256 L	en=
18	-	16	0.0	9022	22012	25	172.	. 16 .	. 10	.3	17	2.1	6.10	.2		TCP		66 8	080	→ 5	1062	[ACK]	Seq	=167	Ack=	:305	5 Wir	1=648	96 L	en=0	TSV
		17	5.2	2004	19405	54	Vmwa	are_	_8b	:13:30	Vm	war	e_8t	:8b	:e1	ARP		60 W	ho h	as	172.1	6.10.	37 Te	211	172.1	16.1	10.2				
		18	5.2	2005	7427	76	Vmwa	are	8b:	:8b:e1	. Vm	war	e 8t	:13	:3c	ARP		60 1	72.1	6.1	0.3 i	s at	00:50):56	:8b:8	Bb:€	1				
4																															_
		Ur	rgei	nt	poin	ter	r: 0)																							
	•	Op	oti	ons	: (1	2 1	byte	s),	No	-Oper	atio	on	(NOF), 1	0-0	per	ation	(NC	P),	Tim	estan	nps									
ι.	•	[5	SEQ.	/AC	K an	aly	ysis]																							
ι.	•	[]	Tim	est	amps]																									
		TO	CP	pay.	load	(3	37 b	yte	s)																						
		тс	CP :	seg	ment	dá	ata	(37	by	tes)		14	-	a seco		a															
	r.	2 0	000	1000	hlor	(T	CD (Com	noni	10 / 20	12 h	uto	c1.	#11	266	<u> </u>	5/27	1			2	-	1.0000								_
	900	Θ	00	50	56	8b	8b	e1	00	50 5	6 8	b 1	.3 3	C 08	00	45	00	· P\	* * * *	PV	1	- E -									
	901	Θ	00	59	6f	91	40	00	40	06 5	e d	a a	ic 1	0 0a	02	ac	10	·Yo	.6.6	<u> </u>	· · · · · ·										
1	902	Θ	0a	03	c7	76	1f	90	6b	99 9	d 2	4 8	0 9	1 ea	32	80	18		V···k	(\$	2 · ·									
1	903	Θ	01	f6	3a	fc	00	00	01	01 0	8 0	a d	13 6	5 33	6e	c9	f8	4.41	* * * *	× 1	· · e3	n · ·									
(904	0	44	6d	7b	22	65	73	73	73 6	5 7	4 7	0 6	f 69	6e	74	22	Dm{	"ess	is e	etpoin	nt"									
			2.0	20	22	20	2.0	20	22	74 6	1 7	2 6	7 6	5 74	73	6f	63		0 "	+ -	rant	202		_							
	905	0	3a	20	33	30	ZC	20	22	14 0	т I	2 0						• •	0,	La	irger	300			At	tac	or.				
	905 906	0	3a 22	20 3a	20	30	2c 2e	39	7d	74 0	1 1	2 0			10	01		÷:`	0.9}	La	irget	300			At	tacl	ker				

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.

Flow Details			
2021-07-28 01:42:	53 POST http://172.16.10.3:8 ← 200 OK text/html 1	080/controllerupdate/ 1b 12ms	
l.	Request	Response	Detail
Host: User-Agent: Accept-Encoding: Accept: Connection: cache-control: content-type: authorization:	172.16.10.3:8080 python-requests/2.18.4 gzip, deflate */* keep-alive no-cache application/json bearer		Attacker
JSON			[n:auto]
{ "esssetpoint" "targetsoc": }	: 30, 0.9		

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.

DCFC Setpoint: 50 The Modbus Register of Campu	is meter is: True	
cut here	is never to. If de	
We are at 4200 kW. We will t		
Campus net load: 4200 [kW]	Site Controller	
This is the current Campus r	1ec 1080. 7200	
We are now setting the setor	aint	
state of charge ta i orsoon	TIJETTER	
The Modbus Register of Campu	us meter is: True	
We are at 0 kW. We will try	to stop charging battery	
Campus net load: 4200 [kW]		
State of Charge is : 0.50044	14452714202	
ine modbus register of campu	JS Meter is: Irue	
Listening on http://127.0.0.1:8080/		
Hit Ctrl-C to quit.		
Connecting to Modbus Server		
Voltage: 399.665915072 Volts SoC:	0.5000555565892753 Seconds: 1 Rate:	327.6 Amp:
Voltage: 399.668714994 Volts SoC:	0.5001111131785505 Seconds: 2 Rate:	327.6 Amp:
Voltage: 399.671515173 Volts SoC:	Battery	327.6 Amp:
Voltage: 399.674315607 Volts SoC:	0.500222226357101 Seconds: 4 Kate:	327.6 Amps
Voltage: 399.677116295 Volts SoC:	0.5002777829463763 Seconds: 5 Rate:	327.6 Amp:
Voltage: 399.679917233 Volts SoC:	0.5003333395356515 Seconds: 6 Rate:	327.6 Amp:
Reporting to Site Controller that w	e have:	
0.5003333395356515 127 0 0 1 [27 Jul (2021 16:22:04	1 "CET coontrollorundate: HTTP:// 0" 20	0.27
We got posted with:		
{'esssetpoint': 0, 'targetsoc': 0.9	}	
We got set with:		
0.9		
127.0.0.1 [27/Ju1/2021 16:32:04 Voltage: 399.682718419 Volts SoC:	J "PUST /controllerupdate/ HTTP/1.0" 2 0.5003888961249268 Seconds: 7 Bate:	00 11 0.0 Amps
Tanget State of Change' A 9		
Current State of Charge: 0.500388899	61249268	
Voltage: 398.506827639 Volts SoC:	0.5003888961249268 Seconds: 8 Rate:	0.0 Amps

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).

lo.	Time	Course	Destination	Protocol	Leoph lofe
10.	6 0 003008060	172 16 10	2 172 16 10 3	TCP	Length Into 74 48774 - 442 TEVNI Son-0 Win-64240 Lan-0 MSS-1460 SACK DEPM-1 TSval-3515168775 TSocr-0 WS-128
	7 0 004014510	172 16 10	3 172 16 10 2	TCP	74 443 _ 46774 [SYN ACK] Samo Ark-1 Win-65160 Lan-0 MS-1466 SACK DEPM-1 TSVa1-116681392 TSpar-35151
	8 0.004035195	172.16.10.	2 172.16.10.3	TCP	66 46774 - 443 [ACK] Sep=1 Ack=1 Win=64256 Len=0 TSval=3515168725 TSecr=116681382
	9 0.004895571	172.16.10.	2 172.16.10.3	TLSv1.2	583 Client Hello
	10 0.004915116	172.16.10.	3 172.16.10.2	TCP	66 443 - 46774 [ACK] Seg=1 Ack=518 Win=64768 Len=0 TSval=116681383 TSecr=3515168726
	11 0.005258130	172.16.10.	3 172.16.10.2	TLSv1.2	1552 Server Hello, Certificate, Server Key Exchange, Server Hello Done
	12 0.005276565	172.16.10.	2 172.16.10.3	TCP	66 46772 → 443 [ACK] Seq=518 Ack=1487 Win=62848 Len=0 TSval=3515168726 TSecr=116681384
	13 0.005729121	172.16.10.	2 172.16.10.3	TLSv1.2	159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	14 0.006165283	172.16.10.	3 172.16.10.2	TLSv1.2	1552 Server Hello, Certificate, Server Key Exchange, Server Hello Done
	15 0.006206088	172.16.10.	2 172.16.10.3	TCP	66 46774 → 443 [ACK] Seq=518 Ack=1487 Win=62848 Len=0 TSval=3515168727 TSecr=116681385
	16 0.006375007	172.16.10.	3 172.16.10.2	TLSv1.2	308 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
	40 0 000011000	170 46 40	9 4 79 46 40 9	TL Dut 0	EF 46172 MT LACK FOR St. Acket 720 Mark440 Long Truck 284460200 Tracet 46604000
	16 0.000044328	1/2.10.10.	2 1/2.10.10.3	11.591.2	SII Appileation Data
	20 0.008421912	172.16.10.	3 172.16.10.2	TLSv1.2	308 New Session Ticket, Change Clipher Spec, Encrypted Handshake Message
	21 0.008466242	172.16.10.	2 172.16.10.3	TCP	66 46774 - 443 [ACK] Seg=611 Ack=1729 Win=64128 Len=0 TSval=3515168730 TSecr=116681387
	22 0.008591142	172.16.10.	3 172.16.10.2	TLSv1.2	285 Application Data
	PP ALAGODOPTIC				200 Mpp12002101 Data
	23 0.008636575	172.16.10.	2 172.16.10.3	TCP	66 46772 - 443 [ACK] Seg=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387
Era	23 0.008636575	172.16.10.	2 172.16.10.3	TCP	109 Apploation Pattern 66 46772 - 443 [ACK] Sea=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387
Fra Eth Int Tra Sec	23 0.008636575 me 18: 311 byte ernet II, Src: ernet Protocol insmission Cont cure Sockets La	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer	2 172.16.10.3 2488 bits), 3 3:3c (00:50:50 Src: 172.16.10 , Src Port: 40	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst	66 46772 - 443 (ACK) Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 c), Dst: Vmware_8b:8b:e1 (00:50:56:8b:8b:e1) 172.16.10.3 Port: 443, Seq: 611, Ack: 1729, Len: 245
Fra Ett Int Tra Sec	23 0.008636575 mme 18: 311 bytm ernet II, Src: ernet Protocol insmission Cont ure Sockets Lay 00 50 56 8b 8	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50	2 172.16.10.3 2488 bits), 3: 3:3c (00:50:5/ Src: 172.16.11 , Src Port: 4/ 56 8b 13 3c	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 0	06 46772 - 443 [ACK] Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 c), DSt: Vmware.8b:8b:e1 (90:50:56:8b:8b:e1) 172.16.10.3 Port: 443, Seq: 611, Ack: 1729, Len: 245 00 PVP V- <e-< td=""></e-<>
 Fra Eth Int Tra Sec 0000 0010 	23 0.008636575 ime 18: 311 byte iernet II, Src: iernet Protocol insmission Cont: iure Sockets Lay 00 50 56 8b 8 01 29 ab 90 4	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50 10 00 40 06	2 172.16.10.3 2488 bits), 3 3:3c (00:50:5 Src: 172.16.1 , Src Port: 4 56 8b 13 3c 22 19 ac 10	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 6 0a 02 ac 1	06 46772 - 443 JACK1 Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0
 Fra Eth Int Tra Sec 0000 0010 0020 	23 0.008636575 mme 18: 311 byt: mernet II, Src: ernet Protocol ismission Cont: ure Sockets Lav 00 50 56 8b 8 01 29 ab 90 4 0a 03 b6 b4 0	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50 10 00 40 06 11 bb 55 df	2 172.16.10.3 2488 bits), 3: 3:3c (00:50:5: Src: 172.16.14 , Src Port: 4 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 0 08 02 ac 1 a9 a3 80 1	06 46772 - 443 443 Kacki Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 () DSt: Vmware.8b:8b:e1 (00:50:56:8b:8b:e1) 172.16.10.3 Port: 443, Seq: 611, Ack: 1729, Len: 245 POV PV - PV - C. 00 PV - PV - C. - - - 10 -) - Q. - - - -
 Fra Etra Tra Sec 0000 0010 0020 0030 	23 0.008636575 me 18: 311 bytr iernet II, Src: ernet Protocol insmission Cont ure Sockets La 00 50 56 8b 8 01 29 ab 90 4 0 80 36 b4 0 01 f5 a4 df 0 01 75 20 0	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50 10 00 40 06 11 bb 55 df 00 00 01 01	2 172.16.10.3 2488 bits), 3 3:3c (00:50:50 Src: 172.16.11 , Src Port: 40 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91 08 0a d1 85	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 0 08 02 ac 1 a9 a3 80 1 37 d8 06 f	100 Application outer 66 46772 - 443 [ACK] Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0
 Fra Etr Int Tra Sec 0000 0010 0020 0030 0040 0050 	23 0.008636575 mme 18: 311 byt: ternet II, Src: ternet Protocol insmission Cont: ture Sockets Lav 00 50 56 8b 8 01 29 ab 90 4 0a 03 b6 b4 0 01 f5 a4 df 0 6a a9 17 03 0 b c7 4 f7 3	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50 16 06 40 06 10 bb 55 df 10 60 61 01 13 00 f0 85 6 60	2 172.16.10.3 2488 bits), 3 3;3c (00:50:55 Src: 172.16.11 , Src Port: 4 55 8b 13 3c 22 19 ac 10 cf 1f 5a 91 08 0a d1 85 99 11 b6 13	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 0 00 02 ac 1 a9 a3 80 1 37 d8 06 f 8e b6 ea a 55 de 6 5	00 PV
 Fra Etr Int Tra Sec 0000 0010 0020 0030 0040 0040 0040 0040 0040 0040 	23 0.008636575 mme 18: 311 byt: ernet II, Src: ernet Protocol insmission Cont: ure Sockets La 00 50 56 8b 8 01 29 ab 96 4 0 a 03 b6 b4 0 01 f5 a4 df 0 01 f5 a4 df 0 ab c7 b4 f7 3 20 c7 2 10 b	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 3b e1 00 50 0 00 40 06 11 bb 55 df 10 00 60 1 01 30 00 f0 85 44 6b 25 80 15 71 ec	2 172.16.10.3 2488 bits), 3 3:3c (00:50:5) Src: 172.16.11 , Src Port: 4 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91 08 0a d1 85 99 11 b6 13 5d 16 23 b7	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 6 0a 02 ac 1 a9 a3 80 1 37 d8 06 f 8e b6 ea a c5 dc 65 b 2 c 55 55	069 694 6772 -443 JACK1 Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 0 0.51: Ymware.8b:8b:e1 (90:50:56:8b:8b:e1) 172.16.10.3 Port: 443, Seq: 611. Ack: 172.9, Len: 245 00
 Fra Etr Int Tra Sec 0000 0010 0020 0030 0030 0030 0030 0050 0050	23 0.008636575 me 18: 311 byte lernet II, Src: ernet Protocol insmission Cont ure Sockets La: 00 50 56 8b 8 01 29 ab 90 4 0a 03 b6 b4 0 01 f5 a4 df 0 6a a9 17 03 0 01 f5 a4 df 0 6a c7 b4 f7 3 80 e5 73 16 b 1 29 41 63 5	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer b e1 00 50 10 06 40 06 10 b5 55 df 10 00 01 01 13 00 70 85 14 6b 25 80 na 16 71 ec 3 e0 8f 10	2 172.16.10.3 2488 bits), 3 3;3c (00:50:50 5rc: 172.16.1; , Src Port: 4/ 56 8b 13 3c 22 19 ac 10 68 0a d1 85 99 11 b6 13 54 16 23 57 34 2d 16 7f 7 a 2 0a 15	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 0 09 02 ac 1 a9 a3 80 1 37 d8 06 f 8e b6 ea a c5 dc 65 t 22 68 55 2 26 55 2 f 6 53 2 f	069 PVP VP VP 09 PVP VP VP 09 PVP V
 Fra Ett Int Tra Sec 0000 0010 0010	23 0.000636575 me 18: 311 byt: rernet II, Src: rernet Protocol nsmission Cont. ure Sockets Lav 00 50 56 8b 8 61 29 ab 90 4 60 63 06 46 6 61 65 a4 df 6 ab 67 47 73 3 ab 65 73 10 b al 29 41 63 5 99 99 54 26 5	172.16.10. es on wire (Vmware 8b:1 Version 4, rol Protocol yer 3b e1 00 50 10 00 40 06 11 bb 55 df 10 00 00 01 01 33 00 f0 85 44 6b 25 80 a 16 71 ec 33 e0 8f 10 f7 70 44 08	2 172.16.10.3 2488 bits), 3 3:3c (00:56:55 Src: 172.16.1; , Src Port: 4/ 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91 08 0a d1 85 99 11 b6 13 5d 16 23 b7 44 2d 16 7f f7 a2 0a 15 24 5d 4 1f	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 6 0a 02 ac 1 9 a3 80 1 37 d8 06 f 8e b6 ea a c5 dc 65 5 22 68 55 5 46 53 2f 6 2e e5 b6 2	069 6646772 - 443 fAcK1 Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 0 0 interface 0 0 0 interface 0
 Fra Ett Int Tra Sec 0000 0010 0020 0030 0030 0040 0050 0050 0070 0080 0090 	23 0.000636575 mme 18: 311 byt: ternet II, Src: turre Sockets La 00 50 50 56 8b 8 01 29 ab 99 4 0a 03 b6 b4 0a 03 b6 b4 0a 03 b6 b4 0a 17 53 d df 6a ap 17 93 0b 75 73 10 b 12 9 57 33 04 13 5 89 99 5d 20 5 89 99 5d 20 5 13 74	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 3b e1 00 50 10 60 40 06 10 bb 55 df 10 00 01 01 13 00 f0 00 11 01 13 00 f0 82 58 14 6b 25 80 13 00 f1 71 ec 3 00 87 10 16 71 ec 3 0 87 10 16 71 ec 16 71 ec 16 29 80 bb	2 172.16.10.3 2488 bits), 3 3:3c (00:63:5 Src: 172.16.11 , Src Port: 4/ 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91 88 0a d1 85 99 11 b6 13 5d 16 23 b7 34 2d 16 7f 7 a2 0a 15 a2 b5 d4 1f 7 a2 0a 15 48 8a 18 4d	TCP 11 bytes c 6:8b:13:3c 0.2, Dst: 6772, Dst 08 00 45 6 0a 02 ac 1 a9 a3 80 1 37 d8 06 f 8e b6 ea a c5 dc 65 b 22 68 55 5 46 53 2f 6 2e e5 b6 2 2e e5 b6 5 2e a 0b 5e 3	064 6772 - 443 / JACK Seq=856 Ack=1948 Win=64128 Len=0 TSval=3515168730 TSecr=116681387 captured (2488 bits) on interface 0 c), D5: Vimware &D:80:801 (00:50:56:80:80:e1) 172.16.16.3 Port: 443, Seq: 611, Ack: 1729, Len: 245 00 PV P V <- E
 Fra Etr Int Tra Sec 0000 0010 0020 0010 0020 0010 0020 0010 	23 0.000636575 me 18: 311 byt. ternet II, Src: ternet Protocol nsmission Cont. ture Sockets La 00 50 56 8b 8 01 59 40 90 40 ab c7 54 f7 3 ab e5 73 10 b a1 29 41 63 5 09 99 54 20 5 dd 89 21 37 4 73 3 dd 89 21 37 4 13 20 30 7	172.16.10. es on wire (Vmware_8b:1 Version 4, rol Protocol yer 8b e1 00 50 00 00 40 06 11 bb 55 df 10 00 60 40 06 11 bb 55 df 10 00 60 40 10 10 00 60 85 14 6b 25 80 a 16 71 ec 33 e0 8f 10 77 0 44 08 id 29 e8 0b be be 8f 94	2 172.16.10.3 2488 bits), 3: 3:3c (00:50:5) Src: 172.16.11 , Src Port: 4/ 56 8b 13 3c 22 19 ac 10 cf 1f 5a 91 08 0a d1 85 99 11 b6 13 5d 16 23 b7 3d 21 66 7f f7 a2 0a 15 62 b5 d4 1f 68 a8 18 4d	TCP 11 bytes c 6:8b:13:3C 0.2, Dst: 6772, Dst 08 00 45 0 09 02 ac 1 37 d8 06 f 8e b6 ea a 37 d8 06 f 8e b6 ea a 55 dc 65 b 22 e5 56 2 0a 05 5e 3 2e e5 b6 2 0a 05 5e 3 10 5c 4c 5	00 PV P V - < - E

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.

No.		Time	Source	Destination	Protocol	Length Info
	739	71.113619	Edgecore_78:4a:e4	PVST+	STP	64 RST, Root = 32768/0/1c:ea:0b:23:10:5e Cost = 500 Port = 0x8002
	740	71.724822	10.79.127.31	10.79.127.30	TCP	109 35792 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=237 Len=43 TSval=65241217
	741	71.726576	10.79.127.30	10.79.127.31	TCP	133 8000 → 35792 [PSH, ACK] Seq=1 Ack=44 Win=1590 Len=67 TSval=290872(
	742	71.727022	10.79.127.31	10.79.127.30	TCP	66 35792 → 8000 [ACK] Seq=44 Ack=68 Win=237 Len=0 TSval=65241218 TSec
	743	72.227692	10.79.127.30	10.79.127.70	MQTT	68 Ping Request
	744	72.227864	10.79.127.70	10.79.127.30	MQTT	68 Ping Response
	745	72.227926	10.79.127.30	10.79.127.70	TCP	66 45384 - 1883 [ACK] Seq=5 Ack=5 Win=502 Len=0 TSval=128283263 TSec
	746	72.265771	10.79.127.7	10.79.127.152	TCP	74 55985 → 502 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
	747	72.266618	10.79.127.152	10.79.127.7	TCP	74 502 - 55985 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_F
	748	72.266638	10.79.127.7	10.79.127.152	TCP	66 55985 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1866932558 TSc
_						
	750	72.266984	10.79.127.152	10.79.127.7	TCP	66 502 → 55985 [ACK] Seq=1 Ack=13 Win=29056 Len=0 TSval=555985 25 TSc
	751	72.267545	10.79.127.152	10.79.127.7	Modbus/TCP	76 Response: Trans: 1; Unit: 1, Func: 2: Read Discrete Input:
						2559
	753	72.267735	10.79.127.7	10.79.127.152	TCP	66 55985 → 502 [FIN, ACK] Seg=13 Ack=11 Win=64256 Len=0 TSval=186693;
	754	72.310383	10.79.127.152	10.79.127.7	TCP	66 502 → 55985 [ACK] Seg=11 Ack=14 Win=29056 Len=0 TSval=555985369 TS
	755	72.628738	10.79.127.7	10.79.127.152	TCP	74 39587 - 502 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
	756	72.629586	10.79.127.152	10.79.127.7	TCP	74 502 - 39587 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_
	757	72.629625	10.79.127.7	10.79.127.152	TCP	66 39587 → 502 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=1866932921 TSc
	758	72.629743	10.79.127.7	10,79,127,152	Modbus/TCP	78 Ouery: Trans: 1: Unit: 1. Func: 2: Read Discrete Inputs

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

5998 617.654832 5999 617.655099 6000 617.655271 6001 617.655275 6002 617.65532 6003 617.65532 6003 617.698872 6451 663.155039 6452 663.195340	10.79.127.99 10.79.127.152 10.79.127.152 10.79.127.99 10.79.127.99 10.79.127.99 10.79.127.99 10.79.127.99 10.79.127.2	10.79.127.152 10.79.127.99 10.79.127.99 10.79.127.152 10.79.127.152 10.79.127.152 10.79.127.199 10.20.6.10 10.79.127.99	P Modbus/TCP TCP Modbus/TCP TCP TCP TCP TCP TCP TCP TCP	78 66 78 66 66 66 74 102 74	Query: 502 → 4463: Response: 44631 → 500 44631 → 500 502 → 4463: 55826 → 53 Destination 41300 = 53	Trans: 1 [ACK] Trans: 2 [ACK] 2 [FIN, 1 [ACK] [SYN] S n unreac	0; Unit Seq=1 Ack= 0; Unit Seq=13 Ack ACK] Seq=1 Seq=13 Ack eq=0 Win=6 thable (Net	: 1, Func 13 Win=29050 : 1, Func =13 Win=642! 3 Ack=13 Win =14 Win=290! 4240 Len=0 M WOFK UNFeac	: 5: W 5 Len=0 : 5: W 56 Len=0 n=64256 56 Len=0 455=1460 hable)	rite Sing TSval=5643 rite Sing TSval=103 Len=0 TSva TSval=564 SACK_PERM	le Coil 383530 TSe 10 Coil 35475158 - al=103547; 4383574 TS 4=1 TSval- 41 TSval-
Unit Identifier: • Modbus <u>IRequest Frame:</u> [Time from reque Reference Number Data: 0000	: 1 <u>5998]</u> sst: 0.000439000 see r: 3	conds]		0							
00000 00 50 56 8b 79 0010 00 40 a0 a0 40 0020 7f 63 01 f6 ac 0030 00 e3 59 b2 00 0040 18 d5 00 00 00 00	f0 d4 9e 6d 57 3f 00 40 06 86 7e 0a 57 cc e4 e0 df c9 00 01 01 08 0a 21 00 00 6 01 05 0a	d6 08 00 45 00 4f 7f 98 0a 4f 2f 98 cf 80 18 a3 cf 2a 3d b8 03 00 00	PV y mW? E. @ @ @ ~00 C	0							

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.

854 120.600760	10.79.127.50	10.79.127.51	TCP	60 51890 → 8000 [RST] Seg=1 Win=0 Len=0
855 120.638690	10.79.127.51	10.79.127.50	TCP	60 42370 → 8000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
856 120.638768	10.79.127.50	10.79.127.51	TCP	60 8000 → 42370 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
857 120.639154	10.79.127.51	10.79.127.50	TCP	60 42370 → 8000 [RST] Seg=1 Win=0 Len=0
858 120.700028	10.79.127.50	10.79.127.51	TCP	60 51891 → 8000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
859 120.700651	10.79.127.51	10.79.127.50	TCP	60 8000 → 51891 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
860 120.700696	10.79.127.50	10.79.127.51	TCP	60 51891 → 8000 [RST] Seq=1 Win=0 Len=0
861 120.738886	10.79.127.51	10.79.127.50	TCP	60 42371 → 8000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
862 120.738979	10.79.127.50	10.79.127.51	TCP	60 8000 → 42371 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
863 120.739337	10.79.127.51	10.79.127.50	TCP	60 42371 → 8000 [RST] Seq=1 Win=0 Len=0
865 121.292979	10.79.127.51	10.79.127.50	TCP	66 38624 → 8000 [ACK] Seq=389 Ack=2760 Win=34816 Len=0 TSval=2569108257 TSecr=22207698
866 121.327446	10 79 127 51	10 79 127 50	TLSv1 3	106 Application Data
	101/0112/101	101/0112/100	1000210	100 Applicación baca
	101751127151	101/0112/100	1000110	
868 121.347956	VMware_8b:d8:75	Broadcast	ARP	60 Who has 10.79.127.51? Tell 10.79.127.50
868 121.347956 869 121.348284	VMware_8b:d8:75 Teltroni_0b:08:3b	Broadcast VMware_8b:d8:75	ARP	60 Mph has 10.79,127.51? Tell 10.79,127.50 61 00.79.127.51 is at 00:04:18:0b:08:3b
868 121.347956 869 121.348284 870 121.398615	V∿ware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b	Broadcast VMware_8b:d8:75 Broadcast	ARP ARP ARP	60 Hpp1ct100 510 60 Hho has 10.79.127.51? Tell 10.79.127.50 60 10.79.127.51 is at 00:04:18:0b:08:3b 66 Who has 10.79.127.50? Tell 10.79.127.51
868 121.347956 869 121.348284 870 121.398615 871 121.398685	VMware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b VMware_8b:d8:75	Broadcast VMware_8b:d8:75 Broadcast Teltroni_0b:08:3b	ARP ARP ARP ARP ARP	60 Who has 10.79.127.51? Tell 10.79.127.50 60 Uho has 10.79.127.51 is at 00.04:18:00:08:30 60 Who has 10.79.127.50? Tell 10.79.127.51 60 10.79.127.50 is at 00:50:56:80:d8:75
868 121.347956 869 121.348284 870 121.398615 871 121.39865 872 121.599941	VMware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b VMware_8b:d8:75 10.79.127.50	Broadcast WWware_8b:08:75 Broadcast Teltroni_0b:08:3b 10.79.127.51	ARP ARP ARP ARP TCP	60 Who has 10.79.127.51? Tell 10.79.127.50 60 10.79.127.51 is at 00:04:18:0b:08:3b 60 Who has 10.79.127.59? Tell 10.79.127.51 60 10.79.127.50 is at 00:50:56:8b:08:75 65 05857 + 8000 [SVN] Seq=0 Wim=1024 Len=0 MSS=1460
868 121.347956 869 121.348284 870 121.398615 871 121.398685 872 121.599941 873 121.600690	VMware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b VMware_8b:d8:75 10.79.127.50 10.79.127.51	Broadcast WHware_8b:d8:75 Broadcast Teltroni_0b:08:3b 10.79.127.51 10.79.127.50	ARP ARP ARP ARP TCP TCP	60 Hpp1101100 J010 60 Hho has 10.79.127.51? Tell 10.79.127.50 60 10.79.127.51 is at 00:04:18:0b:08:3b 66 Who has 10.79.127.50 is at 00:50:56:8b:d8:75 60 58557 + 8000 (SYN] Seq=0 Hin=1024 Len=0 MSS=1460 60 8000 + 58557 [SVN] ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
868 121.347956 869 121.348284 870 121.398615 871 121.398685 872 121.599941 873 121.600690 874 121.600690	Whare_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b Whare_8b:d8:75 10.79.127.50 10.79.127.51 10.79.127.50	Broadcast Whware_Bb:d8:75 Broadcast Teltroni_Bb:08:3b 10.79.127.51 10.79.127.50 10.79.127.51	ARP ARP ARP ARP TCP TCP TCP	60 Who has 10.79.127.51? Tell 10.79.127.50 60 Ho. Phys.127.51 is at 00:04:18:00:08:3b 60 Who has 10.79.127.50? Tell 10.79.127.51 60 Ho. Phys.127.50? is at 00:59:55:05:048:75 60 58557 + 8000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 60 8000 + \$85557 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 60 8000 + \$85557 [SYN] Seq=0 Ack=1 Win=22200 Len=0 MSS=1460 60 58557 + 8000 [GYN] Seq=0 Ack=1 Win=2200 Len=0 MSS=1460
868 121.347956 869 121.348284 870 121.398615 871 121.398685 872 121.599941 873 121.600699 874 121.600731 875 121.650746	VWware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b VWware_8b:d8:75 10.79.127.50 10.79.127.51 10.79.127.50 10.79.127.51	Broadcast Wware_8b:d8:75 Broadcast Teltron1_0b:08:3b 10.79.127.51 10.79.127.59 10.79.127.59	ARP ARP ARP ARP TCP TCP TCP TCP	60 Who has 10.79.127.51? Tell 10.79.127.50 60 Ho.79.127.51 is at 00:04:18:0b:08:3b 60 Who has 10.79.127.50? Tell 10.79.127.51 60 Ho.79.127.50 is at 00:50:56:8b:d8:75 60 58557 + 8800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 60 88557 + 8800 [SYN] Seq=1 Win=0 Len=0 60 58557 4 + 8000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
868 121.347956 869 121.348284 870 121.398615 871 121.398615 872 121.599941 873 121.606699 874 121.606731 875 121.650746 876 121.658870	WWware_8b:d8:75 Teltroni_0b:08:3b Teltroni_0b:08:3b WWware_8b:d8:75 10.79.127.50 10.79.127.51 10.79.127.51 10.79.127.51 10.79.127.50	Broadcast Whware_Bb:d8:75 Broadcast Teltroni_0b:08:3b 10.79.127.51 10.79.127.59 10.79.127.50 10.79.127.50 10.79.127.51	ARP ARP ARP ARP TCP TCP TCP TCP TCP	60 Hho has 10.79.127.51? Tell 10.79.127.50 60 Hho has 10.79.127.51 is at 00:04:18:0b:08:3b 60 Hho has 10.79.127.50 is at 00:56:15:0b:08:75 60 58557 + 8000 [SYN] Seq=0 Hin=1024 Len=0 MSS=1460 60 58557 + 8000 [SYN] Seq=0 Hin=1024 Len=0 MSS=1460 60 58557 + 8000 [SYN] Seq=0 Hin=1024 Len=0 MSS=1460 60 50774 + 8000 [SYN] Seq=0 Hin=1024 Len=0 MSS=1460 60 600 + 50774 [SVN] ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 60 600 + 50774 [SVN] ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

> Frame 864: 130 bytes on wire (1040 bits). 130 bytes captured (1040 bits)

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.

7	766 2689.2892299 10.79.127.30	10.79.127.99	MQTT	177 Publish Message [Tritium/Configure]	
7	906 2737.8089811 10.79.127.30	10.79.127.99	MOTT	102 Connect Command	
7	914 2737.8179595 10.79.127.99	10.79.127.30	MÕTT	70 Connect Ack	
7	916 2737.8196416 10.79.127.30	10.79.127.99	MÕTT	143 Subscribe Request (id=63934) [Tritium/SetPower] [Tritium/GetSchedule] [Tritium/Rem	ote
7	919 2737.8217031 10.79.127.99	10.79.127.30	MÕTT	73 Subscribe Ack (id=63934)	
7	946 2745.7898266 10.79.127.30	10.79.127.99	MÕTT	177 Publish Message [Tritium/Configure]	
8	103 2805.8013980 10.79.127.30	10.79.127.99	MÕTT	68 Ping Reguest	
8	109 2805.8061750 10.79.127.99	10.79.127.30	MÕTT	68 Ping Response	
8	257 2865.8021003 10.79.127.30	10.79.127.99	MOTT	68 Ping Request	
8	262 2865,8069504 10,79,127,99	10.79.127.30	MOTT	68 Ping Response	
8	417 2925.8132276 10.79.127.30	10.79.127.99	MÕTT	68 Ping Request	
8	421 2925,8188889 10,79,127,99	10.79.127.30	MOTT	68 Ping Response	
				5 I	
▶ Fr:	ame 7766: 177 bytes on wire (1416 bit	s), 177 bytes capt	ured (1416 bi	bits) on interface 0	
► Et	ernet II, Src: Ymware 8b:a1:db (00:5	0:56:8b:a1:db), Ds	t: Vmware 8b:	b:79:f0 (00:50:56:8b:79:f0)	
▶ In ²	ernet Protocol Version 4, Src: 10,79	.127.30, Dst: 10.7	9.127.99		
Tr:	ansmission Control Protocol, Src Port	: 59670, Dst Port:	8080, Seq: 3	342, Ack: 67, Len: 111	
► Hv	ertext Transfer Protocol	,	· ·		
- MO	Telemetry Transport Protocol, Publis	h Message			
	Header Flags: 0x30, Message Type: Pu	blish Message, OoS	Level: At mo	nost once delivery (Fire and Forget)	
1 ·	Msg Len: 109				
	Topic Length: 17				
	Topic: Tritium/Configure				

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.



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. <u>https://www.nrel.gov/docs/fy20osti/74142.pdf</u>.

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. <u>https://www.nrel.gov/docs/fy20osti/74697.pdf</u>.

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

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. <u>https://www.nrel.gov/docs/fy21osti/75236.pdf</u>.

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