



Cybersecurity for Energy Delivery Systems

Cybersecurity for DER Systems

Dr. Chris Farnell NCREPT Managing Director

Dr. H. Alan Mantooth Distinguished Professor of Electrical Engineering

University of Arkansas

February 15, 2021















Presentation Outline



Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References















Presentation Outline



Cybersecurity for Energy Delivery Systems

* NCREPT Facility Overview

- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Carnegie Mellon University Electrical & Computer Engineering











Background:

NCREPT was formed in 2005 as a result of the 2003 Northeast Blackout and began investigating advanced power electronic solutions for the grid and transportation applications.

Research Focus:

Design and test advanced, solid-state solutions applicable to:

- Grid Reliability
- Power Interface Applications
- Transportation
- Energy Exploration
- Cybersecurity





JS

Associated Centers

Cybersecurity for Energy Delivery Systems

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

https://seedscenter.uark.edu/

GRid-connected Advanced Power Electronics Systems (GRAPES)

http://grapes.uark.edu/

Power Optimization of Electro-Thermal Systems (POETS)

https://poets-erc.org/















NCREPT Facility

Cybersecurity for Energy Delivery Systems

* 12,000 square foot building

* Cost-effective facility for businesses, national labs, and universities

* IEEE 1547 and UL 1741 testing



Parameter	Rating
Power	up to 6 MVA (3 x 2 MVA Circuits)
Medium Voltage	13.8 kV or 4.16 kV (line-line) Variable from 0 V to 15.18 kV
(ac)	
Low Voltages (ac)	480 V (line-line), Variable from 0 V to 528 V
	40 Hz to 70 Hz
Frequency	Values outside this range (up to 400 Hz or down to 20 Hz) are possible, but require de-rating
	300 A at 13.8 k/
Currents (ac)	1 000 A at 4 16 kV
	2 500 A at 480 V
Loads	Active loads fully programmable: Test energy is recirculated
20000	700 kW Resistive Load Bank
	Various Passive Components Available
Active Cooling	120 ton Chiller (420 kW Heat Rejection)
DC	2.25 MW (1500 Vdc / 1500 A) [Testing In Progress]
	750 kW (660 Vdc / 1.1 kA)
Dynamometer	100 kW with Overload Capability
	6,600 rpm @ 220 Nm

















NCREPT Control Room



Cybersecurity for Energy Delivery Systems



Carnegie Mellon University Electrical & Computer Engineering













NCREPT Bay Area



Cybersecurity for Energy Delivery Systems















interta Linterta





NCREPT One-line Configuration



Cybersecurity for Energy Delivery Systems





Examples of Previous Power Testing



Cybersecurity for Energy Delivery Systems





ROCK

Carnegie Mellon University Electrical & Computer Engineering





Electric Cooperatives of Arkansas The Local Energy Partners











Presentation Outline



Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Carnegie Mellon University Electrical & Computer Engineering











Cyber Testbed: Overview and Purpose



- Allows for Alpha testing in a realistic environment
- Simulated and real-world power flows
- Intra and Inter substation topologies emulated
- Utilize industry standard communication protocols
 - IEC 61850
 - ✓ DNP3
 - OPC UA
 - Modbus TCP
 - ✓ RS-232
- Utilize industry standard hardware devices
 - Real-Time Automation Controllers
 - Protection Relays
 - PLCs

Carnegie Mellon University

Electrical & Computer Engineering

- Security Gateways
- Various Network Devices











Testbed Assets: Hardware Systems



Cybersecurity for Energy Delivery Systems

- 480 V LV 3-Phase Breakers [PRs]
 - INCOM \triangleright
 - Modbus TCP (PXG900)
- 13.8 kV MV 3-Phase Breakers [PRs]
 - INCOM \geq
 - Modbus TCP (PXG900)
- Grid Simulator (750 kVA)
 - Modbus RTU \geq
- **Regenerative Load Banks (3 x 2 MVA)**
 - Modbus RTU \geq
- **PLC Cabinet and SCADA Control**
 - Modbus TCP \succ
 - **OPC UA**



Carnegie Mellon University Electrical & Computer Engineering











Utility XFRM (Testing 12.47kV (Y) - 480V (Y













Testbed Assets: Software Systems



Cybersecurity for Energy Delivery Systems

VMWare ESXI Hypervisor *

- **CheckPoint Security Management Server** \succ
- Kali Linux Pen-Testing Server \succ
- **GNS3 Network Simulator**
- **Virtual Routers and Switches** \triangleright
- **Simulation Resources**
 - Matlab \geq
 - **ETAP** \succ
 - **OpenDSS**
- **Remote Access** *
 - Linux and Windows Workstations \succ
 - **OpenVPN Servers** \succ











of Arkonsas







Testbed Assets: Cross-Domain Systems



Cybersecurity for Energy Delivery Systems

10.004

DPAL-RT

Available HIL/cHIL Systems at NCREPT

- Typhoon HIL
 - 6-Series
- * OPAL-RT
 - OP5030 and OP4520
- * dSPACE
 - MicroLabBox











1

IA PROCESSOR AN



Testing Example: SEEDS CHIL of 3-Phase Inverter *Cybersecurity for Energy Delivery Systems*





LabVIEW/Modbus Control Interface



OPAL-RT IDE and Real-Time Simulation Display

Electric Cooperatives of Arkansas Toy Local Energy Partners

INTERNATIONA

UNIVERSITY

Electrical & Computer Engineering

Testbed Assets: Cross-Domain Systems

of Arkansas

bur Local Energy Parmers

HIL Discussion / Benefits

- ***** Enables Multi-Feeder Simulation in Real-Time
- Analog/Digital I/O of Voltages/Currents
- * PTs/CTs of Protection Relays bypassed
- * IEC 61850 and DNP3 Communications
- * PR Feedback into Simulation

* Shows Greater Grid Impact (PNNL Demo)

UNIVERSITY

SEEDS Cyber-Physical Approach Cybersecurity for Energy Delivery Systems

- **Cyber-Physical Testing Approach**
- Real Power Flows
 - Grid Simulator
 - Regenerative Loads
 - Resistive Loads
 - Integrated Metering
- Emulated Networks
 - Inter and Intra Substation Comms
 - Virtual Hypervisor Networking
 - GNS3 Network Simulations
- Real-Time Simulations
 - Initiate large-scale Fault Scenarios
 - Emulate Fault currents Safely
 - Virtual Devices

Cybersecurity for Energy Delivery Systems

Available Networking Resources at NCREPT

- **Networks** •••
 - Four Physical Network Segments
 - Virtually Infinite Simulated Networks
- VMWare ESXI Hypervisor
 - GNS3 Network Simulator
 - Virtual Routers and Switches

Remote Access

- Linux and Windows Workstations
- OpenVPN Servers

🗸 signderfüsstate 20- K								
e i e g Brood Bros	TA martin Defection	Selectogroup Mar	internet 2003, Junior	4	- 0 à	Q, Seed	н.	0 1
Automatic Egos.						sugnition i su	- 1 (6 hot)	
Chemie C.	CL HEDL, Makers							
Construction C	EXECUTION AND A STATEMENT OF A STATE		n Trysca a Rafer Marce a Rafer	-	beautypaky dispressions mek dispressions mek dispressions mager excentionamic halp dispression halp dispression halp dispression halp dispression halp	Re Re Re Read Landon regrupping out O Re Re		
Build Means	T Annual State				-			
 Step, Joseph Rock and and State 	San Raan Su AD Raan Su AD Raan Su AD Raan Su AD Raan Su AD Raan Su AD	 Sept Sector sector from the sector sect			Subd Execute a content	Read Provide examples Provide examples Provide examples Provide examples Provide Pro		Canal -

Carnegie Mellon University Electrical & Computer Engineering

Protection Relays: SEL Resources

Cybersecurity for Energy Delivery Systems

20

FLORIDA

INTERNATIONAL

UNIVERSITY

Carnegie Mellon University Electrical & Computer Engineering

Real-Time Simulator: Protection Relay Design

Cybersecurity for Energy Delivery Systems

Carnegie Mellon University Electrical & Computer Engineering

Electric Cooperatives Your Local Energy Partners

Future Work: Integration

Cybersecurity for Energy Delivery Systems

- ***** Super Lab and DETER Lab Integration
- Investigate integration and collaboration
- Multi-Site and International Effort
- Unique Challenges for Resource Sharing

Source: https://ieeexplore.ieee.org/document/8458285

FIG 5 The Global RT Superlab participants and their interconnections. (Map courtesy of RWTH Aachen University.)

1410

DV, Maho Falls

EWEH Aschen University

Germany POLITO, Italy

andia National Laboratories

New Mexico MREL Golden, Colocado

Intersity of South Carolina

Columbia

Colorado Stain University

Fort Collins

Washington State Enjoymetry

Pullman

Table 1. The simulation models making up the Global RT Superlab

I Rasses

Series

Phase

125

Minia

Peers

INTH WSU

196, 94,

AREL CSU

INL POLITO

RND

150

caid

Western Systems Coordinating Council

international Council on Large Electric

Sentemo-High Voltage

nternational Council on Large Electric

Systems-Modium Voltage

Distribution grid

Distribution prid

IEE delabation hel volen

IEEE distribution test lorder

Simplified Consortium for Electric Reli-

ability Technology Solutions microgrid

Simulator

RIDS.

pphoon Hill

OP4LET

RTDS.

006-81

006-81

RTDS.

0748-81

0046-87

RUS

HE

PHEL for Philameters

PHIL for wind

Surbines

OIL network emu

Litten

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed

Distributed Energy Resources

- History and Projections
- Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

History and Projections: Solar Energy

Cybersecurity for Energy Delivery Systems

Carnegie Mellon University Electrical & Computer Engineering

History and Projections: Wind Energy

Cybersecurity for Energy Delivery Systems

Trends in wind energy generation [2]

25

UNIVERSITY

History and Projections: Energy Storage

Cybersecurity for Energy Delivery Systems

Central and distributed energy storage [3]

Example: Solar Installation

Cybersecurity for Energy Delivery Systems

- Solar Power is increasing in popularity with home owners and businesses.
 - > According to a recent article solar utilization has doubled since last year in Arkansas
 - It has increased more than 40x since 2007
- Local utilities are also installing solar arrays such as the "Ozark One" project.
 - > Residents may participate in this communal solar installation via purchasing shares.
- Communications between inverters and the utility are critical for optimal operations and accurate billing.

Community Solar Installation Credit: ozarksecc.com/one

Example: BESS Installation

Cybersecurity for Energy Delivery Systems

- With the increasing penetration of renewable energy, intermittent availability is a growing issue
- More efficient use of generation resources, such as peak shaving techniques, also contributes to sustainability
- Battery Energy Storage Systems (BESS) provide solutions to both of these issues
- Advanced Controls, Communication, and Coordination are needed for these systems to operate properly

Tesla PV Installation Credit: Tesla Diagram of Energy Generation and Storage Credit: GE 28

Carnegie Mellon University Electrical & Computer Engineering

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations

Example DER Cybersecurity Problem

- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Carnegie Mellon University Electrical & Computer Engineering

Example DER Cybersecurity Problem SEE DS

Cybersecurity for Energy Delivery Systems

30

FLORIDA

Carnegie Mellon University Electrical & Computer Engineering

Electric Cooperatives of Arkansas Your Local Energy Partners

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem

Advanced Controls for DER

- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Carnegie Mellon University Electrical & Computer Engineering

Advanced Controls

Cybersecurity for Energy Delivery Systems Need for Secondary and Tertiary Control

- Coordination of Resources for Optimal Power Flow
- Maximize Generation while maintaining Power Quality

* Increased Attack Surfaces

Advanced Controls

Cybersecurity for Energy Delivery Systems

Control Level Time-Scales. Credit: IEEE Std 2030.7-2017

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER

Attack Scenarios

- Best Practices
- Research Trends
- Summary
- Further Reading & References

Carnegie Mellon University Electrical & Computer Engineering

SCADA Definition

Cybersecurity for Energy Delivery Systems

♦ What is SCADA?

Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), etc. generally refer to the systems which control, monitor, and manage the nation's critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, natural gas pipelines, and many others. Simply stated, a control system gathers information and then performs a function based on established parameters and/or information it received.

*Source: <u>https://us-</u> <u>cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C</u> .pdf

Attack Scenario I

Cybersecurity for Energy Delivery Systems

Man-in-the-Middle attack diagram. Credit: OPAL-RT

Man-in-the-Middle (MitM)

A MitM situation occurs when an external attacker is capable of intercepting, modifying, suppressing or replaying network packets undetected by tricking two communication nodes to believe they are still communicating normally.

Attack Scenario II

Cybersecurity for Energy Delivery Systems

Denial-of-Service attack diagram. Credit: OPAL-RT

Denial-of-Service (DoS)

DoS can render a service unavailable either through a direct or indirect attack. It also refers to physical attacks on communication infrastructure, such as the cutting of wires or wireless jamming.

Attack Scenario III

Cybersecurity for Energy Delivery Systems

GPS Spoofing attack diagram. Credit: OPAL-RT

GNSS Spoofing/Meaconing

The act of causing Global Navigation Satellite System (GNSS) receivers to lock onto simulated or replayed satellite signals instead of real ones, effectively causing the receiver to locate itself at the wrong position and/or time. This class of attack is a major threat to PMU and synchrophasor systems, which are heavily reliant on time synchronization.

Stuxnet Attack

Cybersecurity for Energy Delivery Systems

Stuxnet diagram. Credit: Trendmicro [7]

- * Advanced Malware Targeting Industrial Systems [4]
- * Allowed Access to Discover Facility Architecture
- Specific System Function Calls Sent to Field Devices [5]
- Destroyed an Estimated 984 Nuclear Centrifuges [6]

Carnegie Mellon University Electrical & Computer Engineering

Electric Cooperatives of Arkansas

TRNATIONA

UNIVERSITY

2015/2016 Ukraine Attack

- Utilized "Black Energy 3" Malware
- Gained Access to Industrial Control Systems (ICSs)
- Target Field Devices Using Custom Malicious Firmware
- 225,000 Customers Without Power (1-6 hours)
- 8 30 Substations Disabled

- Overlapping vulnerabilities and attacks related to Ukraine Event. Source: E-ISAC-TLP Report [8]
- **DoS Attack** Utilized bots to "flood" Call/Service centers
- Malicious Firmware Disabled and/or destroyed devices
- **Spearfishing** Resulted in employees providing credentials
- Malware Implemented DDoS and Trojan Botnet "Black Energy" 40

Cyber Kill Chain

Cybersecurity for Energy Delivery Systems

STAGE 2 Attack

Stage 1: Planning, Preparation, Cyber Intrusion, Management and Enablement (Explore/Exploit), Deployment and Entrenchment (Execute Malware)

Stage 2: Attack Development, Validation, ICS Attack

Diagram of stages of ICS Cyber Kill Chain. Source: Idaho National Labs Aug 2016 "INL/EXT-16-40692" [9]

- **& Common Attack Scenario against Utilities**
- * Incorporates Phishing, Waterhole, Malware, and MiTM Attacks

Carnegie Mellon University Electrical & Computer Engineering

Attacks/Notes

Cybersecurity for Energy Delivery Systems

- Florida's Oldsmar Water Treatment System
 - Sodium hydroxide, or lye, to more than 100 times normal
 - TeamViewer, Potential of shared passwords for remote access
- Aurora Generator Test
 - 27-Ton Generator vs less than 30 lines of code
 - Kinetic Attacks
- Bingham County Ransomware
 - Brute-Force Attack on Open Port
 - Paid Ransom to restore two servers
- Coffee Machine Ransomware
 - Unencrypted WiFi
 - No code signing for firmware updates
- SolarWinds
 - Software Supply Chain and Firmware Attacks
 - Compromised update to SolarWinds' Orion software
 - Currently believed March 2020 Campaign Start Date
 - Backdoor access to allow credential harvesting and pivoting

Solarwinds Orion

Cybersecurity for Energy Delivery Systems

General Digital Signatures	de6e6c41878e95fd95026267daab421 × Security Details Previous Versions		
Digital Signature Deta	ils ? ×		
General Advanced		Attacker	
Signer information	gnature Information signature is OK.	Hostnames Match Victim Environment	
Name:	Solarwinds Worldwide, LLC		
E-mail:	Not available	TEARDROP and BEACON	IP Addresses
Signing time:	Tuesday, March 24, 2020 1:53:43 AM View Certificate	Malware Used UNC2452	Victim's Country
Countersignatures			
Name of signer: Symantec SHA25	E-mail ad Timestamp i6 TimeS Not availa Tuesday, Mar	***	
_	Details	Lateral Movement Using Different Credentials	Temporary File Replacement and Temporary Task Modification

*Source: <u>https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-</u> 43 solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Carnegie Mellon University Electrical & Computer Engineering

DS

S

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Approaches to Cybersecurity

Cybersecurity for Energy Delivery Systems

*Source: Craig Miller - NRECA

RKANSA

Secure Architecture Design

Cybersecurity for Energy Delivery Systems

Carnegie Mellon University Electrical & Computer Engineering

Electric Cooperatives of Arkansas Your Local Energy Parmers

CISA Best Practices

Cybersecurity for Energy Delivery Systems

- **CISA Recommended Practices**
 - Keep Antivirus Software/Definitions Up-to-date \geq
 - Implement ICS Defense-in-Depth Strategies \succ
 - **Create Cyber Forensics Plans for Control Systems** \geq
 - **Develop ICS Cybersecurity Incident Response Plan** \succ
 - **OT/IT Collaborations for Proper Firewall Deployment** \succ
 - **Patch Management** \geq
 - Secure ICS Modems\Access \geq
 - **Cross-Site Scripting Mitigation** \succ

NERC CIP Standards

Cybersecurity for Energy Delivery Systems

NERC Current CIP Standards

- > NERC CIP-002-5.1a (BES Cyber System Categorization)
- NERC CIP-003-8 (Security Management Controls)
- NERC CIP-004-6 (Personnel & Training)
- NERC CIP-005-6 (Electronic Security Perimeter(s))
- NERC CIP-006-6 (Physical Security of BES Cyber Systems)
- NERC CIP-007-6 (System Security Management)
- NERC CIP-008-6 (Incident Reporting and Response Planning)
- NERC CIP-009-6 (Recovery Plans for BES Cyber Systems)
- NERC CIP-010-2 (Configuration Change and Vulnerability Assessments)
- NERC CIP-011-2 (Information Protection)
- NERC CIP-013-1 (Supply Chain Risk Management)
- NERC CIP-014-2 (Physical Security)

*Source: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

TPM Benefits: Encryption

Cybersecurity for Energy Delivery Systems

10	Returned from Wi-Fi					- 0 X
644	Edit View Co. 1	antes Analos Statistic	s Telephone Wiseless	Tank Main		
	tor new co	D Z O + + B Z		TT ISSUE		
1.	12.00			• III.		10
	8007 193 568.66 46	In the second				- LU -
	Packet list	Samovi & tince	Case sensitive string		ne	Find Cancel
190.	Time	Source	Destination	Protocol	Length Info	
	1738 10.858436	192.168.85.46	192.168.85.44	HTTP	547 HTTP/1.1 404 Not Found (text/html)	
	1743 10.891409	192.168.85.44	192.168.85.46	TCP	54 1757 + 80 [ACK] Seq=1314 Ack=2526 Win=130816 Len=0	
	2553 15.751439	192.168.85.46	192.168.85.44	TCP	54 80 - 1757 [FIN, ACK] Seq=2526 Ack=1314 Win=32512 Len=0	
	2554 15.751518	192.168.86.44	192.168.85.46	TCP	54 1757 = 80 [ACK] Seq=1314 Ack=2527 Win=130816 Len=0	
	2664 16.541356	192.168.85.44	192.168.85.46	TCP	54 1757 → 80 [FIN, ACK] Seq=1314 Ack=2527 Win=130816 Len=0	
11	2665 16.542334	192.168.85.44	192.168.86.46	TCP	66 1759 + 88 [SYN] Seq=8 Win+64248 Len+8 P55=1468 WS+256 SACK_PERH+1	
	2667 16.545205	192.168.85.46	192.168.85.44	TCP	54.80 → 1757 [ACK] Seq=2527 Ack+1315 Win+32512 Len+0	
	2668 16.546870	192.168.86.46	192.168.86.44	TCP	66 80 + 1759 [SYN, ACK] Seq+0 Ack+1 Win+29200 Len+0 M55+1460 SACK_PERM+1 W5+128	
	2669 16.546968	192.168.85.44	392.168.85.46	TCP	54 1759 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0	
-	2670 16.547420	192.168.85.44	192.168.85.46	RUIP	874 POST /accounts/login/ HTTP/1.1 (application/x-waw-form-urlencoded)	
	2671 16.550841	192.168.85.46	192.168.85.44	TCP	54.80 = 1759 [ACK] Seq=1 Ack=821 Win=32128 Len=0	
÷	2768 16.951662	192.168.85.46	192.168.85.44	HTTP	758.HTTP/1.1 102 Found	
	Content-Type: User-Agent: M Accept: text/l Referer: http Accept-Encodin Accept-Languag Cookie: carft Cookie pair	application/x-news-fo szilla/5.0 (Windows N tml_application/shtm //raspberrypl/accoun g: gzip_deflate/r/n ge: em-US_eniq=0.9/r/ ken=G5km0KANIXT1ND5j : csrftoken=G5km0KAN	rm-urlencoded\r\n T 10.0; Win54; x54) lxml,application/x ts/login/inext=/\r\ n norWorlCcbilK0cmcMP iXT1M83jnorWorlCcbi	AppleWebKit/ ml;q=0.9,imag n 16dJmpMGyigLFr DGkCmcM916dJmpJ	37.36 (KMTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36\r\n /webp,image/apng,*/*;q+0.8,application/signed-exchange;v+b3;q+0.9\r\n JLEPK4siFLPrZME\r\n yiqLFrE3iEPK4siFLPrZME	
0.20	14 30 24 30 1	4 A. 43 44 44 44 40 40	45 14 20 41 71	a a fa akiat		
07.0	22 66 78 66	6 65 6e 34 47 35 6h	64 44 Ah 41 4e m	ftoken- Gilen	an l	
025	0 69 58 54 6c	18 42 33 6a 6e 6f 72	57 6f 72 31 43 i	XT1H831 norMo	26	
624	0 63 62 69 49	4b 6b 43 6d 63 4d 50	4e 57 55 6d 78 c	bilkkCm cMPNW	np	
RON	44 36 79 69	1 4c 46 72 45 33 69	45 4d 4b 34 73 M	WyigLFr E3iEM	45	
0.2e	69 46 44 59	2 5a 4d 45 @d @a @d	@a 63 73 72 66 1	FLPYZME	rf	
021	64 69 64 64	ic 65 77 61 72 65 74	6f 6b 65 6e 3d #	iddlewa retok	8=	
010	0 4s 70 6d 66	00 44 69 42 68 62 61	32 66 45 39 66 3	pefPOiB hba2f	94	
011	0 61 32 32 54	13 4f 4d 49 6d 32 70	63 39 46 32 56 a	22TcOMI m2pc9	21	
0.32	0 66 36 52 47	18 4e 34 64 4c 6b 50	5a 59 4f 4c 6e f	GROWNAD LIKPITY	Le D	
033	72 48 54 42	11 37 50 79 73 77 53	6a 51 6b 63 64 m	HIBAJPY SH5 JQ	cd.	
0.54	26 75 75 65	2 be 61 6d 65 3d 61	64 6d 69 6e 26 8	susernam c+adm	16.	
33	64 36 69 65	107 72 04 30 70 01	/3 /3 // OF /2 p	Horst-X 26		
0.1	× 20 00 03			And the state		and att (6.86.)
-	- an becnet courses	man intelligence and coprime.			Packata: 53506 ' Dep	Alex are (ware) Profile: Defa

WireShark Capture of Unencrypted User Credentials (HTTP)

Carnegie Mellon University Electrical & Computer Engineering

DS

TPM Benefits: Encryption

Cybersecurity for Energy Delivery Systems

9 == 192.548.84.44 Trive 2000 81.5821275 2011 81.582207					
Time 200 81.582175 201 81.582207	1.42				8
200 81.582175 201 81.582207	Source	Destination	Protocol	Length 3rds	
201 81.582207	192,163,35,46	192,168,85,44	TOP:	54 [TCP Retrementssion] 443 + 1872 [FIN, ACK] Sec-241 Ack-523 Win-30464 Len-0	
And An Manual A	192.168.85.44	192.168.86.46	TCP	54 [TCP Zerokindow] 1872 + 441 [ACK] Seq-621 Ack-242 kin-0 Let-0	
219 81.732138	192.168.86.46	192.168.86.44	TL5v1.3	1514 Application Data	
220 81.732142	192.168.86.46	192.168.85.44	TCP	1514 443 + 1873 [ACK] Seq-1988 Ack-1366 Win-31872 Len-1460 [TCP segment of a reassembled POU]	
21 81.732194	192.168.86.44	192.168.86.46	TCP	54 1873 + 443 [ACK] Seq=1366 Ack=3448 Win=131328 Len=0	
22 81.732570	192.168.86.46	192.168.85.44	TLSv1.3	518 Application Data, Application Data, Application Data	
60 81.772469	192.168.86.44	192.168.85.46	TLSv1.3	635 Application Data	
61 81.775771	192.168.86.46	192,168.86.44	TLSv1.3	578 Application Data	
68 81.816653	192.168.86.44	192.168.85.46	TCP	54 1873 + 443 [ACX] Seq=1947 Ack=4420 Win=130304 Len=0	
75 81.851105	192.168.86.44	192,168.86.46	TL5v1.3	642 Application Data	
78 81,864781	192.163.86.46	192.168.86.44	TLSv1.3	1514 Application Data	
79 81.864785	192.168.86.46	192.168.86.44	TL5v1.3	1513 Application Data	
	a 89 19 34 77 2a	18 08 09 45 00	8(
dc a6 32 25 7b fi	0 80 86 90 12 c0	18 20 ZC CV 88 - 80			
dc a6 32 25 7b f. 02 6d 3a cd 40 00 56 2e 07 51 01 bb	0 80 96 90 12 c0 b eb 25 35 01 c8	40 56 c9 50 18 V.	QX 5V-P		
dc a6 32 25 7b fi 92 6d 3a cd 40 00 56 2e 07 51 01 b0 01 ff 3b e8 00 00	0 80 96 90 12 cð 6 eb 25 35 01 c8 0 17 03 03 02 48	d0 56 c9 50 18 V. 63 64 85 b5 a2	Q X S V P		
dc a6 32 25 7b f. 02 6d 3a cd 40 0 56 2e 07 51 01 b6 01 ff 3b e8 00 0 18 b2 42 5a 36 5v	0 00 06 96 90 12 c0 b eb 25 35 01 c8 0 17 03 03 02 40 a 9d fd 83 2f 93	d0 56 c9 50 18 V. 63 44 85 b5 a2	Q X 5 V.F @cD 26 /		
dc a6 32 25 7b f. 92 6d 3a cd 40 00 56 2e 07 51 91 b0 93 b2 42 5a 36 5v 96 16 fd 71 fb cd 94 5c 22 5a 36 5v 96 16 fd 71 fb cd 95 5c 20 5c 20 5c 20 5c 96 16 fd 71 fb cd 96 16 f	00 00 06 90 12 c0 b eb 25 35 01 c8 00 17 03 03 02 40 0 9d fd 83 2f 93 4 cf 85 62 8c 65	ab 50 20 00 10 d0 56 c9 50 10 V. 63 44 85 55 a2	Q X 5 V F (c) 26 / 0		
dc a6 32 25 7b f 02 6d 3a cd 40 0 55 2m 07 51 01 b 01 ff 3b e8 00 0 18 b2 42 5a 36 5 96 16 fd 71 fb c 21 fe 18 33 a3 2 4 74 52 6	10 90 96 90 12 c0 10 60 25 35 01 c0 10 17 03 03 02 40 10 17 03 03 02 40 10 17 03 03 02 40 10 17 63 62 62 62 14 64 80 67 45 60 14 64 80 67 45 64	40 50 42 50 18 40 56 62 50 18 V 63 44 85 85 82	Q X 5 V F BCD 26 / 1 0 3 5 E Y6-		
dc a6 32 25 7b f 92 6d 3a cd 40 0 56 2m 07 51 91 b 91 ff 3b 88 00 0 18 b2 42 5a 36 0 96 16 fd 71 fb cd 21 fe 18 33 a3 2 4a 74 57 cf 0 al 66 ae b0 ad 7e 22	10 00 06 90 12 c0 10 0 25 15 01 c1 10 17 03 02 48 02 48 10 17 03 02 48 04 fd 83 2f 93 4 cf 85 d2 0c 0c 4c 64 80 07 45 fb 0 ca 38 be 2c 4c 56 bc 2c 4c 2 ca 38 be 2c 4c 56 3c	aiiiii 30 42 C C B 30 aiiiiii diiii 56 C 3 50 11 V. diiii 56 50 21 V. diii 17 08 42 16 38 39 ski 50 64 7e 30 1. 4e 6e 20 44 26 1.0 diii 38 32 38 90 1.0	Q X 5 V F 8cD 26 / 6 3 5 E Y6 ,0% D		
dc a6 32 25 7b f 92 6d 3a cd 40 0 56 2e 07 51 91 b 91 ff 3b e8 00 0 18 b2 42 5a 36 0 96 16 fd 71 fb cd 21 fe 18 33 a3 2 4a 74 57 cf 60 af 66 a6 b0 ad 7e 82 66 44 af a5 34 3	00 00 96 90 12 c0 ho 0h 25 35 01 c8 00 17 03 02 40 03 02 40 w 9.01 fd 83 2.67 9.6 62 48 0.7 45 64 80 0.7 45 60 6.6 4.6 80 0.7 45 60 6.6 4.6 80 0.7 45 60 6.6 4.6 80 0.7 45 60 4.6	ab 30 20 20 10 90 40 56 20 10 90 21 10 63 46 80 55 42 10 10 84 56 42 61 64 10 10 44 56 42 67 10 10 10 4e 66 20 42 46 10 10 4a 33 128 94 10 10	Q X 5 Y F 8cD 26 / 6 3 5 E Y6 0 00 D - 7 C 4273 # K5		
dc a6 32 25 7b f. 92 6d Ta cd 40 0 55 7c 07 51 91 0 18 b2 42 5a 36 90 18 b2 42 5a 36 9 95 16 fd 71 fb c 21 fe 18 33 a3 2 44 72 57 cf 60 a1 d6 ae b0 ad 7e & e6 44 ad a5 34 32 1 a 86 ad 84 34 35 1 a 86 ad 84 35	00 00 965 90 12 c0 sb sb 25 35 01 c1 00 00 17 03 30 24 60 30 22 93 4a cf 85 d12 0c 0c 4c 46 80 07 45 60 0c 4c 46 80 07 45 60 4c 46 80 07 45 60 4c 46 80 97 45 60 4c 46 46 80 97 45 60 45 46 46 46 46 46 46 46 46 46 46 46 46 45 46 </td <td>ab 30 20 20 10 90 63 66 60 50 10 90 10 63 66 60 50 10 90 10 10 63 66 60 50 10 90 10 10 84 56 62 67 63 91 10 10 4e 66 20 44 26 116 116 4a 33 82 28 90 10 10 4b 66 20 44 26 10 10 4b 58 46 24 10 10 10 4b 64 74 49 41 41 41 41</td> <td>Q X 5 V F 8 80 9 5 6 7/ 9 5 6 76 0 7 6 15 7 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7</td> <td></td> <td></td>	ab 30 20 20 10 90 63 66 60 50 10 90 10 63 66 60 50 10 90 10 10 63 66 60 50 10 90 10 10 84 56 62 67 63 91 10 10 4e 66 20 44 26 116 116 4a 33 82 28 90 10 10 4b 66 20 44 26 10 10 4b 58 46 24 10 10 10 4b 64 74 49 41 41 41 41	Q X 5 V F 8 80 9 5 6 7/ 9 5 6 76 0 7 6 15 7 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7		
dc a6 32 25 7b f. 92 6d 1a cd 40 0 55 2a 07 51 91 0 18 b2 42 5a 36 90 96 16 fd 71 fb c 21 fe 18 33 a3 2 4a 72 57 cf 90 at 46 ae b0 ad 7e 82 ef 44 ad a6 34 72 51 1a B6 ad 84 3e 96 c B8 71 ad ef	00 00 965 90 12 c0 sb sb 25 35 01 c8 00 17 03 02 46 03 02 46 10 94 fd 83 27 93 4 cf 88 07 45 fb 04 44 64 38 07 45 fb 04 42 46 38 07 45 fb 04 44 64 38 07 45 fb 04 42 46 38 07 45 fb 0 42 43 88 04 54 54 54 54 35 88 04 36 57 43 38 80 45 41 54 54 54 54 35 36 54 35 36 36 36 36 36 36 36 36 36 36 36 36	ab 30 20 20 10 90 40 56 20 10 90 20 10 90 63 44 30 55 20 10 90 20 10 10 84 56 42 67 10 <td>Q X 5 VF 26 // 0 3 5 E Y6 - 0 - 4213 - 6 K5 c CAg</td> <td>9 6 0</td> <td></td>	Q X 5 VF 26 // 0 3 5 E Y6 - 0 - 4213 - 6 K5 c CAg	9 6 0	
dc a6 32 25 7b f R2 6d Ja cd 40 0 55 2e 07 51 01 bl 18 b2 42 5a 36 90 01 18 b2 42 5a 36 90 18 b2 42 5a 36 90 19 16 16 71 fb c 21 fc 18 33 a3 20 4a 74 57 cf 00 a1 46 ae b0 ad 7e 82 64 ad a5 34 72 63 1m 84 a4 34 10 5c 88 77 ad c0 43 72 64 25 b1 d1 19 16 10	00 000 965 900 1.2 c8 bb eb 25 315 0.1 c8 00 17 0.3 0.3 0.2 4.6 No 9.04 f-dl 8.3 2.7 9.3 A cf 8.5 0.2 0.0 0.0 A cf 8.5 0.0 0.0 0.0 A cf 8.5 0.0 0.0 0.0 Q 10 8.6 0.0 0.0 0.0 Q 10 5.6 0.0 0.0 0.0 Q 5.6 0.5 0.0 0.0 0.0 Q 5.6 0.5 0.0 0.0 0.0 Q 5.6	ab 30 20 20 11 W. 63 66 30 56 12	Q X 5 V6 26 / 0 3 5 E V6 -4213 # K5 -4213 # K5 - 6 - 6 - 7 - 7 - 6 - 7 - 7 - 6 - 7 - 6 - 7 - 7 - 7 - 6 - 7 - 7 - 7 - 6 - 7 - 7 - 7 - 7 - 7 - 7 - 6 - 7 - 7 - 7 - 7 - 7 - 7 - 7 - 7		
dc a6 32 25 7b f d2 d3 ac d40 b 55 2m 07 51 01 bd 55 2m 07 51 01 bd 55 2m 07 51 01 bd 128 b2 42 5a 36 59 95 16 16 17 16 33 32 24 72 57 cf 00 ad 54 36 34 32 4a 72 57 cf 00 ad 76 34 32 34 34 36 34 32 34 34 36 34 32 34 36 34 36 34 32 34 36 34 37 34 36 34 37 34 36 34 32 34 37 34 37 34	00 00 965 90 12 c8 ab ab 25 35 01 c8 00 17 03 02 04 03 02 46 10 91 63 02 04 08 00 12 93 02 04 <td>ab 30 20 20 11 W. 63 66 36 36 36 21 11 63 46 30 55 32 11 W. 11 63 46 30 56 42 11 11 11 44 56 30 56 46 42 56 11</td> <td>Q X 5 V 6 26 / 26 3 5 E V6 3 5 E V6 4 213 # K5 4 214 K5 5 K5 6 K5 6 K5 7 K5 8 K5 7 K5 7 K5 8 K5 7 K5</td> <td></td> <td></td>	ab 30 20 20 11 W. 63 66 36 36 36 21 11 63 46 30 55 32 11 W. 11 63 46 30 56 42 11 11 11 44 56 30 56 46 42 56 11	Q X 5 V 6 26 / 26 3 5 E V6 3 5 E V6 4 213 # K5 4 214 K5 5 K5 6 K5 6 K5 7 K5 8 K5 7 K5 7 K5 8 K5 7 K5		

Carnegie Mellon University Electrical & Computer Engineering

DS

E

S

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices

Research Trends

- Summary
- Further Reading & References

CIA Triad Overview

Information security CIA Triad

 Confidentiality of Data Authorized Use and View > Privacy ✤ Availability of Data > Access > Control Integrity of Data > Validity > Consistency > Predictability Energy Systems > Availability of Power Integrity of Power

|**||i**|

Layered Approach

Cybersecurity for Energy Delivery Systems

Command Layer

- Command Validation
- Communication Encryption
- Supervisory Layer
 - Watchdog Timers
 - Algorithmic State Machines
- Control Layer

Carnegie Mellon University

Electrical & Computer Engineering

- Reference Limits
- State Awareness
- Dead Time Enforcement

UNIVERSITY OF Electric Cooperatives

Arkonsas

ur Local Energy Partners

Cyber-Hard by Design

Cybersecurity for Energy Delivery Systems

- *** Robust Protection Requires Multiple Layers**
- * Hardware-Level sub-Module Authentication
 - Custom Keys Installed on sub-Modules for Identification
 - Encrypted Communication Between sub-Modules
- External Authentication
 - Certificate Keys Managed by Trusted Certificate Authority
 - Custom Hardware Key Required for Firmware Update
 - Encrypted Communications for Local/Remote SCADA
- Software and Hardware Intrusion Detection
- * New Encryption Techniques for Higher Performance
- Control systems (e.g., state machines) must address all possible states
- Non-sensical/destructive acts must be disallowed by design

Cost of Security

Cybersecurity for Energy Delivery Systems

- Processing overhead of encryption
 - Benchmark performances
 - Interrupt Service Routine/Polling/Co-Processor
- Impact on system operation
 - Cost/Benefit analysis of securities
 - Time delay of communication
 - Control algorithm stability with added security
 - Additional resources required, increasing cost or lowering performance

- Additional development time of grid-connected power electronics
 - Possible time savings by reuse of standard and secure techniques
 - Reduced downtime by using robust designs and software
 - Flexible controls to allow upgrades and reduce replacement of hardware

Carnegie Mellon University Electrical & Computer Engineering

Electric Cooperatives of Arkansas

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Cybersecurity for Energy Delivery Systems

Penetration of Distributed Energy Resources is Increasing

Higher-Level Coordination is Required

- Increased Power Quality
- > Optimized Power Flow

Coordination Requires Communication

- Peer-to-Peer
- > TOU Pricing
- Protection Relays
- Dispatch and Load Predictions
- Increased Communications mean Increased Attack Surfaces
- Implement Best Practices to Mitigate Risks
- Additional Research Required
 - Coordinate Resources
 - > Optimize Power Flow
 - Mitigate Current and Future Risk

Presentation Outline

Cybersecurity for Energy Delivery Systems

- NCREPT Facility Overview
- Cyber Testbed
- Distributed Energy Resources
 - History and Projections
 - Example Installations
- Example DER Cybersecurity Problem
- Advanced Controls for DER
- Attack Scenarios
- Best Practices
- Research Trends
- Summary
- Further Reading & References

Further Reading

Cybersecurity for Energy Delivery Systems

- https://us-cert.cisa.gov/ics/Recommended-Practices
- https://us-cert.cisa.gov/ics/Secure-Architecture-Design
- https://blog.rsisecurity.com/what-are-the-10-fundamentals-ofnerc-cip-compliance/
- https://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf
- https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- https://us-cert.cisa.gov/ncas/alerts/aa21-042a
- https://us-

cert.cisa.gov/sites/default/files/documents/Procurement_Lang uage_Rev4_100809_S508C.pdf

https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/

Carnegie Mellon University Electrical & Computer Engineering

References

Cybersecurity for Energy Delivery Systems

[1] https://www.greentechmedia.com/research/subscription/u-s-solar-market-insight#gs.wpfDw8k

[2] "Wind Vision," Energy.gov. [Online]. Available: <u>https://www.energy.gov/eere/wind/maps/wind-vision</u>. [Accessed: 25-Sep-2018].

[3] "Electric energy storage: preparing for the revolution | White & Case LLP International Law Firm, Global Law

Practice." [Online]. Available: //www.whitecase.com/publications/insight/electric-energy-storage-preparing-revolution. [Accessed: 25-Sep-2018].

[4] "Stuxnet worm brings cyber warfare out of virtual world." [Online]. Available: <u>https://phys.org/news/2010-10-</u> stuxnet-worm-cyber-warfare-virtual.html. [Accessed: 25-Sep-2018].

[5] R. Langner, Cracking Stuxnet, a 21st-century cyber weapon. Available:

https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon/transcript. [Accessed: 25-Sep-2018].

[6] "Stuxnet Worm Attack on Iranian Nuclear Facilities." [Online]. Available:

http://large.stanford.edu/courses/2015/ph241/holloway1/. [Accessed: 25-Sep-2018].

[7] "STUXNET Malware Targets SCADA Systems - Threat Encyclopedia - Trend Micro USA." [Online]. Available:

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems. [Accessed: 25-Sep-2018].

[8] R. M. Lee, M. J. Assante, T. Conway, Analysis of the Cyber Attack on the Ukrainin Power grid, 2016, [online] Available: <u>http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf</u>.

[9] Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. (2016). [ebook] Mission Support Center, Idaho National Laboratory. Available at:

https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%2 0the%20U.S.%20Electric%20Sector.pdf [Accessed 25 Sep. 2018].

