Insecure Field Devices on the Smart Grid: Cyber Risks, Damage Potential, and Practical Solutions

Maurice Martin

25 Feb 2016
Distribution utility attack

Enterprise Network
- GIS
- MDM
- Payment Processing
- Engineering Analysis
- Field Design

SCADA Network
- Substation online
- Substation offline
- Substation online

Field Devices
- Smart Meter
- Smart Feeder Switch
- Inverter
- Smart Capacitor
- DER
- Microgrid Controller
- EV Charger

Operations Center

server

Internet

NATIONAL RENEWABLE ENERGY LABORATORY
Today’s Webinar

1. Dangers arising from insecure smart grid field devices

2. Resources available to address the issue (and why they may go unused)

3. Technologies for identifying vulnerabilities in individual devices

4. NREL Research
National Renewable Energy Lab
Our Vision ...

Secure the prosperity of our nation.

Our Mission ...

Apply innovative technology, business processes, and policy to produce tangible improvements in the cyber-physical security posture of critical infrastructure and verticals most important to our economy.
Cyber-Physical Systems Security & Resilience Center (CPSSR)

• **Dr. Erfan Ibrahim, Center Director**
  
  • PhD Nuclear Engineering, UC Berkeley
  
  • Lawrence Livermore National Lab, Pacific Bell, EPRI, Bit Bazaar
  
  • Chief liaison to the Office of Electricity Delivery and Energy Reliability. GMLC Cybersecurity and Resilience team member
  
  • Identifies security requirements, evaluates cybersecurity standards, test cybersecurity controls

• **Tami Reynolds, Business Development Support & Project Leader**
  
  • BS Business-Marketing, Metropolitan State University of Denver
  
  • Business Development for NREL’s Energy Systems Integration
  
  • Leads projects through development, planning, contracting, equipment procurement, and technology transfer
Cyber-Physical Systems Security & Resilience Center (CPSSR)

- Michael Ingram, Group Manager and Business Area Lead
  - MS Engineering/Industrial Management, University of Tennessee - Chattanooga
  - Tennessee Valley Authority, operations specialist and senior advisor
  - Manages research program, develops empirically-based security architectures and resilience best practices

- Ivonne Peña, Policy Area Lead
  - PhD Engineering and Public Policy, Carnegie Mellon University
  - PhD Engineering, Technical University of Lisbon, Portugal
  - Westeva co-lead for business and analytics, United Nations
  - Analyzes and develops policy mechanisms to incentivize cyber security improvements

- Maurice Martin, Technology Area Lead
  - MS Systems Science, Louisiana State University
  - National Rural Electric Cooperative Association, cyber security research lead
  - Manages research projects, provides system-level analysis for cybersecurity initiatives, serves as liaison to utility industry associations
Cyber-Physical Systems Security & Resilience Center (CPSSR)

• Brian Miller, Senior Engineer
  - MS Electrical Engineering, University of Tennessee – Knoxville
  - MS Military Operations, Air Command and Staff College
  - U.S. Air Force, design engineer and project manager
  - Implements power system projects; conducts site assessments, modeling, and analysis of complex systems (including microgrids)

• Randolph Hunsberger, Senior Engineer
  - MS Building Systems, University of Colorado - Boulder
  - Consultant for renewable energy projects around the U.S.
  - Operates CPSSR’s Secure Distribution Grid Management Testbed, manages and maintains network resources for cybersecurity use cases and penetration tests
Smart Grid Field Devices

- Smart meters
- Smart feeder switches
- Inverters
- Smart capacitors
- Distributed Energy Resources (DERs)
- Microgrid controllers
Part 1
Dangers arising from insecure smart grid field devices
Distribution utility attack

Enterprise Network

- GIS
- MDM
- Payment Processing
- Engineering Analysis
- Field Design

SCADA Network

- Operations Center
- Substation online
- Substation offline

Field Devices

- Smart Meter
- Smart Feeder Switch
- Inverter
- Smart Capacitor
- DER
- Microgrid Controller
- EV Charger

Internet

1. Enterprise Network to Field Devices
2. Enterprise Network to SCADA Network
3. SCADA Network to Operations Center
4. SCADA Network to Substation online
5. SCADA Network to Substation offline
6. Enterprise Network to Internet
1) Compromise a field device

Where are field devices?

• Customer homes
  o smart meters

• Utility poles
  o smart switches

• Public spaces

• Substations
  o microgrid controllers
  o Inverters
Since August 2009, metal thefts have steadily increased across the nation, driven by rising prices for base metals... especially copper.

Whether the theft is an expensive personal irritant, like finding your catalytic converter has been stolen, or one that threatens public safety, as when the theft of copper wiring blacked out runway approach lights at the Modesto, CA, regional airport—metal thefts are increasing in frequency and severity.

"Copper thieves are threatening U.S. critical infrastructure... and present a risk to both public safety and national security."

– Federal Bureau of Investigation

WHERE IS COPPER BEING STOLEN FROM?

Over 25,000 claims for the theft of copper, bronze, bress, or aluminum were submitted to ISO ClaimSearch from 2009 to 2011. Of these, **96% concerned copper theft**.

55% of the claims were on commercial policies, while 45% were on personal policies.

Data: The National Insurance Crime Bureau

Graphic: Super | Circuits
Increasingly, field devices have embedded operating systems

- Itron and Cisco have embraced Linux
- Having a full operating system to work with gives hackers more tools
Demonstrated in a lab
Demonstrated in a field: 2012

- Academic researches created a botnet
- Devices with embedded operating systems
- 420,000 devices
- Used to gather data
  - Services
  - IPv4 addresses
- **Weak or absent passwords**
Demonstrated in a field: 2014

- Discovered first IoT botnet
- 100,000 consumer devices
- 750,000 malicious emails
- Included:
  - Home routers
  - multi-media centers
  - televisions
  - at least one refrigerator
The Smart Grid is one instance of the “Internet of Things.”
Attackers shutting off part of the grid.

- Until recently, no instance of this. However...
First power outage due to hacking

(At least, the first we know of...)

23 Dec 2015
4pm

- Two electric utilities:
  - Prykarpattyoblenergo
  - Kyivoblenergo

- 80,000 customers

- All power restored within 3.5 hours
What did the hackers do?

1. Opened circuit breakers in a number of substations, shutting off power.

2. Locked up the screens of dispatchers and operators, slowing response time.

3. Wiped data from the SCADA system.

4. Launched a telephone denial of service (TDOS) attack to disrupt communication/slow recovery.
How did the hackers do it?

<table>
<thead>
<tr>
<th>Action</th>
<th>Theory</th>
<th>Not known</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gained access to the SCADA system</td>
<td>Malware</td>
<td>Which malware? Possibly…</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BlackEnergy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Also: Delivery mode</td>
</tr>
<tr>
<td>Shut off circuit breakers</td>
<td>With SCADA access, hackers were able to manually open circuit breakers</td>
<td>Everything</td>
</tr>
<tr>
<td>Locked up dispatcher’s computer screens/wiped SCADA data</td>
<td>Malware</td>
<td>Which malware? Possibly…</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KillDisk</td>
</tr>
<tr>
<td>Telephone Denial of Service attack</td>
<td>None</td>
<td>Country of origin for incoming calls</td>
</tr>
</tbody>
</table>
Could it happen in the U.S.?

Not to scale

BlackEnergy

Less automation

BlackEnergy

More automation
What happened in Ukraine is a harbinger for the kinds of cyberthreats the US faces, possibly from rival nations such as Russia and North Korea...

(paraphrased)
Christian Science Monitor
12 Jan 2016
5) Move from SCADA network to enterprise network

ICS-CERT says: Air gap your SCADA networks!

But do we?
Value of data (particularly meter data)

Enterprise Network
- GIS
- MDM
- Payment Processing
- Engineering Analysis
- Field Design

SCADA Network
- Substation online
- Substation online
- Substation online

Field Devices
- Smart Meter
- Smart Feeder Switch
- Inverter
- Smart Capacitor
- DER
- Microgrid Controller
- EV Charger
“The Integration of IT and OT is vital to a successful implementation of new technologies under the Smart Grid umbrella”
6) Exfiltrate sensitive data
Distribution utility attack

Enterprise Network
- GIS
- MDM
- Payment Processing
- Engineering Analysis
- Field Design

SCADA Network
- Operations Center
  - Substation online
  - Substation offline
  - Substation online

Field Devices
- Smart Meter
- Smart Feeder Switch
- Inverter
- Smart Capacitor
- DER
- Microgrid Controller
- EV Charger

Internet
Part 2
Resources available to address the issue (and why they may go unused)
Procurement process

Utility

RFP
Proposal
Procurement contract
Product

Vendor
Security Questions for Smart Grid Vendors

NRECA has created a set of questions for utilities to submit with RFPs.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Supplier Brief Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reference: SG.AC-4 Access Enforcement. Can the proposed system enforce assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy? If so, please briefly describe how this is accomplished.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Reference: SG.AC-5 Information Flow Enforcement. Does the proposed system enforce assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy? If so, please briefly describe how this is accomplished.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Reference: SG.AC-8 Unsuccessful Login Attempts. Can the proposed system enforce a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period? If so, briefly describe how this is accomplished.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Reference: SG.AC-9 Smart Grid Information System Use Notification. Does the proposed system display an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance? If so, briefly describe how this is accomplished.</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity Procurement Language for Energy Delivery Systems

DOE funded document that provides sample language for inclusion in contracts.
UTC created this document defining 10 practices for managing supplier relationships.
For vendors

Supply Chain Best Practices

National Electrical Manufacturers Association recommendations on best practices for product development.
Focus: securing the enterprise network

1. Attacks on the enterprise network have been increasing.
   – Crypto-ransomware attacks rose 4000% in 2014.
   – Ransomware attacks rose 165% in Q1 2015.

2. Well-publicized theft of sensitive data in the retail sector.
   – Distribution utilities face same challenge of protecting customer data.

3. Vendors focus on enterprise network.
Part 3
Technologies for identifying vulnerabilities in individual devices
Testing individual field devices

Verifies the final product, independent of the supply chain

- Fuzz testing
- Scan binary code
- Scan source code
- Interface
- Software
- Source Code
Part 4
NREL Research
(past and future)
A different approach to securing the grid

• Rather than focus on individual devices, use a systems approach

• Use only commercially available products

• DON’T lean on encryption
The testbed is a significant NREL asset.
# Open Systems Interconnection (OSI) Model

Breaks the communication functions of a computing system into seven layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application: Skype, Facebook, Youtube, Windows File Sharing, FileZilla</td>
</tr>
<tr>
<td>6</td>
<td>Presentation: CSS, GIF, HTML, XML, JSON</td>
</tr>
<tr>
<td>5</td>
<td>Session: PAP, RPC, TLS, FTP, HTTP, SMTP, SSH, Telnet</td>
</tr>
<tr>
<td>4</td>
<td>Transport: TCP, UDP</td>
</tr>
<tr>
<td>3</td>
<td>Network: AppleTalk, ICMP, IPsec, IPv4, IPv6</td>
</tr>
<tr>
<td>2</td>
<td>Data Link: IEEE 802.2, L2TP, LLDP, MAC, PPP</td>
</tr>
<tr>
<td>1</td>
<td>Physical: DOCSIS, DSL, Ethernet physical layer, ISDN, USB</td>
</tr>
</tbody>
</table>
# GridWise® Architecture Council (GWAC) Stack

Define “degrees of interoperation necessary to enable various interactions and transactions on the Smart Grid”

<table>
<thead>
<tr>
<th>Layer</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Economic/Regulatory Policy</td>
<td>Political and economic objectives as embodied in policy and regulations</td>
</tr>
<tr>
<td>7 Business Objectives</td>
<td>Strategic and tactical objectives shared between businesses</td>
</tr>
<tr>
<td>6 Business Procedures</td>
<td>Alignment between operational business processes and procedures</td>
</tr>
<tr>
<td>5 Business Context</td>
<td>Awareness of the business knowledge related to a specific interaction</td>
</tr>
<tr>
<td>4 Semantic Understanding</td>
<td>Understanding of the concepts contained in the message data structures</td>
</tr>
<tr>
<td>3 Syntactic Interoperability</td>
<td>Understanding of data structure in messages exchanged between systems</td>
</tr>
<tr>
<td>2 Network Interoperability</td>
<td>Mechanism to exchange messages between multiple systems across a variety of networks</td>
</tr>
<tr>
<td>1 Basic Connectivity</td>
<td>Mechanism to establish physical and logical connections between systems</td>
</tr>
</tbody>
</table>
9-Layer Test: Securing DGM

- Collected relevant use cases for Distribution Grid Management from the NIST Interoperability Knowledge Base (IKB)
- Collected relevant failure scenarios for Distribution Grid Management from the DoE funded NESCOR Project
- Distilled the security requirements from the use cases for the logical layers in the various environments
- Distilled the resilience best practices from the failure scenarios
Use Cases

Develop 5 use cases utilizing Distribution Grid Management application:

- Auto sectionalizing and Restoration (ASR)
- Volt-Var Optimization (VVAR)
- Demand Response with EV Charging (DR)
- PV Smoothing with Storage
- Frequency Regulation with Storage

![Image of Real Time System of Systems]
DGM Testbed

Built the distribution grid management (DGM) test bed with

- DMS,
- enterprise SCADA,
- substation automation platform,
- intelligent electronic devices
  - RTUs
  - PLCs
  - field sensors
- electric storage
- electric vehicles
- capacitor banks
- smart switches
Categories of Solutions Used

- Data diode at hardware layer
- Network and file filter at hardware layer
- Transport layer access control
- Operational situational awareness
- Malware protection for web, email and file
- Business process security
The layered approach provides security at all 9 logical layers of a typical information system (7-layer OSI model + 2 upper layers of Gridwise Architecture Council Stack).

Coverage of the 8 vendor products against the 9 layers is shown schematically below.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Testbed Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>GWAC 5-7</td>
</tr>
<tr>
<td>Semantic</td>
<td>GWAC 4</td>
</tr>
<tr>
<td>Application</td>
<td>OSI 5-7</td>
</tr>
<tr>
<td>Network</td>
<td>OSI 3-4</td>
</tr>
<tr>
<td>Physical</td>
<td>OSI 1-2</td>
</tr>
</tbody>
</table>

1  2  3  4  5  6  7  8
## Cybersecurity Technology Vendors

<table>
<thead>
<tr>
<th>Product</th>
<th>Layer(s)</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SecLab Denelis</td>
<td>Physical + semantic</td>
<td>Data filter + data diode</td>
</tr>
<tr>
<td>2. Blackridge TAC</td>
<td>Network</td>
<td>IP and TCP layer protection with authentication</td>
</tr>
<tr>
<td>3. Cisco Firewall + Cisco Switches w access control lists</td>
<td>Network</td>
<td>Stateful inspection</td>
</tr>
<tr>
<td>4. FireEye</td>
<td>Network + semantic</td>
<td>Filtering network, email, and files</td>
</tr>
<tr>
<td>5. NexDefense Sophia</td>
<td>Network + semantic</td>
<td>Anomaly detection</td>
</tr>
<tr>
<td>6. N-Dimension N-Sentinel</td>
<td>Application + semantic</td>
<td>Cloud-based continuous threat monitoring</td>
</tr>
<tr>
<td>7. Synopsys AbuseSA Intrusion Detection for SCADA</td>
<td>Application + semantic</td>
<td>Cloud-based continuous threat monitoring</td>
</tr>
<tr>
<td>8. Albeado PRISM</td>
<td>Business process + semantic</td>
<td>Business process security</td>
</tr>
</tbody>
</table>
Testbed
Distribution Grid Management (DGM) Testbed

• Applied the cybersecurity controls and resilience mechanisms using the technologies from the selected vendors

• Ran the DGM use cases on the test bed; performed vulnerability/penetration testing to identify residual risk

• Confidentially recommended additional security controls to the vendors involved in the project to secure DGM

• Prepared report documenting the results of the project
Results

• Demonstrated the value of layered security in protecting against a variety of threat vectors (internal and external to an organization);

• Proved “off the shelf” cybersecurity technologies today—combined with sound cybersecurity management principles—can successfully protect organizations from these threats;

• Delivered a new R&D capability within NREL to help protect utility infrastructure, and as well as a valuable tool for DOE to secure their national lab infrastructure.
Next steps

• Bring data from all eight vendors into one dashboard

• Make the testbed rapidly reconfigurable

• Improve remote access capabilities

• Demonstrate what can be achieved by hacking field devices, and test defenses against such attacks.
Conclusions

• Need for better field device security?
  o Absolutely!

• However, a systems approach to cyber security can protect against a wide variety of attacks, including those arising from insecure field devices.
Contact

• Maurice Martin
  CPSS&R Technology Lead
  maurice.martin@nrel.gov

• Tami Reynolds
  CPSS&R Business Development Support & Project Leader
  tami.reynolds@nrel.gov