Better Buildings Alliance
Plug and Process Loads (PPL) Project Team Teleconference

September 20, 2018
Technical Lead: Rois Langner, NREL
Plug & Process Load Team

Plug Loads Are...
Figure 1. PPLs account for 33% of the total energy consumed by commercial buildings. Graph by Chad Lobato, NREL; Data source: DOE (2010)
Plug Load Energy Savings

Up to 30%!

Translates to approximately 10% of whole building energy consumption
Agenda

• Team Players
• Team Updates
  – *Rois Langner*, National Renewable Energy Laboratory
• Technical Presentation: Navigating Cybersecurity Implications of Smart Outlets
  – *Dane Christensen*, National Renewable Energy Laboratory
• Open Discussion and Q&A
• Additional Member Updates
Team Players

Technical Team Leads:

Rois Langner
National Renewable Energy Laboratory
[Rois.Langner@nrel.gov](mailto:Rois.Langner@nrel.gov)
Phone (mobile): (303) 204-7026

Dr. Kim Trenbath
National Renewable Energy Laboratory
[Kim.Trenbath@nrel.gov](mailto:Kim.Trenbath@nrel.gov)
Phone (office): (303) 275-3710
Team Players

Technical Team Support:

Katie Vrabel
Waypoint Energy
katievrabel@waypoint-energy.com
ACEEE Summer Study
August 12-17, 2018
Asilomar Conference Grounds, Pacific Grove, CA

• Presentations:
  – Navigating Communication Protocols and Cyber Security Implications of Wireless Meter and Control Technologies for Plug Loads
    • Panel 12: Smart Buildings, Smart Grid, and IoT
  – Using Metered Plug Load Data to Sense Occupancy and Implement Controls
    • Panel 14: Poster Display Presentations
Energy Exchange + Better Buildings Summit
August 21-23, 2018
Cleveland, Ohio

- Presentations:
  - Plug Load Management System Field Study with Ibis Networks
    - Publication coming soon
    - Plan to discuss results during next BBA PPL Team Call
  - Ask an expert table
Better Integrating PPL Controls into BAS and EMIS Platforms – A Landscaping Study:

- Research to investigate:
  - State of the wireless plug load meter & control market
  - How PPL controls already integrate into BAS and EMIS platforms
  - Ease & cost of integration
  - Where the market is heading
  - Gaps to fill in order to push market forward

→ Recommended research areas for the Labs
Better Integrating PPL Controls into BAS and EMIS Platforms:

- Thanks to our reviewers!
  - ACEEE
  - CalPlug
  - D+R International
  - Eversource Energy
  - MEEA
  - MNCEE
  - NEEA
  - NEEP
  - PG&E
  - SEEA
  - Seventhwave
  - SPEER
Potential New Research Areas for FY19:

• PPL Controls + EMIS Platform Integration:
  – Smart outlet data collection & data management
  – Interoperability of plug load controls with other building systems
  – Development of more advanced plug-and-play capabilities for smart outlets
Dane Christensen
Researcher and Mechanical Engineer
National Renewable Energy Laboratory
Navigating Cybersecurity
Implications of Smart Outlets

Dane Christensen
National Renewable Energy Laboratory

September 20, 2018
Plug & Process Loads

Figure 1. Percentage of whole-building energy attributed to plug loads in residential and commercial buildings in 2017 and projections for year 2040 (data from [EIA 2018]).
Wireless Meter & Control Technologies
Wireless Meter & Control Technologies
Navigating Cybersecurity Implications

- Pros & cons of plug load controllers
- Framework for assessing cybersecurity of connected devices
- Example of how to use framework
- Goal: Simplify and support appropriate cybersecurity consideration
Connected Plug Load Controls
Connected Plug Load Controls
Plug Load Control Standards

Standards Require Plug Load Controls (...since 2010!)

- ASHRAE 90.1
- California Title 24
- 50% of outlets in specified spaces must have automatic shut-off control
  - Workstations
  - Private offices
  - Conference rooms
  - Print/copy rooms
  - Break rooms
  - Classrooms
- Plug-in control devices are not allowed
Smart Outlets: Pros

• Provide in-depth understanding of plug load energy consumption
• Help reduce plug load run times
• Help save plug load energy
• Monitor equipment health
• Identify operational faults
• Ensure sensitive equipment is not tampered with

<table>
<thead>
<tr>
<th>SAVINGS POTENTIAL*</th>
<th>Individual Equipment</th>
<th>Whole Building</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential</td>
<td>17-33%</td>
<td>5-10%</td>
</tr>
<tr>
<td>Commercial</td>
<td>10-48%</td>
<td>6-10%</td>
</tr>
</tbody>
</table>

*Based on numerous studies
Smart Outlets: Cons

• Internet of Things (IoT) landscape is rapidly changing

• Many communication protocols and standards to choose

• Technologies could quickly be outdated
Data Privacy & Cybersecurity

Examples of concerns:

• **Retail:**
  o Risk of business losses or exposure to sensitive data belonging to customers

• **Medical:**
  o Unauthorized access to sensitive patient data or unauthorized control of critical building systems or equipment

• **Government:**
  o Unauthorized access to sensitive or confidential data, and unexpected exposure of data
Data Privacy & Cybersecurity

Top 3 Concerns:

1. Sensitive data exposure and loss of data privacy

2. Unauthorized access or control or loss of device functionality or service

3. System attacks
High-Level Security Considerations

• Secure network access
  o Data authentication and user identification
  o Secure data transfer & storage

• Digital watermarks + cryptographic methods of protecting data during information exchange

• Standard filters & protocols to restrict incorrect formatting

• Network monitoring systems

• Use of separate network for IoT devices
Risk Assessment

5 Step Process:

1. Identify Potential Security Vulnerabilities
2. Evaluate the Barriers to Exploit Each Vulnerability
3. Evaluate the Impact of Each Vulnerability
4. Evaluate the Severity of Exploitation
5. Specify/Adapt Security Requirements and Identify Solutions
Step 1:
Identify Potential Security Vulnerabilities

- Threats can come from outsiders & insiders
- List potential vulnerabilities through both physical and network pathways
Step 2:
Evaluate the Barriers to Exploit Each Vulnerability

- How long will it take for a vulnerability to be compromised?
- Who has physical access to the device, and does that matter?
- What skill is required to access the physical data?
- What skill is required to access the software and data?
- How is the attack launched?
- Have similar attacks been observed previously?
- What vulnerabilities of your system are common to others?
Step 2:

Evaluate the Barriers to Exploit Each Vulnerability

Table 1. Numerical Risk Values to Assess a Device’s Barriers to Exploitation

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Barrier Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Required to Overcome the Security Barrier</strong></td>
<td></td>
</tr>
<tr>
<td>&lt;= One Day</td>
<td>0</td>
</tr>
<tr>
<td>&lt;= One Week</td>
<td>1</td>
</tr>
<tr>
<td>&lt;= Two Weeks</td>
<td>2</td>
</tr>
<tr>
<td>&lt;= One Month</td>
<td>4</td>
</tr>
<tr>
<td>&lt;= Three Months</td>
<td>10</td>
</tr>
<tr>
<td>&lt;= Six Months</td>
<td>17</td>
</tr>
<tr>
<td>&gt; Six Months</td>
<td>19</td>
</tr>
<tr>
<td><strong>Expertise Required to Overcome Security Barrier</strong></td>
<td></td>
</tr>
<tr>
<td>Layman</td>
<td>0</td>
</tr>
<tr>
<td>Proficient</td>
<td>3</td>
</tr>
<tr>
<td>Expert</td>
<td>6</td>
</tr>
<tr>
<td>Multiple Experts</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Barrier Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Knowledge of the Target Product</strong></td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>0</td>
</tr>
<tr>
<td>Restricted Personnel</td>
<td>3</td>
</tr>
<tr>
<td>Sensitive Personnel</td>
<td>7</td>
</tr>
<tr>
<td>Critical Personnel Only</td>
<td>11</td>
</tr>
<tr>
<td><strong>Opportunity Window for Cybersecurity Attack</strong></td>
<td></td>
</tr>
<tr>
<td>Unnecessary/Unlimited Access</td>
<td>0</td>
</tr>
<tr>
<td>Easy</td>
<td>1</td>
</tr>
<tr>
<td>Moderate</td>
<td>4</td>
</tr>
<tr>
<td>Difficult</td>
<td>10</td>
</tr>
<tr>
<td><strong>Equipment Needed to Overcome Security Barrier</strong></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>0</td>
</tr>
<tr>
<td>Specialized</td>
<td>4</td>
</tr>
<tr>
<td>Bespoke</td>
<td>7</td>
</tr>
<tr>
<td>Multiple Bespoke</td>
<td>9</td>
</tr>
</tbody>
</table>
Step 3:

Evaluate the Impact of Each Vulnerability

- More subjective and can be estimated in many ways
- Potential impacts include:
  - Health and safety
  - Financial harm
  - Operational harm
  - Ecological harm
  - Restoration
  - Liability
  - Scale of impact
Step 4:

Evaluate the Severity of Exploitation

- Sum the numerical values assigned to risk in Step 2
- Combine with the impact of vulnerability in Step 3
- Prioritize which vulnerabilities should be mitigated
Step 4:

Evaluate the Severity of Exploitation

Table 2. Example of How to Categorize Risk Severity

<table>
<thead>
<tr>
<th>Barrier Value</th>
<th>Likelihood of Exploitation</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–9</td>
<td>Almost Certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>10–13</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>14–19</td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>20–24</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>=&gt;25</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Icon from Flaticon.com
Step 5:

Specify/Adapt Security Requirements and Identify Solutions

- Based on risk tolerance, review product specifications
- Ensure that extreme, high, and possibly moderate risks are mitigated with proper countermeasures
Conclusions

- Landscape of IoT devices is rapidly changing
- Increased risks of cybersecurity attacks
- Important to consider:
  - System architecture
  - Communication protocols
  - Vulnerabilities
  - Impact of cyberattacks
  - Risk mitigation techniques
  - When possible: isolate IoT products onto separate network
- Framework provides guidance on how to assess and mitigate cyber-physical risk of smart outlets
• ACEEE 2018 Summer Study Conference Proceedings:
  o Navigating Communication Protocols and Cyber Security Implications of Wireless Meter and Control Technologies for Plug Loads
Discussion:

Questions, comments, or member updates?
Thank you!

Next PPL Tech Team call: February/March 2019