Multistakeholder Process; Internet of Things (IoT) Security
Upgradability and Patching

Incentives and Barriers: How do we foster greater adoption of good
patching and updating practices?

~Status Update~
Jaunary 31, 2017
Working Groups Logistics and Composition

• Wide-range of experts representing different perspectives
• 39 members representing industry, academia, and advocacy groups
• 1- Hour Weekly meeting to share perspectives and commentaries

Our observations and current suggestions

• There is no consensus in IoT Security Upgradability and Patching
• We attempt to build a taxonomy to describe the scope and outline various incentives and barriers
## Taxonomy Overview

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Category</th>
<th>Next slide for details</th>
</tr>
</thead>
</table>
| Produce IoT       | Software               | Environmental (Barriers/Incentive)  
|                   |                        | Interactive (Barriers/Incentive)  
|                   |                        | Scale (Barriers/Incentive)  
|                   | Hardware               | Environmental (Barriers/Incentive)  
|                   |                        | Interactive (Barriers/Incentive)  
|                   |                        | Scale (Barriers/Incentive)  
| Regulate IoT      | ‘Macro’ environment     | Environmental (Barriers/Incentive)  
|                   |                        | Interactive (Barriers/Incentive)  
|                   |                        | Scale (Barriers/Incentive)  
| Use IoT           | Human user             | Environmental (Barriers/Incentive)  
|                   |                        | Interactive (Barriers/Incentive)  
|                   |                        | Scale (Barriers/Incentive)  
|                   | Machine user           | Environmental (Barriers/Incentive)  
|                   |                        | Interactive (Barriers/Incentive)  
|                   |                        | Scale (Barriers/Incentive)  |
# Producer > Software > Barriers

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental</td>
<td>Ability to patch the entire landscape</td>
</tr>
<tr>
<td></td>
<td>Media of delivery, via Internet?</td>
</tr>
<tr>
<td></td>
<td>Ability to track outstanding consumer devices (similar use of MDM)</td>
</tr>
<tr>
<td>Interactive</td>
<td>Consumer disable connectivity of device.</td>
</tr>
<tr>
<td></td>
<td>Consumer 'jail-break' device compromising security integrity (Firmware?)</td>
</tr>
<tr>
<td></td>
<td>Consumer perception of control and privacy</td>
</tr>
<tr>
<td>Scale</td>
<td>Need to track all code-lines, different technology divert code-lines.</td>
</tr>
<tr>
<td></td>
<td>number you can support (~4 trillion devices)</td>
</tr>
<tr>
<td></td>
<td>Support of legacy technology protocol</td>
</tr>
</tbody>
</table>
Some Future Directions

- Narrow and define our scope
  - Recognize consumer-grade IoT may quickly intercept with industry-control IoT
- Build a list of reference of prior work on best practices
- Build consensus on what is a barrier vs. incentive
  - Consider building a one-to-one match between barrier and incentive
- Define success-criteria and end-goal of the working group
- Define who is the audience of our deliverable