Improving IoT Security: the role of the manufacturer

Eliot Lear
Introduction
A View Through a Light Bulb

- Connected Spaces is a big deal
- Automated and efficient lighting
- Room assignment and scheduling
- Changing of conditions for different customer profiles
A non-networked light bulb

- On/Off
- Dim (Power)
- Color (R,G,B,W) %
A networked lightbulb

<table>
<thead>
<tr>
<th>On/Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dim</td>
</tr>
<tr>
<td>(Power)</td>
</tr>
<tr>
<td>Color</td>
</tr>
<tr>
<td>(R,G,B,W) %</td>
</tr>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>Crypto</td>
</tr>
<tr>
<td>Data model</td>
</tr>
<tr>
<td>Discovery</td>
</tr>
<tr>
<td>S/W management</td>
</tr>
<tr>
<td>Network</td>
</tr>
</tbody>
</table>

Enterprise + Internet
What do manufacturers wish to avoid
Why Light Bulbs May Be the Next Hacker Target

By JOHN MARKOFF  NOV. 3, 2016
General Threats To Defend Against

• Attacker causes device to not perform its function or to malfunction

• Attacker uses device to attack other systems
The Network Administrator’s Problem: Number of **Types** of Things
Cost of configuration

Static environments

Dynamic systems
What is needed?

• What is this thing?
  • Who made it?
  • Who owns it?
• **What access does it need?**
A common design pattern: the cloud

Clouds offer-

- A rendezvous point
- Substantial processing power

Cloud capabilities will continue to expand.
Understanding the attack surface
Introducing the Manufacturer Usage Descriptions (MUD)
## Assumptions and Assertions

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Assertions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Thing has a single use or a small number of uses.</td>
<td>Because a Thing has a single or a small number of intended uses, it all other uses must be unintended</td>
</tr>
<tr>
<td>Things are tightly constrained. Very <strong>VERY</strong> dumb. Resource constraints are tight.</td>
<td>Any intended use can be clearly identified</td>
</tr>
<tr>
<td>Even those Things that can protect themselves today may not be able to do so tomorrow</td>
<td>All other uses can be warned against in a statement</td>
</tr>
<tr>
<td>Network administrators are the ultimate arbiters of how their networks will be used</td>
<td>Manufacturers are in a generally good position to make the distinction</td>
</tr>
</tbody>
</table>
Translating intent into config

Any intended use can be clearly identified by the manufacturer

access-list 10 permit host controller.mfg.example.com

All other uses can be warned against in a statement by the manufacturer

access-list 10 deny any any
Expressing Manufacturer Usage Descriptions

Device emits a URI using DHCP, LLDP, or through 802.1ar

Router or firewall queries connected.example.com for policy associated with that URI

https://example.com/.well-known/mud/…

Device

Access Switch

MUD Controller

Internet

MUD File Server
How to locate the policy? A URL

The MUD File

```json
{
    "ietf-acl:access-lists": {
        "ietf-acl:access-list": [
            {
                "acl-name": "mud-10387-v4in",
                "acl-type": "ipv4-acl",
                "ietf-mud:packet-direction": "to-device",
                "access-list-entries": {
                    "ace": [
                        {
                            "rule-name": "clout0-in",
                            "matches": {
                                "ietf-mud:direction-initiated": "from-device"
                            },
                            "actions": {
                                "permit": [null]
                            }
                        },
                        {
                            "rule-name": "entin0-in",
                            "matches": {
                                "ietf-mud:controller": "http://dvr264.example.com/controller",
                                "ietf-mud:direction-initiated": "to-device"
                            },
                            "actions": {
                                "permit": [null]
                            }
                        }
                    ]
                }
            },
            {
                "acl-name": "mud-10387-v4out",
                "acl-type": "ipv4-acl",
                "ietf-mud:packet-direction": "from-device",
                "access-list-entries": {
                    "ace": [
                        {
                            "rule-name": "clout0-out",
                            "matches": {
                                "ietf-mud:direction-initiated": "to-device"
                            },
                            "actions": {
                                "permit": [null]
                            }
                        },
                        {
                            "rule-name": "entin0-out",
                            "matches": {
                                "ietf-mud:controller": "http://dvr264.example.com/controller",
                                "ietf-mud:direction-initiated": "from-device"
                            },
                            "actions": {
                                "permit": [null]
                            }
                        }
                    ]
                }
            }
        ]
    }
}
```
Expressing Manufacturer Usage Descriptions

https://example.com/.well-known/mud/

More precise config is instantiated

File server returns abstracted JSON (based on YANG)

Device

Access Switch

MUD Controller

Internet

Allow access to just controller.connected.example.com

Manufacturer's MUD File Server
## Benefits

**Customer**

- Reduces threat surface of exploding number of devices
- Almost no additional CAPEX
- Avoids lateral infections in the network
- Eases and scales access management decisions

**Manufacturer**

- Reduces manufacturer product risk at almost no cost
- Will increase customer satisfaction and reduce support costs
- Avoids the front page
- Standards-based approach
What does it mean to be connected?

<table>
<thead>
<tr>
<th>Open Access</th>
<th>Limited Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Innovation</td>
<td>Only published uses to authorized devices</td>
</tr>
</tbody>
</table>
In search of that happy middle: MUD Classes

- (same) manufacturer
- (my) controller
- local
Summary: Manufacturer Usage Descriptions

- A URI
- Use of \{dhcp, EAP-TLS, lldp\} to get it out
- Retrieval of a MUD file from a server
- Instantiation of class information onto the router
So… what should manufacturers do?

1. Recognize that they have to do some stuff
2. Make use of good coding practices (like turning off unused services)
3. Establish an incident response capability
4. Establish appropriate software management processes
5. Identify device and its profile to the network

(Nearly) all of this has been done by others!
Future work: the heavy lifting

- WPA Personal in the home is suboptimal
  (shared keys)
More information

- mud-interest@cisco.com
- lear@cisco.com
- draft-ietf-opsawg-mud-04
- draft-ietf-anima-bootstrap-keyinfra-04