Improving IoT Security: the role of the manufacturer

Eliot Lear
Introduction
The latest IoT Growth Chart

IoT Units Installed Base

Grand Total


3.8b 4.9b 6.4b

25b+
The Network Administrator’s Problem: Number of Types of Things
Cost of configuration

Static environments

Dynamic systems
How to secure manageability and security?

Device protects itself
- Secure development practices

Network protects device
- Device identification
- Automated segmentation
Assumptions and Assertions

**Assumptions**

A Thing has a single use or a small number of uses

Things are tightly constrained. CPU and memory resource constraints are tight.

Even those Things that can protect themselves today may not be able to do so tomorrow

Network administrators are the ultimate arbiters of how their networks will be used

**Assertions**

Because a Thing has a single or a small number of intended uses, it all other uses must be unintended

Any intended use can be clearly identified

All other uses can be warned against in a statement

Manufacturers are in a generally good position to make the distinction
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

Device emits a 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",
   ....
  }
}
```
In search of that happy middle: MUD Classes

- (same) manufacturer
- (my) controller
- local
- DNS-based ACLs
Expressing Manufacturer Usage Descriptions

More precise config is instantiated

File server returns abstracted JSON (based on YANG)

https://example.com/.well-known/mud/…

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, devices get own3ed</td>
<td>Permission required to innovate, but safer applications.</td>
</tr>
</tbody>
</table>
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
Recently…

- draft-ietf-opsawg-mud-13 has completed both WGLC and IETF last call
- A few changes coming out of these last calls
  - Improved privacy considerations
  - Improved terminology consistency
  - A few editorial issues
  - Clarity on use of HTTPS processing
  - MASA server pulled out of core document and moved to an extension
- One issue:
  - Normative dependency on draft-ietf-netmod-acl-model
    (That draft has some issues – for our draft this is syntax – we should be able to easily accommodate changes)
Looking forward

- Probably a new draft in response to previous slide to resolve comments
- Extensions
  - MASA server from BRSKI
  - Some want means to find semantic definitions
  - Pointers to other Thing descriptions (various databases)
More information

• mud-interest@cisco.com
• lear@cisco.com
• draft-ietf-opsawg-mud-13