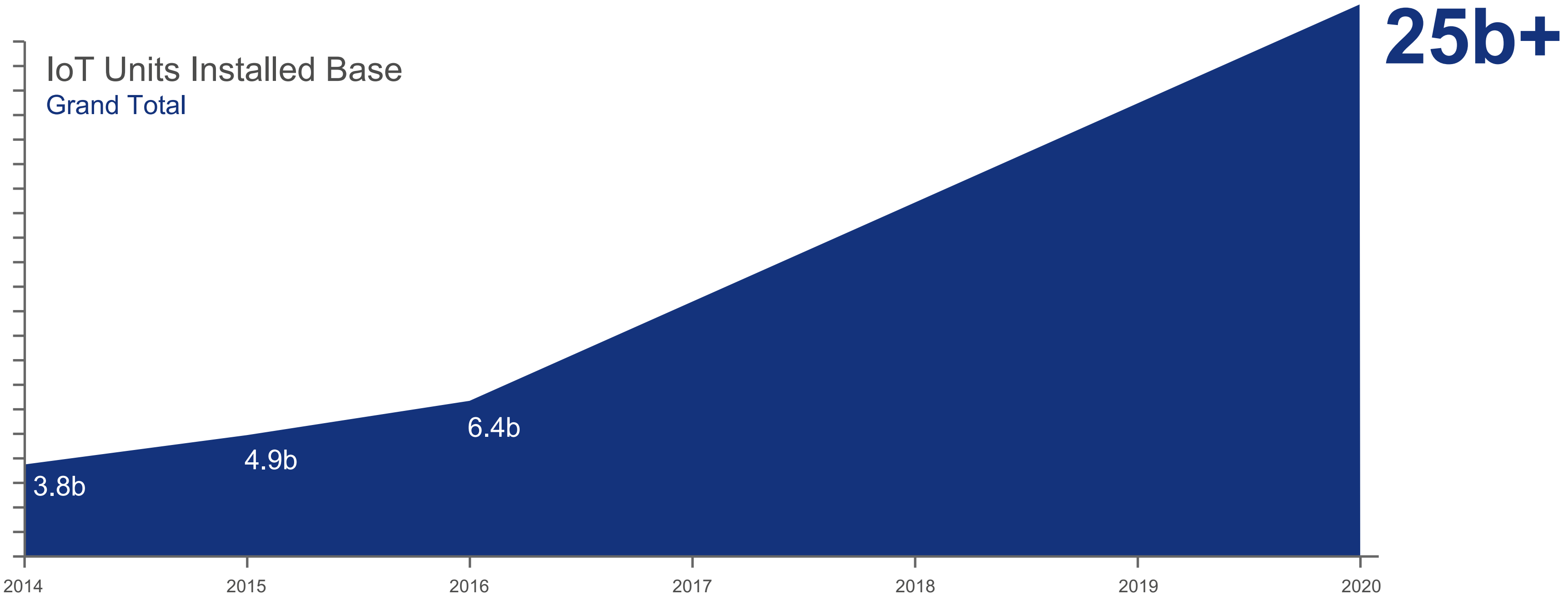
Improving IoT Security: the role of the manufacturer

Eliot Lear

Introduction

The latest IoT Growth Chart



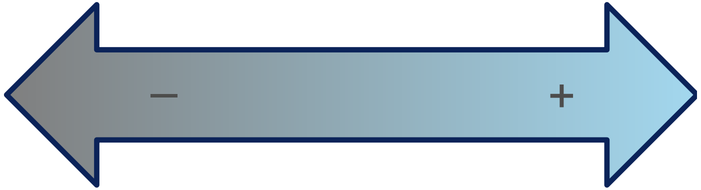
Source: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

The Network Administrator's Problem: Number of **Types** of Things

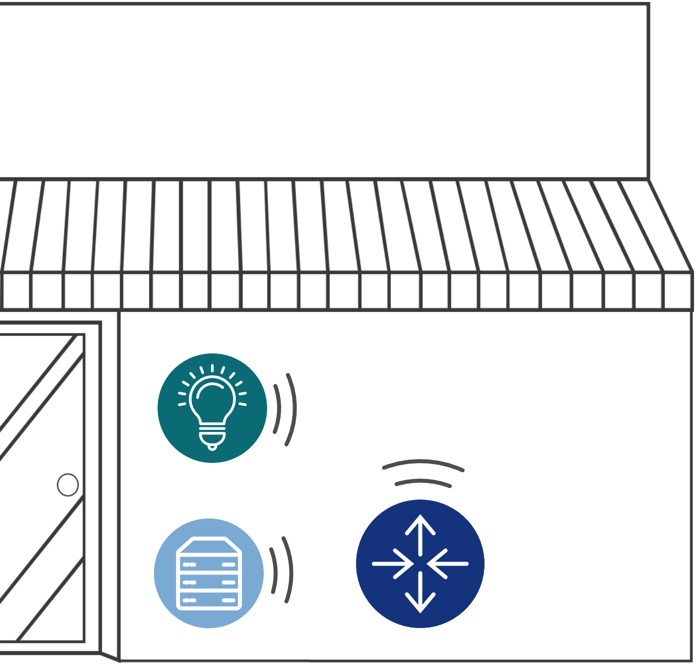
Cost of configuration

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	Assertions
A Thing has a single use or a small number of uses	Because a Thing has a single or a small number of intended uses, it all other uses must be unintended
Things are tightly constrained. CPU and memory resource constraints are tight.	Any intended use can be clearly identified
Even those Things that can protect themselves today may not be able to do so tomorrow	All other uses can be warned against in a statement
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to make the distinction

Drug Facts

Active Ingredient (in each tablet) **Purpose**
Aspirin 81 mg...Pain reliever

Uses
for the temporary relief of minor aches and pains or as recommended by your doctor. Because of its delayed release action, this product will not provide fast relief of headaches or other symptoms needing immediate relief.

Do not use ·if you have ever had an allergic reaction to any other pain relievers/ fever reducers.

Warnings
Reyes syndrome: Children and teenagers who have or are recovering from chicken pox or flu-like symptoms should not use this product. When using this product, if changes in behavior with nausea and vomiting occur, consult a doctor because these symptoms could be an early sign of Reye's syndrome, a rare but serious illness.

Ask a doctor before use if you have ·stomach problems (such as heartburn, upset stomach, or stomach pain) that last or come back ·bleeding problems ·ulcers ·asthma
Ask a doctor or pharmacist before use if ·you are taking a prescription drug for ·diabetes ·gout ·arthritis

Allergy alert: Aspirin may cause a severe allergic reaction which may include: ·facial swelling ·asthma (wheezing) ·shock ·hives

Alcohol warning If you consume 3 or more alcoholic drinks every day. Ask your doctor whether you should take aspirin or other pain relievers/fever reducers. Aspirin may cause stomach bleeding.

Stop use and ask doctor if an allergic reaction occurs. Seek medical help right away. ·Pain gets worse or lasts more than 10 days ·redness or swelling is present ·new symptoms occur
the ears or loss of hearing occurs

If pregnant or breast-feeding ask a health professional
It is espcially important not to use aspirin during th
of pregnancy unless definitely directed to do so
because it may cause problems in the unborn
complications during delivery.

Keep out of the reach of children. In case of
help or contact a Poison Control Center imme

Directions
·drink a full glass of water with each dose. ·A
12 years of age and over: take 4 to 8 tablets e
exceed 48 tablets in 24 hours unless directed
·Children under 12 years: consult a doctor

Other Information ·store at room temperature

Inactive Ingredients collodial silicon dioxide
sodium, FD&C Yellow #10 al lake, FD&C Yel
methacrylic and copolymer, microcrystalline
acid, talc, titanium dioxide, triethyl citrate

GOODSENSE
For Adults
Safe Pain Relief Plus Lifesaving Benefits**
Aspirin
Pain Reliever/Fever Reducer (NSAID)
Fast, Safe Pain Relief
• Headaches
• Everyday Aches & Pains
Compare to active ingredient of Bayer® Aspirin
500 Coated Tablets - 325 mg

Translating intent into config

Any intended use can be clearly identified by the manufacturer

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

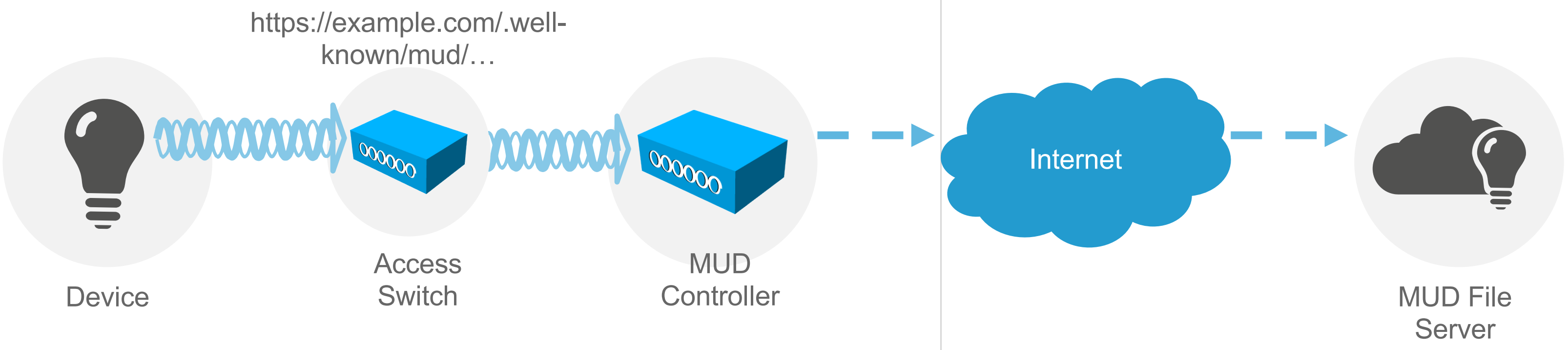
All other uses can be warned against in a statement by the manufacturer

```
access-list 10 deny any any
```

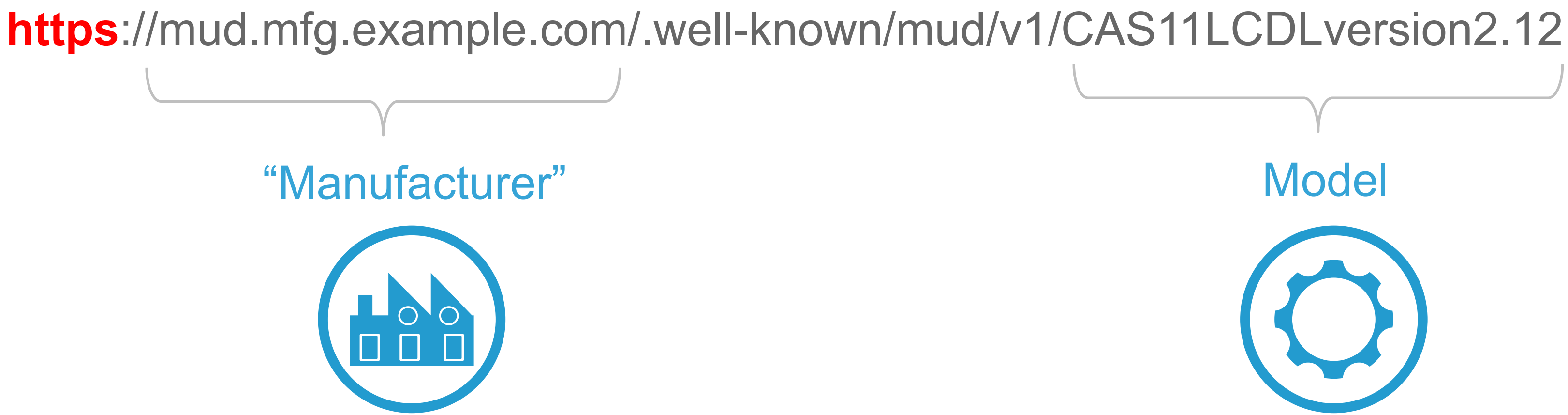
Expressing Manufacturer Usage Descriptions

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

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



How to locate the policy? A URL



https://mud.mfg.example.com/.well-known/mud/v1/CAS11LCDLversion2.12

“Manufacturer”

Model

The MUD File

```
{
"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",
….
```

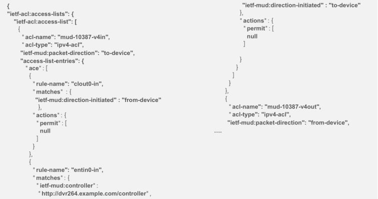
In search of that happy middle: MUD Classes

- (same) manufacturer
- (my) controller
- local
- DNS-based ACLs

Expressing Manufacturer Usage Descriptions

More precise config is instantiated

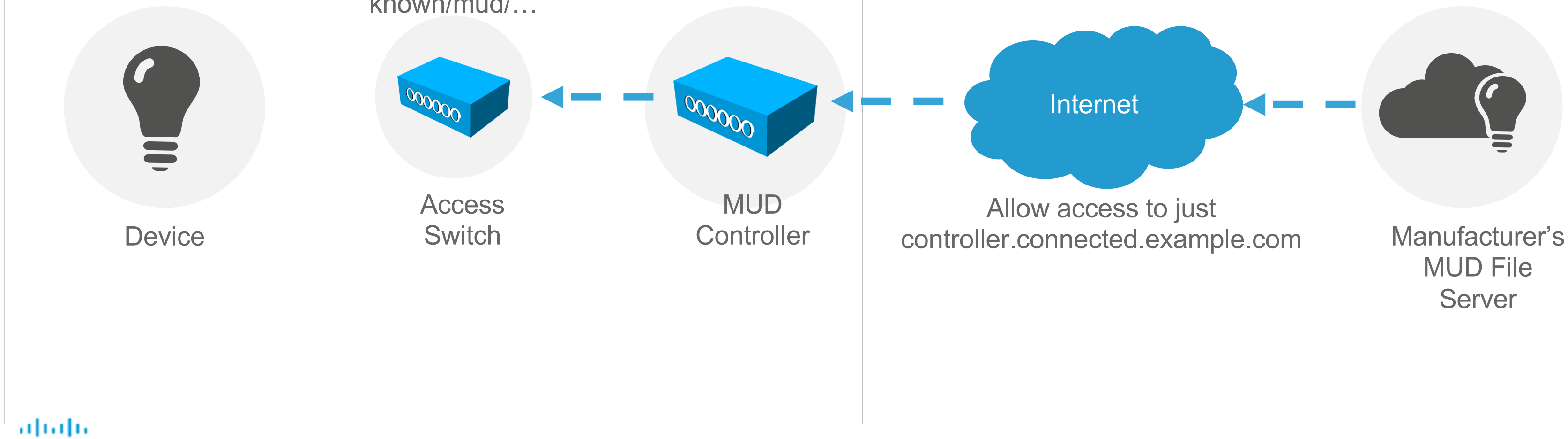
File server returns abstracted JSON (based on YANG)



```
{
"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",
   ....
```

https://example.com/.well-known/mud/…



Allow access to just controller.connected.example.com

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?

Open Access	Limited Access
Open Innovation, devices get 0wn3ed	Permission required to innovate, but safer applications.

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