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

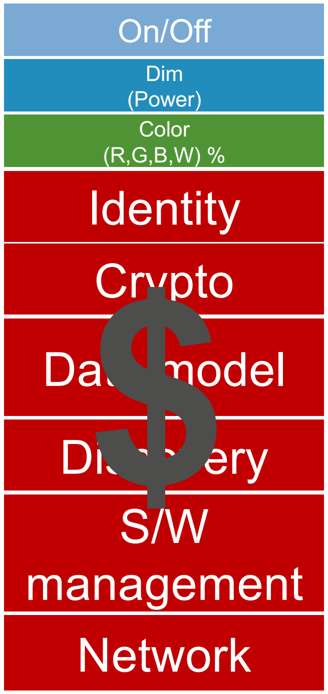
A non-networked light bulb

On/Off

Dim
(Power)

Color
(R,G,B,W) %

A networked lightbulb



On/Off

Dim
(Power)

Color
(R,G,B,W) %

Identity

Crypto

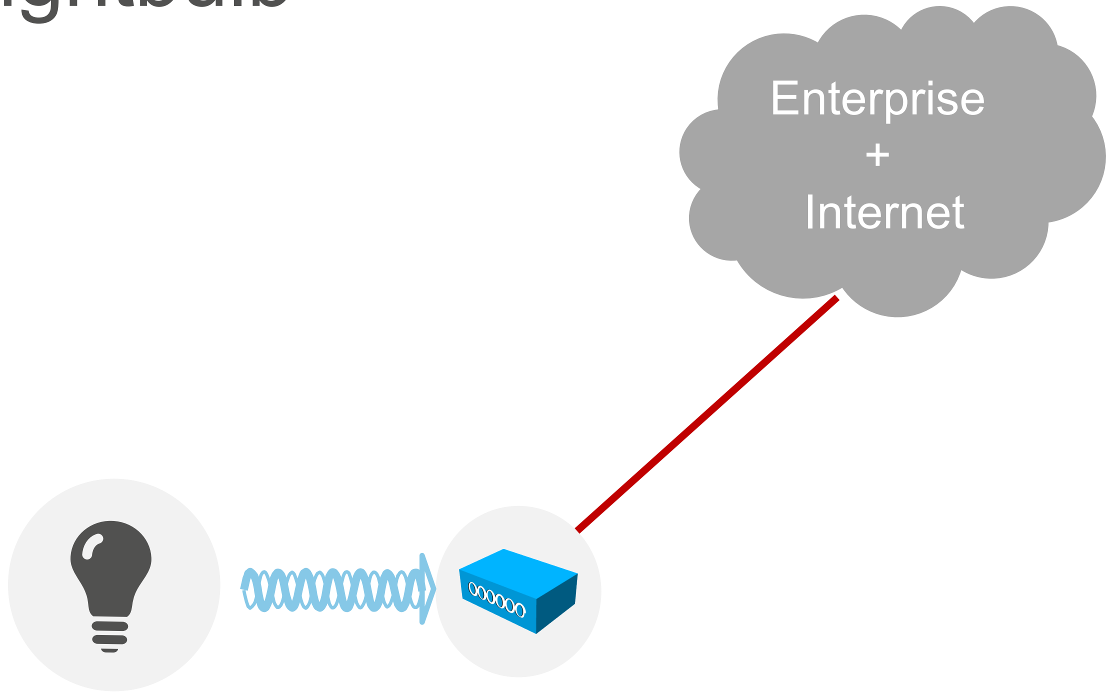
Data model

Discovery

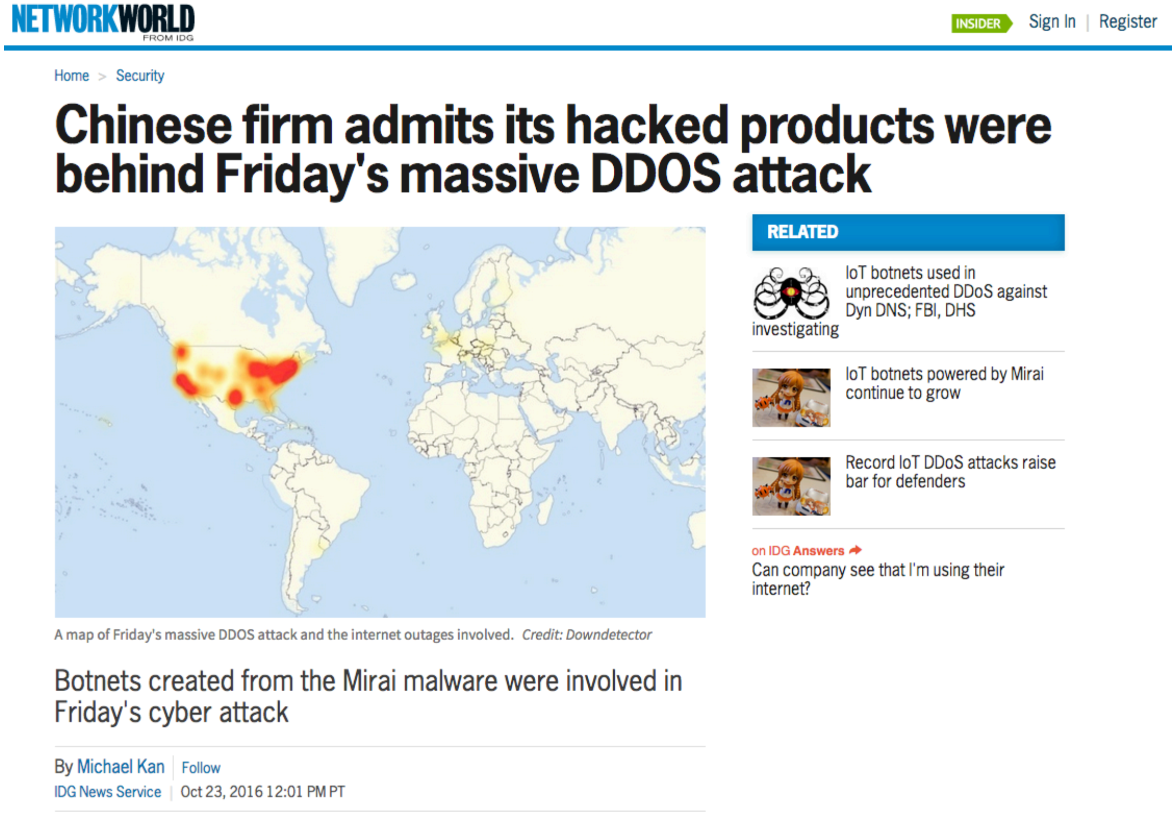
S/W
management

Network

$



What do manufacturers wish to avoid



NETWORKWORLD FROM IDG

INSIDER Sign In | Register

Home > Security

Chinese firm admits its hacked products were behind Friday's massive DDOS attack

A map of Friday's massive DDOS attack and the internet outages involved. *Credit: Downdetector*

Botnets created from the Mirai malware were involved in Friday's cyber attack

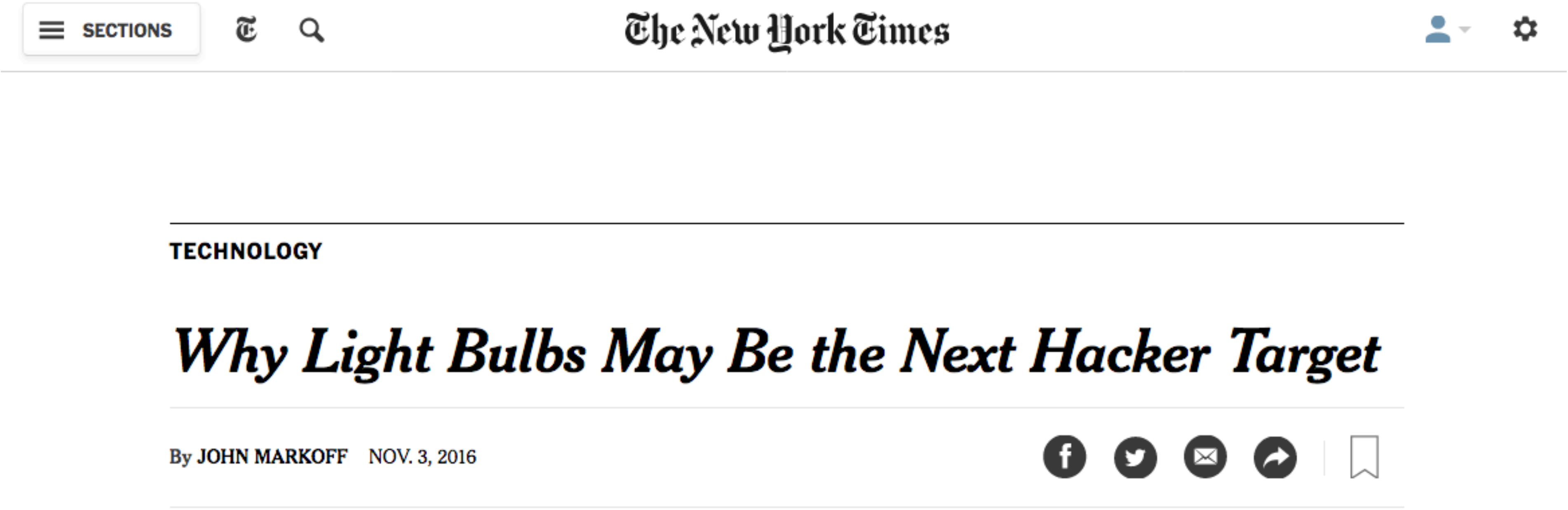
By Michael Kan | Follow
IDG News Service | Oct 23, 2016 12:01 PM PT

RELATED

- IoT botnets used in unprecedented DDoS against Dyn DNS; FBI, DHS investigating
- IoT botnets powered by Mirai continue to grow
- Record IoT DDoS attacks raise bar for defenders

on IDG Answers

Can company see that I'm using their internet?



The New York Times

TECHNOLOGY

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

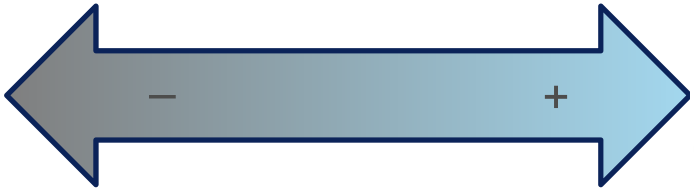
By AMIR MARINE (Wikimedia) - Own work, CC BY-SA 3.0,

- Attacker uses device to attack other systems

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

Cost of configuration

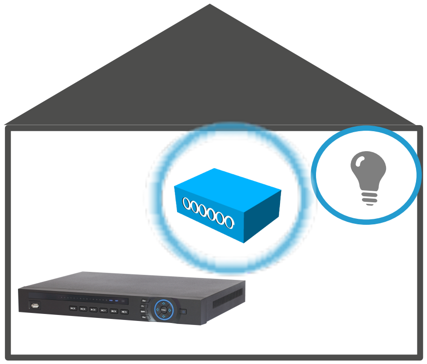
Static environments



Dynamic systems

What is needed?

- What is this thing?
  - Who made it?
  - Who owns it?
- **What access does it need?**

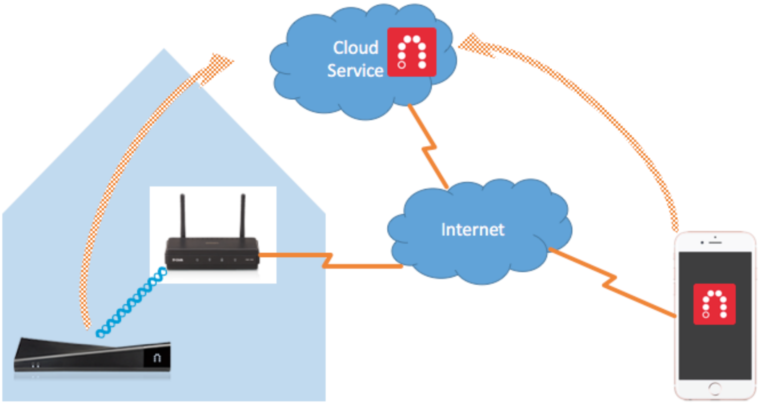


A common design pattern: the cloud

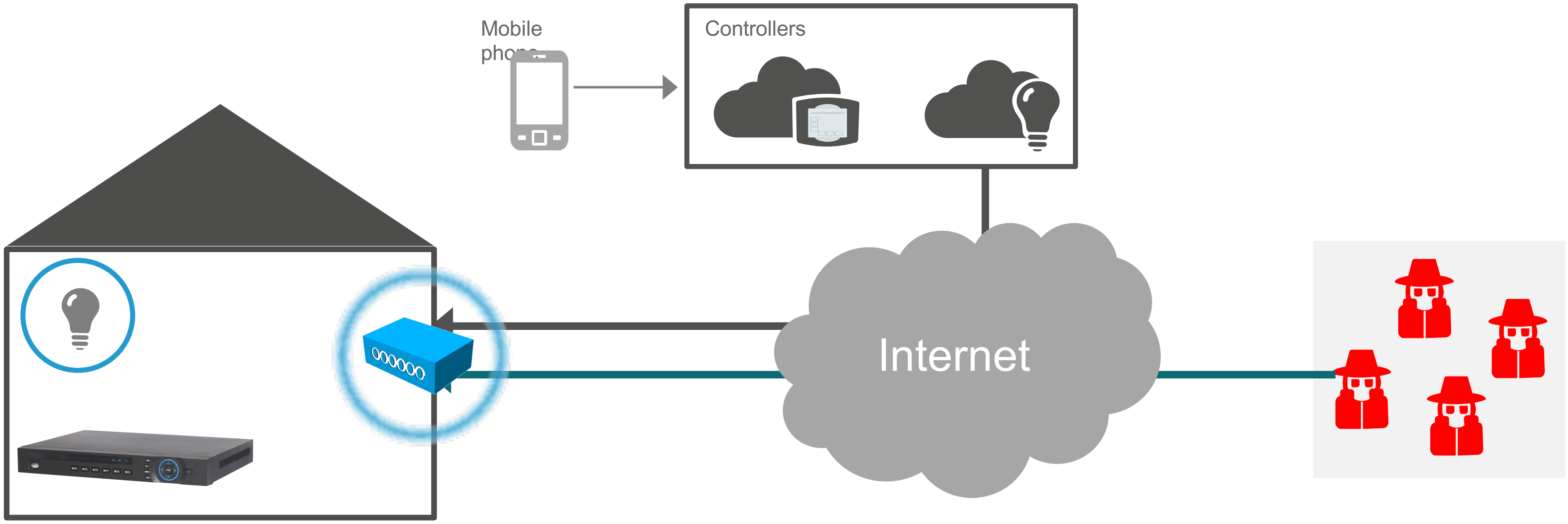
Clouds offer-

- A rendezvous point
- Substantial processing power

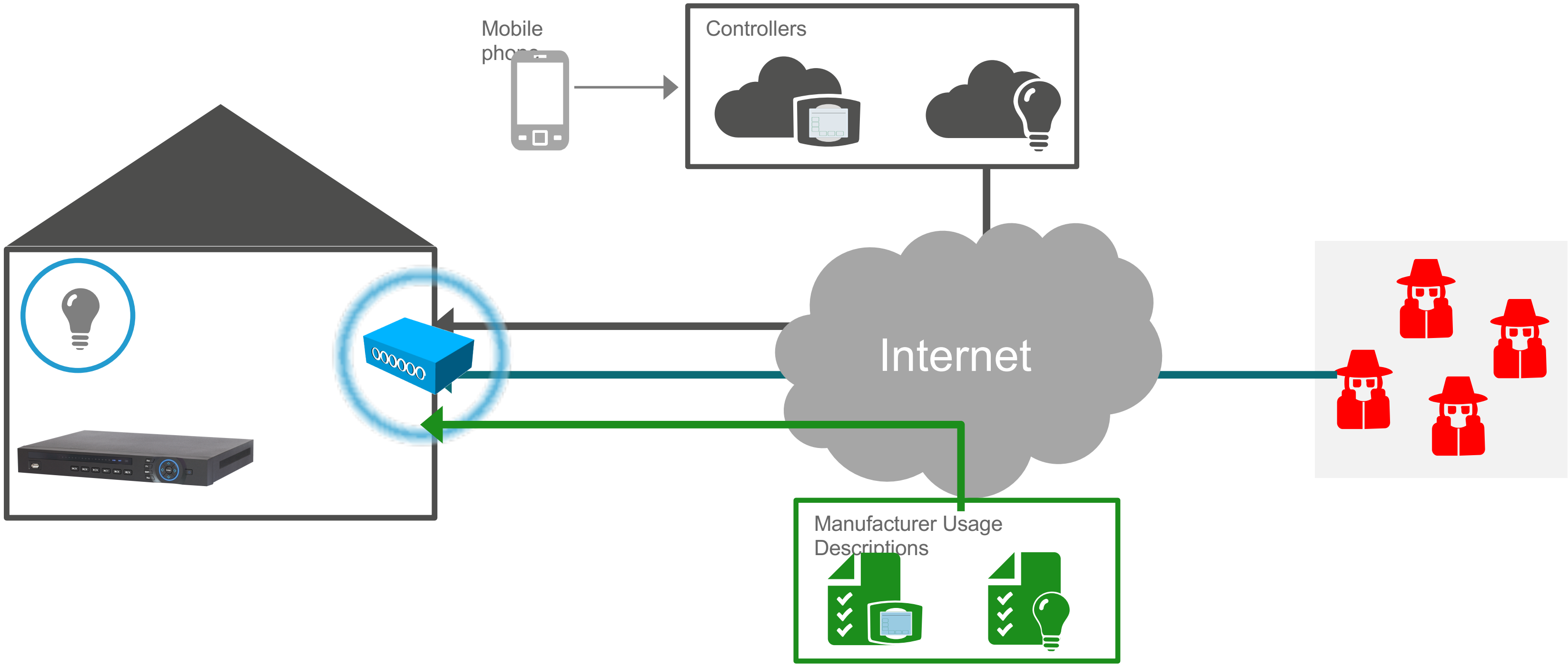
Cloud capabilities will continue to expand.



Understanding the attack surface

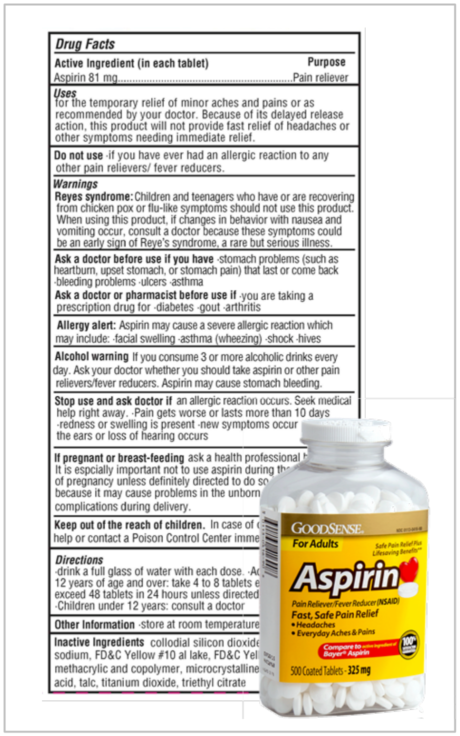


Introducing the Manufacturer Usage Descriptions (MUD)



Assumptions and Assertions

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. Very **VERY** dumb. 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
100%
500 Coated Tablets - 325 mg

Translating intent into config

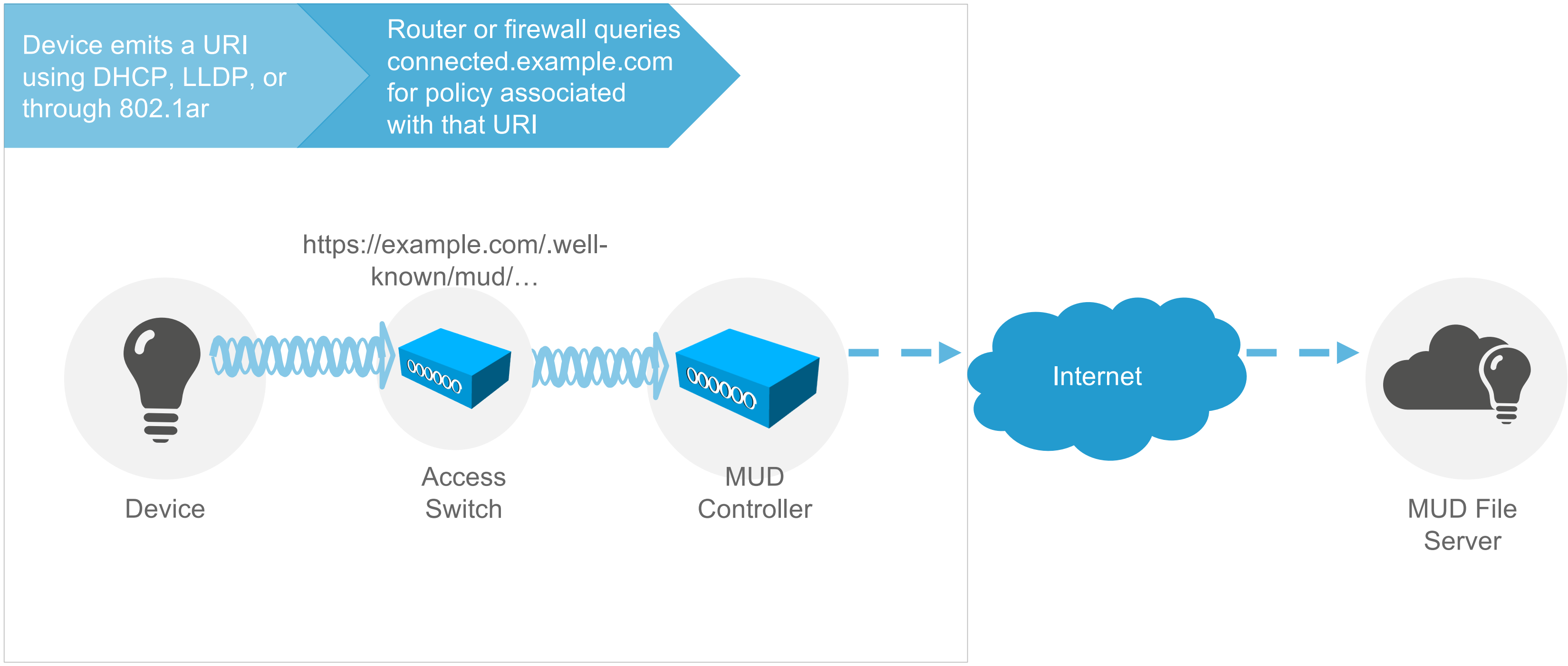
Any intended use can be clearly identified by the manufacturer

```
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

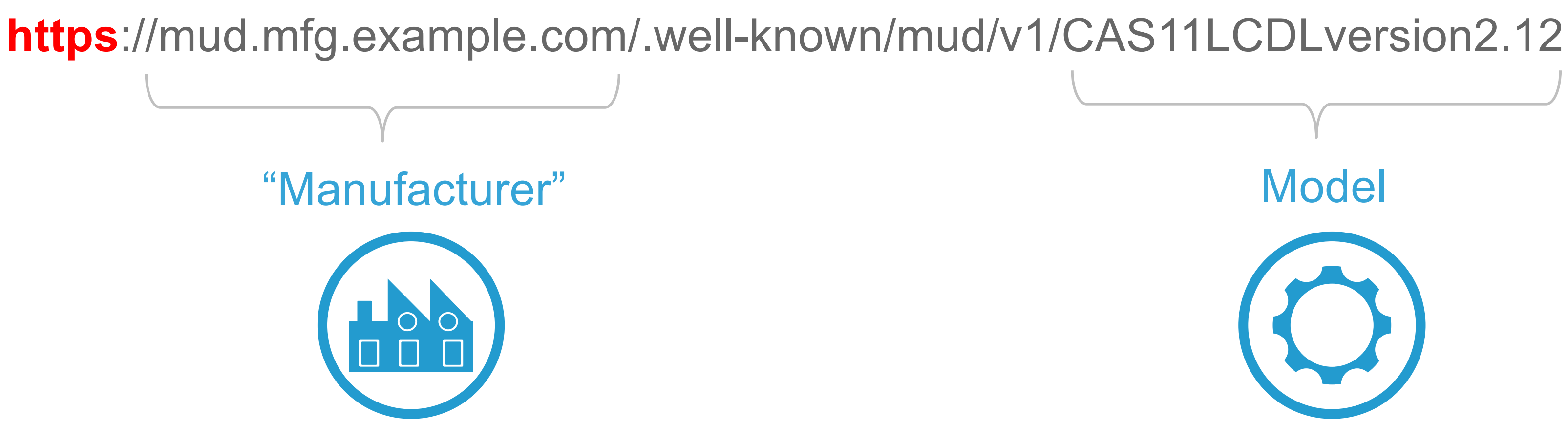


Device emits a URI using DHCP, LLDP, or through 802.1ar

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

https://example.com/.well-known/mud/…

How to locate the policy? A URL



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

“Manufacturer”

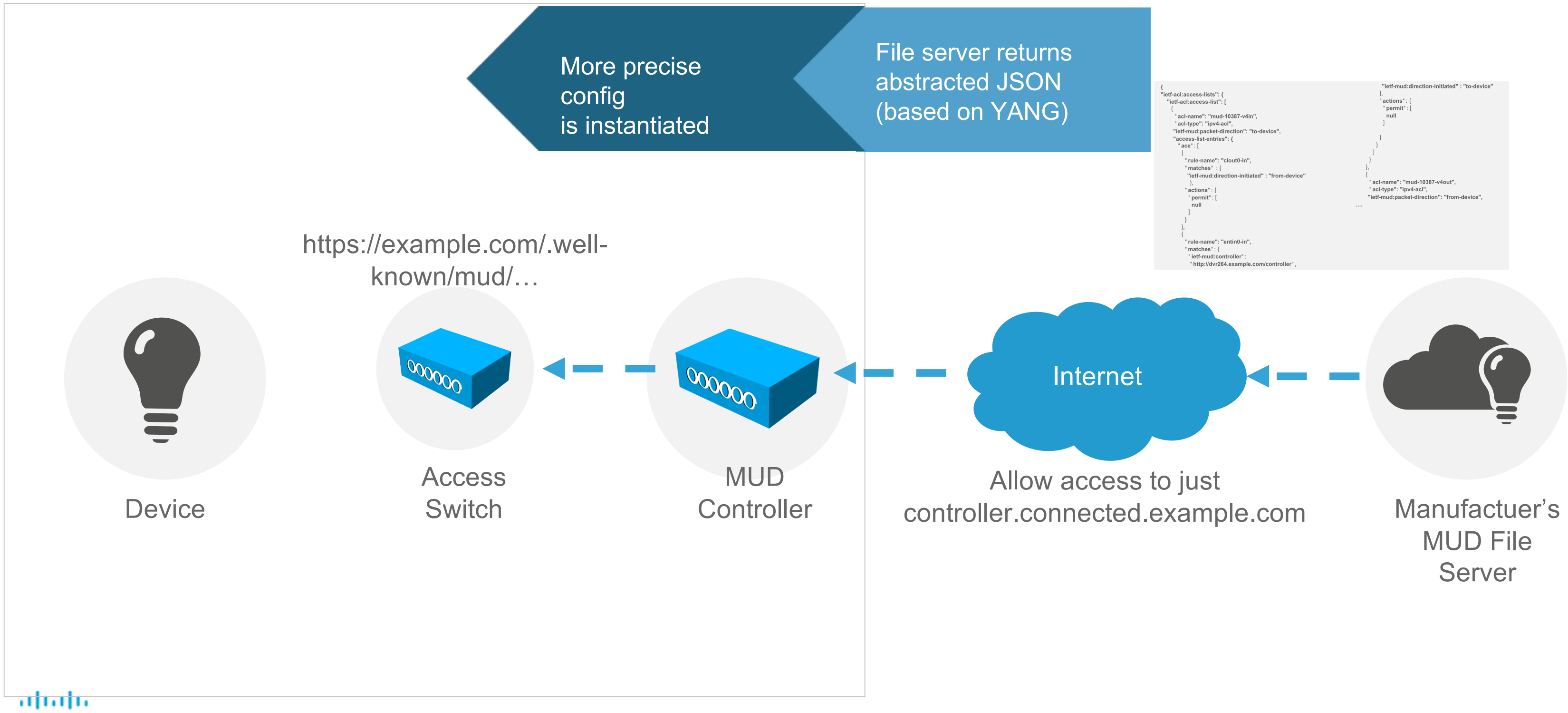
Model

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",
….
```

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

Manufactuer’s MUD File Server

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

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	Only published uses to authorized devices

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?

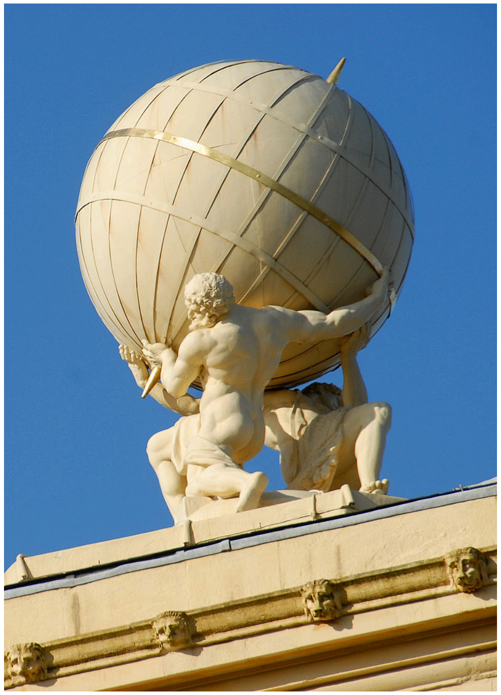
1. Recognize that they have to do some stuff
2. Make use of good coding practices (like turning off unused services)
3. Establish an incident response capability
4. Establish appropriate software management processes
5. **Identify device and its profile to the network**

(Nearly) all of this has been done by others!

Future work: the heavy lifting

- WPA Personal in the home is **suboptimal**

  (shared keys)



By Cwawebber - Own work, CC BY 3.0

More information

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

cisco