

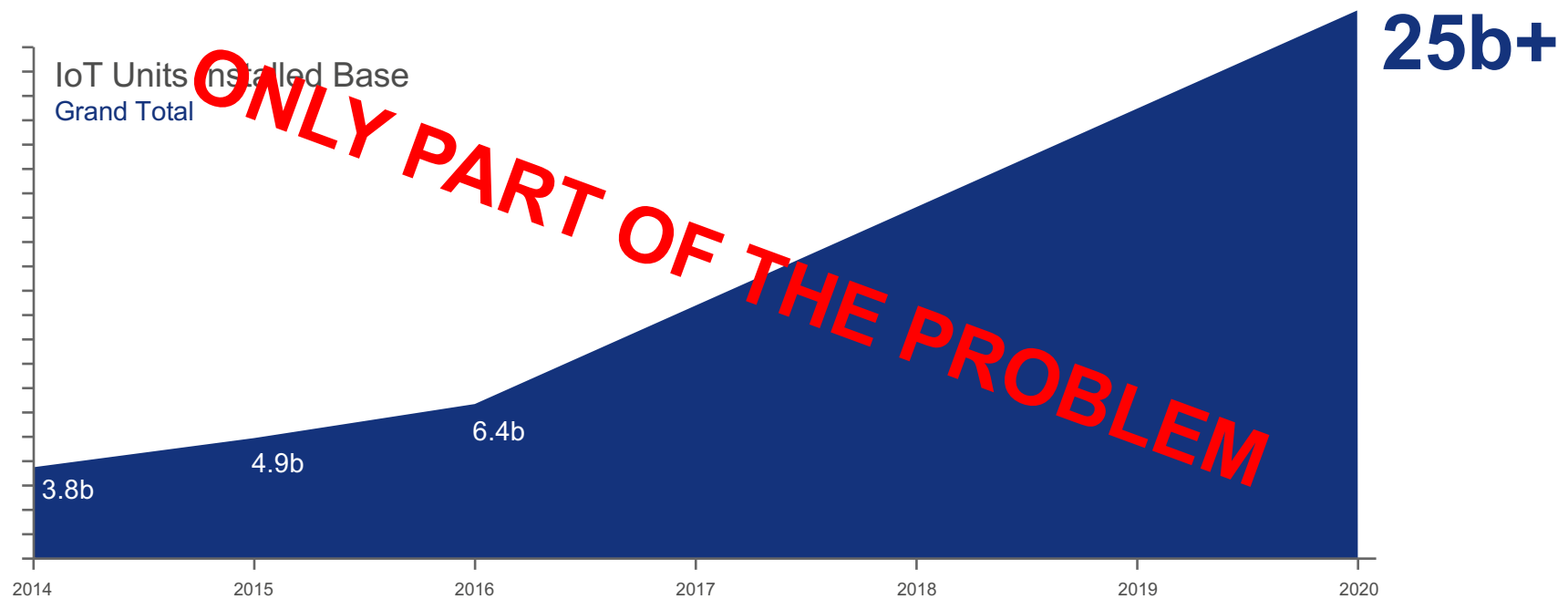


Improving IoT Security: the role of the manufacturer

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>



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

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 Reyes'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 especially important not to use aspirin during the last 3 months of pregnancy unless definitely directed to do so, because it may cause problems in the unborn child or complications during delivery.	
Keep out of the reach of children. In case of emergency, get help or contact a Poison Control Center immediately.	
Directions	
drink a full glass of water with each dose. Adults and teenagers: take 1 to 2 tablets every 4 to 6 hours. Do not exceed 48 tablets in 24 hours unless directed by a doctor. Children under 12 years: consult a doctor.	
Other information store at room temperature.	
Inactive ingredients colloidal silicon dioxide, croscarmellose sodium, FD&C Yellow #10 lake, FD&C Yellow #6 lake, hydroxypropyl methylacrylate copolymer, microcrystalline cellulose, talc, titanium dioxide, triethyl citrate.	



Translating intent into config

Any intended use can be clearly
identified by the manufacturer



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

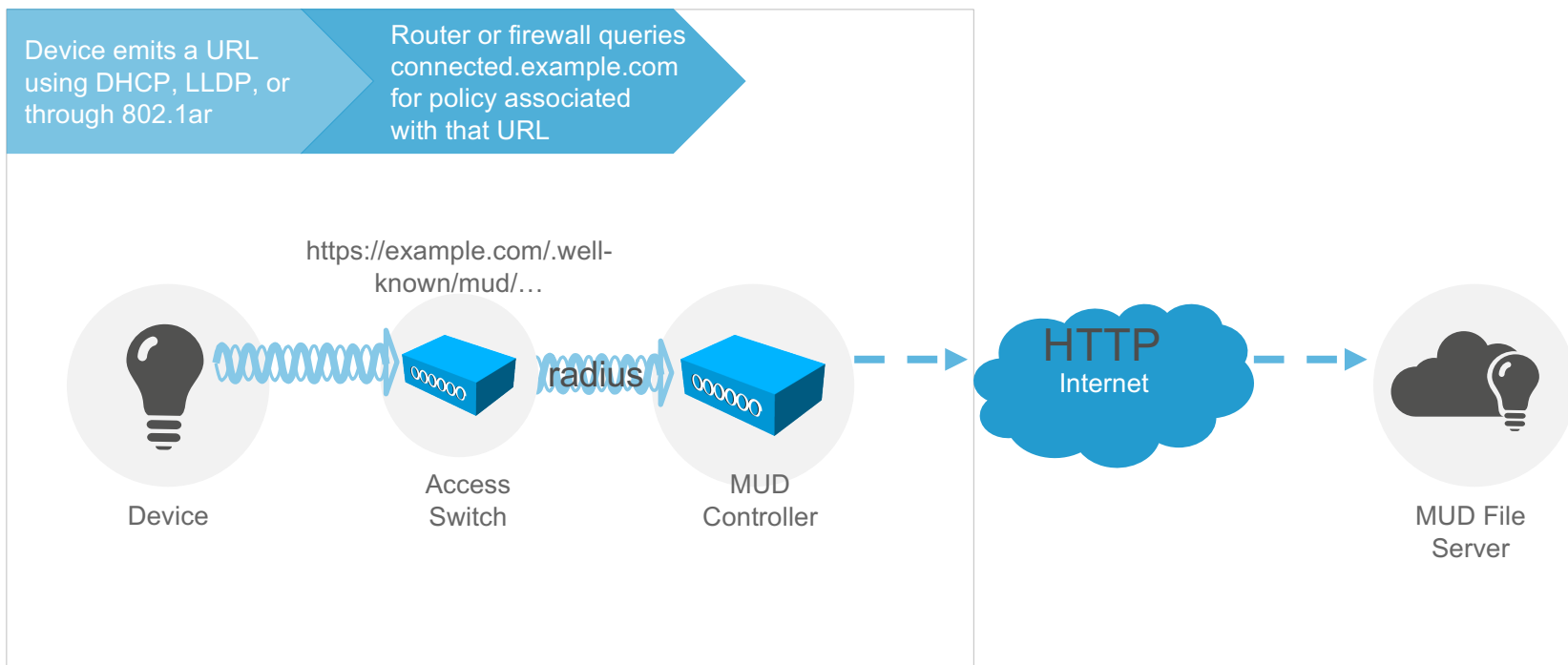
All other uses can be warned against
in a statement by the manufacturer



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



Expressing Manufacturer Usage Descriptions



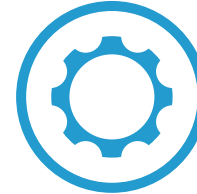
How to locate the policy? A URL

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

“Manufacturer”



Model



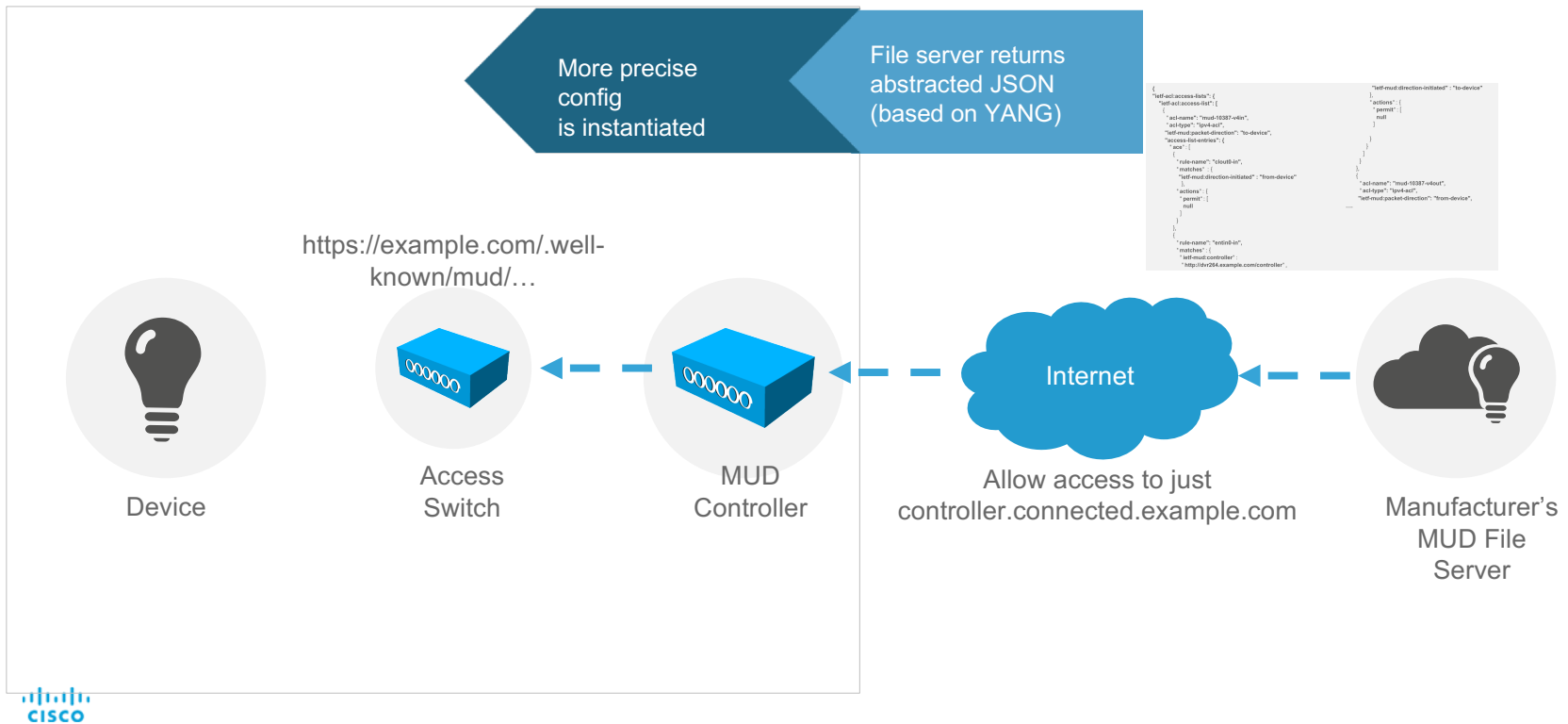
The MUD File

```
{
  "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
                ]
              }
            }
          ]
        }
      },
      {
        "rule-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



Summary: Manufacturer Usage Descriptions

- MUD doesn't use NETCONF – no capabilities exchange
- MUD doesn't configure devices, nor contain device models
- MUD is-
 - A URI
 - Use of {dhcp, EAP-TLS, lldp} to get it out
 - Retrieval of a MUD file from a server via HTTP
 - Instantiation of class information onto the router, switch, or firewall

More information

- mud-interest@cisco.com
- lear@cisco.com
- draft-ietf-opsawg-mud-07

