Securing IoT Devices with Manufacturer Usage Descriptions

Eliot Lear
Principal Engineer, Enterprise Chief Technology Office
10 Apr 2019
Today's latest threat: printers

Study cites multi-function printers as some of the most dangerous members of the IoT family

Bitdefender.com, 28 February 2019
What Sort of Access Do These Printers Require?

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer</td>
<td>xmpp009.hpeprint.com</td>
<td>TCP</td>
<td></td>
<td>80, 443, 5222,5223</td>
</tr>
<tr>
<td>Printer</td>
<td>DNS Server</td>
<td>UDP</td>
<td></td>
<td>53</td>
</tr>
<tr>
<td>Printer</td>
<td>chat.hpeprint.com</td>
<td>TCP</td>
<td></td>
<td>80,443</td>
</tr>
<tr>
<td>Printer</td>
<td>224.0.0.251/32</td>
<td>UDP</td>
<td></td>
<td>5353</td>
</tr>
<tr>
<td>Printer</td>
<td>220.0.0.252/32</td>
<td>UDP</td>
<td></td>
<td>5355</td>
</tr>
<tr>
<td>Printer</td>
<td>h10141.www1.hp.com</td>
<td>TCP</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td>Printer</td>
<td>Local Networks</td>
<td>UDP</td>
<td>5353</td>
<td></td>
</tr>
<tr>
<td>Printer</td>
<td>Local Networks</td>
<td>TCP</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

Source: University of New South Wales, using mudgee

(not shown: L2 packets)
Our First Three Questions

• Is that information correct?
  • Maybe: Not sourced from vendor

• How does the administrator learn it?
  • Scanned network for some number of days

• What vulnerabilities does that device have?
  • Can’t tell because we probably don’t have model information

And consider how much time it will take for that one device.
## 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, all other uses must be unintended.</td>
</tr>
<tr>
<td>Things are tightly constrained. Very little CPU, memory, and battery.</td>
<td>Any intended use can be clearly identified.</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 provide guidance to administrators.</td>
</tr>
<tr>
<td>Even those Things that can protect themselves today may not be able to do so tomorrow</td>
<td>A mechanism is needed to protect devices that may have vulnerabilities.</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
```
Introducing Manufacturer Usage Descriptions (MUD)

A URL:
https://manufacturer.example.com/mydevice.json

A MUD File:
```
"ace": [ { "name": "db-kdevel", "match": { "set:mud:md": [ "my-controller": [ null ] ] }, "actions": { "forwarding": "accept" } } ]
```

The MUD Manager:

The MUD File Server:
Expressing Manufacturer Usage Descriptions

Device emits a URL

Access Switch forwards

ISE/DNA-C queries manufacturer

https://example.com/mud/…

Enterprise Network

DHCP, LLDP, or 802.1X

Radius

MUD Manager

Internet

MUD File Server

© 2019 Cisco and/or its affiliates. All rights reserved.
Getting from the MUD file to deployment config

```json
... "acl": [  
  {  
    "name": "mud-76228-v4to",
    "type": "ipv4-acl-type",
    "aces": {  
      "ace": [  
        {  
          "name": "myctl0-todev",
          "matches": {  
            "ietf-mud:mud": {  
              "my-controller": [  
                null
              ]
            }
          },
          "actions": {  
            "forwarding": "accept"
          }
        }
      ]
    }
  }
] ...
```

Whatever is appropriate in the local deployment.

10.1.2.3
10.4.5.6

https://mudmaker.org
## Manufacturers Use Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Used for</th>
<th>Filled in by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td>Cloud-based controllers</td>
<td>IOS</td>
</tr>
<tr>
<td>(My) Controller</td>
<td>Access to controllers</td>
<td>Administrator</td>
</tr>
<tr>
<td>same-manufacturer</td>
<td>Access to devices that are built by the same manufacturer</td>
<td>MUD Manager</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Access to devices that are built by specified manufacturer</td>
<td>Manufacturer and MUD Manager</td>
</tr>
<tr>
<td>Local</td>
<td>Used when device needs access to the local network</td>
<td>Administrator</td>
</tr>
</tbody>
</table>
Make Your Own MUD File

Welcome to MUD File Maker!

This page will help you create a Manufacturer Usage Description (MUD) file for your web site. MUD files can be used by local networks to determine how they should protect your products. You should only list communications on this page that you have designed your product to have. For more information, see RFC 8520.

Some resources you might find interesting (apart from this page):

- The MUD specification
- The Cisco POC MUD Manager
- The OSmud.org MUD Manager

Some Samples

<table>
<thead>
<tr>
<th>A device that just needs to talk to a single cloud service</th>
<th>Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>A device that just needs to talk to its local controllers</td>
<td>My Controller</td>
</tr>
<tr>
<td>A device that just needs to talk to devices from the same manufacturer</td>
<td>Same Manufacturer</td>
</tr>
</tbody>
</table>

If you use the samples, you will need to modify some of the fields, and of course sign them.

Make Your Own!
So for instance…

(Just a snippit)
Expressing Manufacturer Usage Descriptions

devices segmented

Device

Access Switch

MUD Manager

Enterprise config created

Approval

Internet

https

MUD File Server

Enterprise Network

Manufacturer JSON file returned

© 2019 Cisco and/or its affiliates. All rights reserved.
Results: Micro-segmentation of that printer

- Access limited to devices based on manufacturer recommendations
- Policy choices easily identified by MUD file
- Hacked devices can’t probe for holes
- An additional layer of security
  - BUT- manufacturers should still **always** secure their devices
Next Steps

- More MUD tooling
- MUD for 5G
- More implementations!
Thank You!
Credit to... (Creative Commons Licensing)

• The Printer