Manufacturer Usage Descriptions

draft-lear-mud-framework-01

Eliot Lear
6 April 2016
Number of connected devices (Billions)
The Real Problem

• We don’t know how to manage larger numbers of *types* of devices
• We don’t even know how to count how many types of devices there are
When this matters

Static environments  -  Dynamic systems

6 April 2016
The Network Needs Two Pieces of Information

• What the device is

• How the network should protect it
We have some constraints

- Devices have very few resources to devote to security.
- The larger the footprint on the endpoint, the larger the threat surface (more code = more bugs)
- Strong security will not be possible in some instances.
### How Should the Network Protect the Device?

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Assertions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A thing has an IP stack and a use or a single number of uses.</td>
<td>Because a Thing has a single or a small number of intended uses, it all other uses must be unintended.</td>
</tr>
<tr>
<td>With many <strong>types of things</strong>, it will not be possible for security vendors to profile them all.</td>
<td>Any intended use can be clearly identified by the manufacturer.</td>
</tr>
<tr>
<td>Even those Things that can protect themselves today may not be able to do so in the future.</td>
<td>All other uses can be warned against in a statement by the manufacturer.</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 make the distinction.</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 any
How to locate the policy? A URI


“Manufacturer”

Model

Version
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/…

Device

Access Switch

MUD Controller

Internet

MUD File Server

6 April 2016
Makes use of YANG-based XML

<?xml version = '1.0' encoding = 'UTF-8'? >
<edit-config
<mud:supportInformation>
<mud:lastUpdate>2015-05-12T20:00:50Z</mud:lastUpdate>
<mud:cacheValidity>1440</mud:cacheValidity>
</mud:supportInformation>
<config>
<top>
<acl:access-list>
<acl:access-list-entries>
<acl:access-list-entry>
<acl:rule-name>access-thermostat-controller</acl:rule-name>
<acl:matches>
/inet:hostname>controller.example.com</inet:hostname>
</acl:matches>
<acl:actions>
</acl:actions>
</acl:access-list-entry>
</acl:access-list-entries>
</acl:access-list>
</top>
</config>
</edit-config>

<acl:matches>
<mud:sameManufacturer/>
</acl:matches>
<acl:actions>
<acl:permit/>
</acl:actions>
<acl:access-list-entry>
<acl:rule-name>deny-other</acl:rule-name>
<acl:actions>
<acl:deny/>
</acl:actions>
</acl:access-list-entry>
</acl:access-list-entries>
</acl:access-list>
</top>
</config>
</edit-config>

Only the text in red would have to change with the proposed standardization
Expressing Manufacturer Usage Descriptions

More precise config is instantiated

Site returns abstracted XML (based on YANG) to device or firewall

https://example.com/.well-known/mud/…

Device

Access Switch

MUD Controller

Internet

Allow access to just controller.connected.example.com

MUD File Server

6 April 2016
So what do we need to do this?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A way to communicate identifiers</td>
<td>IEEE 802.1AR &amp; IEEE 802.1X, DHCP, LLDP</td>
</tr>
<tr>
<td>A way to express network configuration</td>
<td>YANG</td>
</tr>
<tr>
<td>A way to retrieve the policy</td>
<td>HTTP/TLS</td>
</tr>
<tr>
<td>An access-list model</td>
<td>draft-ietf-netmod-acl-model</td>
</tr>
<tr>
<td>A URI to point at the policy</td>
<td>draft-lear-ietf-netmod-mud</td>
</tr>
<tr>
<td>Use of DNS Names in ACLs</td>
<td>draft-lear-ietf-acl-dnsname-00</td>
</tr>
<tr>
<td>A new PKIX constraint for the URI</td>
<td>draft-lear-ietf-pkix-mud-extension-00</td>
</tr>
<tr>
<td>A DHCP option for the URI (2nd best)</td>
<td>draft-lear-ietf-dhc-mud-option-01</td>
</tr>
<tr>
<td>An LLDP TLV</td>
<td>(later)</td>
</tr>
</tbody>
</table>
IEEE 802.1AR has stronger security properties

DHCP is the 2nd choice to deliver the MUD URI

DHCP is still useful - assertion is from the device for its protection.

No code impact for systems already implementing 802.1AR

Very easy to implement and deploy for any system already implementing DHCP
Some comments

- New use of YANG model
  - Not tied to NETCONF
  - MUD files need to be signed
  - Extensibility is a little tricky (no capabilities exchange)
  - Perhaps some challenges around input versus output policies
  - Only covers access – not QoS (yet)
- Manufacturers have an operational role in this model (but this only mirrors a need for them to support their products)
What is needed...

• Feedback!
• Would like more eyes on the draft and the concept
• What to do with this draft?