draft-weis-radext-mud-00

RADIUS Extensions for Manufacturer Usage Description (MUD)

Brian Weis

November 15, 2016

IoT Devices are Prone to Attack

- IoT devices connected to Ethernet networks will often be relatively unprotected against physical and network attacks
  - They are also notoriously insecure (open ports, default passwords, etc.)
- When an IoT device is vulnerable, so is the network to which it is attached.

The Goal

Protect the IoT Devices from attack by restricting network access to and from the devices

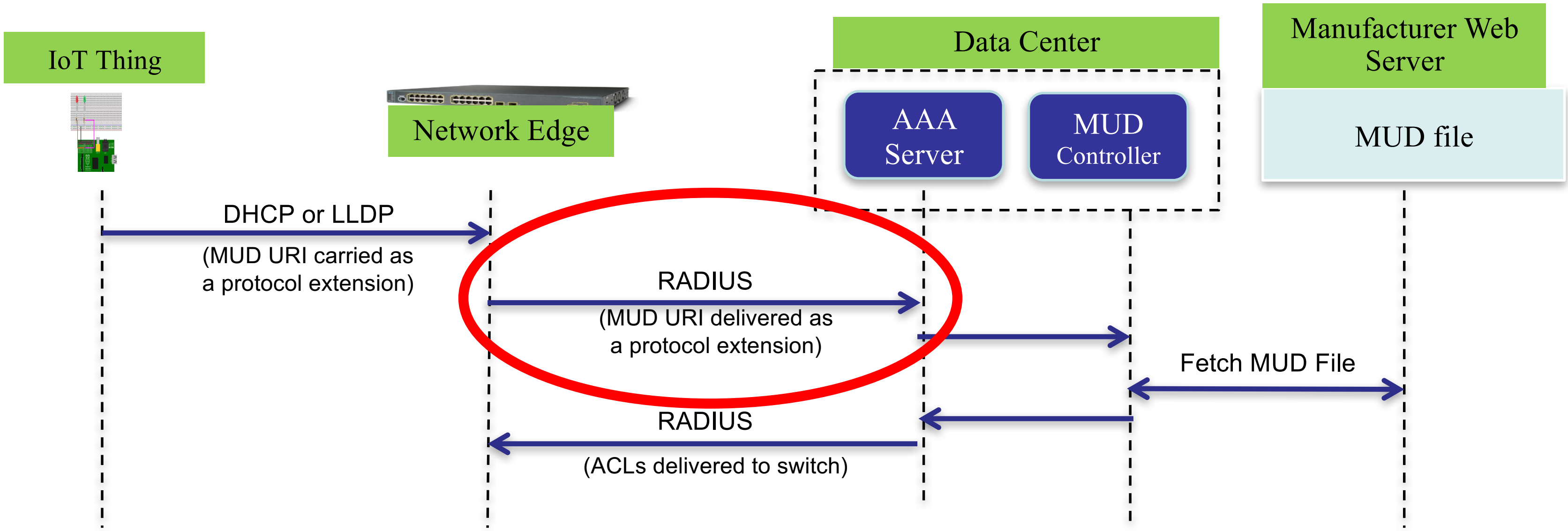
- The best protection the network can provides is at the Access Port connecting the Things to the rest of the network.
- In many cases, the device won’t authenticate itself (e.g., IEEE 802.1X)
- We’d like to be able to apply a network policy that restricts it’s access to just what it needs to support.
  - For example, an IoT device may only needs to obtain an address from a DHCP server, and then setup a TLS session with a management server (in the network or on the Internet),

Manufacturer Usage Description (MUD) is a tool that allows the IoT Devices to help the network know what network access is needed

MUD Specifications

- **draft-ietf-opsawg-mud-01**
  - Defines a MUD file with a JSON specification for describing policy about a device, such as its network access policy.
  - Defines a new URI for referencing the MUD file, which is expected to be placed on a public web server.
  - Defines protocol extensions that a IoT device can use to forward the URI to network devices (X.509 certificate extension, DHCP option, LLDP TLV)
- **draft-weis-radext-mud-00**
  - Describes how the URI can be captured by an edge network device and passed to a AAA server along with a MAC Address. This might be part of a MAC Address Bypass (MAB) message.
  - The AAA server resolves the URI, recovers the access requirements in the file, turns this into ACLs, and sends them to the edge network device

MUD Message Flow: (DHCP or LLDP)



MUD URI Attribute Definition

- One RADIUS Extended Attribute
  - Value is a string representing the MUD URI
  - Next version will replace the ASCII art with a reference to the data types draft

```
     0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    | Extended-Type |    Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Security Considerations

- Version -00 contains some guidance on accepting a MUD URI from an unprotected DHCP or LLDP message
- Version -01 will add some guidance for a RADIUS Server or MUD Controller accepting a MUD URI from a RADIUS message resulting from MAB.

Next Steps

- Publish version -01 addressing Alan’s comments
- When the MUD draft progresses, it would be good to consider whether this draft can progress.