Authorized update to MUD URLs

Michael Richardson
IETF111 OPSAWG meeting
July 30, 2021

`draft-ietf-opsawg-mud-acceptable-urls-02`

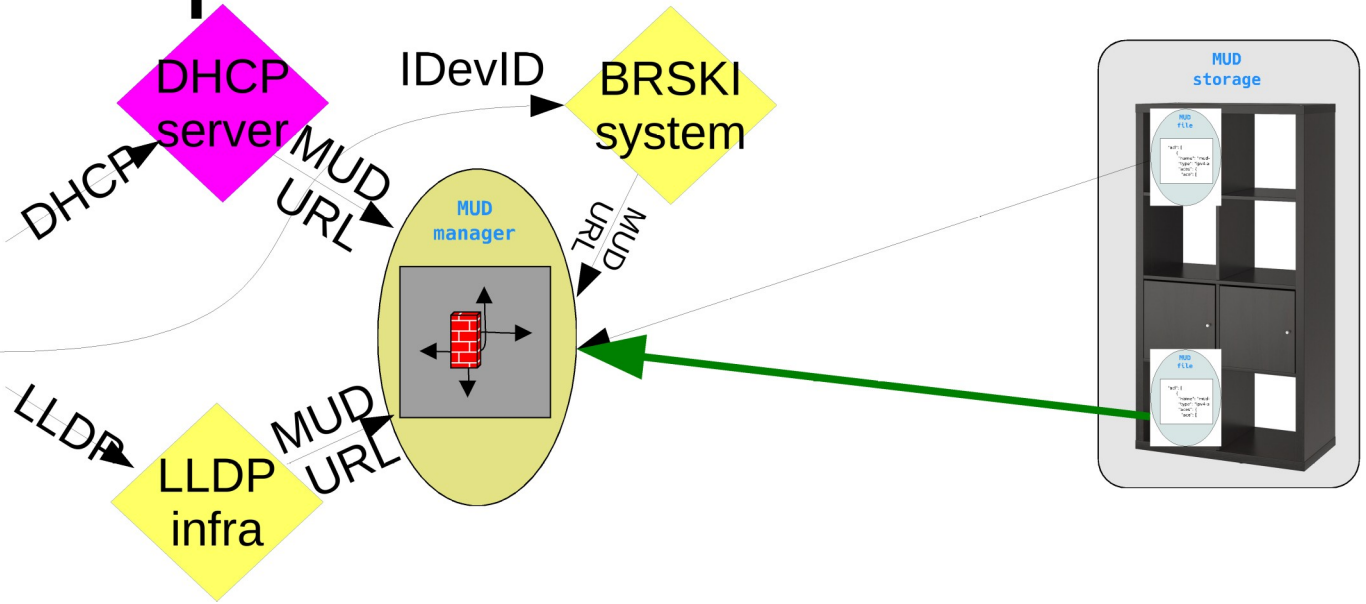
MUD URLs vs MUD files

- Update MUD file in place
  - PRO: no security problems
  - CON: opens issues with mis-matches of firmware
    - e.g., TLS profiles!
- Update MUD URL, provide new MUD file
  - PRO: every major revision can have specific rules
  - PRO: different operating modes for device can express different preferences
    - (commercial, pro-user, residential)
    - Features enabled via accessories
  - CON: risk that MUD file link could be changed by malware

Two ideas

- Update RFC8520 to say that the base URL must always be the same
- ~~Add extension to RFC8520 say allow base URL to be specified~~

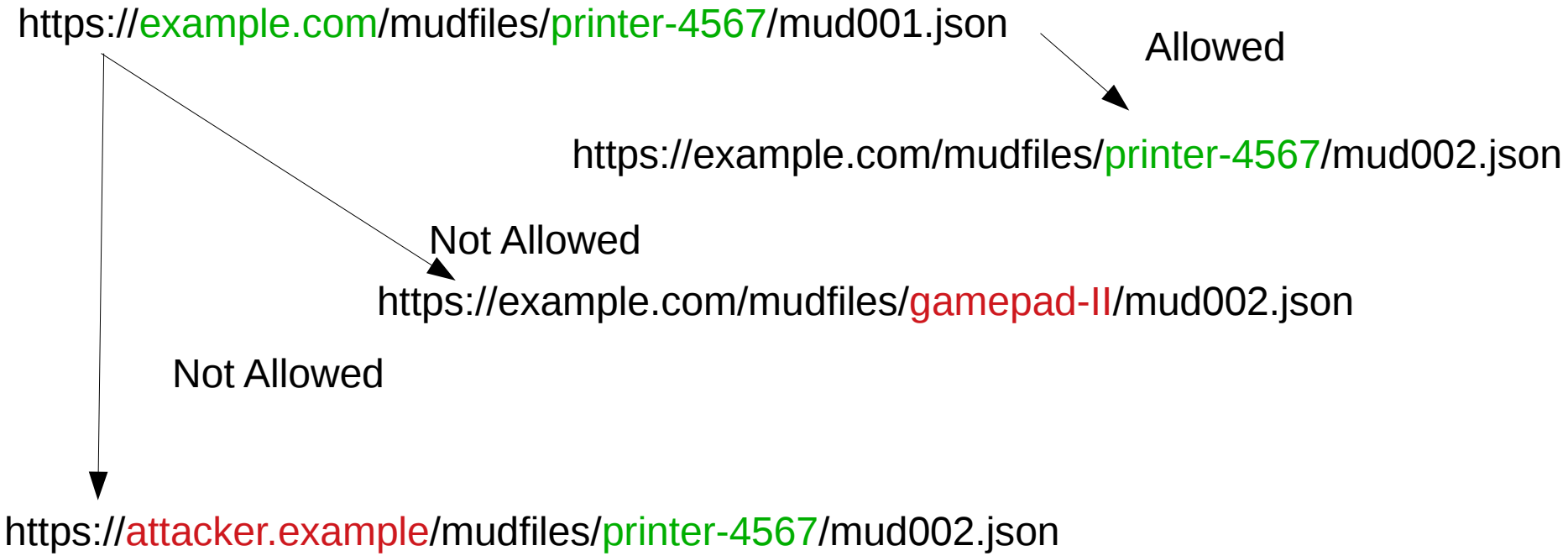
Shape of Solution



- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
  - Or may TOFU on DHCP/LLDP
- Updates to URL would be restricted to the last component

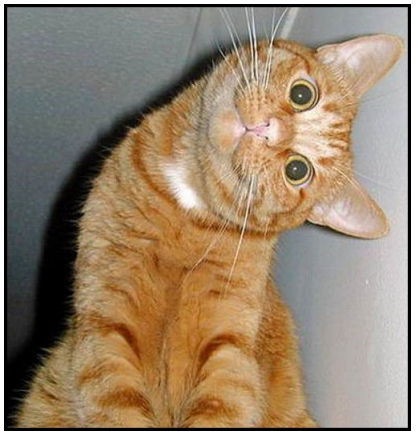
What kind of updates?

- Updates to URL would be restricted to the last component



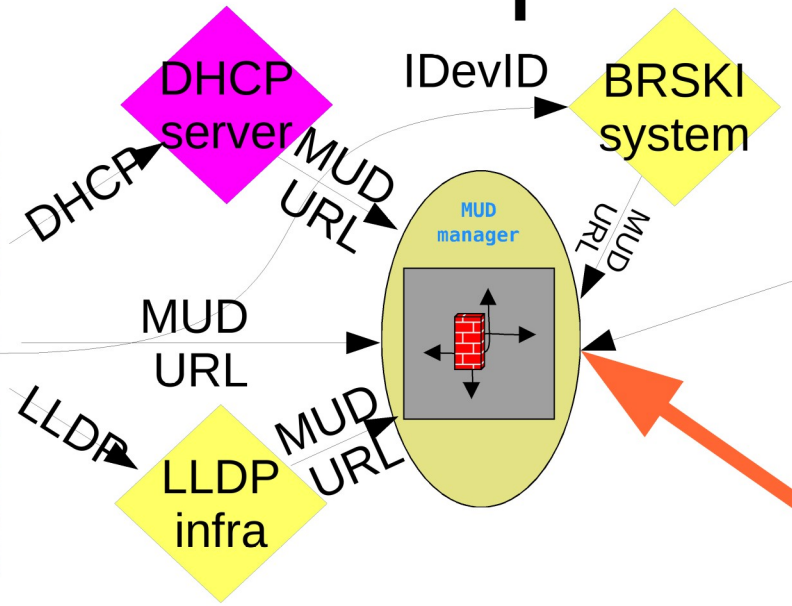
Now what?

- WG adopted in January, 2021
- Eliminated one of two solutions
  - Thus, this document has to normatively Update (Amends) RFC8520, so needs to be Standards Track
- Stable for awhile: ready for reviews and WGLC
- QUESTIONS?



LAST SLIDE
AUX slides after

What is the problem?



- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file
- Malicious device could lie in DHCP or LLD

MALICIOUS MUD FILE

Updates to IDevID?

- If IDevID is the most secure, why not update that?
  - Not easy to do for many products, IDevID is ideally stored in TPM
- If the IDevID can be updated, then can a malware update it too?