Doing an Inventory of IoT devices using IDevID scanning

draft-richardson-iotops-mud-query-00

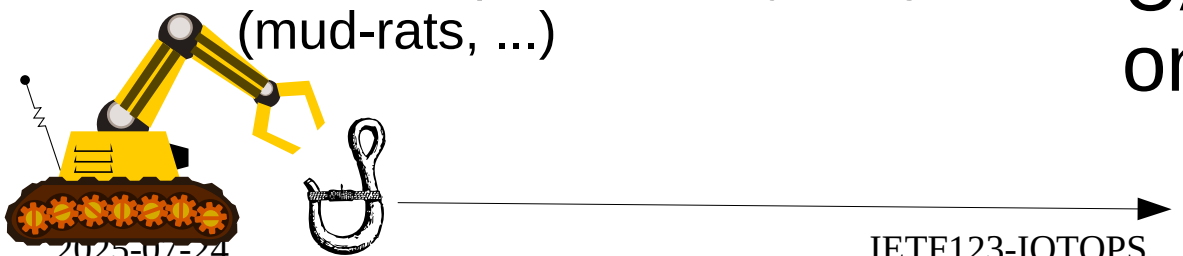
Michael Richardson
<mcr+ietf@sandelman.ca>

Motivation

- Intrusion Detection Systems (IDS) use a variety of heuristics to discover what kind of systems are present.
  - they create databases of assets, and at a trivial level the entities in the list can grow or shrink
  - new devices may be a source of concern.
  - double counting can look like new device, which is a source of false alarm
- in order to know if devices are compliant to new regulations (e.g., no default password, available firmware updates, how to report vulnerabilities, ...) an operator needs to have some assurance as to what each device is.
- bad guys have better heuristics, and already have more information than the defenders
- enterprise and industrial situations are different than coffee shops, hotels or residential networks
  - each has unique privacy concerns, with different tradeoffs. What might be verboten for some networks is sometimes mandatory elsewhere.

Initial Device ID (IDevID)

- IEEE 802.1AR defined manufacturer installed certificate
- Signed by manufacturer
- Can contain a MUD URL (RFC8520)
  - MUD can point to many things (mud-rats, ...)



Who I am

- not yet popular outside of enterprise IP routers, but common in a few places
- already needed by BRSKI,MATTER,OPC UA and other onboarding protocols

How can network see IDevID?

- Onboarding protocols usually see IDevID already
- enterprise-private LDevID is sometimes deployed

- but many existing ad-hoc onboarding mechanisms do not
  - type-in WPA-PSK with TV remote...
- other brownfields of existing OT systems
- wired systems might have no onboarding protocol: just plug in cable.

Get the device to use the IDevID

respond to a TLS connection.

BUT...

- won’t the bad guys discover my insecure devices?

BUT...

- won’t the bad guys discover my insecure devices?

- Yes. But the bad guys already know.
- Do you know about all the devices?
  - The bad guys already do.

BUT...

- random people will know what kind of devices are on my network, and my privacy will be violated.

BUT...

- random people will know what kind of devices are on my network, and my privacy will be violated.

- Yes.
- So don’t put random people on your (IoT) network

Proposed Solution

- derive list of systems from neighbor list from switch (home router even has this)
- use IPv6 Link-Local connection derived IPv6 address on port TBD2.
- Initiate TLS on this port.
- Device uses it's IDevID certificate to respond to TLS request.
- Do **some** trivial request over TLS.
- Extract MUD URL from IDevID certificate.

```
%ip neigh show
fe80::b846:dff:fe5e:4ff4 dev wired FAILED
fe80::200:5eff:fe00:2ff dev wlp0s20f3 lladdr 00:00:5e:00:02:ff router REACHABLE
2607:f0b0:f:60:5054:ff:fef6:630 dev virbr0 lladdr 52:54:00:f6:06:30 REACHABLE
2001:67c:1232:144::1 dev wlp0s20f3 lladdr 00:00:5e:00:02:ff router REACHABLE
fe80::c43e:43ff:fe38:2b09 dev virbr0 lladdr c6:3e:43:38:2b:09 router STALE
fe80::18a2:5856:80f4:9b3f dev wlp0s20f3 lladdr 1c:b3:c9:0b:c7:3c router STALE
fe80::5054:ff:fef6:630 dev virbr0 lladdr 52:54:00:f6:06:30 STALE
```

Features of this solution

- using IPv6 Link-Local, so all attacks need to be local
- does not require a new discovery mechanism
- creates a strong device identity
- encourages use of MUD for more information
  - but MUD link could be absent
  - MUD file might have no ACLs (today)
- we could consider if src address of probe has to be same as IPv6 router-advertisement source
- MUD provides anchors for other uses: remote attestation, finding latest firmware, ...

Technical Problems with this solution

- requires minimal IPv6
  - could use IPv4 Link-Local, but many devices do not configure it if DHCPv4 works
  - could limit access to same subnet as RFC1918
    - ARP proxy/spoofing is common for remote access solutions, attacks via malware on laptops, phones that have tunnels could be an concern (malware could be hidden in a smartphone app)
    - maybe this is not a concern
- requires IDevID on device
  - some vendors could upgrade their devices in the field, and could enroll some identity
  - operators could deploy something, particularly for devices where they have thousands of units, and units are sometimes lost (a real problem for hospitals, apparently)
- probably more

RelAted ThingS

- In a number of circumstances, a security auditing system needs to do continuous assurance.
- I.e., have a protocol that can collect fresh Evidence from devices
  - even after they have onboarded
- This TLS connection could be the collection mechanism....
- RATS

Market Problems with this solution

- getting high quality vendors to do this for new products might be doable
- getting this as an update for existing products.... harder
- getting lower quality vendors to do this might be difficult
  - and these are probably the vendors one **most** want to know about
- like MUD this has a chicken/egg problem between gateways/IDS and devices
- could a regulator require this in order to know if the device is complliant to regulations?

Discussion

?

draft-richardson-iotops-mud-query-00