Provisioning of IoT devices: Home Routers

Provisioning Initial Device Identifiers into Home Routers

draft-richardson-homerouter-provisioning-0

Michael Richardson
<mcr@sandelman.ca>
Motivation

• Insert “Murai” story (now close to 5 years ago!)
• admin/admin password is not good enough, but as soon as one does better, malware might collect/observe http. How?
  – ARP spoofing of 192.168.1.1 is trivial, and even used intentionally to add VPN-security
• Implementation of t2trg-idevid-considerations, anima-masa-considerations document
Motivation (2)

Implicitely Insecure  VS  Explicitely Insecure

These images from IoTSF ManySecured
Solution Outline part 1: put IDevID in

- IPv6 LL LAN
- Enhanced JSON w/ CSR + ULA
- IDevID Registrar
- LetsEncrypt?
- Dynamic Update To DNS w/ challenge (dns-01)
- Zone Controlled by Manufacturer dev.manu.example

Certificate: n983287.dev.manu.example
Solution Outline part 2: populate DNS with name

IDevID
Cert Authority

Dynamic Update
To DNS w/ AAAA

Zone
Controlled by
Manufacturer
dev.manu.example

IPv6 LL
LAN

n983287.dev.manu.example
IN AAAA fdd4:444c:fc9f::1

Certificate: n983287.dev.manu.example

ULA: fdd4:444c:fc9f::1
Solution Outline part 3: deployment

https://n983287.dev.manu.example

ULA: fdd4:444c:fc9f::/48
n983287.dev.manu.example IN AAAA fdd4:444c:fc9f::1
Also in /etc/hosts

Zone Controlled by Manufacturer
dev.manu.example
Issues

• Expiry of Certificate while device in in the box
  - Requires online renewal when device online
  - What is device needs human intervention to get online?

• Unwillingness of some browsers to do IPv6 lookups
  - Hack, also include 192.168.1.1 in /etc/hosts ICK.
  - May be limited to Alphabet browsers/systems
Conclusion

Needs some work
Co-authors sought
Some overlap with DANISH (maybe)