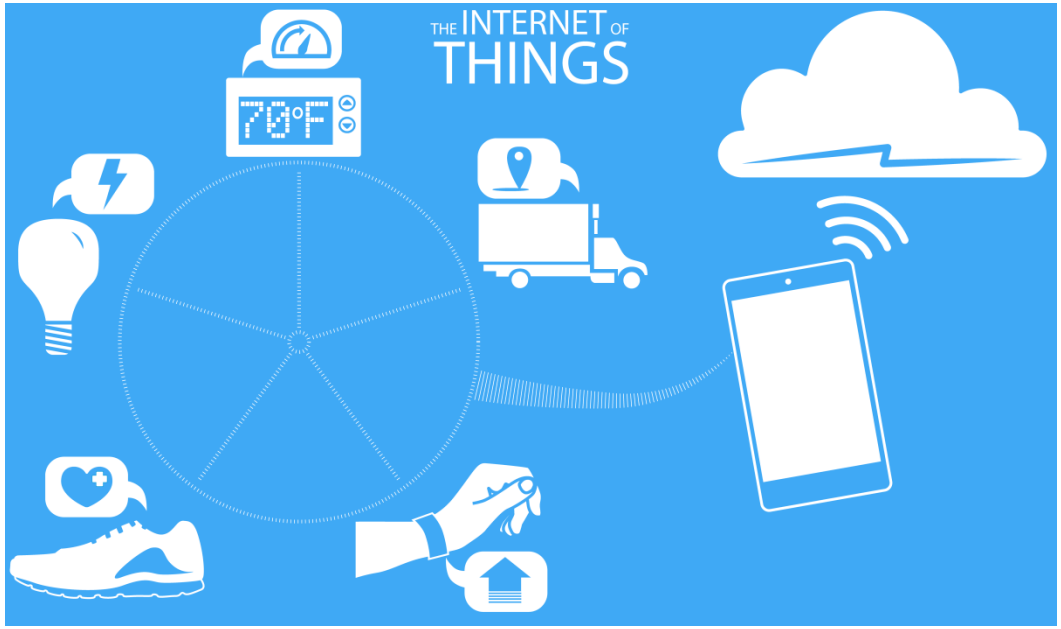


Image source

Local Network Discovery and HTTPS

Tatsuya Igarashi
Sony Corporation

W3C TPAC 2016@Lisbon

Problem Statement

User-Agents can not use HTTPS to IoT devices discovered on local network, e.g. Home, WiFi Spots.

- Unless a user agent is managed by the administrator like Intra-network, it would be hard for consumers to install a local CA's certificate for IoT devices.

- W3C standards, e.g. CORS with Credentials, Mixed Contents, Secure Context, are designed to require a secure origin, but a self-signed server certificate of IoT devices has an issue with a commercial user-agent.

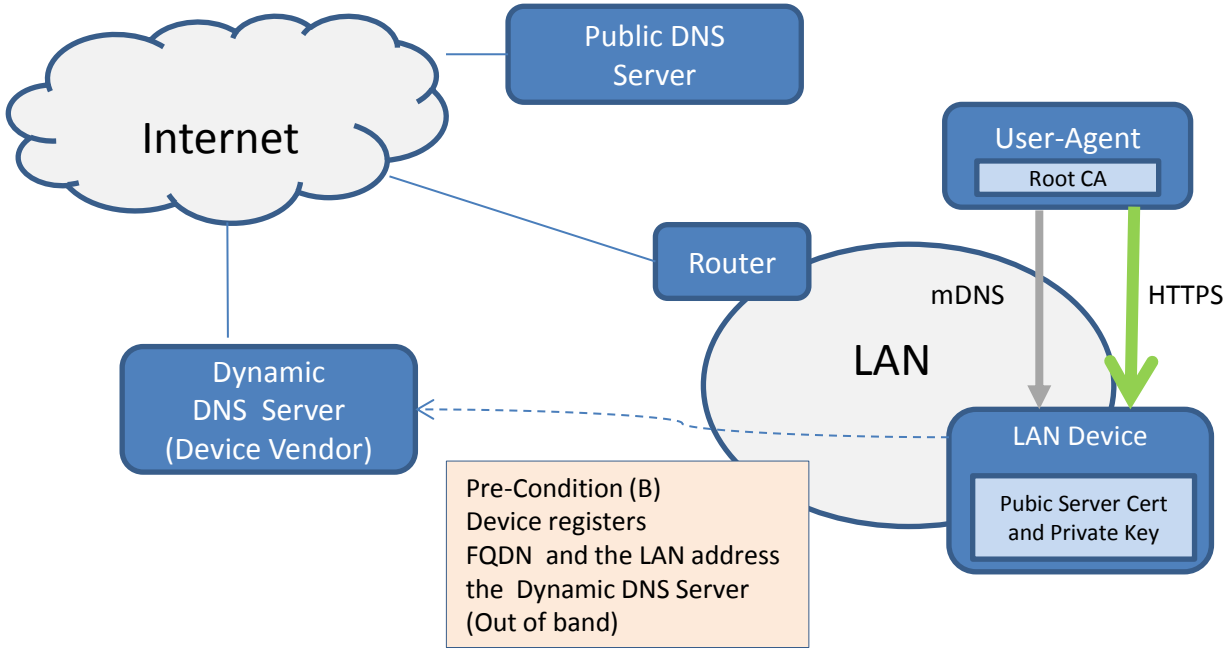
- Fundamentally, HTTP connection in local network should be encrypted and a local server can be validated as well as those in the Internet

“Straw Man”

To use TLS server certificates with FQDN and public DNS for a LAN device

A) Device has a TLS server certificate with FQDN authorized by the RootCAs

B) Device registers its LAN address with the FQDN to a dynamic DNS server (Out of band)



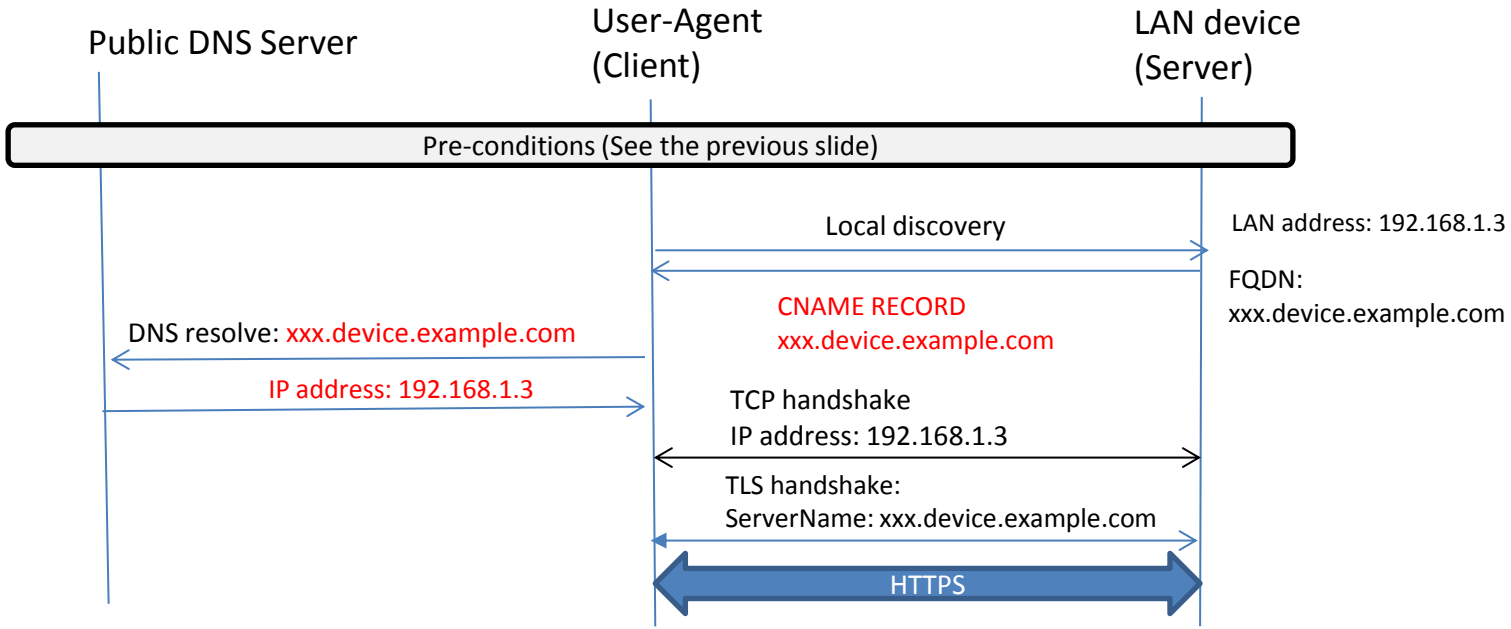
“Straw Man” (Cont.)

With the two preconditions, to use mDNS extended to response CNAME record

(1) LAN device responses CNAME record with FQDN, e.g. xxxx..device.example.com

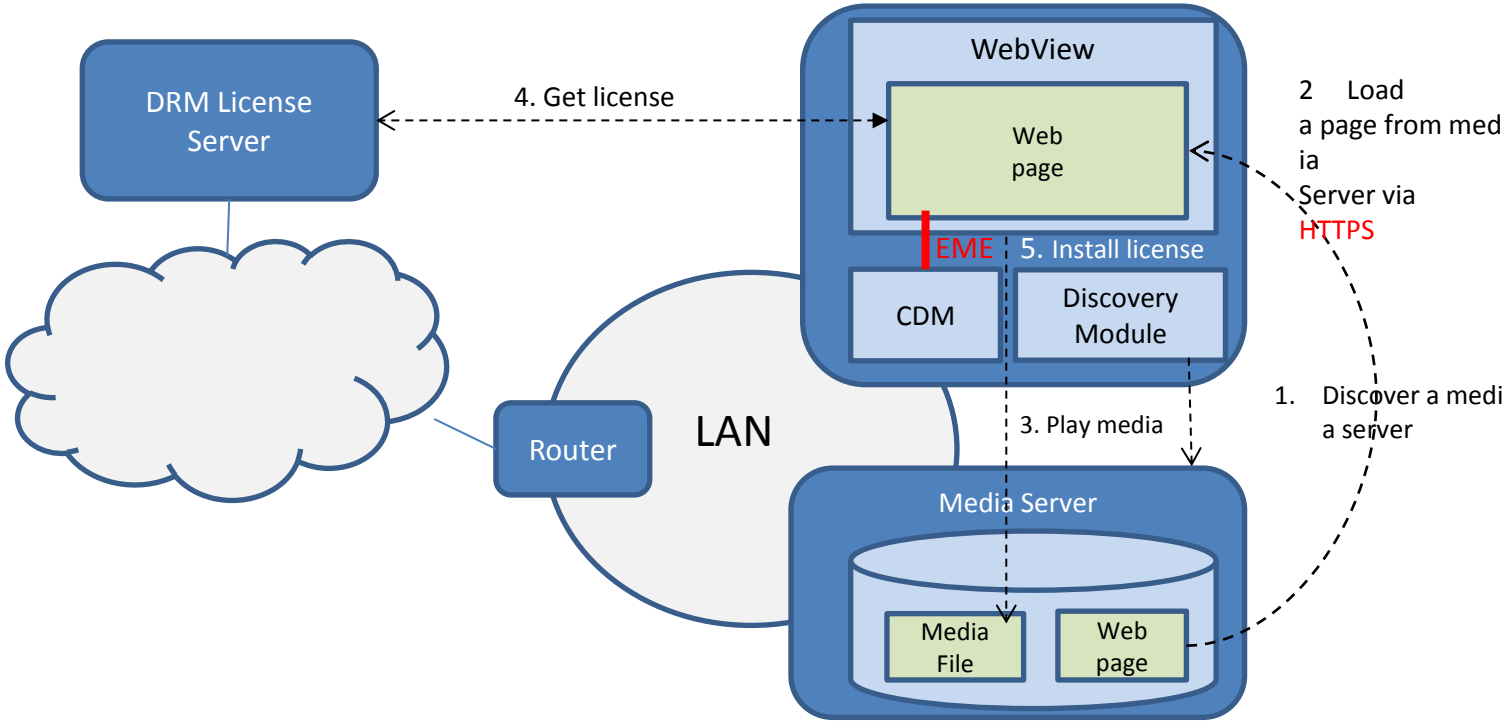
(2) User-Agent resolves LAN address with the FQDN using public DNS server

(3) User-Agent establishes HTTPS to the LAN address by specifying the FQDN to ServerName



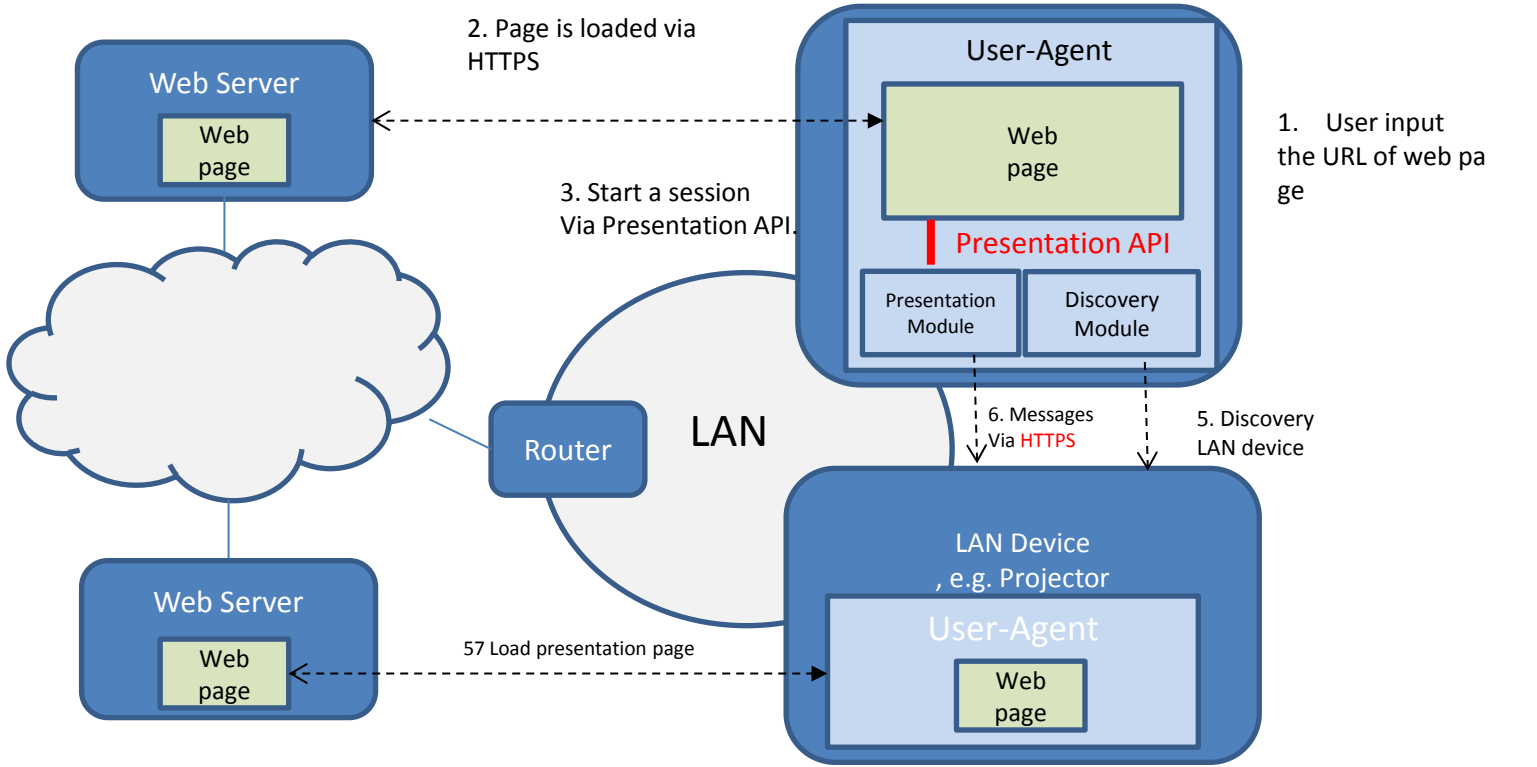
Example of use case (1)

A web page from LAN device uses the EME in Secure Context



Example of use case (2)

User-Agent uses HTTPS for the Presentation API to communicate with a LAN device in secure



Conclusion

User-Agents should be able to use HTTPS to IoT devices discovered on local network, e.g. Home, WiFi Spots.

- The “Strawman” is based on the assumption that a TLS certificates with FQDN authorized by the ROOT CAs can be used for a local network server
  - Is there any security/privacy concern on the assumption?

  •If the “Strawman” is good approach, local discovery protocol should be extended as an normative way to establish HTTPS to the local discovered service
  - IETF may be the best to standardize this work

  •Anyway, W3C should move forward this discussion to make a local network a part of Open Web
  - Please join this discussion. Any group to handle this ?