HTTPS For Local Networks

carlosil@chromium.org

https://pad.w3.org/p/HTTPSForLocalNetworks_2024-09-25

Why?

-Privacy/Security issues with HTTP

-Common point of annoyance for features that require secure contexts.

Current Options

- Self signed certificates (with warnings)
- Adding a root cert (complicated; risky, especially without constraints)
- Dynamic DNS + Port Forwarding + certificate from trusted CA (complicated and security exposure inappropriate for e.g. a smart bulb)
- Just use HTTP (see prior slide)
- Wildcards certs + domains that resolve to local IPs (e.g. Plex)

Plex’s Solution

- Give users wildcard certs for *.<user-specific-hash>.plex.direct
- Resolve <ip>.<user-specific-hash>.plex.direct to <ip>

(Some) Use cases

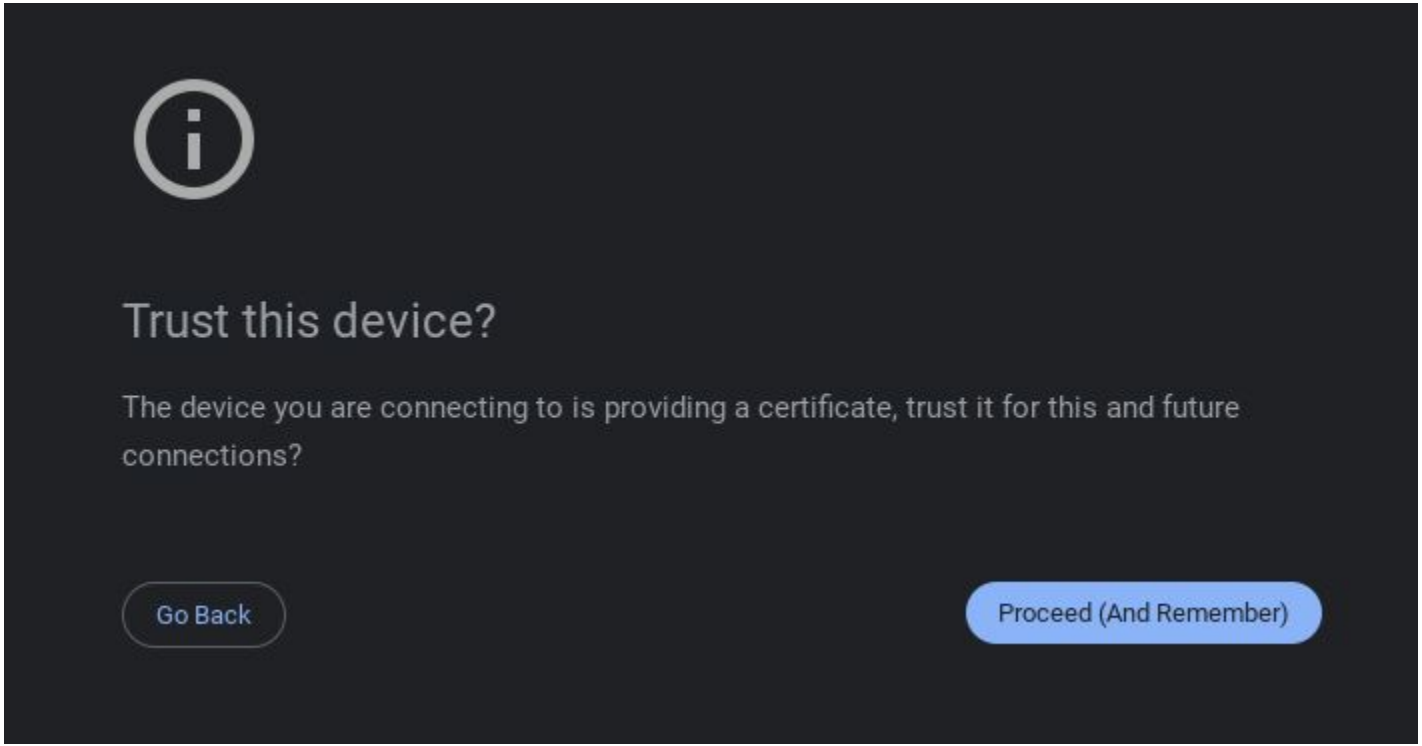
- Routers
- Enterprise intranet devices (printers, etc.)
- Home Servers/Raspberry Pi/Hobbyist type things
- Cloud-backed IoT devices
- Non Cloud-backed IoT devices

Previous attempts

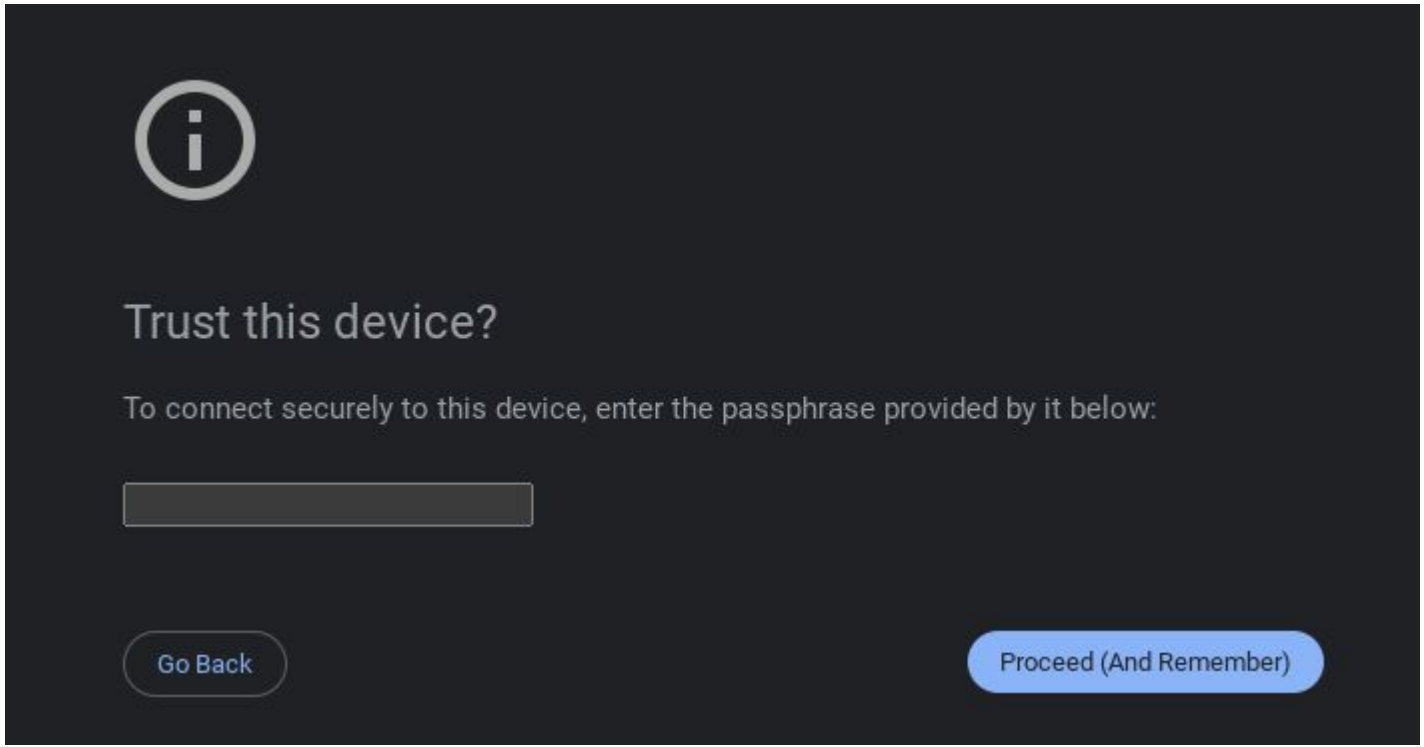
- HTTPS For Local Networks Community Group (closed last year)
- Martin Thomson’s proposal (2015)
- IETF discussion

Potential Solutions

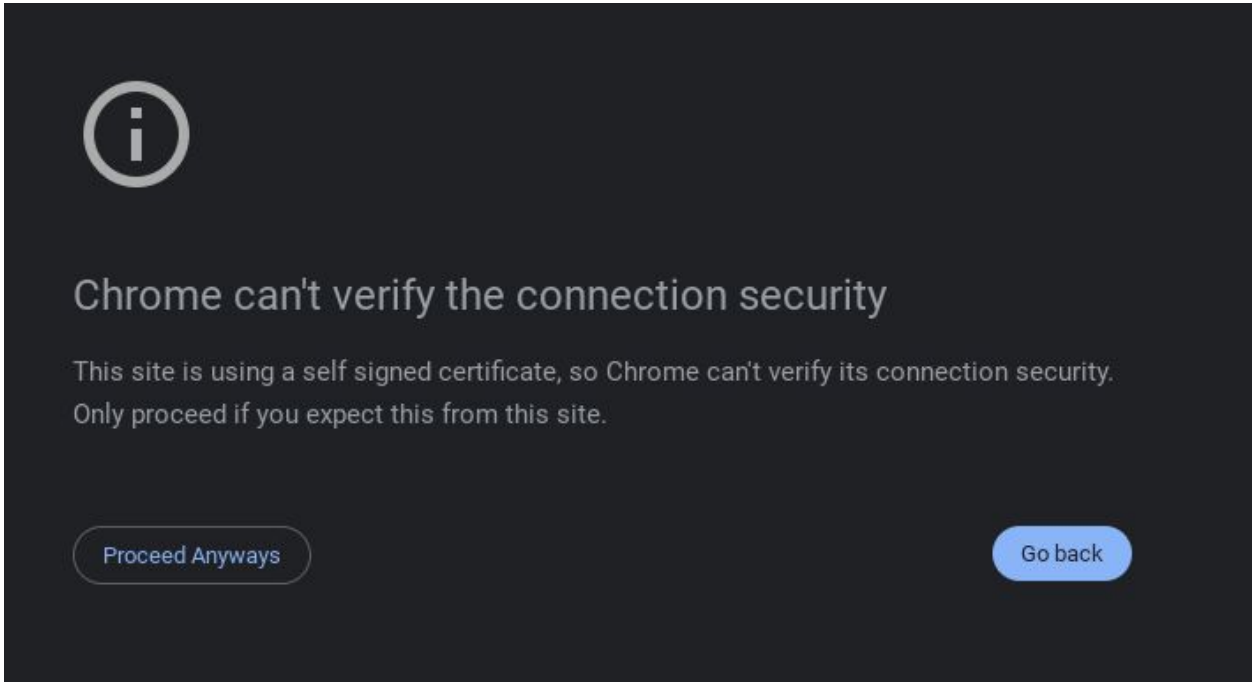
TOFU (Trust on First Use)



PAKE (Password Authenticated Key Exchanges)



Better self-signed experience
(Similar to TOFU, Seitan? Paneer?)



Disambiguating non-unique origins

- example.com is always Example, Inc
- 192.168.1.1 can be different things at different times

Alternative (from Martin Thomson’s proposal): append a hash of the server’s public key to the origin. 192.168.1.1.<hash> would now refer to a specific server

Mismatched Device Certificate

You previously trusted this device, but it is now using an unknown certificate, it is possible someone could be eavesdropping right now.

Advanced

Back to safety

@@@@@@@@@@@@@@@@@@@@@@@@@@@
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Advanced

Back to safety