HTTPS For Local Networks

carlosil@chromium.org

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

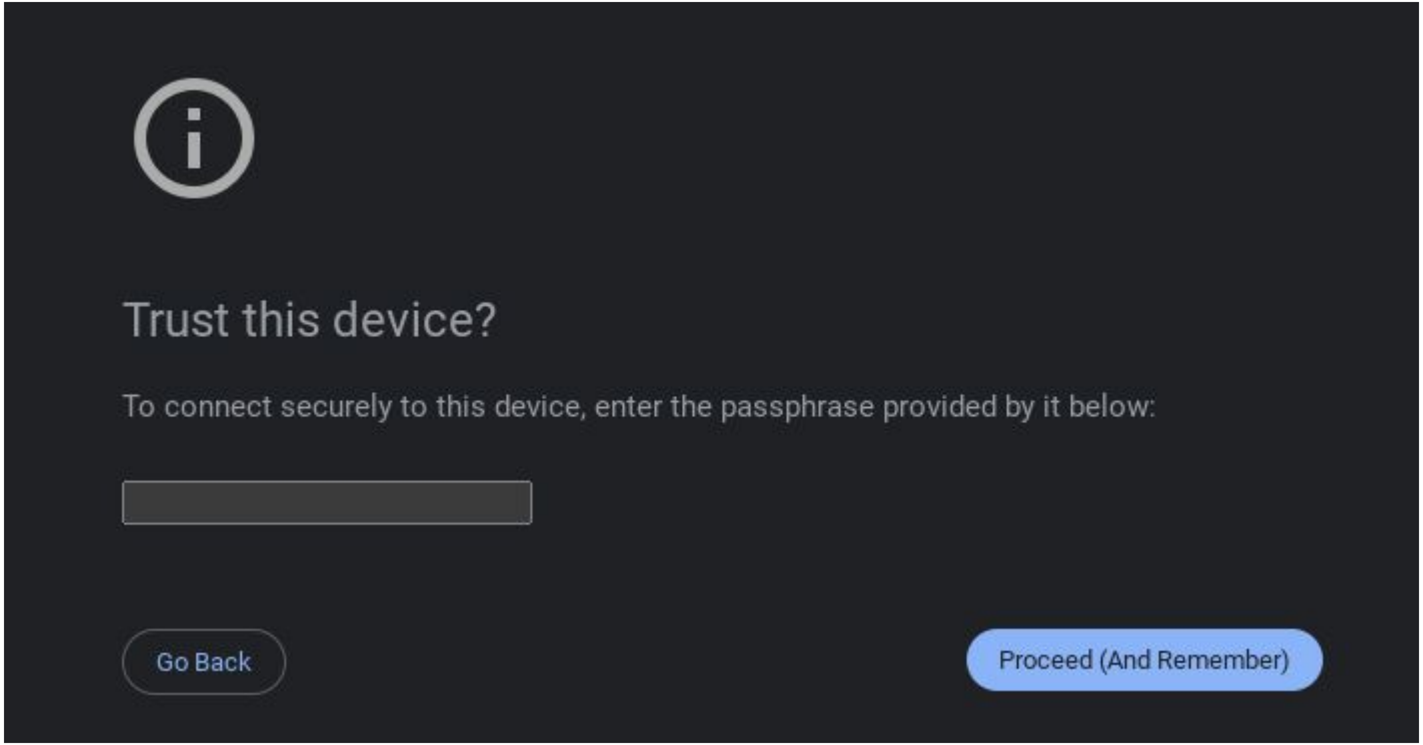
- Routers
- Enterprise intranet devices (printers, etc.)
- Home Servers/Raspberry Pi/Hobbyist type things
- Cloud-backed IoT devices
- Non Cloud-backed IoT devices

Previous/Current attempts

- HTTPS For Local Networks Community Group (closed 2023)
- Martin Thomson’s proposal (2017)
- IETF settle WG proposal

Potential Solutions

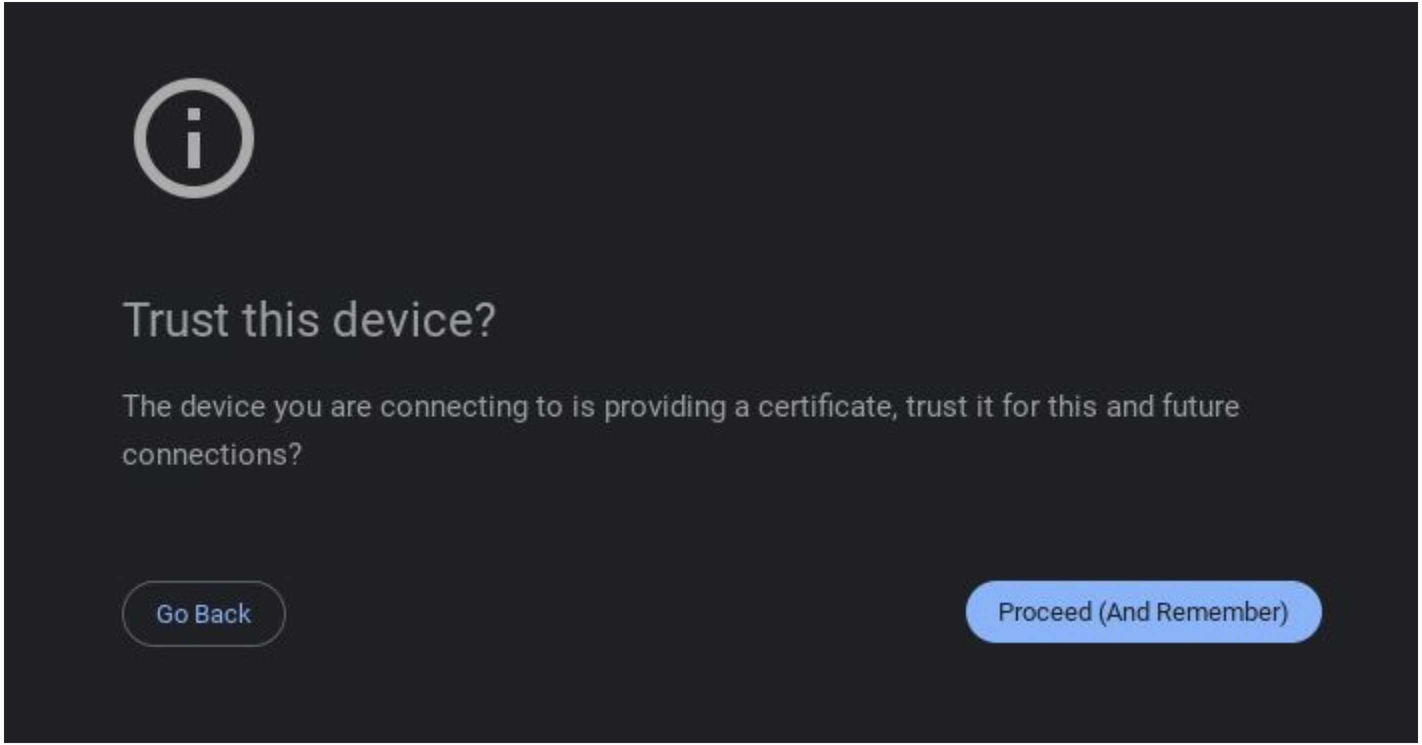
PAKE (Password Authenticated Key Exchanges)



Trust this device?

To connect securely to this device, enter the passphrase provided by it below:

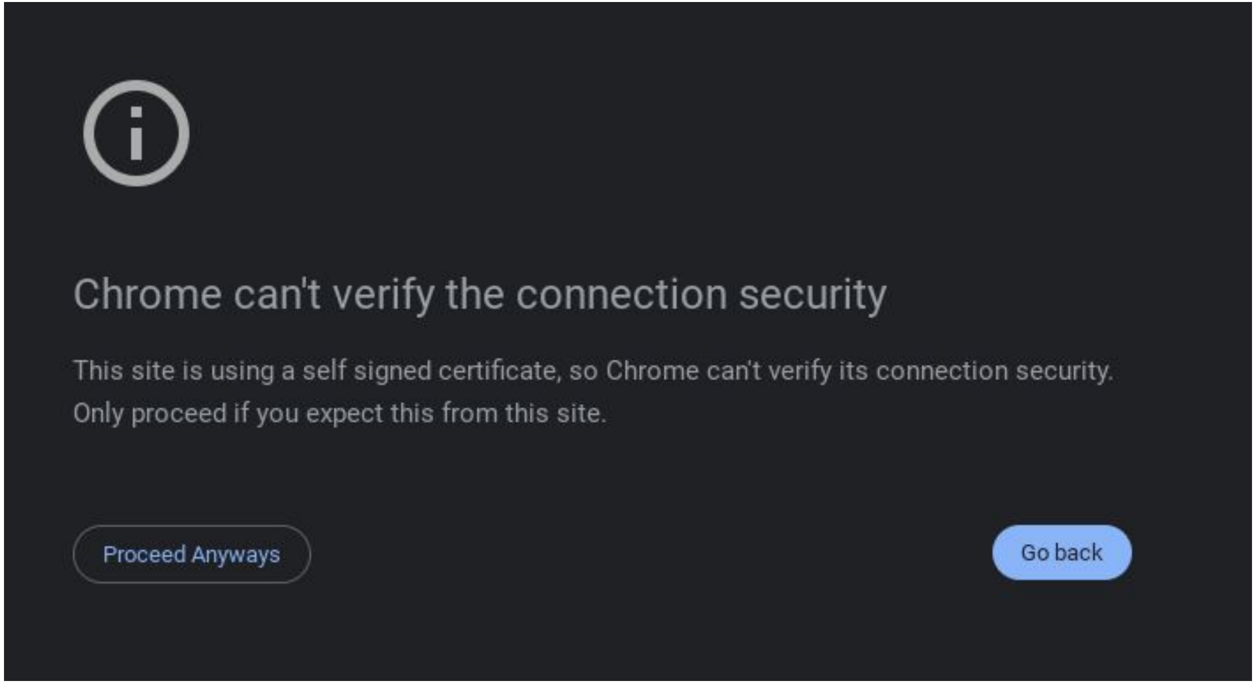
TOFU (Trust on First Use)



Trust this device?

The device you are connecting to is providing a certificate, trust it for this and future connections?

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



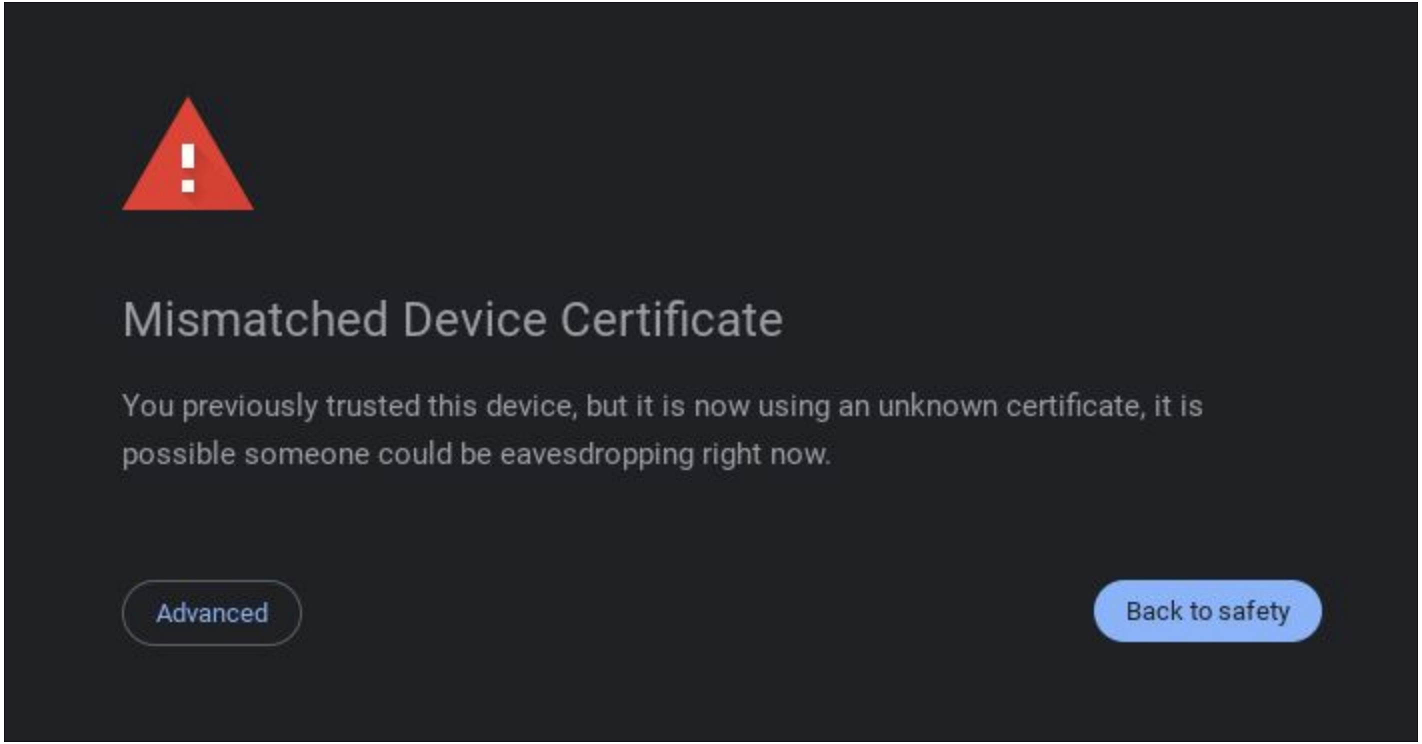
Chrome can't verify the connection security

This site is using a self signed certificate, so Chrome can't verify its connection security. Only proceed if you expect this from this site.

Disambiguating non-unique origins

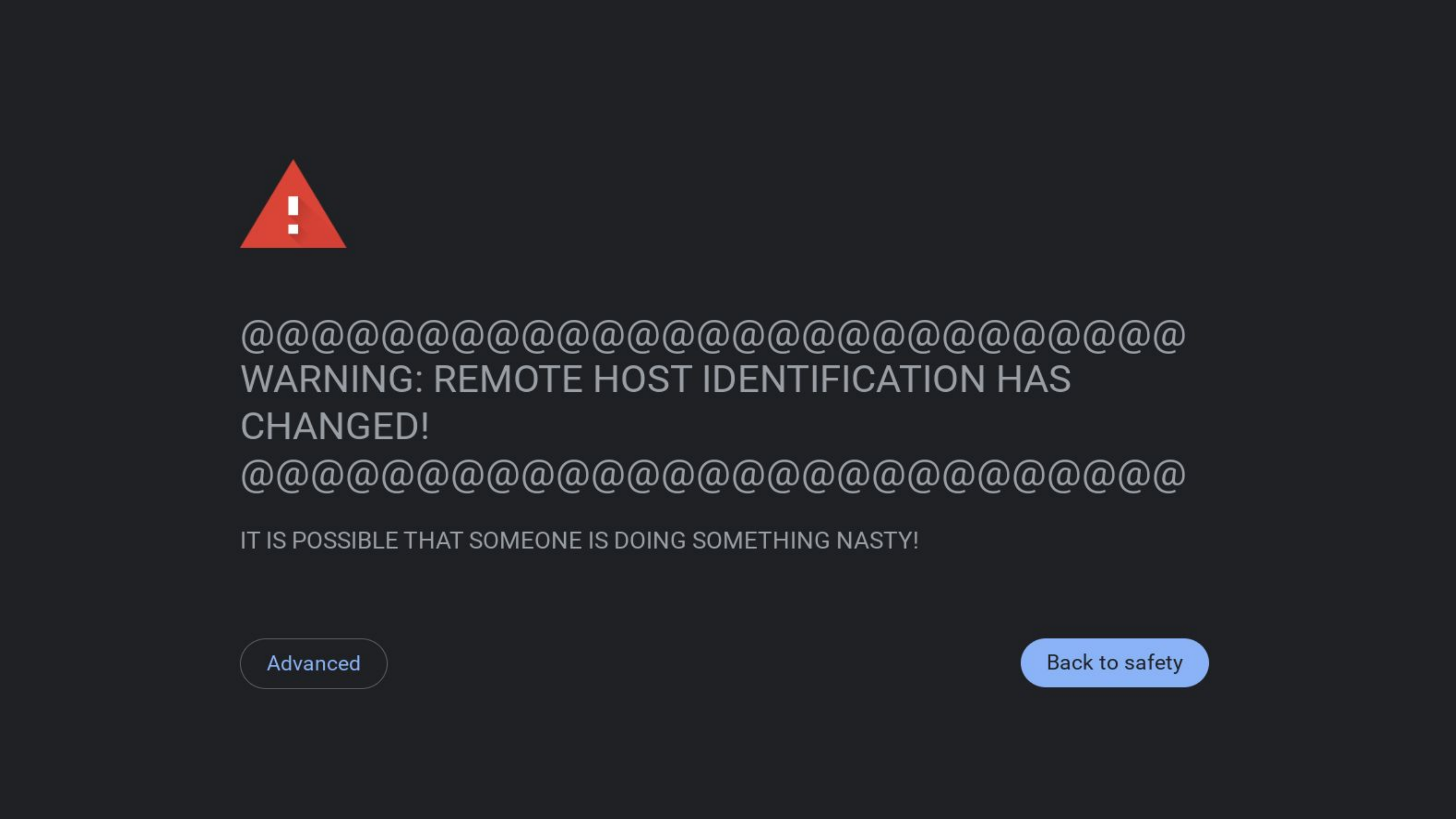
- example.com is always Example, Inc
- 192.168.1.1 can be different things at different times

Alternative: 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.



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

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!