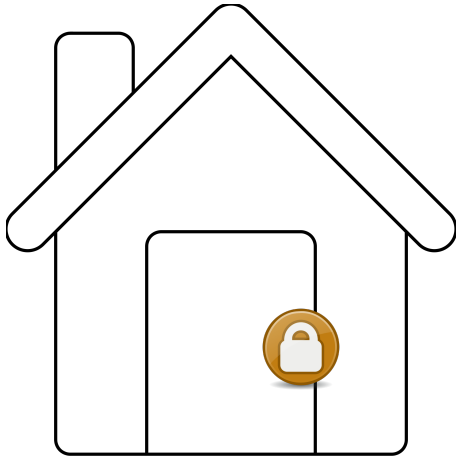
Secure Home Networking Control Protocol



draft-barth-homenet-hncp-security-trust-01

Steven Barth (author) & Pierre Pfister (speaker)

(see https://github.com/fingon/ietf-drafts for draft sources & individual diffs)

HNCP draft and security state

Current state

hncp-01: unsecured, manual IPsec or unspecified certificate-security

bonnetain-hncp-security-00: public-key web-of-trust security in HNCP

→ reinventing algorithm mobility, replay protection, …

draft-barth-homenet-hncp-security-trust-01 (for hncp-02)

temporarily split security bits from hncp-02 for discussion and later merge

HNCP-specific: excludes existing single-link threats (RA, DHCPv6, ...)

assets: topology, addressing, naming / SD, IGP-capability payloads

Border Determination

General

manually defined or automatic (tricky!) on per-link scale

Automatic Border Discovery

presence of a "non-homenet" DHCP(v6) server → link is external

done with non-participating routers → HNCP auth/encryption doesn't help

links might only have clients → pure absence of auth'd routers != external

usual lack of bi-di authentication from ISPs → impossible to identify reliably

however, securing links between ISP and CPE is out-of-scope here

Automatic Border Discovery

Threats for Automatic Border Discovery

external attacker (e.g. compromised ISP) **disables DHCP(v6)-server** or classifies it as "homenet" → border **firewall breach**

internal attacker runs **DHCP/v6 server** causing adjacent HNCP routers to announce it as uplink → **MITM** on traffic directed to external (like rogue RA/DHCP(v6)-server on single-link homenet?)

⟶ physical, link-layer or similar underlying security on every link

⟶ OR manual border config (hncp-02 enforces advanced support)

Threats for HNCP payloads

multicast traffic (link-local UDP)

announcing unique **device IDs** and **MD5-hashes** of HNCP-state

only used to discover devices and changes, triggering unicast exchanges

→ **no sensitive data** so enough to rate-limit triggered unicast exchanges?

unicast traffic (link-local UDP)

synchronizing HNCP state

eavesdropping, replaying, spoofing etc. is possible

consensus-nature: even regularly announced state can be malicious

→ manipulation of routing, naming or other payloads is possible

Securing HNCP payload

Isolating or securing router-to-router links

does not require authentication or encryption of HNCP itself

detailed interface categories (“leaf”, “guest”, …) can help

→ threatening devices (e.g. clients) are isolated from HNCP/IGP-traffic

Authentication and Encryption of HNCP-traffic

(D?)**TLS** to not reinvent the wheel (or IPsec/IKE?)

PSK, PKI usually provided by implementation

OR Trust Consensus using custom verification hook + new TLV

Certificate-based trust consensus

General Design (based on X.509 certificates)

Each device may announce a verdict (trusted, untrusted) on a certificate.

Effective Verdict: verd. with the highest priority among announced ones

→ A certificate is trusted **iff.** it has an effective verdict of "trust".

Types of Verdicts (in order of ascending priority)

neutral, cached trust, cached distrust, configured trust, configured distrust

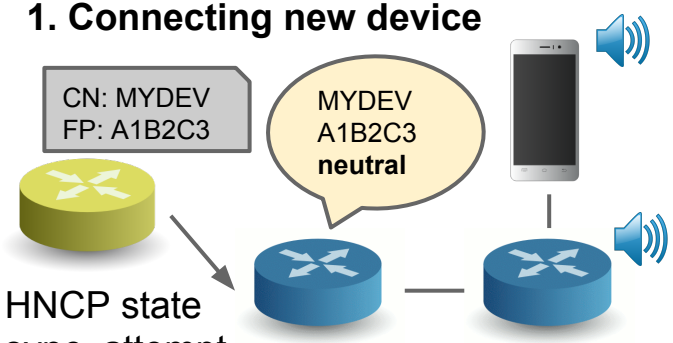
neutral: unknown trust state (used to announce join attempts)

cached: last-known effective verdict (if no configured one is announced)

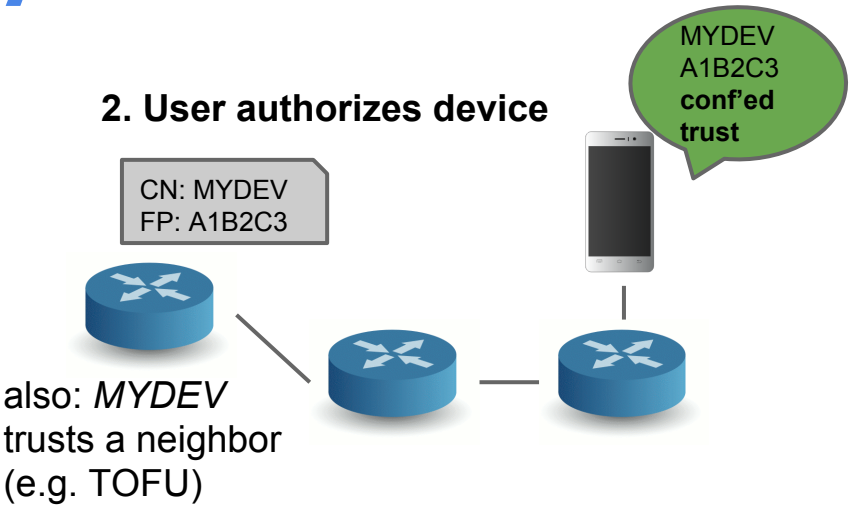
configured: explicitly configured / acquired by trust bootstrap ceremony

Example: Trust Lifecycle

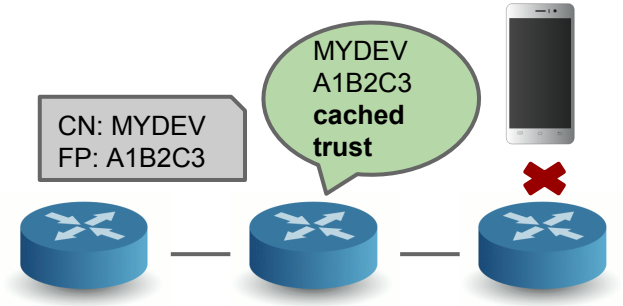
1. Connecting new device



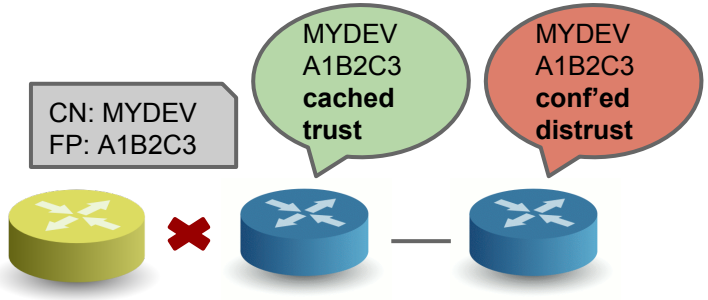
2. User authorizes device



3. Device with verdict disconnects



4. A device is configured to distrust



Trust Bootstrap

Trust by Identification

Devices MUST offer an interface to list all known certificates in the homenet incl. their effective verdicts + allow to set a configured verdict.

Other possible ceremonies

Preconfigured Trust	(if meaningful, no per-se trust of vendors etc.)
Trust on Button Press	(similar to WPS-PBC)
Trust on First Use	(if device has never been associated before)

→ **2** ceremonies needed: new device → homenet & homenet → new device

Other protocols in the home

Security Aspects

IGPs et al. usually **unencrypted** with only **PSK-authentication**

→ may influence usefulness of HNCP-encryption (information leaks)

→ PSKs must be maintained to authenticate them

HNCP Managed-PSK

one device generates and shares a **random 32-Byte key**

MUST be regenerated whenever any HNCP-device is distrusted

per-protocol-PSKs derived with HMAC-SHA256 with predefined "secrets"

Thank You

Do you have questions or feedback?

Please also visit www.homewrt.org for source code, binaries and some documentation.