HNCP Security Based on Routers Trust

draft-bonnetain-hncp-security-00

Author: Xavier Bonnetain

Presenter: Pierre Pfister

Presentation Outline

- Threats and Assumptions
  - Authentication
    - Authorization
      - Shared Secret Establishment
        - Pros and cons
          - Other possibilities

Threats and Assumptions

Existing home networks are not *secured*

Wired link is left unsecured (and maybe it's okay !)

Wireless is usually secure

There are plenty of possible attacks

RA generation

DHCP spoofing

IP spoofing

…

Threats and Assumptions

Homenet makes it worse ! An attacker can:

Threats	How to protect against
Fake an uplink Fake a client	Secure interface type
Prevent network config. Spoof domain names	Secure HNCP
Attack the routing protocol	Secure the routing protocol

What homenet does is:

Extending the home network to multiple links

Securing HNCP is:

Preventing an attacker from interfering with a link it is not connected to.

Authentication Mechanism

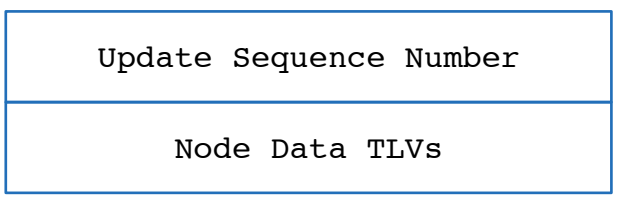
Each node uses a public key as identifier

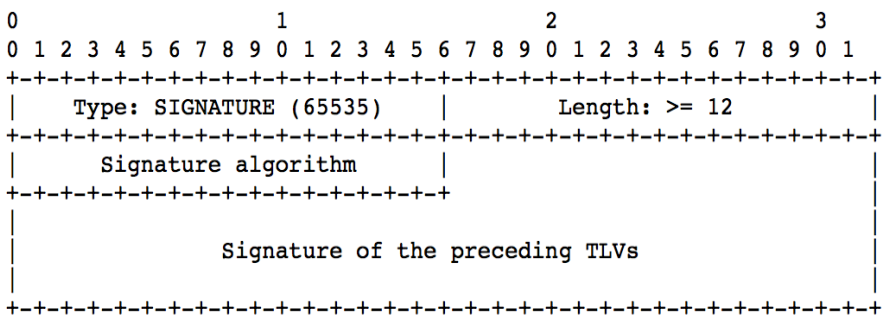
Identity is tied to the public key

HNCP makes use of the MD5 of the public key as shortened ID

```
Note: Using MD5 is not that bad. But a real crypto
hash would ensure cryptographic binding.
```

Each HNCP update is signed

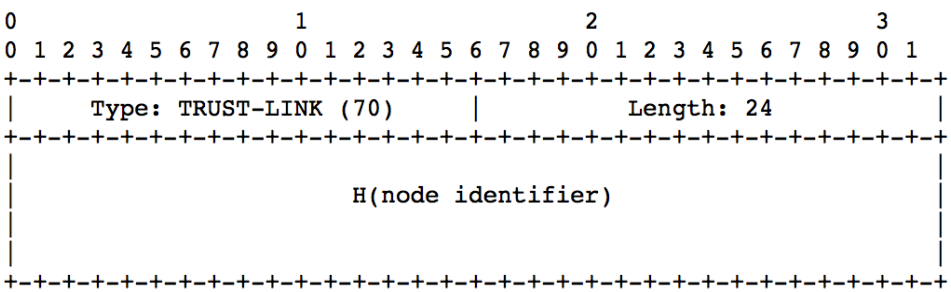




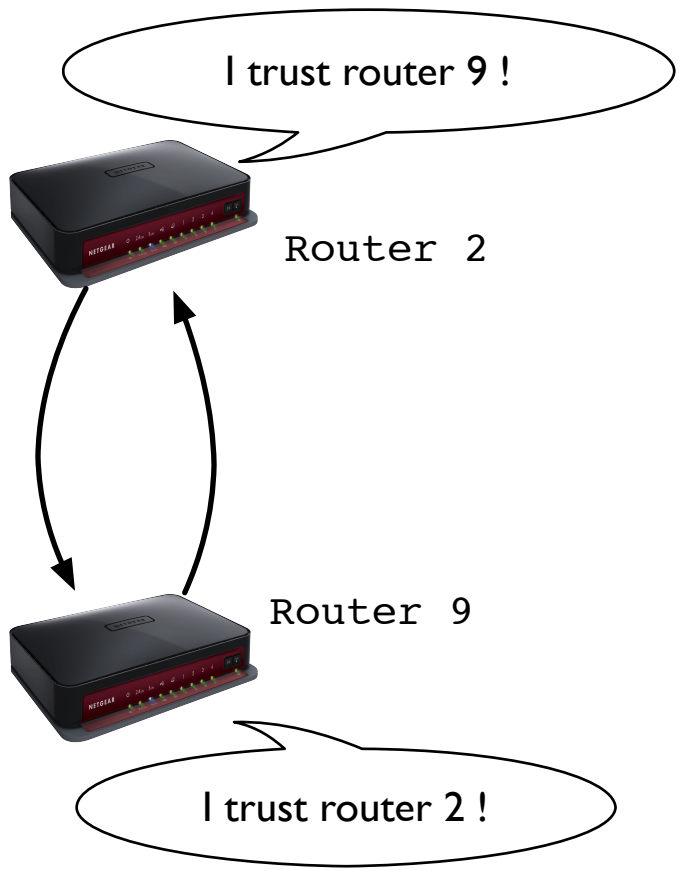
Authorization Mechanism

Decentralized approach at HNCP level

Nodes advertise a set of trust relationships

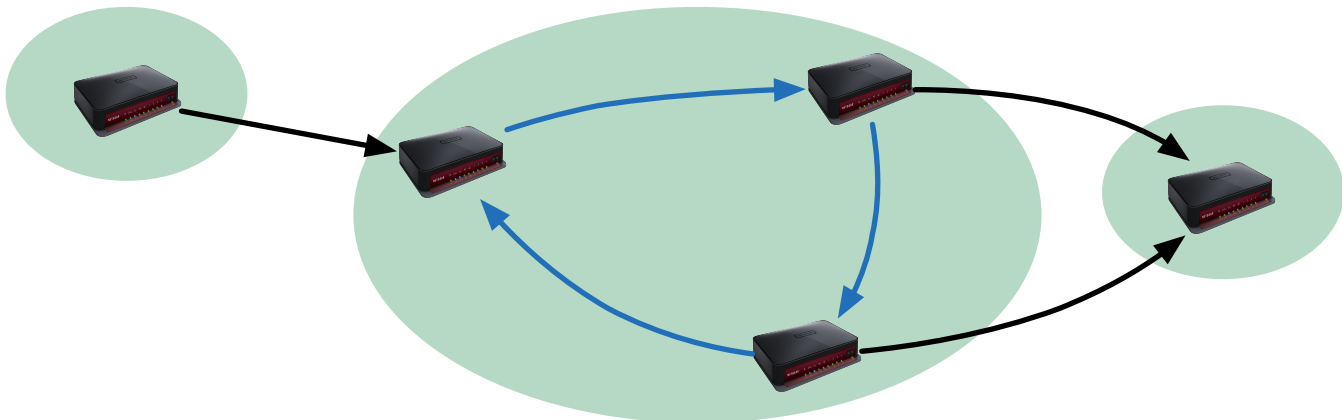


Trust links are shared with HNCP



Authorization Mechanism

Ending-up with a trust network



Defining the trusted node set

Set of nodes you have bidirectional trust relationship with.

Untrusted nodes updates are relayed but rate-limited

Only trust related TLVs are used from nodes that are not trusted

Authorization Mechanism

Trust bootstrapping

User interaction (UI, pressing buttons, PIN codes)

Centralized management

Certificate based management

Revocation

Can't use time (configuration prior to internet access)

Revoke a trust relationship by not advertising it anymore

Shared Secret Establishment

Master key generation

Encrypted for all trusted nodes

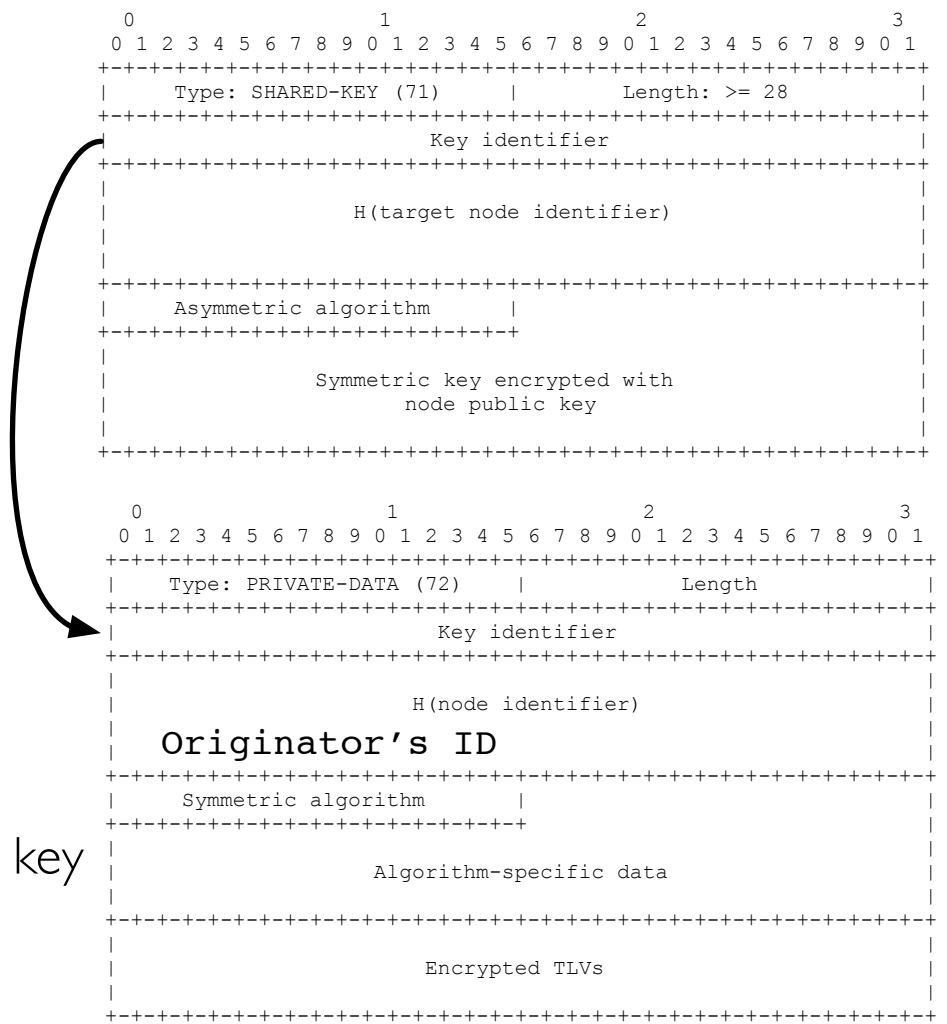
Asymmetric crypto.

Identified by originator + ID

Other TLVs are later encrypted

Symmetric crypto.

Allows sharing routing protocol session key



Pros and cons

+ HNCP data is protected (configuration)

+ Shared secret for other protocols (routing protocol)

- No link security (neither for hosts or routers)

- No active deprecation

- No uplink security

- Shared key must be renewed when a trusted node is revoked

Other possibilities

Password based (IPSec or symmetric crypto)

+ More efficient crypto
+ Simpler to implement
- Bootstrap a bit less secure
- Key management is hard

Static interface configuration

o No crypto.
+ Uplink security

CA based

- Centralized
- Revoking is hard
- Complex implementation

Discuss !