Homenet Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 17, 2015

S. Barth

October 14, 2014

HNCP - Security and Trust Management
draft-barth-homenet-hncp-security-trust-01

Abstract

This document describes threats and a security and trust bootstrap mechanism for the Home Networking Control Protocol (HNCP).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 17, 2015.

Table of Contents

1. Introduction

HNCP is designed to make home networks self-configuring, requiring as little user intervention as possible. However this zero-configuration goal usually conflicts with security goals and introduces a number of threats.

This document describes imminent threats and different security and trust management mechanisms to mitigate them.

2. Requirements language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Scope

This draft is based on HNCP as described in [I-D.ietf-homenet-hncp] and the additional threats it introduces. Many of these already exist in a similar form in current single-link home networks due to the usually unauthenticated use of protocols like NDP [RFC4861] or DHCPv6 [RFC3315]. This document intentionally does not cover these and other Homenet-related threats not explicitly introduced by HNCP.

HNCP is a generic state synchronization mechanism carrying information with varying threat potential. This draft will mainly consider the currently specified payloads:

Network topology information such as homenet routers and their adjacent links

Address assignment information such as delegated and assigned prefixes for individual links

Naming and service discovery information such as auto-generated or customized names for individual links and routers

IGP capabilities and preferences of individual routers

4. Border Determination

In general an HNCP-router determines the internal or external state on a per-link scale and creates a firewall-perimeter and allows HNCP- and IGP-traffic based on the individual results. These are provided by either automatic border discovery or a predefined configuration indicated by e.g. the link-type, a physically dedicated (labeled) port or the administrator.

Threats concerning automatic border discovery cannot be mitigated by encrypting or authenticating HNCP-traffic itself since external routers do not participate in the protocol and often cannot be authenticated by other means. These threats include propagation of forged uplinks in the homenet in order to e.g. redirect traffic destined to external locations and forged internality by external routers to e.g. circumvent the perimeter firewall.

It is therefore imperative to either secure individual links on the physical or link-layer or preconfigure the adjacent interfaces of HNCP-routers to an adequate fixed-category in order to secure the homenet border. Depending on the security of the external link eavesdropping, man-in-the-middle and similar attacks on external traffic can still happen between a homenet border-router and the ISP, however these cannot be mitigated from inside the homenet.

5. HNCP Payload Security

Once the homenet border has been established there are several ways to secure HNCP against internal threats like manipulation or eavesdropping by compromised devices on a link which is enabled for HNCP-traffic. If left unsecured attackers may cause arbitrary spoofing or denial of service attacks on HNCP-services such as address assignment or service discovery. Furthermore they may manipulate routing or external connection information in order to perform eavesdropping or man-in-the-middle attacks on outbound traffic. The following security mechanisms are defined to mitigate these threats:

5.1. Isolated router-to-router links

Given that links containing HNCP routers can be sufficiently secured or isolated it is possible to run HNCP in a secure manner without using any form of authentication or encryption. Detailed interface categories like "leaf" or "guest" can be used to integrate not fully trusted devices to various degrees into the homenet by not exposing them to HNCP and IGP traffic or by using firewall rules to prevent them from reaching homenet-internal resources.

5.2. Authentication and Encryption of HNCP-traffic

The end-to-end mechanism DTLS [RFC6347] is used to authenticate and encrypt all HNCP unicast-traffic in order to protect its potentially sensitive payload. Methods for establishing and managing trust for this mechanism are described in the following section.

HNCP also uses multicast signaling to announce changes of HNCP information but will not send any actual payload over this channel. An attacker may learn hash-values of HNCP-information and may be able to trigger unicast synchronization attempts between routers on the local link this way. An HNCP-router should therefore limit its unicast synchronizations attempts to avoid a multicast-induced denial-of-service.

6. Trust Management for Authentication and Encryption

6.1. Pre-shared secret based trust

A PSK-based trust model is a simple security management mechanism that allows an administrator to deploy devices to an existing network by configuring them with a pre-defined key, similar to the configuration of an administrator password or WPA-key. Although limited in nature it is useful to provide a user-friendly security mechanism for smaller homenets.

6.2. PKI-based trust

A PKI-based trust-model enables more advanced management capabilities at the cost of increased complexity and bootstrapping effort. It however allows trust to be managed in a centralized manner and is therefore useful for larger networks with a need for an authoritative trust management.

6.3. Certificate-based trust consensus

The certificate-based consensus model is designed to be a compromise between trust management effort and flexibility. It is based on X.509-certificates and allows each connected device to give a verdict on any other certificate and a consensus is found to determine whether a device using this certificate or any certificate signed by it is to be trusted.

6.3.1. Trust Verdicts

Trust Verdicts are statements of HNCP-devices about the trustworthiness of X.509-certificates. There are 5 possible verdicts in order of ascending priority:

0 Neutral: no verdict exists but the homenet should find one

1 Cached Trust: the last known effective verdict was Configured or Cached Trust

2 Cached Distrust: the last known effective verdict was Configured or Cached Distrust

3 Configured Trust: trustworthy based upon an external ceremony or configuration

4 Configured Distrust: not trustworthy based upon an external ceremony or configuration

Verdicts are differentiated in 3 groups:

Configured verdicts are used to announce explicit verdicts a device has based on any external trust bootstrap or predefined relation a device has formed with a given certificate.

Cached verdicts are used to retain the last known trust state in case all devices having configured verdicts about a given certificate have been disconnected or turned off.

The Neutral verdict is used to announce a new device intending to join the homenet so a final verdict for it can be found.

The current effective trust verdict for any certificate is defined as the one with the highest priority from all verdicts announced for said certificate at the time. A device MUST be trusted for participating in the homenet if and only if the current effective verdict for its own certificate or any one in its certificate hierarchy is (Cached or Configured) Trust and none of the certificates in its hierarchy have an effective verdict of (Cached or Configured) Distrust. In case a device has a configured verdict which is different from the current effective verdict for a certificate the current effective verdict takes precedence in deciding trustworthiness however the device still retains its configured verdict in its configuration.

6.3.2. Trust Cache

Each device maintains a trust cache containing the current effective trust verdicts for all certificates currently announced in the homenet. This cache is used as a backup of the last known state in case there is no device announcing an configured verdict for a known certificate. It SHOULD be saved to a non-volatile memory at reasonable time intervals to survive a reboot or power outage.

Every time a device (re)joins the homenet or detects the change of an effective trust verdict for any certificate it will synchronize its cache and store the new effective verdict overwriting any previously cached verdicts. Configured verdicts are stored in the cache as their respective cached counterparts, Neutral verdicts are never stored.

6.3.3. Announcement of Verdicts

A device always announces any configured trust verdicts it has established by itself. It also announces cached trust verdicts it has stored in its trust cache if one of the following conditions applies:

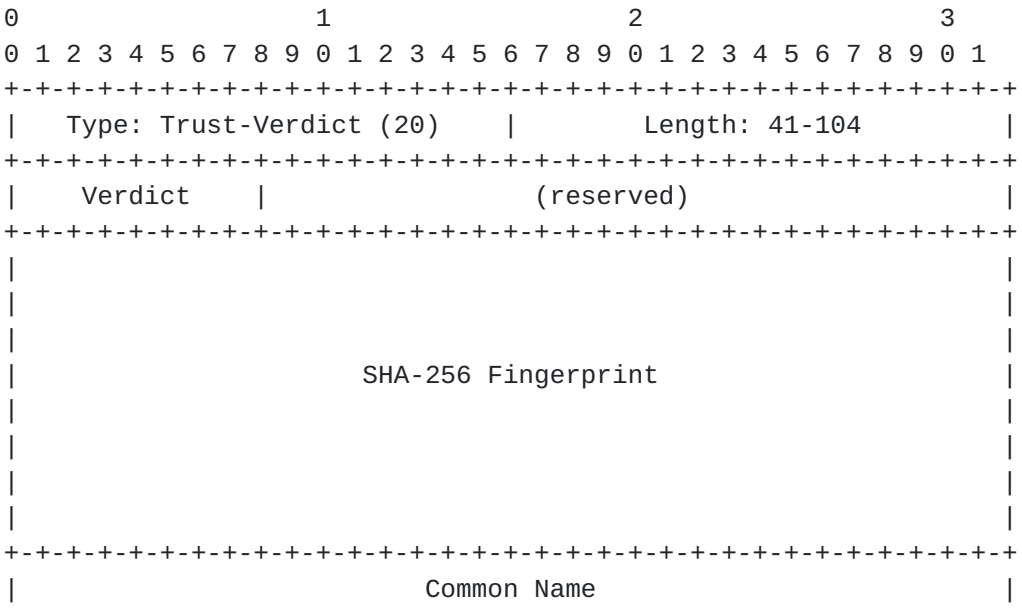
The stored verdict is Cached Trust and the current effective verdict is Neutral or does not exist.

The stored verdict is Cached Distrust and the current effective verdict is Cached Trust.

A device rechecks these conditions whenever it detects changes of announced trust verdicts anywhere in the network.

Upon encountering a device with a hierarchy of certificates for which there is no effective verdict a router announces Neutral verdicts for all certificates found in the hierarchy until an effective verdict different from Neutral can be found for any of the certificates or a reasonable amount of time (10 minutes is suggested) with no reaction and no further connection attempts has passed. Such verdicts SHOULD also be limited in rate and number to prevent denial-of-service attacks.

Trust verdicts are announced using Trust-Verdict TLVs:



Verdict represents the numerical index of the verdict.

(reserved) is reserved for future additions and MUST be set to 0 when creating TLVs and ignored when parsing them.

SHA-256 [RFC6234] Fingerprint contains the fingerprint of the certificate.

Common Name contains the variable-length (1-64 bytes) common name of the certificate.

6.3.4. Bootstrap Ceremonies

The following methods are defined to establish trust relationships between HNCP-routers and router certificates. Trust establishment is a two-way process in which the existing homenet must trust the newly added device and the newly added device must trust at least one of its neighboring routers. It is therefore necessary that both the newly added device and an already trusted device perform such a

ceremony to successfully introduce a device into a homenet. In all cases an administrator MUST be provided with external means to identify the device belonging to a certificate based on its fingerprint and a meaningful common name.

6.3.4.1. Trust by Identification

A device implementing certificate-based trust MUST provide an interface to retrieve the current set of effective trust verdicts, fingerprints and names of all certificates currently known and set configured trust verdicts to be announced. Alternatively it MAY provide a companion HNCP-device or application with these capabilities with which it has a pre-established trust relationship.

6.3.4.2. Preconfigured Trust

A device MAY be preconfigured to trust a certain set of device or CA certificates. However such trust relationships MUST NOT result in unwanted or unrelated trust for devices not intended to be run inside the same network (e.g. all other devices of that manufacturer).

6.3.4.3. Trust on Button Press

A device MAY provide a physical or virtual interface to put one or more of its internal network interfaces temporarily into a mode in which it trusts the certificate of the first HNCP-device it can successfully establish a connection with.

6.3.4.4. Trust on First Use

A device which is not associated with any other homenet-router MAY trust the certificate of the first HNCP-device it can successfully establish a connection with. This method MUST NOT be used when the device has already associated with any other HNCP-router.

7. Other homenet protocols

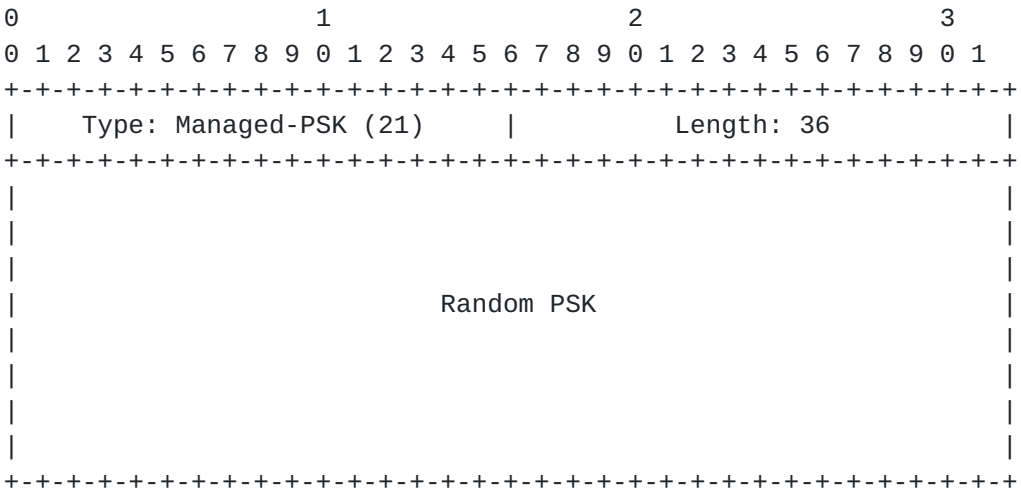
An IGP is usually run alongside HNCP in a homenet therefore the individual security aspects of the respective protocols must be considered. It can however be summarized that current candidate protocols (namely Babel, OSPFv3, RIP and IS-IS) provide - to a certain extent - similar security mechanisms. All mentioned protocols do not support encryption and only support authentication based on pre-shared keys natively. This influences the effectiveness of any encryption-based security mechanism deployed by HNCP as homenet routing information is usually not confidential.

As a PSK is required to authenticate IGP-traffic and potential other protocols, HNCP is used to create and manage it. The key length is defined to be 32 Bytes to be reasonably secure. The following rules determine how a key is managed and used:

If no Managed-PSK-TLV is currently being announced, an HNCP-router creates one with a random key and adds it to its node-data.

In case multiple routers announce such a TLV at the same time, all but the one with the highest router-ID stop advertising it and adopt the remaining one.

The router currently advertising the Managed-PSK-TLV must generate and advertise a new random one whenever the HNCP security mechanism stops trusting one or more trusted devices - i.e. HNCP is secured with a PSK itself and it was changed or a certificate has changed from trusted to distrusted.



PSKs for individual protocols are derived from the random PSK through the use of HMAC-SHA256 [RFC6234] with a pre-defined per-protocol HMAC-key in ASCII-format. The following HMAC-keys are currently defined to derive PSKs for the respective protocols:

"ROUTING": to be used for IGPs. If a Random PSK exists then the derived PSK MUST be used to secure the chosen IGP.

8. Security Considerations

8.1. Revocation of Trust

Revoking trust in a protocol intended for bootstrapping is non-trivial, since neither an accurate clock nor network connectivity to

retrieve authenticated revocation information can be assumed in all situations.

The Certificate-based trust consensus mechanism defined in this document allows for a consenting revocation, however in case of a compromised device the trust cache may be poisoned before the actual revocation happens allowing the distrusted device to rejoin the network using a different identity. Stopping such an attack might require physical intervention and flushing of the trust caches. However such an attack is often times more easily detectable than threats discussed earlier in this document such as a silent manipulation of routing information and related man-in-the-middle attacks.

9. IANA Considerations

IANA should add HNCP TLV types with the following contents:

20: Trust-Verdict

21: Managed-PSK

10. References

10.1. Normative references

[I-D.ietf-homenet-hncp]
Stenberg, M. and S. Barth, "Home Networking Control Protocol", draft-ietf-homenet-hncp-01 (work in progress), June 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

10.2. Informative references

[RFC6234] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

Appendix A. Draft source

As usual, this draft is available at https://github.com/fingon/ietf-drafts/ in source format (with nice Makefile too). Feel free to send comments and/or pull requests if and when you have changes to it!

Appendix B. Acknowledgements

Thanks to Markus Stenberg, Pierre Pfister and Mark Baugher for their contributions to the draft and Xavier Bonnetain for ideas on a web of trust and PSK-management in I-D.bonnetain-hncp-security-00.

Author's Address

Steven Barth

Email: cyrus@openwrt.org