Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2013

M. Behringer
M. Pritikin
S. Bjarnason
Cisco

October 15, 2012

Bootstrapping Trust on a Homenet
draft-behringer-homenet-trust-bootstrap-00.txt

Abstract

A homenet must be aware of its borders, and the realms within those. This document proposes an approach to bootstrap trust in such an environment. The idea is to select one device as the trust anchor and to enroll other devices into the domain. The result is the creation of a domain of trust in the homenet, with a common trust anchor. This trust model can subsequently be used to determine boundaries, and to autonomically bootstrap network services.

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 18, 2013.

Copyright Notice

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Problem Statement

[I-D.ietf-homenet-arch] states that "It should be possible to automatically perform border discovery for the different borders." Simple approaches, such as terminating a homenet on a particular interface type do not easily allow for devices from different administrative realms to be locally connected.
[I-D.ietf-homenet-arch] states further that "It is important that self-configuration with 'unintended' devices is avoided. Methods are needed for devices to know whether they are intended to be part of the same homenet site or not."

An approach is needed that allows to establish trust inside a homenet according to a policy set by the admin of the homenet.

2. Approach

An autonomic device can be a router, switch, PC, smartphone, or any other device, independent of its role in the network, which has the autonomic functionality mentioned below . A homenet consists of autonomic devices and non-autonomic devices. This approach requires at least one autonomic networking device, such as a router or switch.

One autonomic device in the homenet takes on a registrar function. This could be manually enabled, for example on a smartphone autonomic app; in the absence of a registrar function, a device can also auto-select itself to take on this function, using some detection mechanism to resolve potential conflicts.

The registrar creates a trust anchor for the homenet, and subsequently acts as a registration authority, granting domain certificates to other devices.

Every autonomic device discovers neighbouring autonomic nodes through an autonomic neighbour discovery protocol. This could be implemented for example through IPv6 neighbour discovery, using a to-be-assigned well-known multicast address indicating "all autonomic nodes on this subnet".

An autonomic device signs its neighbour discovery packets. If it has a domain certificate from the domain registrar, it uses that. If not, it uses either a vendor certificate (e.g., an IEEE 802.1AR

[IDevID] credential) or a self-signed certificate.

If two autonomic homenet devices use the same trust anchor they can verify each other's certificate thus establishing that the peer is a member of the same local domain.

If one autonomic homenet device is member of a domain, and its neighbour is not, it invites the neighbour to join the domain. The device without domain credentials requests to join the first domain it is presented with. The device MUST only join a homenet domain when it is in the factory default configuration (e.g. it is not currently a member of a homenet). The domain device proxies the request to the registrar, including the device credentials of the device without domain credentials.

The registrar accepts or declines a request to join the domain, based on the credentials presented and other policy defined criteria such as proxy identity. Any authorized device currently within the domain MAY provide supplemental criteria for help making this decision. A smartphone autonomic application would be an ideal domain member to provide user interface functionality for the obtaining of supplemental criteria from end users.

If a device is accepted into the domain, it is invited to request a domain certificate through a certificate enrollment process.

The result is a common trust anchor and device certificates for all autonomic devices in a domain. These certificates can subsequently be used to determine the boundaries of the homenet, to authenticate other domain nodes, and to autonomically enable services on the homenet.

3. Security Considerations

The approach as outlined in this document is open to a number of attacks at bootstrap time. For example, a malicious device could pretend to be an expected device and assume its role. This is however no different to current security models in home networks.

4. Informative References

[I-D.ietf-homenet-arch]
Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "Home Networking Architecture for IPv6", draft-ietf-homenet-arch-04 (work in progress), July 2012.

[IDevID] IEEE Standard, "IEEE 802.1AR Secure Device Identifier", December 2009, <http://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

Authors' Addresses

Michael H. Behringer
Cisco

Email: mbehring@cisco.com

Max Pritikin
Cisco

Email: pritikin@cisco.com

Steinthor Bjarnason
Cisco

Email: sbjarnas@cisco.com