Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

M. Behringer
M. Pritikin
S. Bjarnason
Cisco

February 13, 2014

Bootstrapping Trust on a Homenet
draft-behringer-homenet-trust-bootstrap-02.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 enrol 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 August 17, 2014.

Table of Contents

1. Problem Statement

[I-D.ietf-homenet-arch] states that "A homenet will most likely also have internal borders between internal realms, e.g. a guest realm or a corporate network extension realm. It should be possible to automatically discover these 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. There should be a way for a user to administratively assert in a simple way whether or not a device belongs to a homenet."

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

2. Approach

This approach is based on making homenet devices behave in autonomic mode where devices discover each others and autonomically establish trust boundaries. See [I-D.behringer-autonomic-network-framework] for more information on autonomic networking.

The document "Bootstrapping Key Infrastructures" [I-D.pritikin-bootstrapping-keyinfrastructures] explains in detail how key infrastructures can be securely and automatically deployed. This document applied those concepts to a homenet.

2.1. Summary of the approach

In short, the approach is:

- The user pairs a smart phone (or similar device) with one of the devices in the homenet, for example the CPE. The smart phone acts as a user interface only.

- The selected device automatically becomes the trust anchor of the homenet. Technically, it acts as a certification authority (CA) as well as a registration authority (RA) (see section 3.1 and 3.2 of [I-D.pritikin-bootstrapping-keyinfrastructures]).

- Devices in the homenet use a protocol to exchange identities.

- A new device is added to the homenet by the user accepting it on the smart phone, and the CA issuing a domain certificate to the new device.

- The boundary of the network is determined by checking the certificates of devices.

2.2. Autonomic devices

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.

2.3. User interface

The user interface can be provided by the devices themselves or for example through a smart phone interface. It is also possible to access the devices indirectly through the manufactures web site. Options are:

- The user connects a PC to a physical port on network device and gets access to devices's user interface.

- Using a smartphone app which is automatically downloaded when scanning a QR code on the device. This will then allow the user to connect to the device on an SSID which is dynamically created based on the device serial number. The device will only allow connections from smartphones using the manufactures app.

2.4. The Registrar

One autonomic device in the homenet takes on a registrar function, which contains a registration autority and a certificate authority. In a homenet, the simplest method should be chosen: The first device the user connects to automatically takes on these functions. Therefore, the function of the registrar is essentially hidden to the user.

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

2.5. Autonomic Adjacency Discovery

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

The identity exchanged in this protocol is either a domain certificate, for devices that have already joined the domain, or a vendor certificate (802.1AR) [IDevID] if available, or an insecure device identity (serial number).

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.

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.

2.6. Validating a new device's identity

If one autonomic homenet device is member of the homenet domain, and its neighbour is not, 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 informs the user about the new device, using the user interface, for example the smart phone.

The user decides to accept the device based on various criteria:

- Allow any device to join within a specific time period.

- Allow only devices with specific serial numbers to join. These can either be entered manually into the registrar or by scanning a QR code using the manufactures autonomic app on a smartphone.

- Allow only devices to join on a specific proxy device, or interface on that proxy.

- If the device has a vendor certificate (e.g., an IEEE 802.1AR [IDevID] credential), the device can be validated using a Cloud service from the vendor.

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

A device MAY require an invitation to be signed by the manufacturer, stating that it has been claimed by the user before it decides to join the domain.

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.

Section 4 of [I-D.pritikin-bootstrapping-keyinfrastructures] explains the functional overview of the solution, including all the functional elements and additional options, for example how to securely claim a device. The homenet case can be significantly more restrictive, for example work with serial numbers only, or using physical methods, such as pressing a button to pair a device, or typing a key displayed on an LED display into the registrar.

2.7. Services

As the devices have a common trust anchor, device identity can be securely established, making it possible to automatically deploy services across the domain in a secure manner.

Examples of services are device management, routing authentication, and service discovery.

2.8. Network boundaries

When a device has joined the domain, it can validate the domain membership of other devices. This makes it possible to create trust boundaries where domain members have higher level of trusted than

external devices. Using the autonomic User Interface, specific devices can be grouped into to sub domains and specific trust levels can be implemented between those.

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.

There are counter-measures against these attacks, with various security levels, and corresponding various ease of use. The options are (in order of increased security):

- Only allow new devices to join in a specific time period.
- Only allow specific devices to join by matching their serial numbers.
- Validating the vendor certificate on new devices using the vendors Cloud portal.

In order to support a variety of use cases, devices can be claimed by a registrar without proving possession of the device in question. This would result in a nonceless, and thus always valid, claim. Future registrars are recommended to take the audit history of a device into account when deciding to join the device into their network.

4. Informative References

[I-D.behringer-autonomic-network-framework]
Behringer, M., Pritikin, M., Bjarnason, S., and A. Clemm, "A Framework for Autonomic Networking", draft-behringer-autonomic-network-framework-01 (work in progress), October 2013.

[I-D.ietf-homenet-arch]
Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", draft-ietf-homenet-arch-11 (work in progress), October 2013.

[I-D.pritikin-bootstrapping-keyinfrastructures]
Pritikin, M., Behringer, M., and S. Bjarnason, "Bootstrapping Key Infrastructures", draft-pritikin-bootstrapping-keyinfrastructures-00 (work in progress), January 2014.

[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