Device Pairing

To add a device to an existing BlazeNet network, it will need to be paired to the network. This pairing process can take place over both an in-band mechanism (over the air) or out of band (via additional interfaces) but the general scheme of operation is the same regardless.

Overview

Pairing is the process of registering a device's authentication key (which is the public part of a public/private keypair unique and internal to the device) with the network control element. This allows the network control element to issue authentication challenges (and more importantly, verify the responses) to the device when it attempts to join the network.

Additionally, during the pairing process, the end device will receive a list of all public keys used by coordinators in the network. This allows the device to verify the identity of the network when joining. (This list can be updated over the air whenever the device associates to the network, though these changed key lists must be cross-signed with the key of a coordinator the end device already trusts.)

Depending on the pairing mechanism, additional data (such as the network identity, channel, regulatory region, etc.) may be provided to the device as well. Regardless of the way pairing takes place, the secondary stage of pairing is the same.

Pairing Exchange

This describes the exchange of messages to perform pairing; it's assumed that by this point, we've established some sort of communications channel between the control plane of the BlazeNet network, and the device through another means.

1. Request pairing: Device notifies the coordinator control plane it wishes to pair to the network.
    1. Depending on the current security policy and network configuration, this request may be declined: for example, a network may not allow new devices at all, or may not permit devices paired in-band.
    2. The network responds with supported pairing methods and algorithms
2. Perform key exchange: Perform a supported key exchange mechanism to derive encryption keys for the rest of the pairing communications
    1. Currently, only Ed25519 is implemented
    2. These keys will encrypt all subsequent packets during the pairing exchange. This provides confidentiality over potentially non-secure pairing channels. (Note that the device is unable to verify the coordinator's keys, and vice versa at this point)

3. Request pairing challenge: The coordinator provides random data to the device to sign
4. Submit device challenge: Sign the provided random data, concatenated with a constant
    1. Constant serves to guard against using this as a signing oracle
    2. If pairing is in band, the pairing code is concatenated as well
5. Receive network information: Coordinator provides various information about the network, such as the public keys of all coordinator nodes.
    1. At this point, the device's key is registered and it may join the network normally

At the end of the pairing process, the node should (re)associate to the network. It is not required to do so: pairing is considered successful as long as the pairing exchange completes successfully.

Out-of-band Pairing

In this section is a description of how devices are paired to the network using out-of-band communication mechanisms.

NFC

The end device exposes an NFC "dynamic tag," which can be read and written by a separate user device (such as a mobile phone,) or by specifically outfitted coordinator devices. This tag contains a fixed region, which holds information about the device type, as well as its public key.

During the pairing process, the end device and user device exchange messages:

1. Read out information: User device queries the read-only area of the NFC tag, which holds the device's public key, and stores it for later reference.
    1. 1. The reader device SHOULD upload the public key (which it read out from the EEPROM earlier) to the coordinator, to allow it to join the network
2. Upload network configuration: This consists of the network name (UUID,) channel, regulatory information, as well as the public keys of all coordinator nodes
3. Associate to network (using device key)

Once this is complete, the end device will attempt to associate to the network. During this process, the user device may periodically poll the end device as to its association status to determine when it's completed the process. The pairing process is considered complete when the end device either successfully associates to the network, or the association fails (due to invalid credentials, inability to find a coordinator, timeout, or cancelled by user device.) If the pairing process fails at any stage prior to successful association, the network information is not saved and the end device will continue to use its previous network settings, if any.

In-band Pairing

This section describes the process of pairing a new device to a network in-band. It exists as a fall-back for other pairing mechanisms, but should be used as a last resort as it is less secure, less

convenient, and much slower than other supported out-of-band mechanisms. Due to its nature, the end device will have to blindly trust the network it is associating to, and must already know the regulatory region the network is operating in.

The basic premise of in-band pairing is that every device will have an unique “pairing code” associated with it. It’s usually derived from its serial number, and should be printed on the device itself. The device will use this pairing code to authenticate to the network during association, instead of its device key.

First Stage

A network will need to be made “joinable,” which sets a flag in its beacon. This also activates an additional authentication mechanism during association, allowing the device to attempt to authenticate with its pairing code instead of its key. Coordinator nodes *should* have a timeout that disables the joinable mode (and purges all permitted pairing codes) automatically after some time.

During this time, the end device will scan all radio channels in the currently active bandplan to find active networks broadcasting beacon frames. It will attempt to authenticate with the pairing code against all networks that are currently joinable. (Note that this does *not* allow the radio to be updated with a new regulatory region, as with out-of-band pairing.)

Second Stage

If the device can associate successfully with its pairing code, it should perform the standard pairing exchange immediately after. It should *not* attempt to negotiate group encryption keys, power saving modes, or attempt to pass any other traffic, as it will be dropped by the coordinator for all end devices authenticated with pairing codes.

Once complete, the end device is expected to re-associate to the network using its device key. The coordinator will invalidate the device’s association at the conclusion of the pairing process, or if any of the steps during the second stage fail.

Revision #5
Created 29 September 2022 00:49:39 by Tristan
Updated 25 October 2022 16:12:17 by Tristan