Security Schemes

This page describes the security/authentication mechanisms in use by the protocol.

Background

Each coordinator and device are required to have a public/private key pair, using an elliptic curve. These are used to authenticate devices and coordinators, as as deriving encryption keys.

Rekeying

Devices *must* support rekeying both unicast and multicast keys at arbitrary intervals. Rekeying can be initiated by the coordinator or the device. In the unicast case, the new key is used immediately for all subsequent packets, once the rekeying process has completed.

For multicast rekeying, the new key is provided via the existing multicast group, with a new key id. Clients are expected to acknowledge receipt of the new key, and packets will switch to using the new key once all clients have confirmed the key change, or after a pre-defined timeout period (which will cause an error message to be logged.)

Unicast Keys

There are several key derivation schemes supported, which are used to derive the unicast keys that protect direct communication between the coordinator and end device node.

Key Based

In this scheme, the device will authenticate using its device key. It is the default scheme for devices that wish to pass actual BlazeNet traffic. The coordinator and device negotiate a shared session key used to encrypt and authenticate all subsequent messages.

This key exchange takes place in two stages. In the first stage, a shared secret is calculated, using ECDH (with their known and previously exchanged public keys.) This shared secret is then appended with two nonces (one provided by the coordinator, the other by the device) and hashed using Poly1305 to produce the final session key. Hashing the key with nonces is used to further diversify the key, and hides some potential underlying biases in ECDH (relating to the resulting keys not being evenly distributed in the key space.)

As part of the association, the coordinator issues a challenge (a random 32-byte blob) the device must sign with its device private key (using EdDSA/Ed25519) and return to the coordinator before

being allowed on the network.

Passphrase Based

This scheme is used when performing over-the-air pairing for a peripheral.

A session key is negotiated with the coordinator by using ECJ-PAKE, with the pairing code as the input. This modes does *not* mutually authenticate either the device or coordinator based on previously exchanged public keys; it’s intended to allow a device to easily join a network, based on a fixed pairing code.

Coordinators may place additional requirements on nodes that associated with this scheme.

Multicast Keys

All multicast (and by extension, non-beacon broadcast packets) are encrypted using one of several pre-defined keys. These keys are generated and managed entirely by the coordinator, and provided to client devices through the key management interface exposed by the coordinator.

Revision #4
Created 18 October 2022 05:30:26 by Tristan
Updated 25 October 2022 16:12:17 by Tristan