Request for feedback on: RADIUS profile for Bonded Bluetooth Low Energy peripherals

draft-grayson-radext-rabble

Authors: Mark Grayson (Cisco) & Eliot Lear (Cisco)

IETF 116 Yokohama, 2023-03-28
Background:
Bluetooth - from wired replacement to mobile system

• A bonded Bluetooth Low Energy connection is between a peripheral and a central device
• Both peripheral and central are configured with 48-bit global public MAC addresses
• Bluetooth vendors have enhanced their enterprise access point/central functionality to virtualize a central’s MAC address
• This enables the bonded connection to “follow” the BLE peripheral as it moves between single-vendor access points in a single administrative domain
Leveraging operation of Bluetooth privacy in RADIUS Exchange

- 64-bit Identity Resolving Key (IRK) known to both peripheral and central (exchanged during the bonding procedure)
- Peripheral generates a new 24-bit prand value (every 1-3600 seconds) together with a 24-bit hash which is a function of prand and IRK
- Peripheral uses a Resolvable Public Address including prand and Hash:

```
| LSB | Hash (24-bits) | prand (22-bits) | MSB |
```

- Conventional central performs a hash of prand with all known IRKs to see whether address is resolvable and peripheral is “known”
- RABBLE defines transport of prand as user-name and hash as user-password attributes
- RADIUS sever authenticates peripheral by performing the same hash of prand with known IRKs
Enabling BLE mobility in multi-vendor and/or multi-domain environments

1) Pairing, BLE bonding and IRK exchange

2) Expose IRK to DB

3) Peripheral Moves Between Access Points

4) Generate new RPA [hash (prand, IRK), prand]

5) Advertisement with RPA

6) Access Request [prand, hash]

7) Check hash against known IRKs

8) Access-Accept/Reject

Bonded BLE Peripheral

BLE Central/Access Point

BLE Security Database

RADIUS Server

NAS
Handling Non-IP messages with appendix describing MQTT based forwarding – intended to be moved to another document.
Proposed RADIUS Profile

• RADIUS Attribute Type #61 (NAS-Port-Type)
  • New value to represent "Wireless - Bluetooth Low Energy"
• New Attributes:
  • GATT-Service-Profile: 32 octet value(s) advertised by the peripheral
  • BLE-Keying-Material: At least including peripheral’s permanent MAC address and peripheral’s IRK
  • MQTT-Broker-URI: For BLE message forwarding
  • MQTT-Token: Optionally used in MQTT connect and can be used to associate a connection with a specific NAS
Next steps

• Understand that new profiles are out of scope of current radext charter

• Seeking technical feedback from the RADIUS experts on radext list and using github tracker: https://github.com/iot-onboarding/rabble

• Reviewers, co-authors, and implementations welcome!