
Xiaomi's MiHome Binary protocol

Summary

Xiaomi is a manufacturer of smart home devices under the “MiHome” label. These devices use an encrypted, proprietary network protocol to communicate with the official smartphone app. It operates on UDP port 54321.

This repository documents the protocol, henceforth referred to as “mihobi”, and contains exemplary source code to parse and analyze.

The main goal is to remove the dependence on proprietary software, and to regain control over your own devices.

It has been developed with the *Yeelight RGBW smart bulb*. Other devices might use yet unimplemented features.



Documents

`doc/PROTOCOL.md`

Tools

pcap-decrypt.py

Recovers the protocol from pcap-ng dumps and attempts to decrypt the packet payloads.

Dependencies:

- Python 3.5+
- tshark, the command-line version of Wireshark

-
- PyShark, a Python wrapper for tshark
 - cryptography, a Python library which exposes cryptographic recipes and primitives.

Installation:

```
1 apt-get install tshark
2 pip3 install pyshark
3 pip3 install cryptography
```

Usage:

```
1 ./pcap-decrypt.py capture.pcapng.gz
```

Example output:

```
1 ### 192.168.13.2 => 192.168.13.1 (xx:xx:xx:xx:xx:xx => yy:yy:yy:yy:yy:
  yy)
2 META: Hello
3
4 ### 192.168.13.1 => 192.168.13.2 (yy:yy:yy:yy:yy:yy => xx:xx:xx:xx:xx:
  xx)
5 META: device yy:yy:yy:yy:yy:yy has token:
  abcdef1234567890abcdef1234567890
6
7 ### 192.168.13.2 => 192.168.13.1 (xx:xx:xx:xx:xx:xx => yy:yy:yy:yy:yy:
  yy)
8 {"id":1234567890,"method":"miIO.config_router",
9 "params":{"ssid":"WiFi name","passwd":"WiFi password","uid":987654321}}
10
11 ### 192.168.13.1 => 192.168.13.2 (yy:yy:yy:yy:yy:yy => xx:xx:xx:xx:xx:
  xx)
12 {"result":["ok"],"id":1234567890}
```

miio.py

Core Python library that parses and generates MiHoBi packets.

Notes

As of 2017-02-10, the initialization process (“SmartConnect”) leaks the user’s WiFi credentials, due to weak encryption. See [PROTOCOL.md](#) for more details. I do not recommended connecting MiHome devices to your main WiFi network.

Appendix

Legal

Xiaomi is a registered trademark and service mark of Xiaomi Inc., which is not affiliated with the maker of this program and does not endorse, service or warrant the functionality of this product.

Author

The source code and documentation in this repository

(c) 2016-2017 Wolfgang Frisch

Licensed under the GPLv3.