

Find My (?:Device)? 101

The technologies behind Bluetooth location trackers



Agenda



Bytes	Description	Requirement
0-5	MAC address	REQUIRED
6-8	Flags TLV; length = 1 byte, type = 1 byte, value = 1 byte	OPTIONAL
9-12	Service Data TLV; length = 1 byte, type = 0x16, value = 0xFCB2	REQUIRED
13	Network ID	REQUIRED
14	Near-owner bit (1 bit, least significant bit) + reserved (7 bits)	REQUIRED
15-36	Proprietary company payload data	OPTIONAL

Table 1: Location-Enabled Payload Format

```
Bluetooth Low Energy Link Layer
Access Address: 0x8e89bed6
> Packet Header: 0x2340 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
  Advertising Address: 4a:3c:7e:91:95:b2 (4a:3c:7e:91:95:b2)
  < Advertising Data
    < Flags
      Length: 2
      Type: Flags (0x01)
      000. .... = Reserved: 0x0
      .... .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
      .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
      .... .1. = BR/EDR Not Supported: true (0x1)
      .... ..1 = LE General Discoverable Mode: true (0x1)
      .... ...0 = LE Limited Discoverable Mode: false (0x0)
    < Service Data - 16 bit UUID
      Length: 25
      Type: Service Data - 16 bit UUID (0x16)
      UUID 16: Google LLC (0xfeaa)
      Service Data: 40e634838959dcb03a426189d5f5941f245b76275a4
      CRC: 0x98795d
```

What?!

- Problem statement
- Functional goals

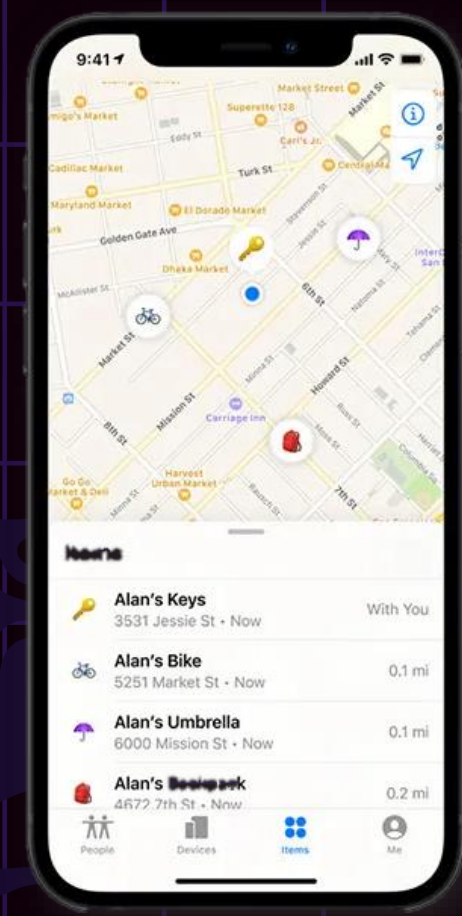
How?

- Protocol description(s)
- Standards and publications

And now?

- Radio sniffing
- Software reverse engineering

Active Bluetooth beacons: Emit locally, find globally



Actively powered beacons,
unidirectional, emit local radio signals

Global network makes device position
available to authorized owner

(no advertisement or trademark infringement intended. yada yada, etc. pp.)

Technological Convergence of BLE trackers



Bluetooth: Discovery procedures

Bluetooth
"Classic"

Device is
"discoverable"

Inquiry Scan

Inquiry Scan

Inquiry Scan

Scanning device

Inquiry

Bluetooth
Low Energy

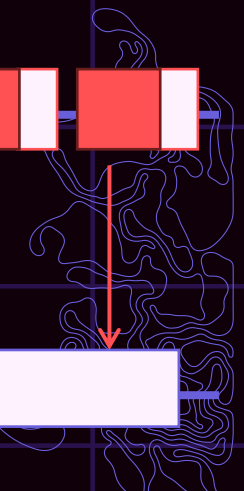
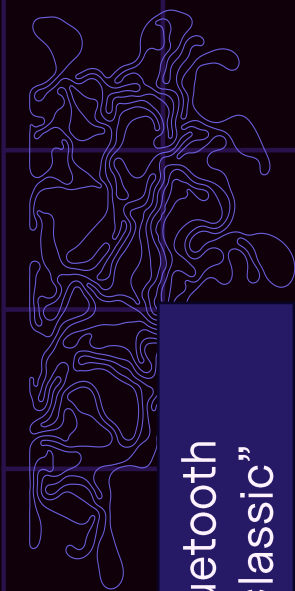
Device is
"advertising"

Advertisement

Listening device

Listening

(Not to scale)

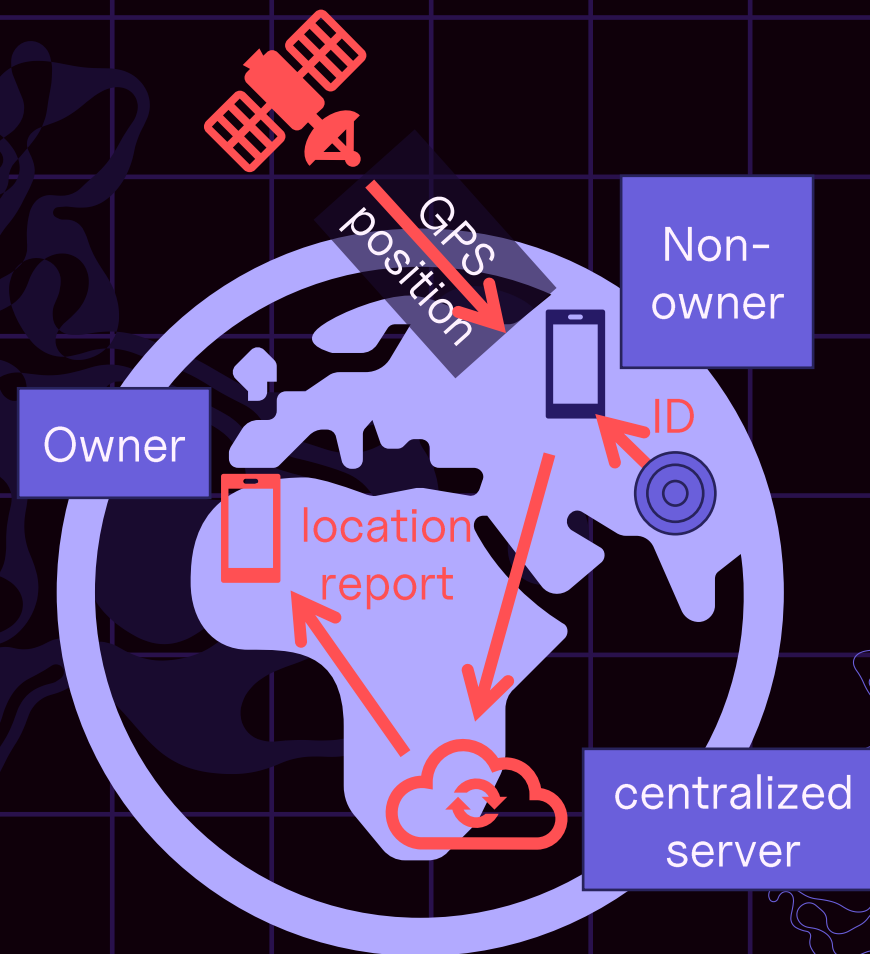


Construct a tracking network

BLE advertisements contain source MAC address and arbitrary advertisement information (up to 31 bytes)

Common use cases: iBeacon/Eddystone

Trivial to construct a centralized tracking network (e.g. Tile “Community find”)



Trivial tracking, Attacker model

Privacy issue: globally unique MAC address can be

- recognized across sightings
- correlated across receivers

Partial solution: Random MAC addresses, optionally “resolvable”.

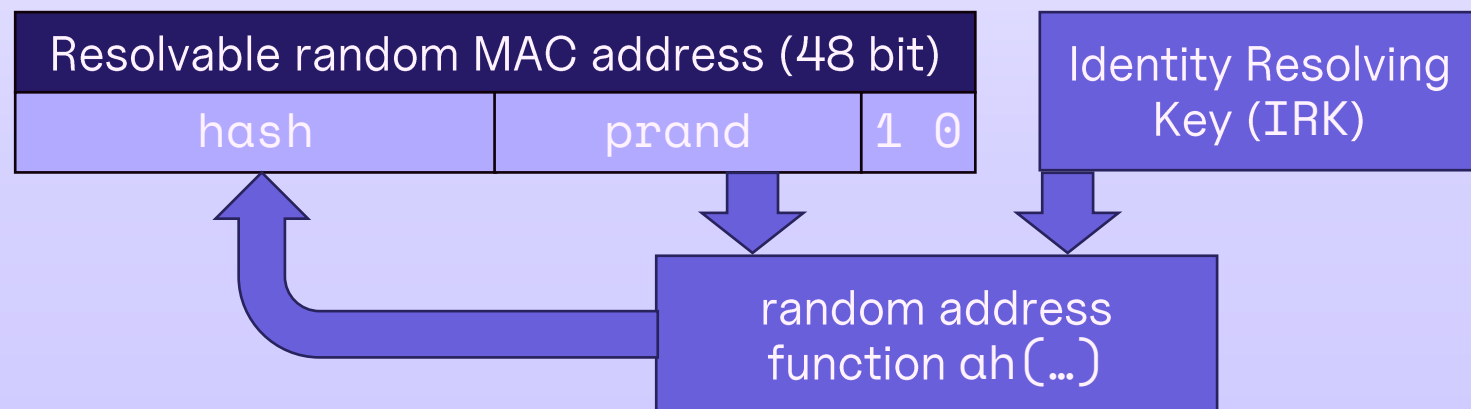
Attacker model

- Assume the attacker has one or more radios capable of receiving BLE advertisements
- Attacker radios can cooperate, possibly globally

Attacker goals

- Track device (= person?) from location to location
- Observe dwell time at a static location

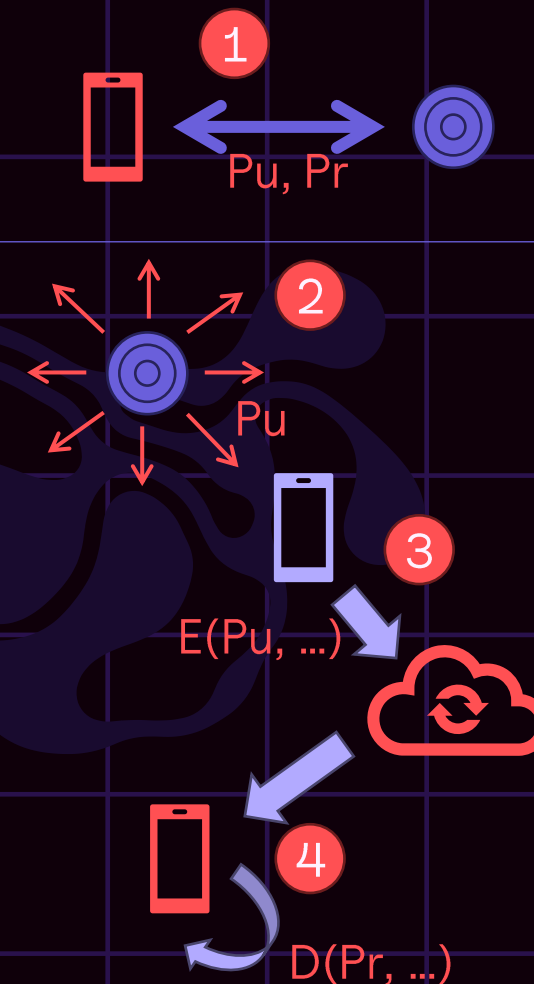
Resolvable Private Address generation



Note: Trivially applies to centralized server operator

Core idea: Encrypt location reports

1. On accessory initialization: Setup keys between owner device and accessory
2. In BLE advertisement: Broadcast public key
3. Non-owner devices: Encrypt location with public key and upload to server
4. Owner device: query for location reports, download and decrypt

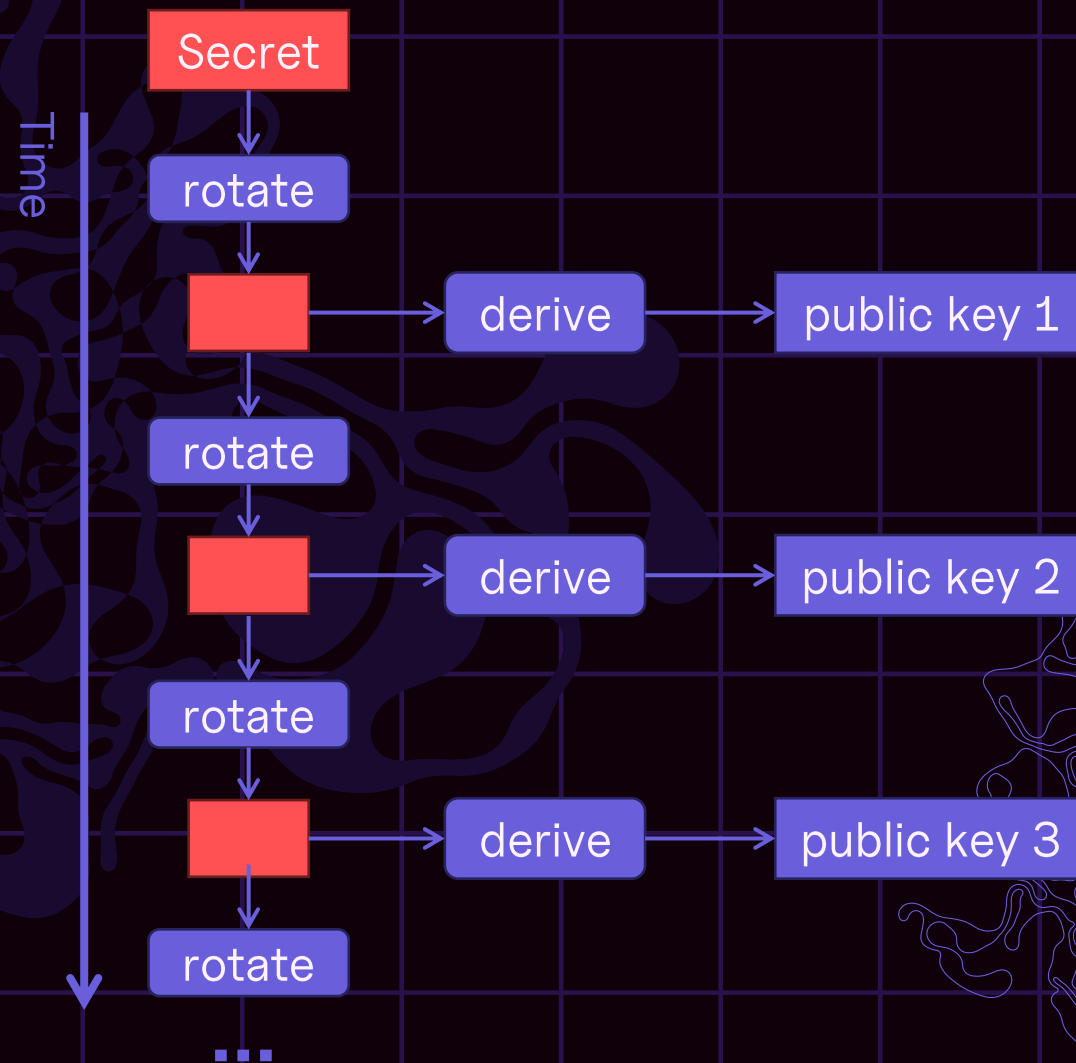


Key setup

Broadcasting, Location reporting

Core idea: Rotate public key

- A static broadcast public key would, in effect, be a static identifier
- Countermeasure: Accessory changes public key in pre-defined intervals
- Owner device can reproduce same sequence
- Non-owner devices are oblivious this is going on



“Two of every kind”

Apple/iOS

- “Find My” network (FMN)



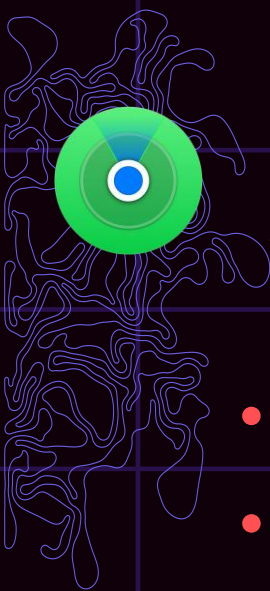
Google/Android

- “Find My Device” network (FMDN)



Also ran

- Tile
- Samsung



Apple: “Find My”

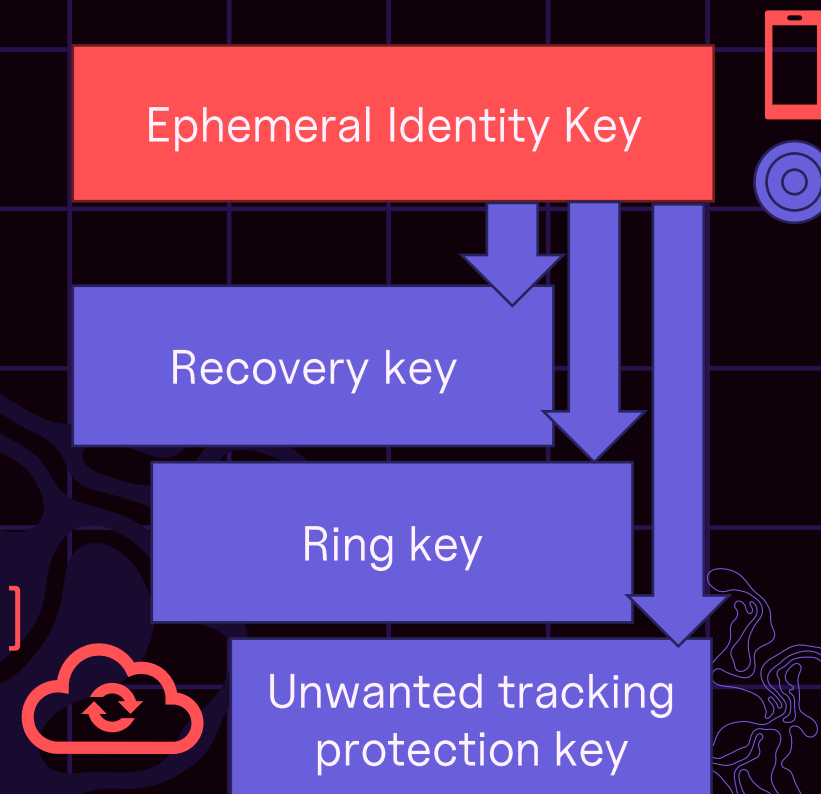
- NIST P-244 curve, 28 byte public key
- Use “random” source MAC address, for parts of the public key

Bytes	Content
0-5	BLE address $((pi[0] \mid (0b11 \ll 6)) \parallel pi[1..5])$
6	Payload length (30)
7	Advertisement type (0xFF, manufacturer specific)
8-9	Company ID (0x004C)
10	OF type (0x10)
11	OF data length (25)
12	Status (e.g. battery level)
13-34	Public key bytes $pi[6..27]$
35	Public key bits $pi[0] \gg 6$
36	Hint

- Alexander Heinrich, Milan Stute, Tim Kornhuber, Matthias Hollick. **Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System.** *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2021. [doi:10.2478/popets-2021-0045](https://doi.org/10.2478/popets-2021-0045)
- Alexander Heinrich, Milan Stute, **OpenHaystack**, <https://github.com/seemoo-lab/openhaystack>

Google: “Find My Device”

- Extension to Google Fast Pair Service (GFPS)
- Secret key EIK (Ephemeral Identity Key) chosen by owner phone
- Derived keys stored on backend:
 - Recovery key: $\text{SHA256}(\text{EIK} \parallel 0x01) [:8]$
 - Ring key: $\text{SHA256}(\text{EIK} \parallel 0x02) [:8]$
 - Unwanted tracking protection key: $\text{SHA256}(\text{EIK} \parallel 0x03) [:8]$



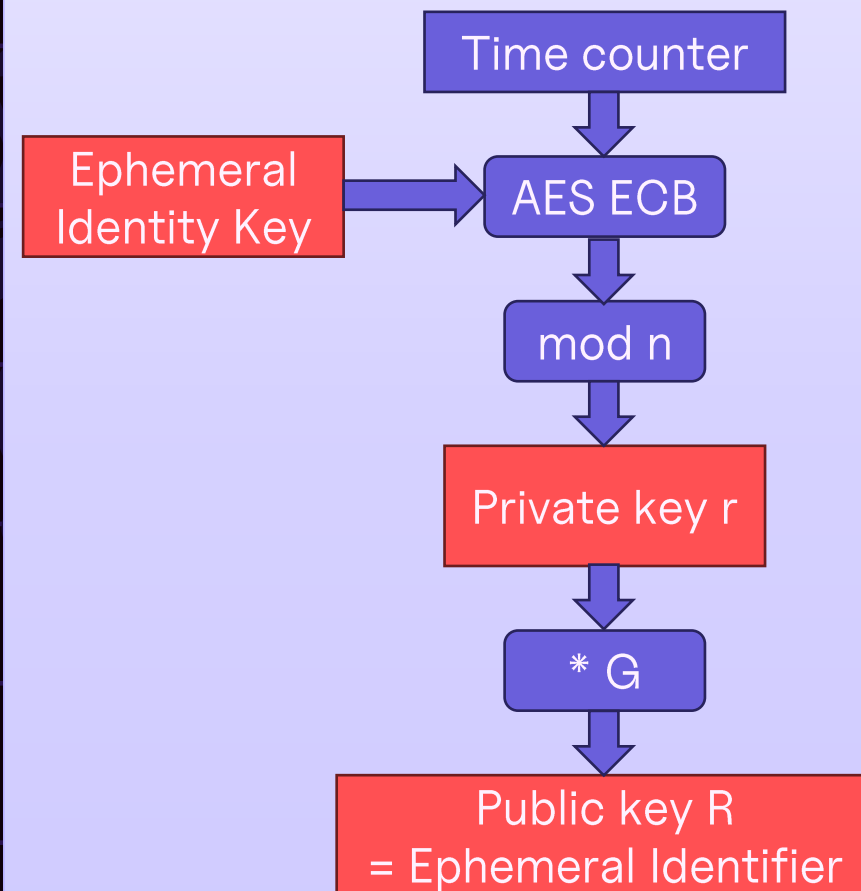
Find My Device Network Accessory Specification,

<https://developers.google.com/nearby/fast-pair/specifications/extensions/fmdn>

“Find My Device” advertisements

- Curve: SECP160R1 (20 bytes), or SECP256R1 (32 bytes, BLE 5 extended advertising)
- Extension of Eddystone format, UUID 0xFEAA
 - Eddystone: Types 0x00, 0x10, 0x20, 0x30
 - Find My Device type: 0x40, or 0x41 (unwanted tracking protection)
- 20 bytes ephemeral ID == public key, 1 byte hashed flags

EID generation



Abusing BLE trackers for stalking

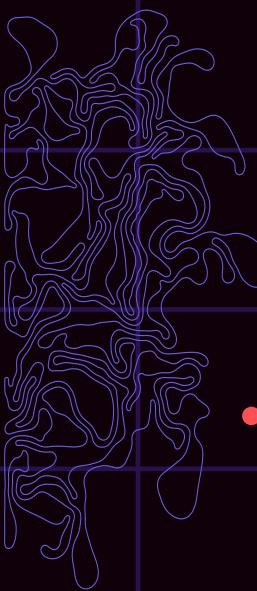
- Low cost and high accessibility mean increased potential for non-consensual abuse of BLE trackers
- Reaction: Apple/Google trackers monitor connection to owner device and initiate countermeasures when away for too long
- Countermeasures:
 - Emit sound periodically, or on movement
 - Reduce identifier rotation frequency
 - Allow easier detection and pinpointing of tracker

See also:

- **Escaping Big Brother (or Your Ex)**, erlern, day 2

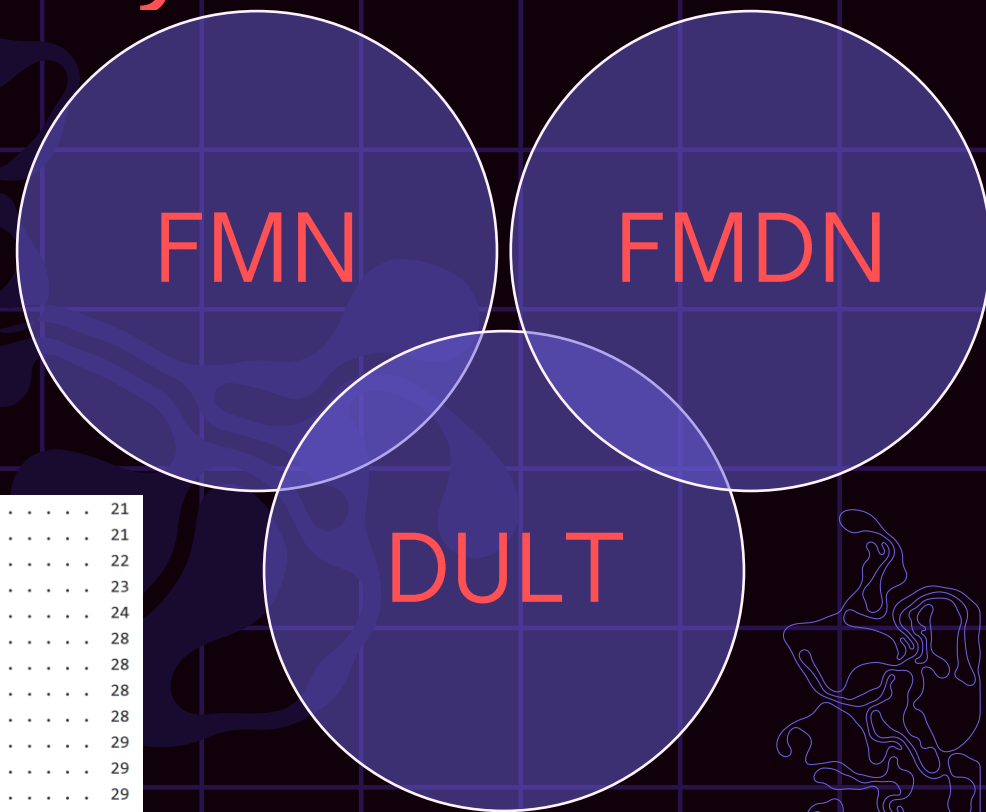


media.ccc.de



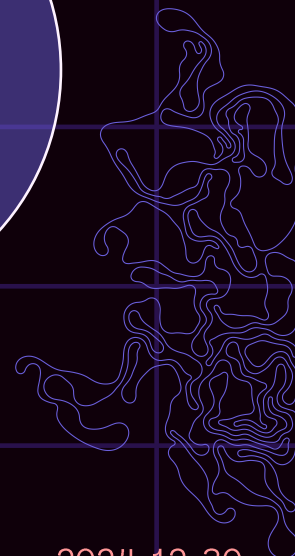
“Detecting Unwanted Location Trackers” (DULT)

- IETF WG specifies threat model and behavior for tracker (-like) devices
- Command for “non-owner” devices are available unauthenticated, if device is not in “near-owner” state



3.13. Non-Owner Finding	21
3.13.1. Hardware	21
3.13.2. Motion detector	22
3.13.3. Sound maker	23
3.13.4. Non-owner controls	24
3.13.5. Alternate finding hardware	28
3.13.6. Recommended Finding Options	28
3.13.7. Future hardware	28
3.14. Disablement	28
3.14.1. Disablement instructions	29
3.15. Identification	29
3.15.1. Serial number identification	29
3.15.2. Identifier retrieval capability	29
3.15.3. Identifier retrieval over Bluetooth LE	29
3.15.4. Identifier retrieval from a server	29
3.15.5. Identifier over NFC	30
3.16. Owner registry	30
3.16.1. Obfuscated owner information	31
3.16.2. Persistence	31
3.16.3. Availability for law enforcement	31

Detecting Unwanted Location Trackers Accessory Protocol,
<https://datatracker.ietf.org/doc/raft-ietf-dult-accessory-protocol/>



SDR sniffing with rad10

```

^Cfelix@flx-vivobook-asuslaptop-x415ja-r465ja:~/BTLE/host/build$ ./btle-tools/src/btle_rx | grep --line-buffered aafe4
0032000us Pkt002 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032977us Pkt030 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0131169us Pkt042 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569e9ee01 CRC1
0098087us Pkt067 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0033610us Pkt086 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032613us Pkt139 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94549f9ee05 CRC1
0556880us Pkt158 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0000784us Pkt203 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC1
0032437us Pkt223 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79ceb8ce92d3c22d68ac8d94569f9ee05 CRC1
0098258us Pkt290 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd75a813bfff14d5c7ae971dd328811286 CRC1
0163826us Pkt304 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8d7126055c Data:0201061916aafe400e7ed99eb79eeb8de92d1c22d68ac8d94569f9ee05 CRC1
0262727us Pkt391 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032244us Pkt419 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC1
0196449us Pkt444 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0066313us Pkt518 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0130473us Pkt558 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569b9276a CRC1
0032711us Pkt584 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032732us Pkt596 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0000328us Pkt660 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8cc92d1c22d68ac8d96469f9ee05 CRC1
0294961us Pkt675 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0032748us Pkt698 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032528us Pkt709 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:519d046241f3 Data:0201061916aafe414d65d3e96bd71a813bfff14d5c7ae971df328811286 CRC0
0032771us Pkt720 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0
0032614us Pkt740 Ch37 AA:8e89bed6 ADV_PDU_t0:ADV_IND T1 R0 PloadL35 AdvA:5b8df126055c Data:0201061916aafe400e7ed99eb79eeb8ce92d1c22d68ac8d94569f9ee05 CRC0

```

<https://github.com/JiaoXianjun/BTLE>
 BTLE sniffer on bladeRF or HackRF, such
 as rad1o (the CCCamp 2015 badge)

Nordic Sniffer: nRF52 SDK

Apply a display filter ... <Ctrl-/>

Interface COM8-4.4 Device "" -32 dBm 51:9d:4:62:41:f3 random Key Legacy Passkey Value Adv Hop 37,38,39 Clear

No.	Time	Source	Destination	Protocol	Length	Info
615	266.506567	43:1a:d3:f7:7f:de	51:9d:04:62:41:f3	LE LL	38	SCAN_REQ
616	267.349558	Anonymous	Broadcast	LE LL	47	ADV_EXT_IND[Malformed Packet]
617	267.510191	Anonymous	1c:11:2a:de:65:7f	LE LL	38	ADV_EXT_IND[Malformed Packet: length of contained item exceeds length of containing item]
618	267.925861	Anonymous	Broadcast	LE LL	38	ADV_EXT_IND[Malformed Packet]
619	268.284572	Anonymous	ff:1e:69:ce:f7:5c	LE LL	63	ADV_EXT_IND[Malformed Packet]
620	268.510541	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
621	268.512125	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
622	268.513709	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
623	269.334980	Anonymous	33:c6:18:de:65:ff	LE LL	38	ADV_EXT_IND[Malformed Packet]
624	269.757645	Anonymous	Broadcast	LE LL	46	ADV_EXT_IND[Malformed Packet]
625	270.513457	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
626	270.513968	4b:b3:00:6c:c0:e3	51:9d:04:62:41:f0	LE LL	38	SCAN_REQ
627	270.515041	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
628	270.516625	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND
629	272.520029	51:9d:04:62:41:f3	Broadcast	LE LL	61	ADV_IND

> Frame 629: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface COM8-4.4, id 0

- nRF Sniffer for Bluetooth LE
- Bluetooth Low Energy Link Layer
 - Access Address: 0x8e89bed6
 - Packet Header: 0x2340 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
 - Advertising Address: 51:9d:04:62:41:f3 (51:9d:04:62:41:f3)
 - Advertising Data
 - Flags
 - Length: 2
 - Type: Flags (0x01)
 - 000. = Reserved: 0x0
 - ...0 = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
 -0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
 -1... = BR/EDR Not Supported: true (0x1)
 -1.1. = LE General Discoverable Mode: true (0x1)
 -1.0 = LE Limited Discoverable Mode: false (0x0)
 - Service Data - 16 bit UUID
 - Length: 25
 - Type: Service Data - 16 bit UUID (0x16)
 - UUID 16: Google LLC (0xfeaa)
 - Service Data: 41cae3593eb4cdcdeee3ea6426650a0a609e5bf74dfa

CRC: 0xd29df5

```

0000 08 36 00 03 ba a7 02 0a 01 25 1a 00 00 4c 1b d3  -6.....%...L..
0010 59 d6 be 89 8e 40 23 f3 41 62 04 9d 51 02 01 06  Y....@#. Ab..Q...
0020 19 16 aa fe 41 ca e3 59 3e b4 cd cd ee e3 ea 64  ....A..Y >.....d
0030 26 65 0a 0a 60 9e 5b f7 4d fa 4b b9 af          &e...[. M.K..
    
```


nRF Connect (Android)

12:11 74% battery

Devices SCAN

SCANNER	BONDED	ADVERTISER	N/A
0xAAFE		67:03:99	
	N/A (Find My Device)	51:9D:04:62:41:F3	CONNECT
	NOT BONDED	-61 dBm ↔ 2004 ms	
	N/A (Find My Device)	65:EF:C9:36:DC:22	CONNECT
	NOT BONDED	-79 dBm ↔ N/A	
	N/A (Find My Device)	60:EA:A8:C5:DA:42	CONNECT
	NOT BONDED	-45 dBm ↔ 2007 ms	
	N/A (Find My Device)	44:15:83:A9:DA:1A	CONNECT
	NOT BONDED	-46 dBm ↔ 2003 ms	
	N/A (Find My Device)	78:1D:07:26:2F:BB	CONNECT
	NOT BONDED	-69 dBm ↔ 10012 ms	

12:03 69% battery

Devices DISCONNECT

BONDED ADVERTISER N/A 51:9D:04:62:41:F3

CONNECTED NOT BONDED CLIENT SERVER

UUID: 0x1800
PRIMARY SERVICE

Device Information
UUID: 0x180A
PRIMARY SERVICE

Accessory Non-Owner Service
UUID: 15190001-12f4-c226-88ed-2ac5579f2a85
PRIMARY SERVICE

Accessory Non-Owner Characteristic
UUID: 8e0c0001-1d68-fb92-bf61-48377421680e
Properties: INDICATE, WRITE
Value: (0x) 01-03
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications and indications disabled

Google Fast Pair Service
UUID: 0xFE2C
PRIMARY SERVICE

Unknown Service
UUID: 0xFC7C
PRIMARY SERVICE

SMP Service
UUID: 8d53dc1d-1db7-4cd3-868b-8a527460aa84
PRIMARY SERVICE

Unknown Service

Android “Find My Device” app

METHOD: POST +

URL

+ https://android.googleapis.com/nova/nbe_list_devices

HEADERS

+ accept-language: en-DE

+ authorization: Bearer ya29.m.CoYCAQ1IaZhgd1oXk2vBMGarYXZxgswqpNDaOxIuSBo0--2-51p.JYTaoFEWa_5BM1ekT06melBph4NFeKZ4F1tauf6Cl1Ns5YDXSn-

- Handled by `com.google.android.gms` and `fmd`
- HTTPS public key pinning

```

246 1: {
247   "1": {
248     "1": "670d244d-0000-219e-b338-30fd381716e4"
249   },
250   "2": {
251     "1": "moto tag15",
252     "2": 22,
253     "9": {
254       "1": "https://lh3.googleusercontent.com/
f-yUCket_o8g0Izb5iscX4P03SoVtMFzTjzryxKuJuAUKkccGrnjrgI1qVyGCdClho0-1oDcPLMQvZRJwE3c",
255       "2": 1
256     },
257   "12": {

```

Call for Reverse Engineering

- Research question:
Communication between

A [https://github.com/leonboe1/
GoogleFindMyTools](https://github.com/leonboe1/GoogleFindMyTools)

by Leon Böttger,
December 2024

of
own Find My Device
accessories

- Is there anything in the lower layer radio protocol that might compromise anonymity?

As a

User Story

Me

I want to

**be able to derive the
broadcast keys of my own
devices**

So that I

**can have my Home Assistant
detect whether the devices
are at home**

The End

Signal [henryk.42](#)

[threema://36C48UCS](#)

<https://chaos.social/@henryk>

See also:

- [From fault injection to RCE: Analyzing a Bluetooth tracker](#), Nicolas Oberli, day 1

 media.ccc.de