

Ich weiß wo dein Haus wohnt

GRUNDLAGEN ZU BLUETOOTH-TRACKERN

LEA RAIN

CN: STALKING,
DIGITALE GEWALT
GPN 23
@ZKM
HIDDEN PATTERNS

20.6.

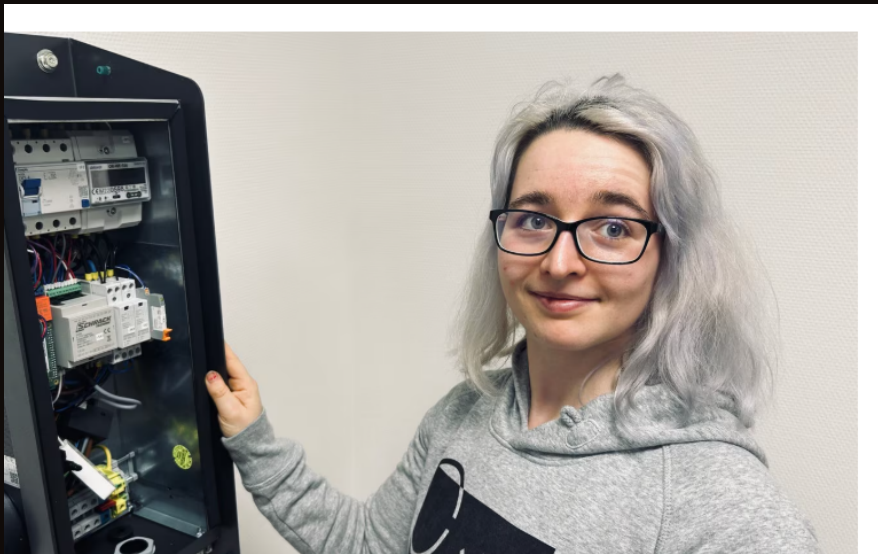


- 1 Einführung
- 2 Bluetooth Low Energy Tracker
- 3 Crowd-Sourcing-Networks
 - Apple Find My
 - Google Find My Device
- 4 Stalking und Digitale Gewalt mit BLE-Trackern
- 5 Fazit

Einführung

- Kein Vortrag zu schwerwiegenden Sicherheitslücken und endgültigen Zerlegen von BLE-Trackern und Crowd-Sourcing-Netzwerken...
... sondern Grundlagen zu Bluetooth Low Energy, Standortdiensten und Crowd-Sourcing
- Keine fundamental kaputten einzelnen Tracker...
... sondern Design-Schwächen einzelner Punkte
- Keine Möglichkeiten, sämtliche Standortdaten von allen Geräten zu extrahieren...
... sondern kreative Wege mit den Netzwerken umzugehen (mit bisschen Code)
- Leider kein Rundum-Sorglos-Paket für Stalkingprävention und -detektion...
... sondern Hilfestellungen existierender Ansätze und etwas Sensibilisierung

✨ Sicherheitsforscherin ✨



- lea@gpn23 (they/them, sie/ihr, she/her)
- Binary Kitchen Regensburg
- Koffeinabhängiges Punguin 
- ITlerin & your friendly neighborhood hacker
- Informatikstudium mit Forschungsfoo & IT (Security) Brötchen
-    

- Generell IT Security, Fokus auf alles, was unter IoT fällt
- Bluetooth Low Energy Tracker, kaputtes Carsharing, Ladeinfrastruktur, ...
- Freie Software, Systeme und Pinguine

⇒ alles, was mir so Spaß macht

Bluetooth Low Energy Tracker

BLE-Tracker

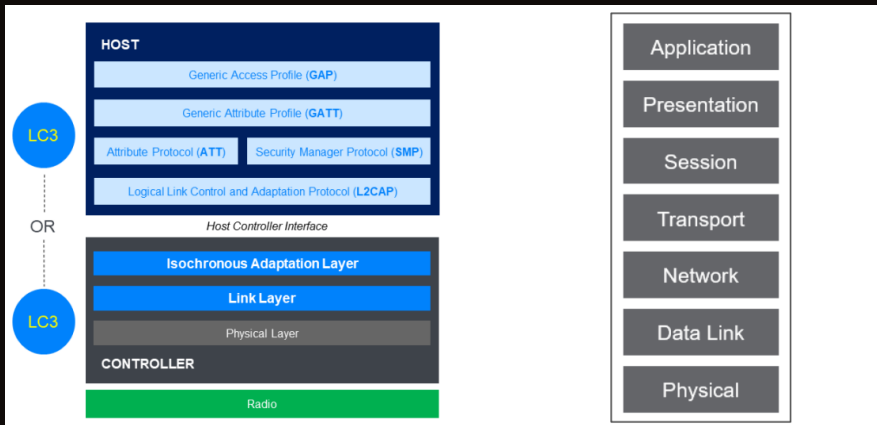


- Kleine Geräte zum Anbringen an oder Einstecken in wertvolle Gegenstände (Koffer, Fahrrad, Geldbeutel, Schlüssel, ...)
- Alarmfunktion für eigenen Tracker in der Nähe $\Rightarrow$ Klingeln von wichtigen Gegenständen
- State of the art: Tracker mit Crowd-Sourcing-Network – Tracker finden mit umliegenden Geräten eines Netzwerkes
- Tracker nur mit Bluetooth (Low Energy) eher historisch
- Start mit Tile Trackern und steigender Beliebtheit in 2014
- Starker Anstieg der Beliebtheit durch Apple AirTag in 2021
- Verwendung von Bluetooth Low Energy

BLUETOOTH LOW ENERGY

- Kommunikationsprotokoll für Geräte mit physischer Nähe ähnlich zu Bluetooth
- Einführung zu Bluetooth-Spezifikation 4.0 in 2009 (optional, unabhängig)
- (Hier relevanter) Unterschied: Geringerer Stromverbrauch, geringere Datenrate (weniger Daten, dafür frequentierter), ggf. größere Reichweite, keine Kopplung notwendig
- Ideal für alles, was mit IoT zu tun hat (Sensoren, Fitnesstracker, Smart Watches, Item Tracker)
- Tendenziell sehr viele Geräte mit B(LE) ausgerüstet, im 2.4 GHz-Spektrum viel los

BLE STACK



<https://www.bluetooth.com/wp-content/uploads/2022/05/the-bluetooth-le-primer-v1.2.0.pdf?hsCtaAttrib=165312078942>

- Broadcast: hallo, hier bin ich und das bin ich!
- Entweder Verbindungsabsicht oder -möglichkeit (bidirektionale Verbindung) für andere BLE-Geräte oder Broadcast von Daten
- Tracker: Verbindung mit Owner Device (initialisieren) und periodisches Advertisement
- Wenn exklusive Verbindung hergestellt: Funktionen und Werte mit GATT (Generic ATtribute Profile)

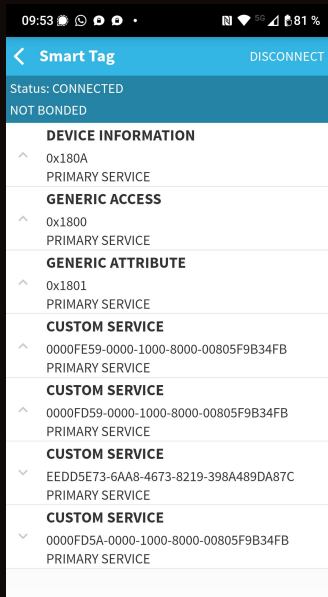
- Verbindungsbasierte Interaktionen zwischen BLE-Geräten
- Profile: Spezifikation zur Implementierung bestimmter Anwendungsfälle
- Service: Gruppierung von zusammengehörigen Funktionen (Characteristics) mit eigener UUID
- Characteristic: Einzelne Funktionen mit Werten zum Lesen/Schreiben
- Zum Selbstaushandeln auf dem Smartphone: GATT Browser

- Alle modernen Smartphones mit BLE-Funktionalität
- Verschiedene Services mit Characteristics relativ intuitiv bis simpel
- GATT-Browser auch auf deinem Smartphone
- Hier GATTBrowser von Renesas

GATT-BROWSER – BEISPIELE

GATTBrowser	SCAN	GATTBrowser	SCAN	GATTBrowser	SCAN
<No name> 09:DD:D8:62:79:46	📶 -91	CMF Watch Pro 2-6FDF 2C:BE:EB:E7:6F:DF	📶 -88	HUAWEI WATCH FIT-937 B8:8E:82:E9:C9:37	📶 -96
<No name> D7:1D:28:58:52:FB	📶 -88	<No name> F5:73:CA:8A:CB:99	📶 -94	<No name> 4A:B4:19:C0:F2:12	📶 -88
<No name> 53:1A:AF:50:6F:98	📶 -87	Apple Pencil 59:90:07:BF:9C:7F	📶 -83	<No name> 43:93:5D:45:A2:86	📶 -94
<No name> 4E:F2:AF:B8:52:F4	📶 -86	<No name> 42:31:6B:DF:77:7E	📶 -95	<No name> E3:C5:53:EC:55:1B	📶 -93
<No name> 43:59:9F:71:92:F2	📶 -91	<No name> 6D:85:63:BD:49:60	📶 -75	<No name> CF:03:00:1C:B0:8B	📶 -93
<No name> 7C:30:8D:23:2A:FB	📶 -83	<No name> 6E:BD:A5:1F:14:AD	📶 -96	<No name> 29:3C:68:D8:E8:CB	📶 -85
<No name> 6A:E9:E5:C0:D4:65	📶 -88	<No name> 66:0E:5B:FA:9F:36	📶 -85	Aranet4 28025 E7:AD:18:61:66:F2	📶 -97
<No name> 7A:55:F3:A5:8D:79	📶 -87	<No name> 62:0A:F5:AF:A2:EF	📶 -96	<No name> EF:B6:B1:86:7D:25	📶 -97
<No name> 71:73:61:75:CA:F9	📶 -79	<No name> 3E:24:A5:AE:94:55	📶 -93	<No name> 6D:EE:66:48:60:3A	📶 -85
<No name> 54:A7:84:87:F0:1A	📶 -89	<No name> D5:FF:A1:96:B3:4F	📶 -81	<No name> E8:1E:46:38:75:9C	📶 -89
	📶 -88	<No name>	📶	<No name>	📶

GATT – BEISPIEL SMARTTAG



TRACKER OHNE CROWD-SOURCING

- Idee: Permanente Verbindung zu Owner Device
- Keine Gegenstände vergessen, Alarm bei Verbindungsabbruch (konfigurierbar)
- Gegenstände finden mit Signalstärke des Trackers
- ... sehr kostengünstig bei Händler des Vertrauens 🐼

Preis

★★★★☆ 4,7 | 2.000+ verkauft
 € 17,47€ sparen
 Kostenloser Versand ab 10€

★★★★☆ 4.6 | 1.000+ verkauft
 € 9,6€ sparen
 Kombi-Knaller >

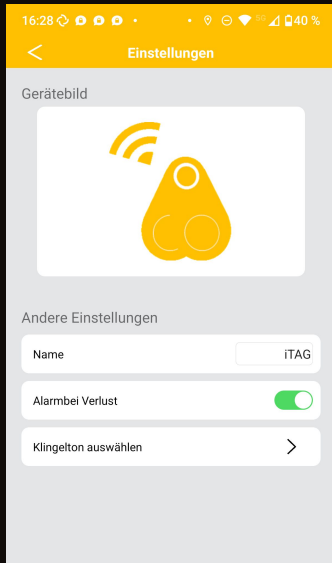
★★★★☆ 4.4 | 2.000+ verkauft
Kostenloser Versand ab 10€

★★★★☆ 3.3 | 60 verkauft
🔴 1,57€ sparen
Kostenloser Versand ab 10€

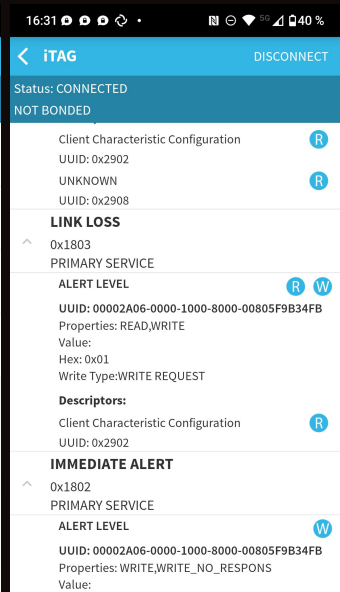
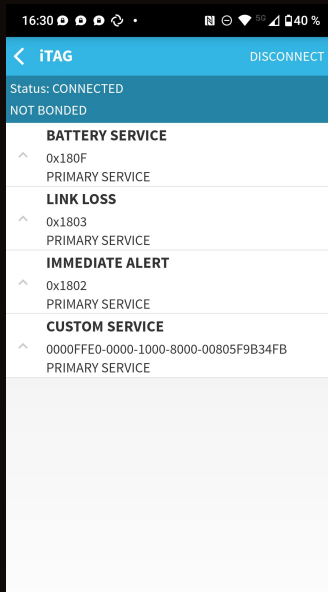
★★★★☆ 4.7 | 600+ verkauft
 🔥 9,68€ sparen
 🏆 Auf AliExpress meistverkauft

★★★★☆ 4.5 | 2.000+ verkauft
🔥 0,7€ sparen
🔥 Auf AliExpress meistverkauft

BEISPIEL: iSEARCHING/iTAG



17



63


```
for device in BLEScanner.discover():
    if "iTag" in device.name:
        client = BLEClient(device)
        for service in client.services:
            for char in service.characteristics:
                if "write" in char.properties:
                    client.write_gatt_char(char.handle,
                                           b"\0x00")
```

⇒ Diebstahl mit ausgeschalteten Alarm einfach, permanentes Klingeln auch einfach

Crowd-Sourcing-Networks

- Standort von Trackern nur auffindbar, wenn Owner Device in Nähe ist/Verbindung hat $\Rightarrow$ starke Limitierung
- Ziel: Standort von Trackern am besten überall und jederzeit
- GPS-Tracker als Alternative: Teurer (Anschaffung und Betrieb), geringere Akkulaufzeit, fehlende Alarmfunktion, keine Vereinheitlichung des Ökosystems
- Umsetzung: BLE nicht nur mit Owner Device – sondern mit umliegenden Geräten mit Standort
- BLE bereits implementiert, BLE Advertisements bereits vorhanden
- Permanentes hallo hier bin ich von Trackern als Basis für Identität, Weitergabe des Standorts durch umliegende am Netzwerk teilnehmenden Geräte für Standortspende

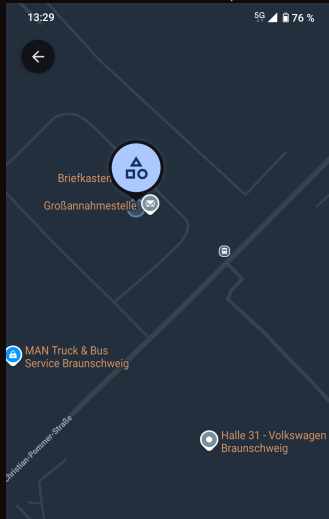
ANWENDUNGSFALL – KATZE



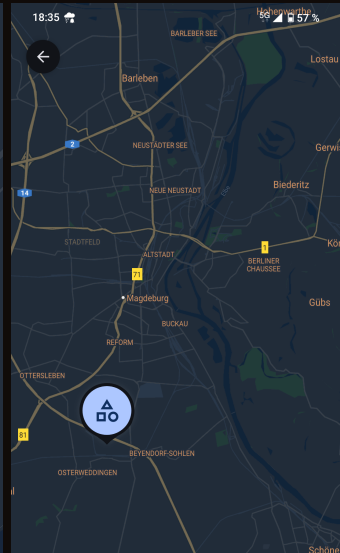
- Initiale Idee: Geldbeutel, Schlüssel, Rucksäcke (auch für lokale Verpeiltheit)
- Reisen: Koffer im Aufgabengepäck
- Reisen, aber für Gegenstände: Pakete
- Outdoor-Abenteuer von Katzen
- Sicherheitsfeature für Fahrräder
- dein Anwendungsfall, hier

ANWENDUNGSFALL – PAKET

Danke an @zeroday@podcasts.social/Stefan



22

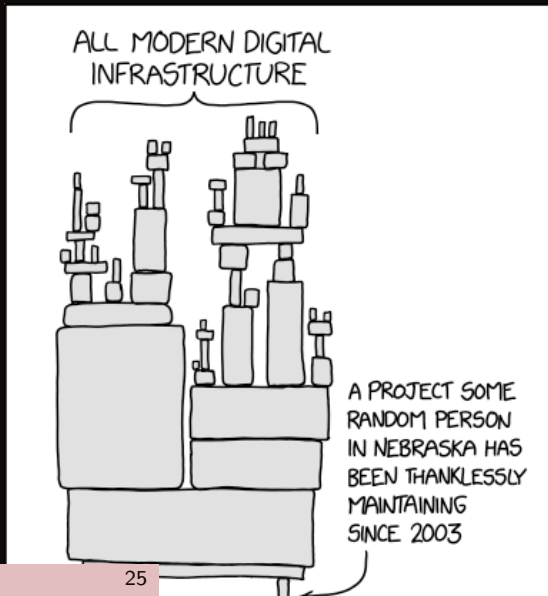


63

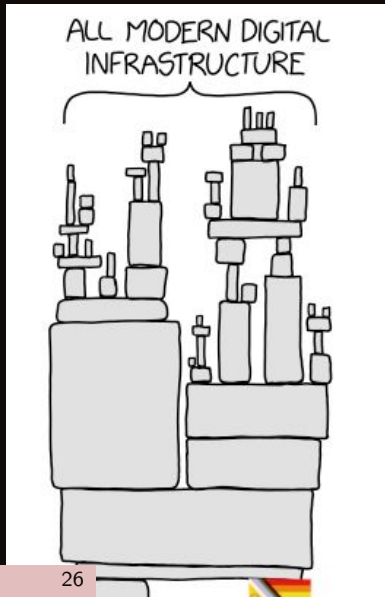
- Apple – Find My bzw. Wo ist? – AirTag, Apple-Geräte (MacBook, AirPods, iPhone, ...), kompatible Geräte
- Google – Find My Device bzw. Mein Gerät finden – Spezifikations-kompatible Tracker (Chipolo One, Point, Pebblebee Tag, ...), Android-Geräte, kompatible Geräte
- Tile – Tile Tracker, eigenes Ökosystem
- Samsung – SmartTag, in SmartThings integrierte Geräte, eigenes Ökosystem

- Kompatibel mit Samsung-Geräten, walled garden
- Eigene Tests: In Städten okayishe Abdeckung
- Ganzes Smart Home Ökosystem mit SmartThings
- Kompatibilität mit allen Android-Geräten über uTag
<https://github.com/KieronQuinn/uTag>
- uTag: Implementierung von SmartThings-Features, Installation modifizierter Version als Third Party App notwendig

XKCD: DEPENDENCY

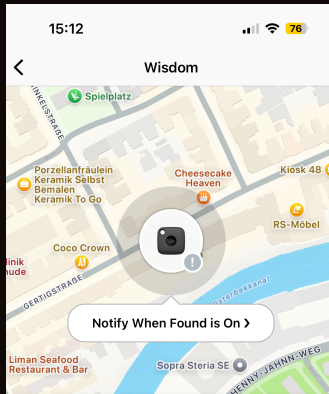


QUEER: DEPENDENCY



- Seit etwa 2014 bekannter, von Crowdfunding zu Life360
- Eigene Tests: Netzwerk-Abdeckung so na ja
- Statische MAC-Adresse (dauerhaft identifizierbar)
- Zwang zur Tile App
- Tile Premium: Standortverlauf der letzten 30 Tage, Benachrichtigung für vergessene Gegenstände und Garantie für Tracker während Abo
- Highlight bei gefundenen Tracker: Mail an Eigentümer:in

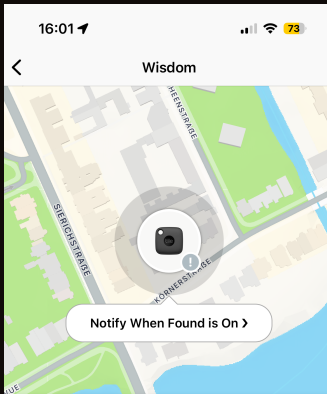
TILE: ABDECKUNG



The Tile Network is searching for your Tile's most recent location.

Most recent location (2 min ago):

28



The Tile Network is searching for your Tile's most recent location.

Most recent location (33 min ago):

Körnerstraße, Hamburg.



- Premiumfeatures bis auf Garantie technisch lösbar
- pytile: Einfacher Zugriff auf die Tile API mit Python-Bibliothek
<https://github.com/bachya/pytile>
- `tiles = await pytile_api.async_get_tiles()`, Werte wie `tile.latitude`, `tile.longitude`, `tile.altitude` und `tile.kind` für eigene Anwendungen analog zu premium

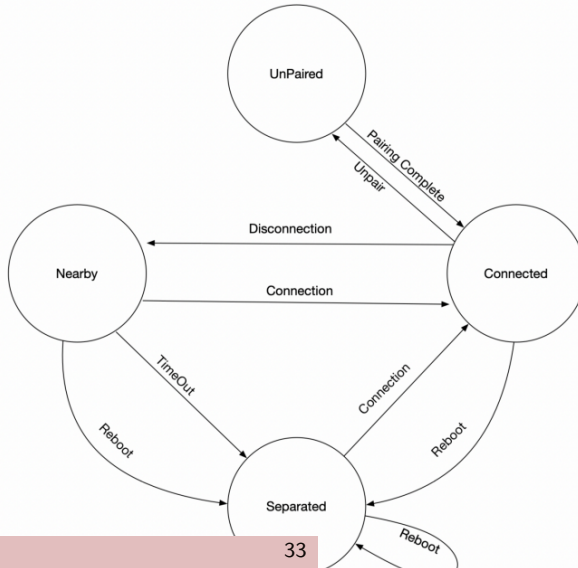
- Apple-Netzwerk für alle Apple-Geräte und deren Standort, Popularität besonders durch AirTags (2021)
- Standortdaten per Default über alle Apple-Geräte, zusammengefasst in einem iCloud-Account $\Rightarrow$ Gute Abdeckung
- Speicherung der verschlüsselten Standortdaten durch Apple
- Verschiedene Zustände: Unpaired, Connected, Nearby, Lost

FIND MY INITIALISIERUNG & FUNKTIONSWEISE

- Verbindungsaufbau zwischen AirTag und Apple-Gerät
- Generierung von Public und Private Key (Elliptic Curve Digital Signature Algorithm, Curve: P-224), 256 Bit Secret und Counter, Speicherung auf eigenen Geräten durch iCloud Keychain (Apples Secretmanager)
- Mit Secret und Key Derivation Function Erzeugung von zwei Zufallszahlen für temporären Public und Private Key
- Wenn anderes Gerät BLE Advertisement findet: Standortinformationen mit Public Key verschlüsselt und Hash des Public Keys für serverseitige Identifikation
- Berechnung von temporären Werten durch Owner, Entschlüsselung $\Rightarrow$ Standort des Gerätes

- Unpaired: Initialisierung möglich, noch kein Owner Device/iCloud Account zugeordnet
- Connected: Mit Owner Device verbunden, keine Broadcasts
- Nearby: Verbindung zu Owner Device verloren, Advertisements mit ersten Teil des Public Keys, somit keine Standortteilen durch umgebende Geräte möglich
- Separated: Verbindung zu Owner Device mindestens 15 Minuten verloren, volle Advertisements, je nach Key Änderung alle 15 Minuten/24 Stunden

AIRTAG – STATES



- OpenHaystack: Framework zur Integration von eigenen Trackern in Apples Netzwerk
- Voraussetzungen: System mit macOS (Custom Plugin für Apple Mail für Zugriff auf Apples API für Standorte)
- Keine Rotation des Public Keys, potentiell trackbar
- <https://github.com/seemoo-lab/openhaystack>

- Google-Netzwerk für alle Android-Geräte und deren Standort, Popularität besonders durch AirTags (2021) gefördert
- Google-Netzwerk seit 2024 vergleichbar mit Apple, inklusive Crowd-Sourcing-Ansatz
- Speicherung der verschlüsselten Standortdaten durch Google für eigenes Smartphone
- Crowd-Sourcing-Network nur, wenn PIN/Passwort für Find My Device eingerichtet
- Geräte bzw. BLE-Tracker mit Implementierung der Spezifikation
- Minimum: Android 9, davor nur Find My Device ohne Crowd-Sourcing

- Aus: Keine Teilnahme am Netzwerk, nur Speicherung der letzten Standorte eines Gerätes bei Google mit eigener Online-Funktion (z.B. Smartphone)
- Ohne Netzwerk: Integration von Offline-Zubehör mit Bluetooth-Kommunikation zu Smartphone (wie bestimmte Kopfhörer), BLE-Tracker ausgenommen
- Netzwerk an stark frequentierten Orten: Aggregation mehrerer Standorte von mehreren Geräten (default)
- Netzwerk überall: Permanente Verwendung von Standortinformationen

- Ähnlich zu Apple (prinzipiell)
- Asymmetrisches Schlüsselpaar aus Public und Private Key: Ephemeral Identity Key (EIK)
- Wieder temporärer Key für Advertisements, Rotation alle 24 Stunden
- <https://developers.google.com/nearby/fast-pair/specifications/extensions/fmdn>

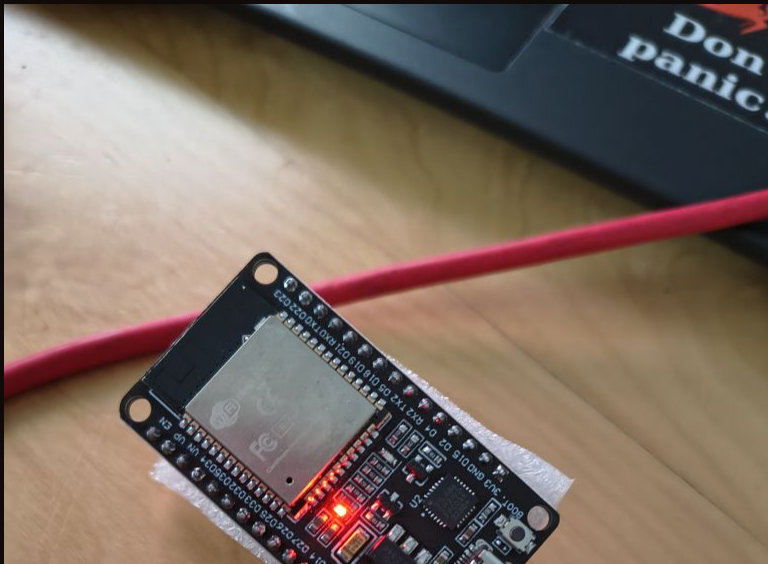
- Keine Tracker von Google direkt (wie AirTags von Apple)
- Drittanbieter zur Implementierung der Spezifikation
- Beispiele: Pebblebee Tag, Chipolo One Card, Motorola Moto Tag, MiLi MiTag, ...
- Hier getestet: Pebblebee Tag, MiLi MiTag, DIY
- DIY-Tracker möglich

DIY – CLONES



- <https://github.com/leonboe1/GoogleFindMyTools>
- Spezifikation verfügbar, ESP32 oder Zephyr als Basis
- Gerät mit Standort nicht in App auf Android-Gerät, aber über Python-Skript
- Achtung: Keine Key Rotation, Identifizierung möglich
- GoogleFindMyTools mit etwas mehr Output

CUSTOM GOOGLE TRACKER



OUTPUT: EIGENES SMARTPHONE

Loading...

[UploadPrecomputedPublicKeyIds] Updating your
registered µC devices...

Welcome to GoogleFindMyTools!

The following trackers are available:

1. Motorola ...: 67536acf-...
- 2.
3. GoogleFindMyTools µC: 6827f3b5-...
4. Mi-au-Tag : 68337862-...

If you want to see locations of a tracker,
type the number of the tracker and press 'Enter'.

If you want to register a new ESP32- or Zephyr-based tracker,

OUTPUT: EIGENES SMARTPHONE

```
[LocationRequest] Requesting location data for Motorola...  
[FCMReceiver] Listening for notifications.  
    This can take a few seconds...  
[LocationRequest] Location request successful.  
    Decrypting locations...  
-----  
[DecryptLocations] Decrypted Locations:  
Latitude: 50.8965067  
Longitude: 4.7107066  
Altitude: 65  
Google Maps Link: https://www.google.com/maps/search/  
?api=1&query=50.8965067,4.7107066  
Time: 2025-06-18 16:52:56  
Status: 1  
Is Own Report: True
```

OUTPUT: MiLi TAG I

```
[LocationRequest] Requesting location data for Mi-au-Tag ...
```

```
[FCMReceiver] Listening for notifications.
```

```
    This can take a few seconds...
```

```
[LocationRequest] Location request successful.
```

```
    Decrypting locations...
```

```
-----  
[DecryptLocations] Decrypted Locations:
```

```
Latitude: 50.6969696
```

```
Longitude: 6.0500546
```

```
Altitude: 294
```

```
Google Maps Link: https://www.google.com/maps/search/  
?api=1&query=50.6969696,6.0500546
```

```
Time: 2025-06-18 17:38:44
```

OUTPUT: MiLi TAG II

Status: 3

Is Own Report: False

Latitude: 50.7087247

Longitude: 6.0434704

Altitude: 293

Google Maps Link: <https://www.google.com/maps/search/?api=1&query=50.7087247,6.0434704>

Time: 2025-06-18 17:39:42

Status: 3

Is Own Report: False

Latitude: 50.7167587

Longitude: 6.0409694

OUTPUT: MiLi TAG III

Altitude: 286

Google Maps Link: <https://www.google.com/maps/search/?api=1&query=50.7167587,6.0409694>

Time: 2025-06-18 17:39:51

Status: 3

Is Own Report: False

Latitude: 50.7452045

Longitude: 6.0717603

Altitude: 0

Google Maps Link: <https://www.google.com/maps/search/?api=1&query=50.7452045,6.0717603>

Time: 2025-06-18 17:41:35

Status: 3

OUTPUT: MiLi TAG IV

Is Own Report: False

Latitude: 50.63407

Longitude: 5.8029966

Altitude: 156

Google Maps Link: <https://www.google.com/maps/search/?api=1&query=50.63407,5.8029966>

Time: 2025-06-18 17:31:04

Status: 1

Is Own Report: True

- Tracker existieren
- Abdeckung je nach Netzwerk und Anwendungsfall okayish bis gut
- Daten liegen (verschlüsselt) bei Apple/Google/\$ Anbieter
- ... case closed?
- Menschen sind mies

Stalking und Digitale Gewalt mit BLE-Trackern

- Tracker mit Netzwerk zum Teilen des Standorts $\Rightarrow$ Missbrauchspotential
- Durch Anbietende der Netzwerke in Nutzungsbedingungen ausgeschlossen
- Verschiedene Ansätze zur Prävention und Detektion (inzwischen) verfügbar

- Eigene Tracker: Soweit möglich nicht als eigene Tracker deklariert
- Pebblebee-Tracker von @zeroday@podcasts.social/Stefan: Explizit an seinen Account gekoppelt
- Generelle Scans der Umgebung durch aktive Schutzmechanismen
- Noch offen: "Hey Lea, du darfst mir gerne jederzeit einen Tracker unterschieben!"

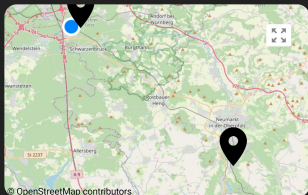
- Tracker-Detektion durch Apple und Google auf Smartphones
- Unknown Tracker Alerts
- Limitiert auf Googles/Apples Netzwerk
- Im Praxistest eher untauglich
- Lowlight: 1 Woche bis zur Erkennung der Pebblebee-Tracker

- Smartphone-App für iOS und Android zur Detektion von Trackern
- <https://github.com/seemoo-lab/AirGuard>
- Verschiedene Sensitivitäten, falsche Alarme und Klassifizierung möglich
- Praxistest ziemlich zufriedenstellend, insbesondere im Vergleich zur OS-Detektion
- Mittel der Wahl zur Detektion

AIRGUARD – BEISPIELE

17:26 60 %

← Gerät mit ID: F7:0F:6C:C9:EC:47



Feedback

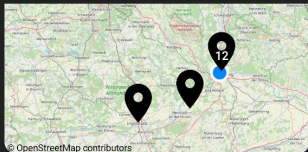
Apple Find My 2315 Anzahl gesehen
Entdeckt: 25.04.25, 16:55
Zuletzt gesehen 25.04.25, 17:26 **2**

Gerät orten

Tracker beobachten

Fehlalarm

← Gerät mit ID: CB:C2:14:08:87:5E



Feedback

Tile 1496 Anzahl gesehen
Entdeckt: 09.04.25, 09:57
Zuletzt gesehen 15.04.25, 15:44 **232**

Gerät orten

Tracker beobachten

Gerät ignorieren

Fehlalarm

13:49 63 %

← Tracker erkannt

Tracker erkannt, Alle Geräte

Tile 1496 Anzahl gesehen
Entdeckt: 09.04.25, 09:57
Zuletzt gesehen 27.05.25, 13:45 **1337**

Google Mein Gerät finden 3084 Anzahl gesehen
Entdeckt: 24.05.25, 23:52
Zuletzt gesehen 25.05.25, 22:48 **19**

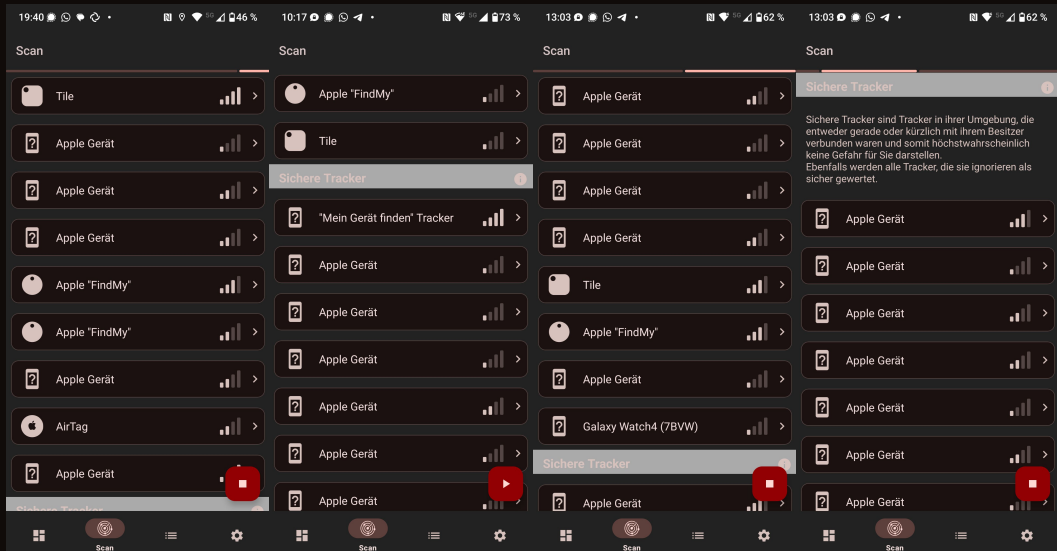
Google Mein Gerät finden 3094 Anzahl gesehen
Entdeckt: 25.05.25, 09:44
Zuletzt gesehen 25.05.25, 21:48 **10**

Google Mein Gerät finden 3055 Anzahl gesehen
Entdeckt: 23.05.25, 22:52
Zuletzt gesehen 24.05.25, 19:07 **18**

Google Mein Gerät finden 3054 Anzahl gesehen
Entdeckt: 23.05.25, 22:52
Zuletzt gesehen 24.05.25, 19:07 **13**

Google Mein Gerät finden 3019 Anzahl gesehen
Entdeckt: 22.05.25, 22:36
Zuletzt gesehen 18.06 **19**

AIRGUARD – SCANS



- Manueller Scan: Scan nach BLE-Trackern in direkter Umgebung
- Identifizierte Tracker: Hilfe beim Auffinden durch Sound und Distanzberechnung
- Hintergrundscan: Regelmäßiger Scan nach Trackern und Erkennung von persistierenden/mitreisenden Trackern
- Alarm im Default: Mindestens 30 Minuten Zeitintervall, 400 Meter Radius, 3 Mal Tracker erkannt
- Klassifizierung von Fehlalarmen möglich
- Historie für erkannte Tracker

- Detecting Unwanted Location Trackers – Standard für Crowd-Sourcing Netzwerke
- "The goal of the DULT WG is to standardize an application protocol for information exchange between location-tracking accessories and nearby devices, along with actions that these accessories and devices should take once unwanted tracking is detected. This protocol is intended to protect people against being unknowingly tracked."
<https://datatracker.ietf.org/group/dult/about/>
- Juli 2025 mit entsprechender Spezifikation als Milestone
- Unter anderem: Verschiedene States, Standard zu BLE-Advertisements, potentielle Owner-Identifikation

TRACKER ERKANNT! WAS TUN?

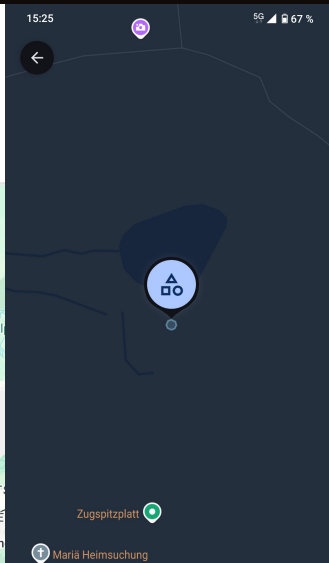
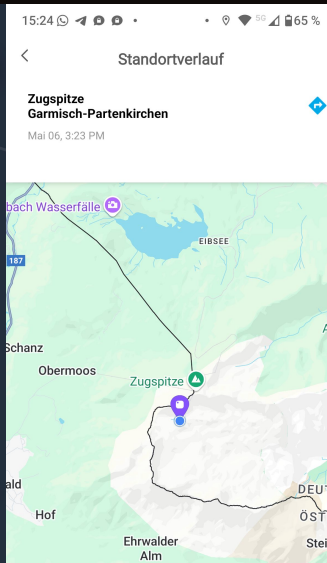
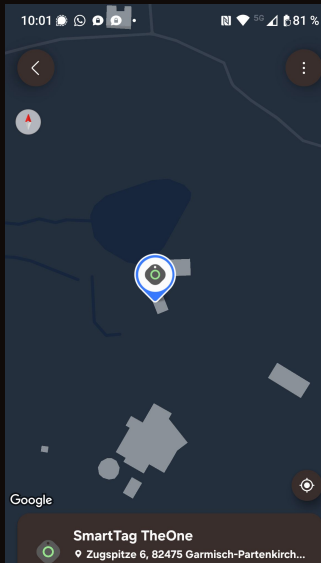
- Identifizierung, ggf. auch mit Hilfsmitteln wie AirGuard
- Screenshots, Nachweise, alles, was geht
- Sicherstellen des Trackers, wenn möglich
- Aufbewahrung an sicherem Ort (nicht eigener Aufenthaltsort)
- Ggf. juristische/strafrechtliche Schritte, Kontaktieren von Hilfestellen, ...

- Hilfetelefon – Gewalt gegen Frauen (auch Chat möglich) 116 016
- Regionale Beratungsangebote
- Generell: BLE-Tracker nur ein winziger Aspekt der Thematik
- Tieferer Einblick: Digitale Gewalt gegen Frauen – Anne Roth (Talk gestern)

- Möglichkeiten zur Detektion existent
- Präsenz der Thematik eher dürftig (insbesondere Betroffene)
- Wie immer in der IT Security: Sensibilisierung, Sensibilisierung, Sensibilisierung

- Wir als Community mit technischen Verständnis
- Betroffene ggf. nicht so tief drin
- Nach außen gehen und helfen, sensibilisieren!

AUSBLICK: KORREKTER STANDORT?



Fazit

- Ein weiteres Spielzeug im Werkzeugkasten mit legitimen Anwendungsfällen
- Daten (aktuell?) bei Apple und Google für gute Netzwerkabdeckung, wenn auch verschlüsselt
- Tools zum Hacken und DIY da
- Problemfeld Stalking und digitale Gewalt leider relevant

- Danke für eure Aufmerksamkeit, passt auf euch auf, viel Spaß am Gerät
- blue1337blood@nerdculture.de
- Danke an @zeroday@podcasts.social für Tracker
- Danke en Élia @kopfkrieg@chaos.social für Katzenbilder :3 (morgen, 12:30, hier)

