AirGuard - Protecting Android Users From Stalking Attacks By Apple Find My Devices

Alexander Heinrich

TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE MOBILE NETWORKING

Basics of Offline Finding

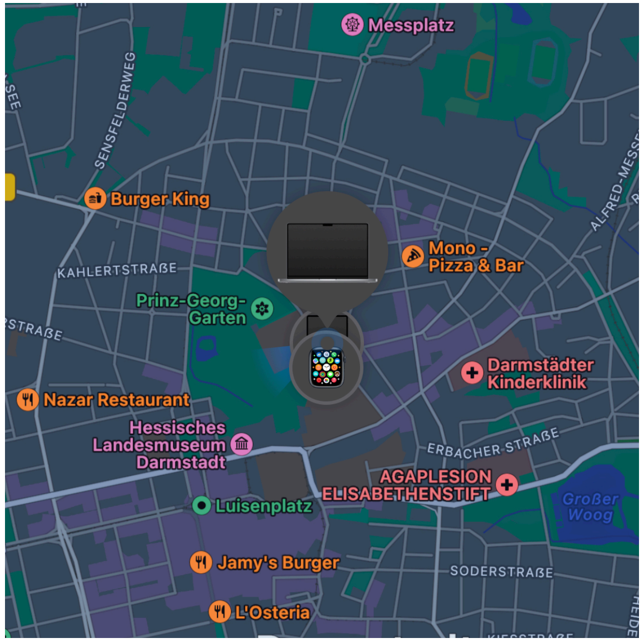
Oh no I lost my MacBook, but where?

At the café?

In the train?

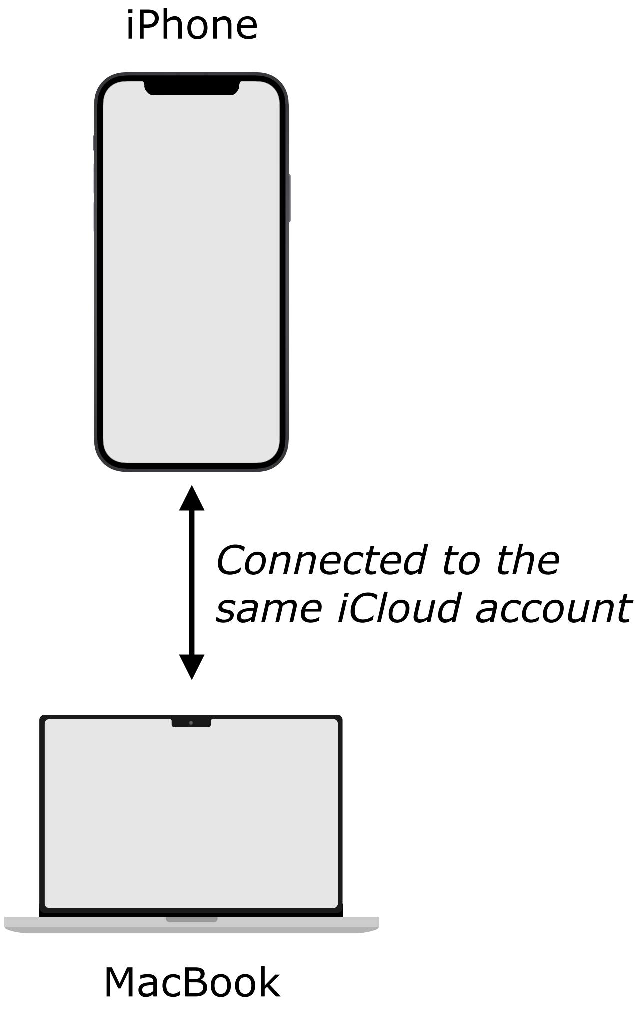
In the gym?

In the office!



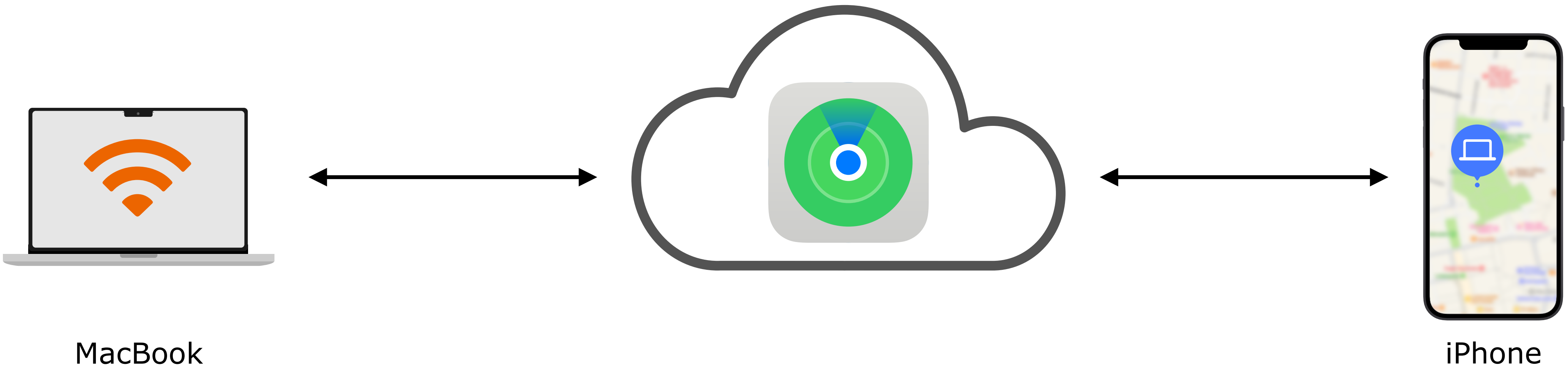
Find My

SECURE MOBILE NETWORKING



Connected to the same iCloud account

Find My

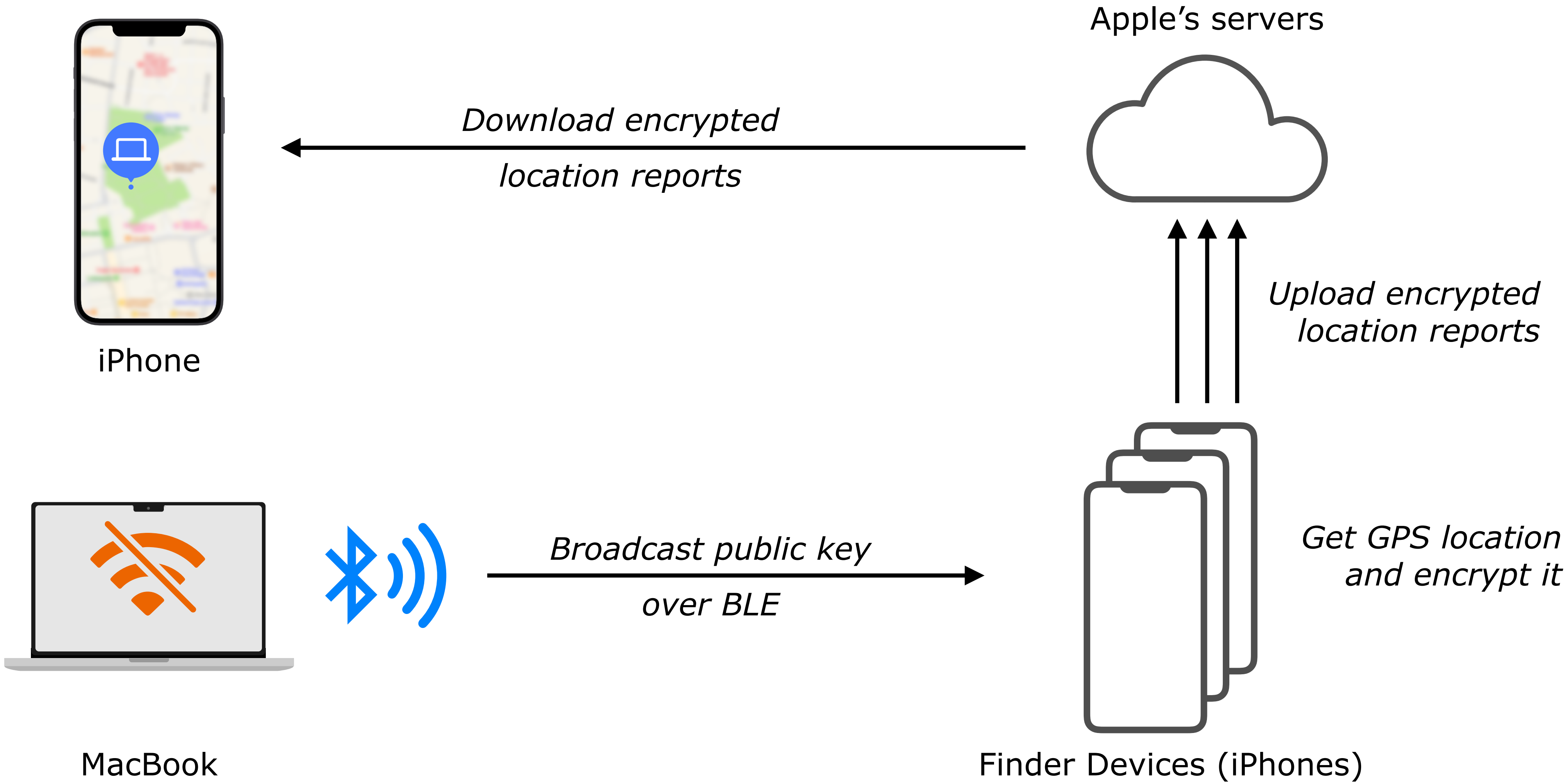


Find My

MacBook

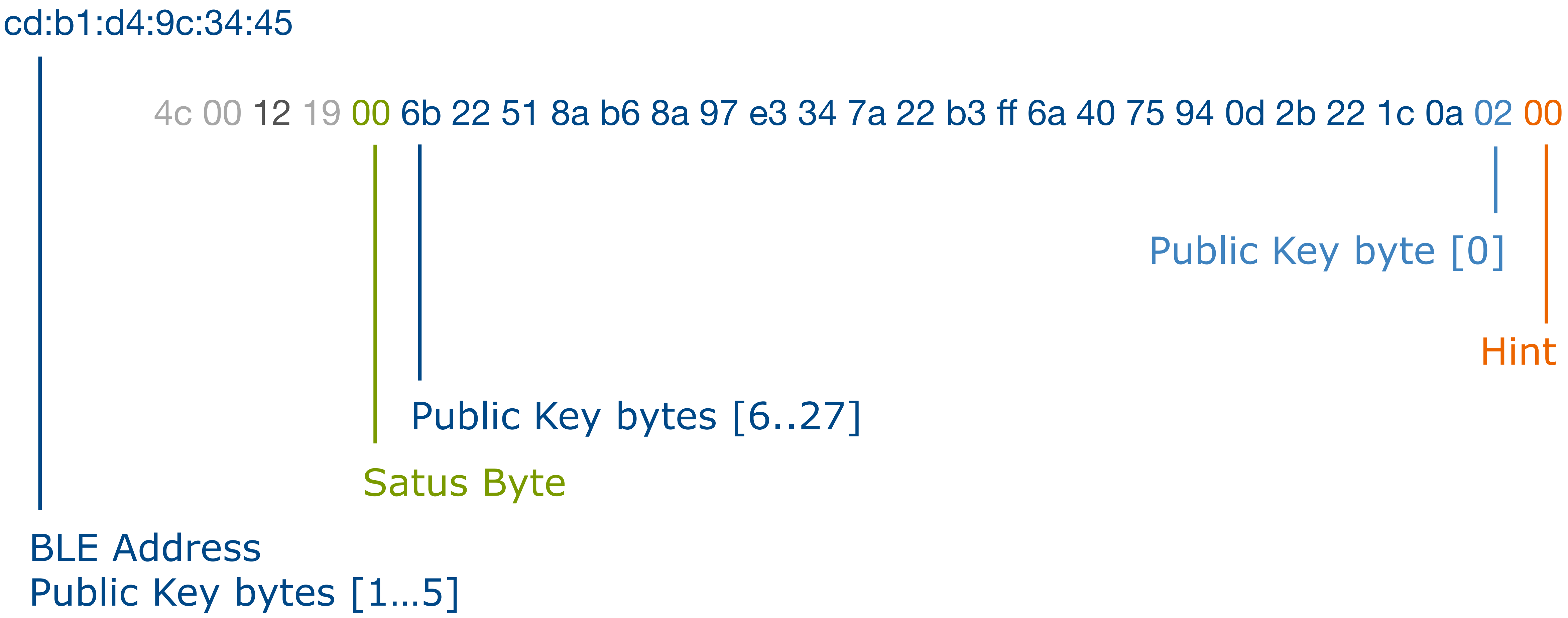
iPhone

Find My Network



Apple’s servers
Download encrypted location reports
iPhone
Upload encrypted location reports
Get GPS location and encrypt it
Broadcast public key over BLE
MacBook
Finder Devices (iPhones)

Bluetooth Low Energy Communication



cd:b1:d4:9c:34:45

4c 00 12 19 00 6b 22 51 8a b6 8a 97 e3 34 7a 22 b3 ff 6a 40 75 94 0d 2b 22 1c 0a 02 00

Public Key byte [0]

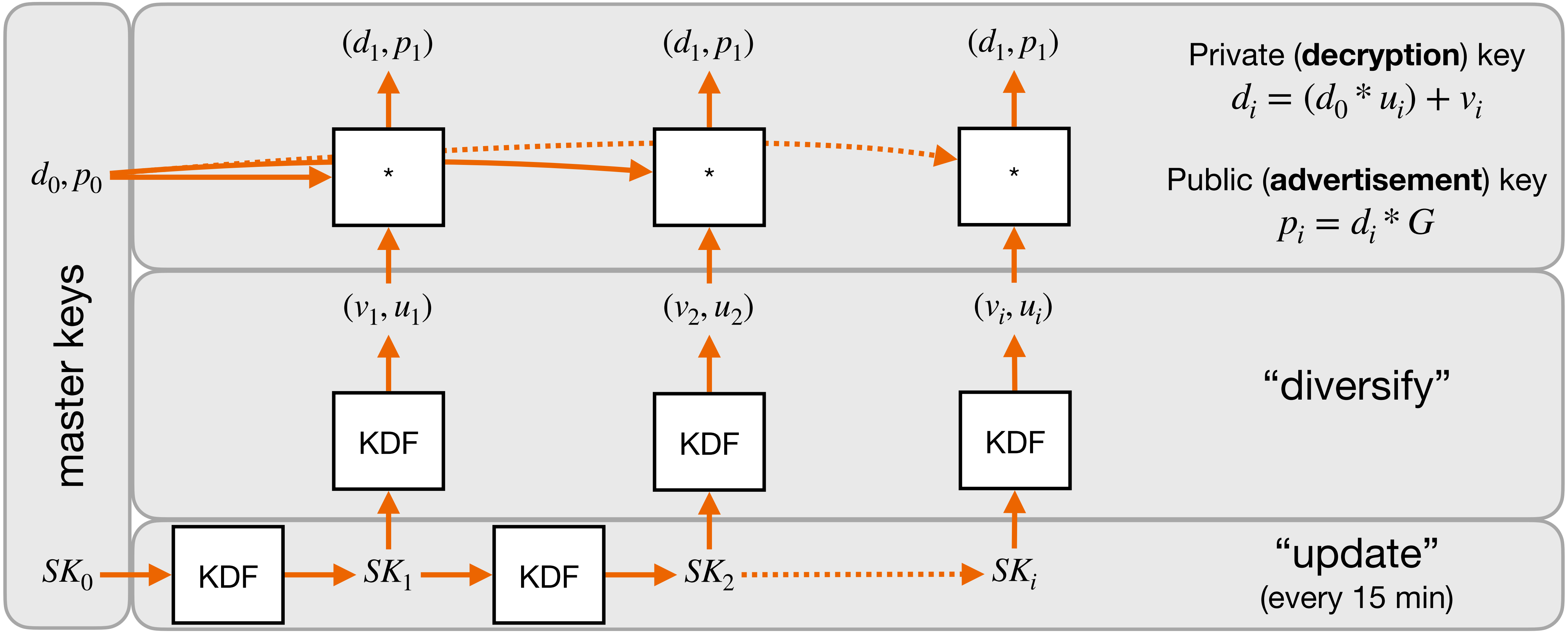
Hint

Public Key bytes [6..27]

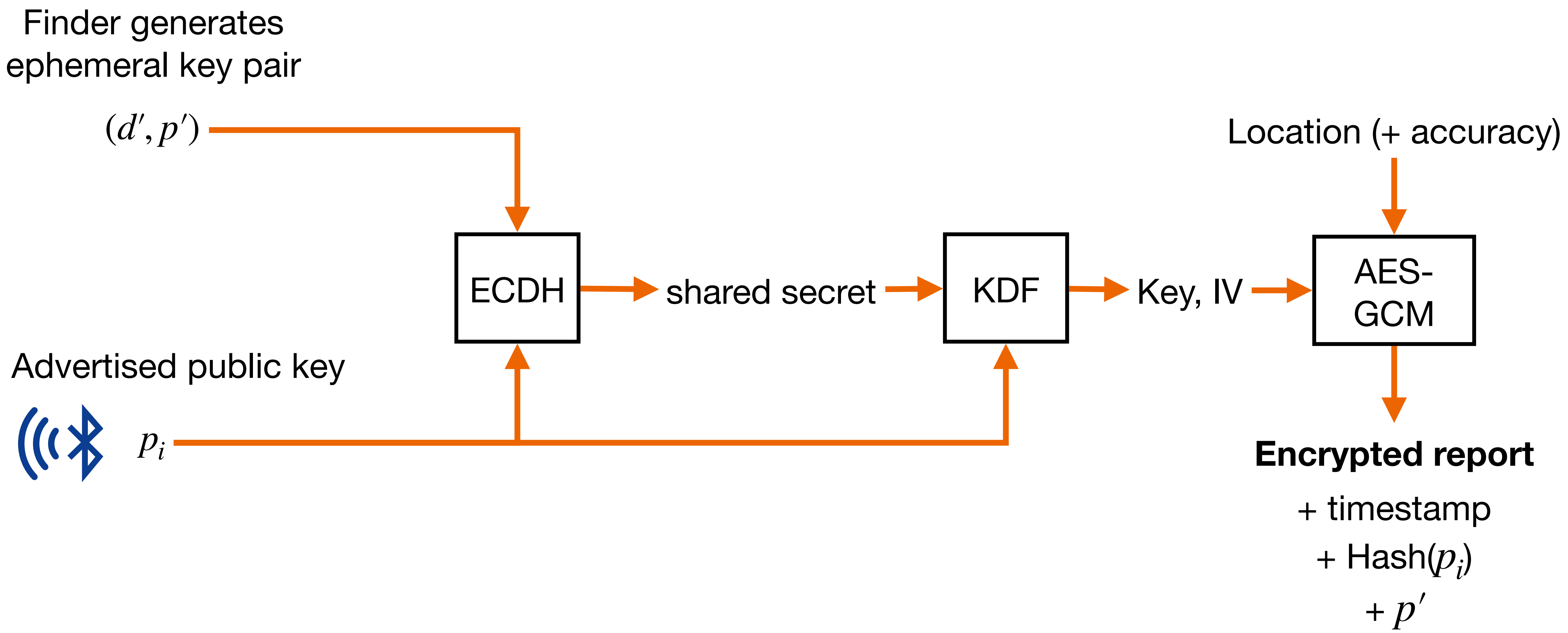
Satus Byte

BLE Address
Public Key bytes [1...5]

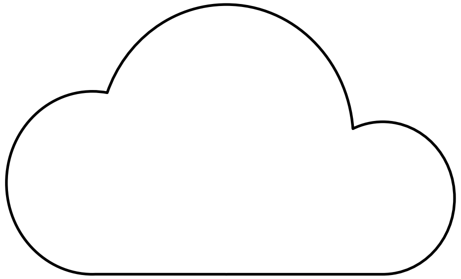
Key generation



End-to-End-Encrypted Location Reports



Apple’s Cloud database

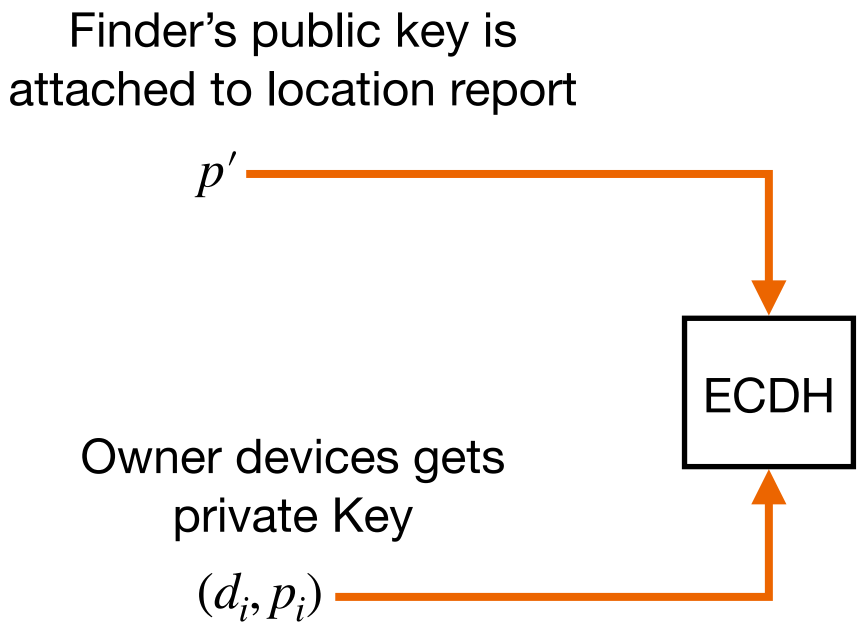


Apple’s Cloud database

Public Key ID	Date Published	Location report
G1rfbUicM6QSH…	2022-06-29 09:30	XXXXXXXXXXXXXXXXXXX<Finder public key>
G1rfbUicM6QSH…	2022-06-29 09:32	XXXXXXXXXXXXXXXXXXX<Finder public key>
d8tzwKrhT+V6w…	2022-06-29 09:35	XXXXXXXXXXXXXXXXXXX<Finder public key>
d8tzwKrhT+V6w…	2022-06-29 09:38	XXXXXXXXXXXXXXXXXXX<Finder public key>

Security of Find My

Encrypted Location reports



Finder’s public key is attached to location report

p'

ECDH

Owner devices gets private Key

(d_i, p_i)

- Private key d_i needed
- Depending on NIST-P224 Curve security
- No security issues detected

Secure Key Storage

SECURE MOBILE NETWORKING

Encryption Keys

✓

Stored in Keychain

Synced over
E2E encrypted
iCloud Keychain

Master Beacon Keys

✓

Keys only stored encrypted

Decryption keys stored
in Keychain

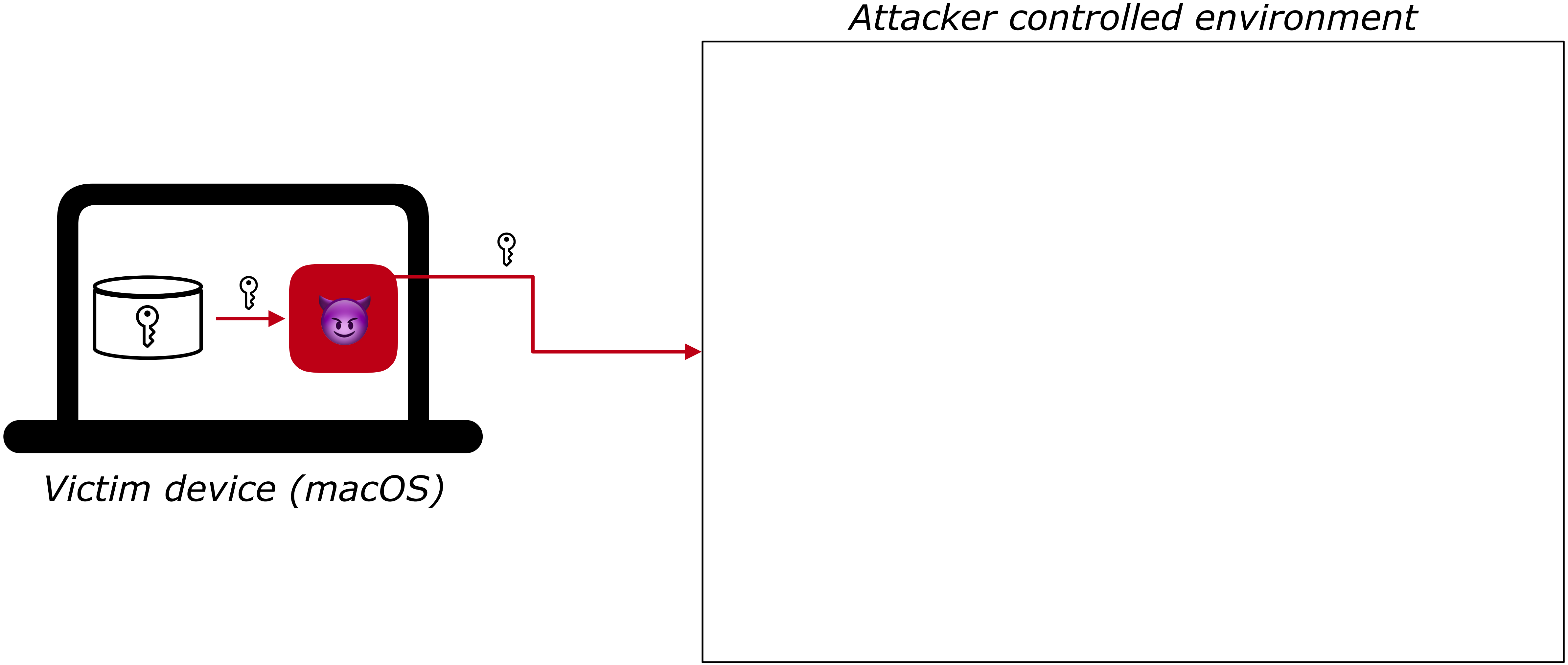
Precomputed keys

✗

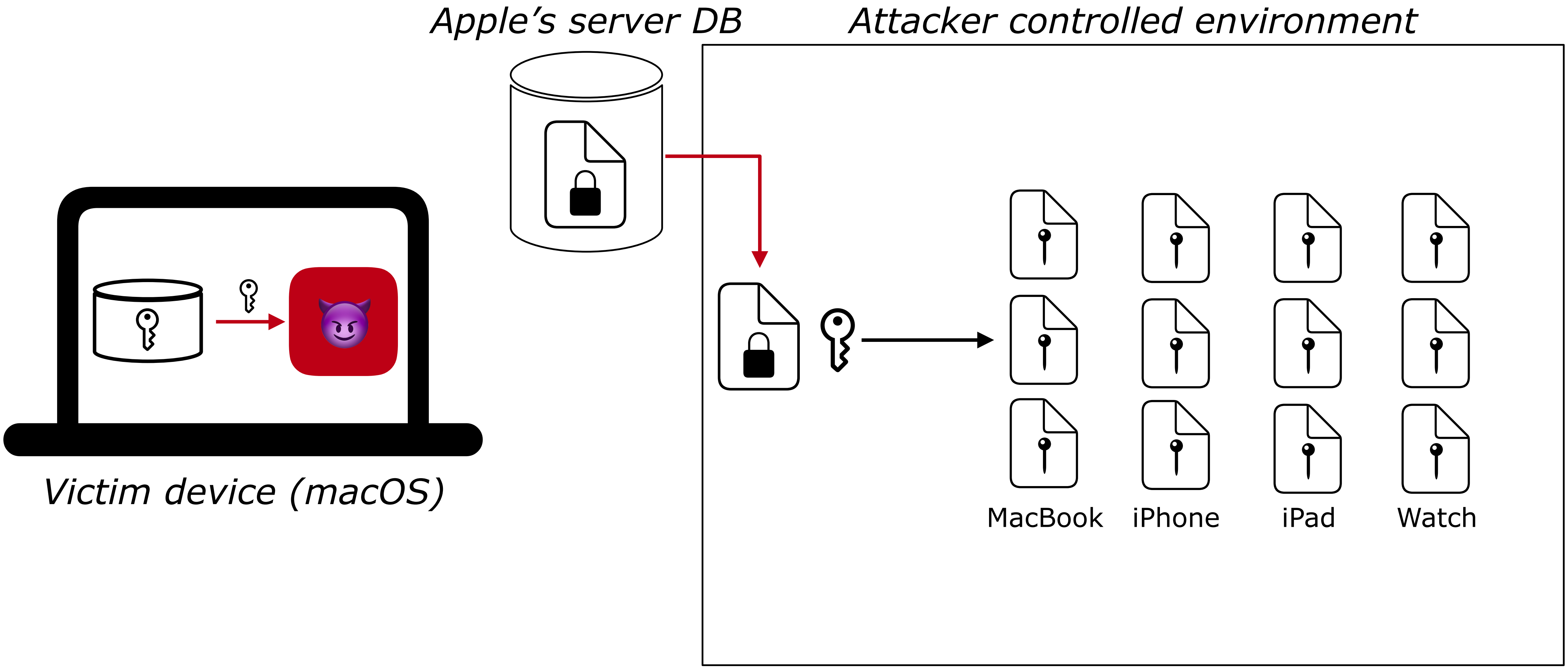
Cache file for pre-calculated
key pairs

No access protection /
encryption

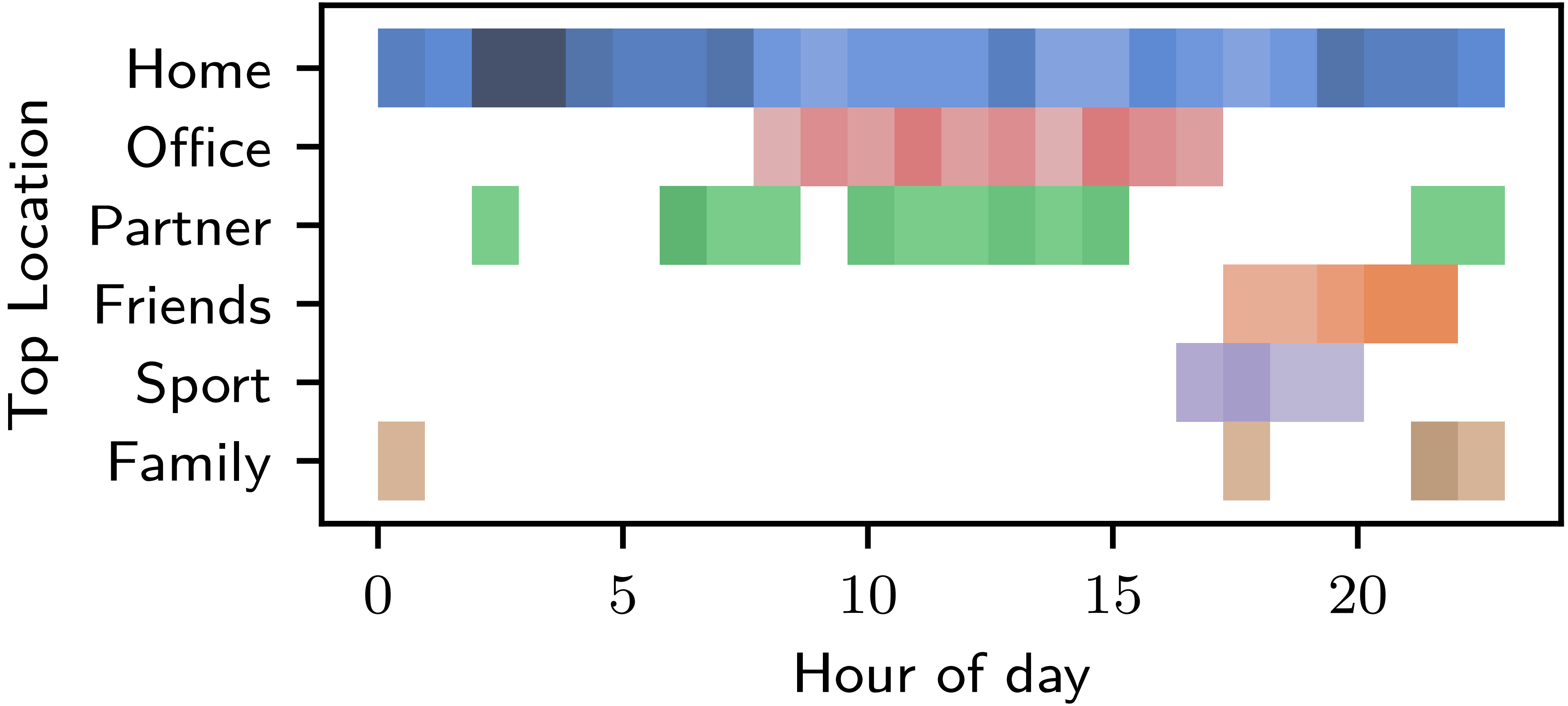
Unauthorized locaiton access



Unauthorized locaiton access



Identifying the victim



Is it fixed?

Precomputed keys

✓

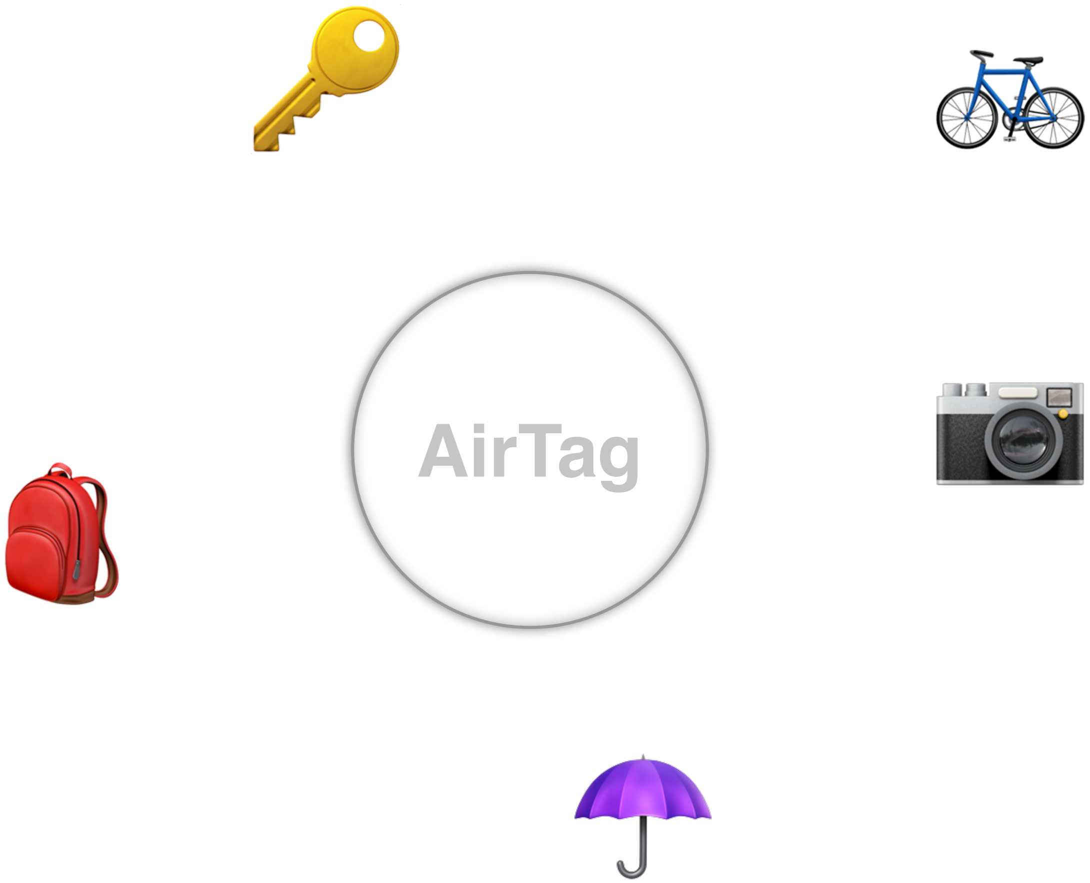
macOS 10.15.7 (2020)
macOS 11.0 (2020)

Cache file for pre-calculated key pairs

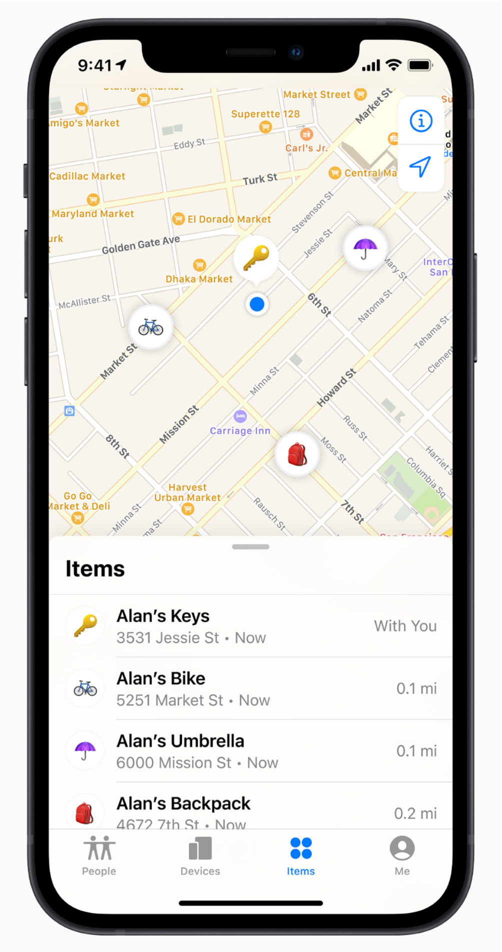
Access protected through an entitlement

AirTags and Find My

AirTags



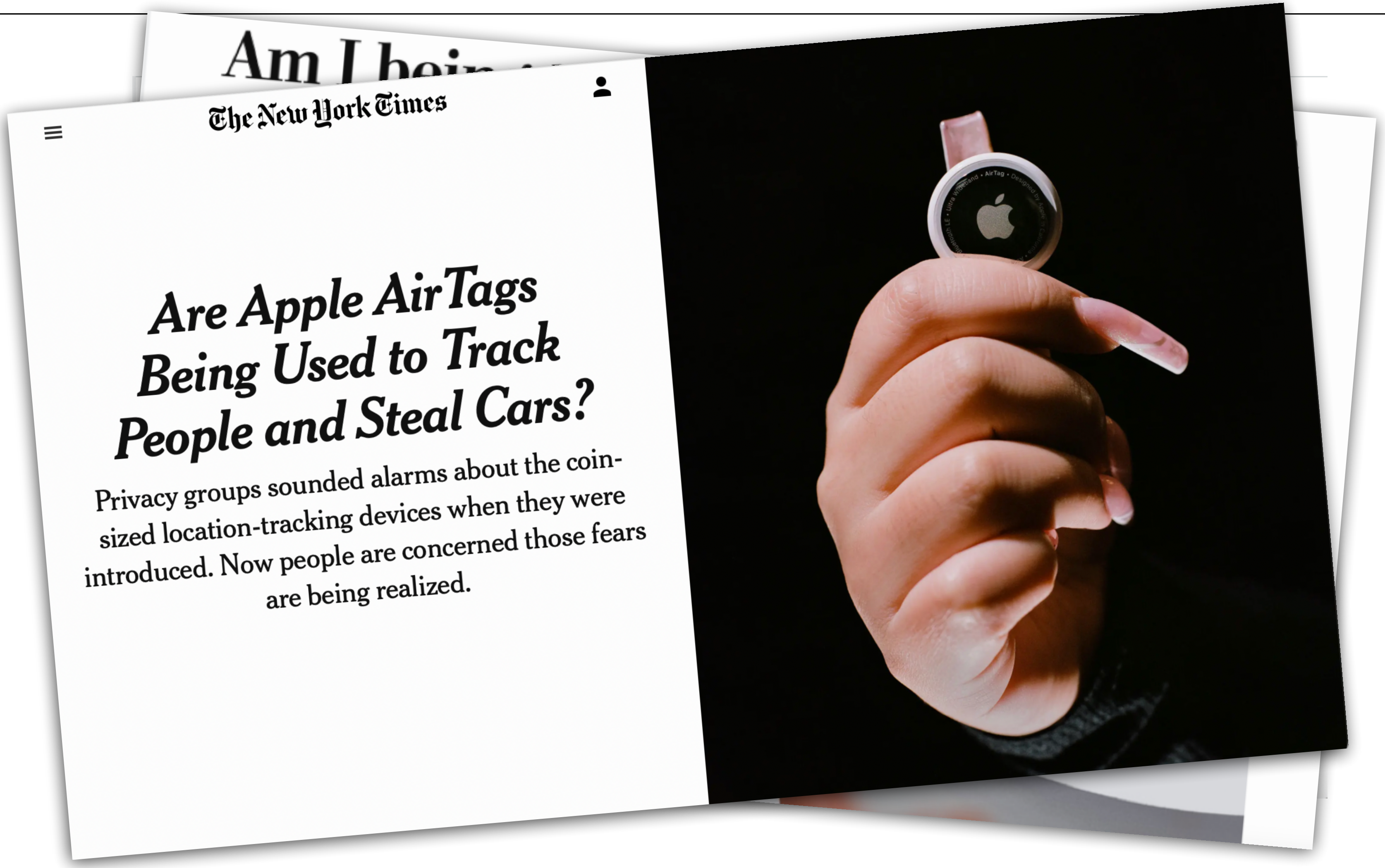
AirTags



Items

- Alan's Keys — 3531 Jessie St • Now — With You
- Alan's Bike — 5251 Market St • Now — 0.1 mi
- Alan's Umbrella — 6000 Mission St • Now — 0.1 mi
- Alan's Backpack — 4672 7th St • Now — 0.2 mi

What should go wrong?



Am I bein

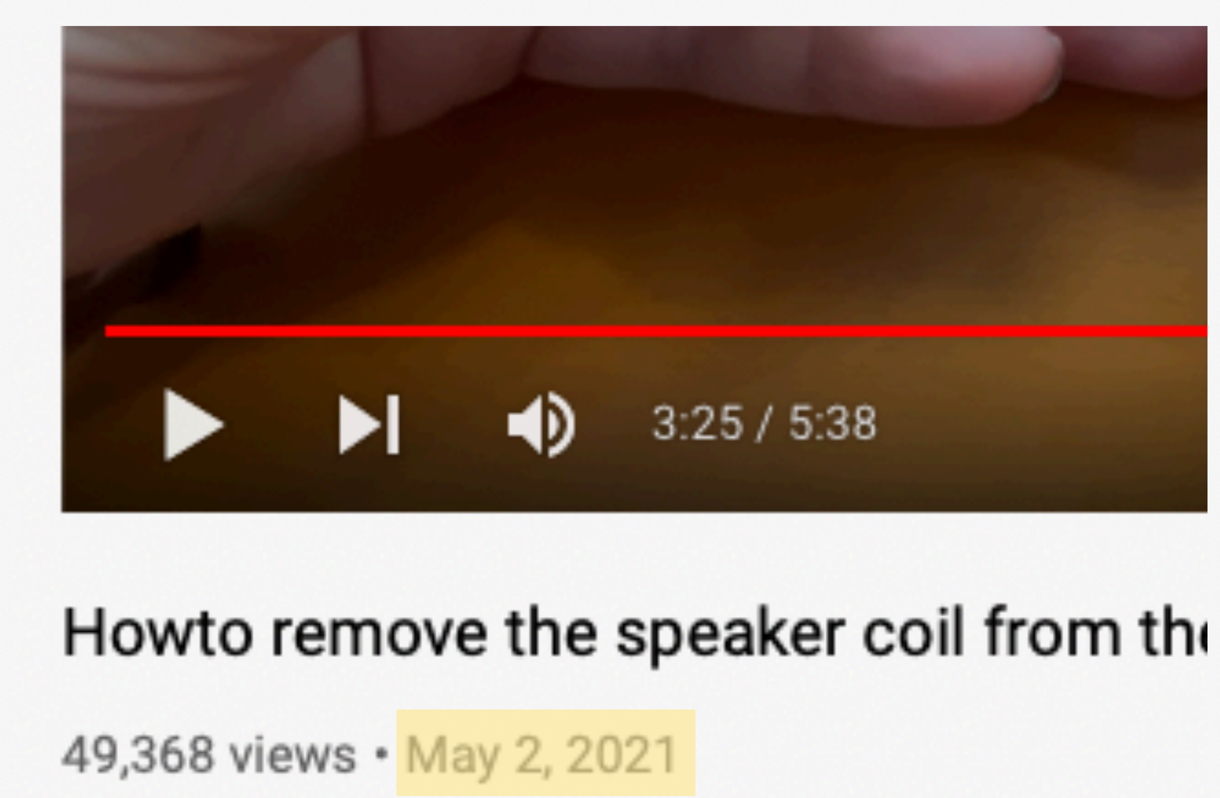
The New York Times

Are Apple AirTags Being Used to Track People and Steal Cars?

Privacy groups sounded alarms about the coin-sized location-tracking devices when they were introduced. Now people are concerned those fears are being realized.

Protection mechanisms

Protection mechanisms



Howto remove the speaker coil from th

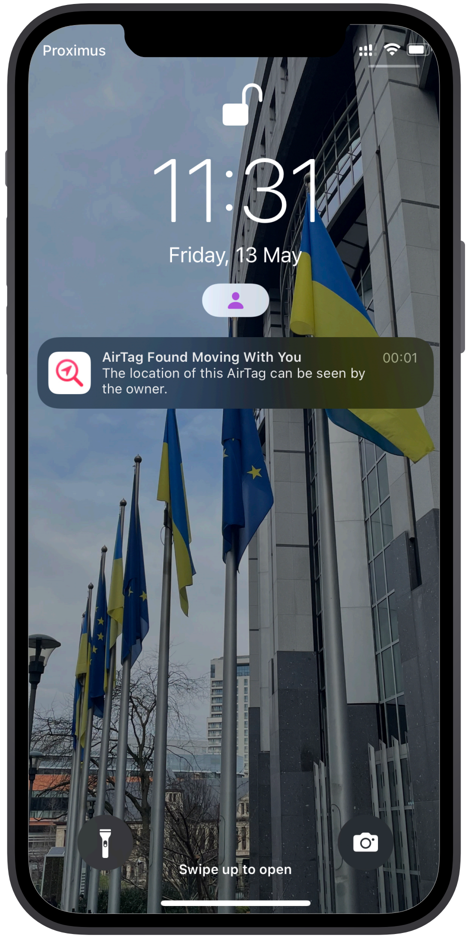
49,368 views • May 2, 2021

AirTag Release

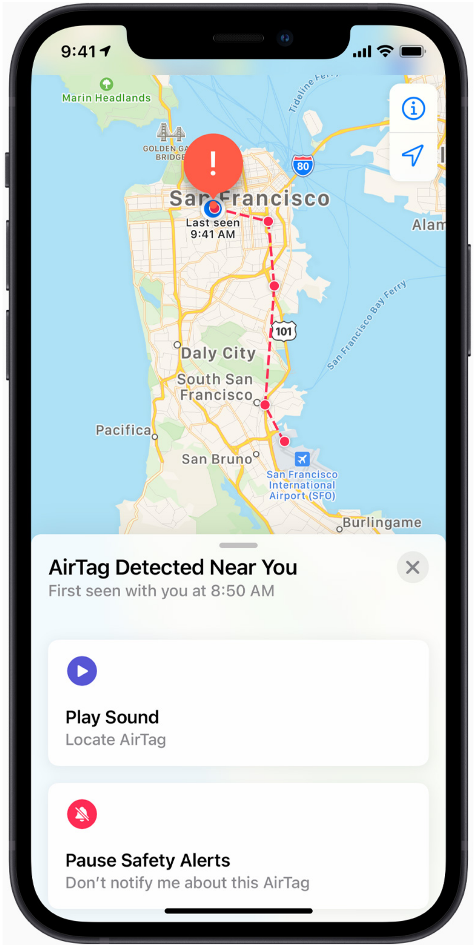
April 30, 2021

iOS Tracking Detection

Protection mechanisms for iOS



AirTag Found Moving With You 00:01
The location of this AirTag can be seen by the owner.

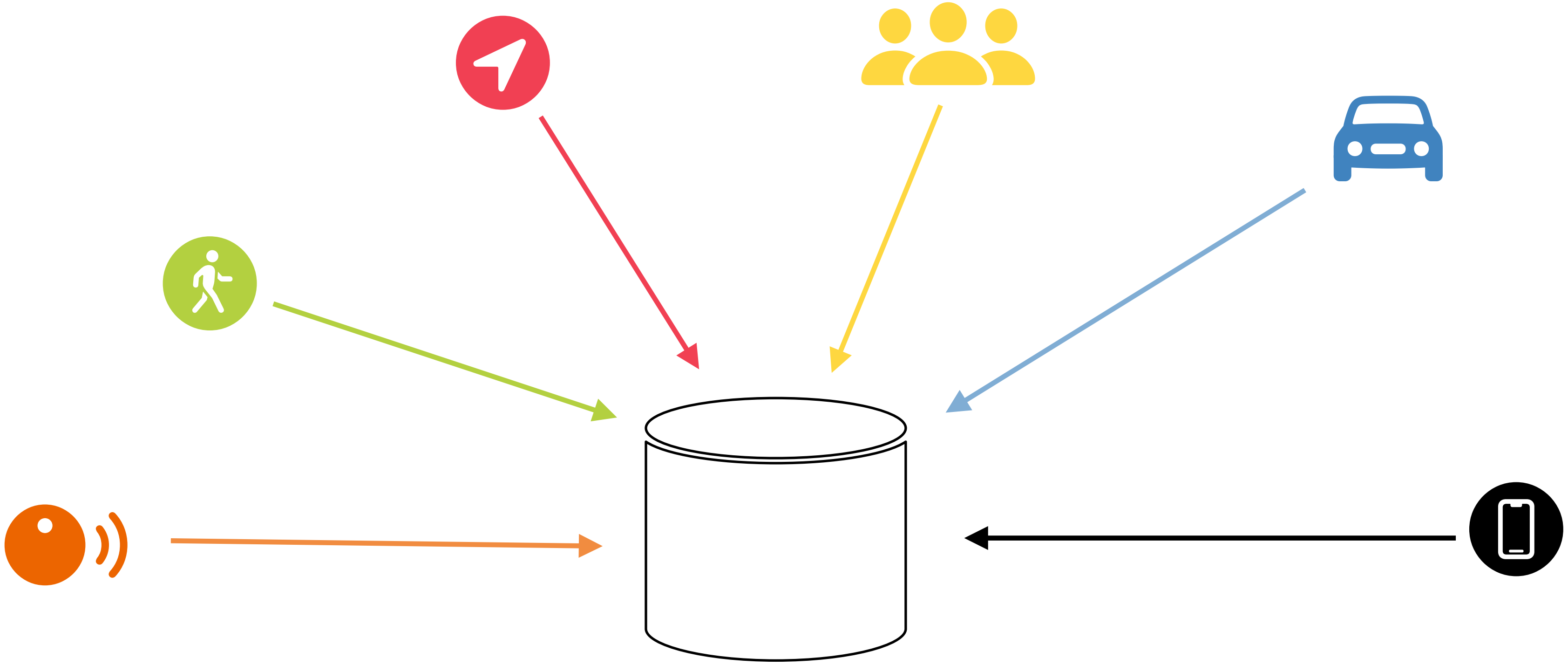


AirTag Detected Near You
First seen with you at 8:50 AM

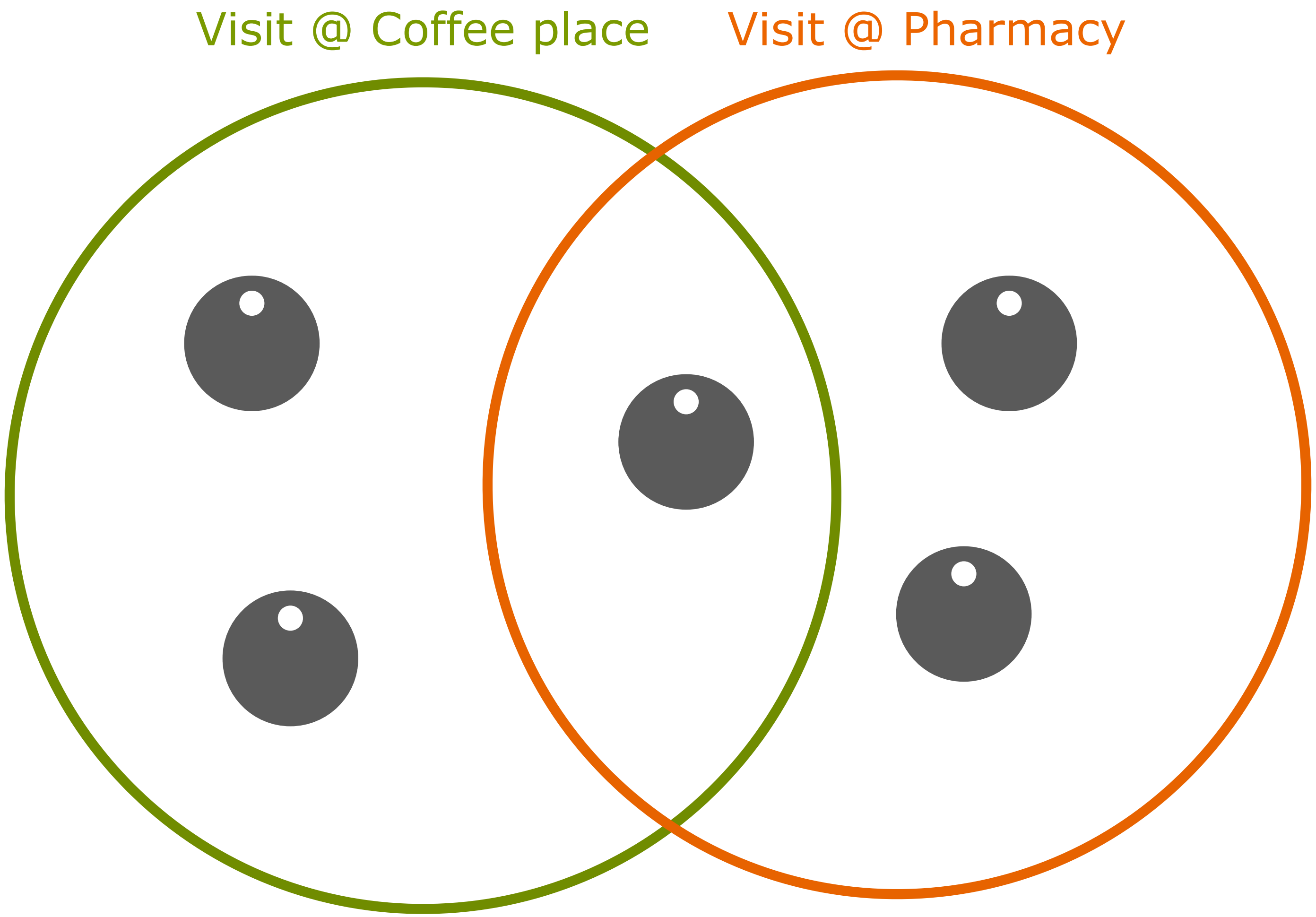
Play Sound
Locate AirTag

Pause Safety Alerts
Don't notify me about this AirTag

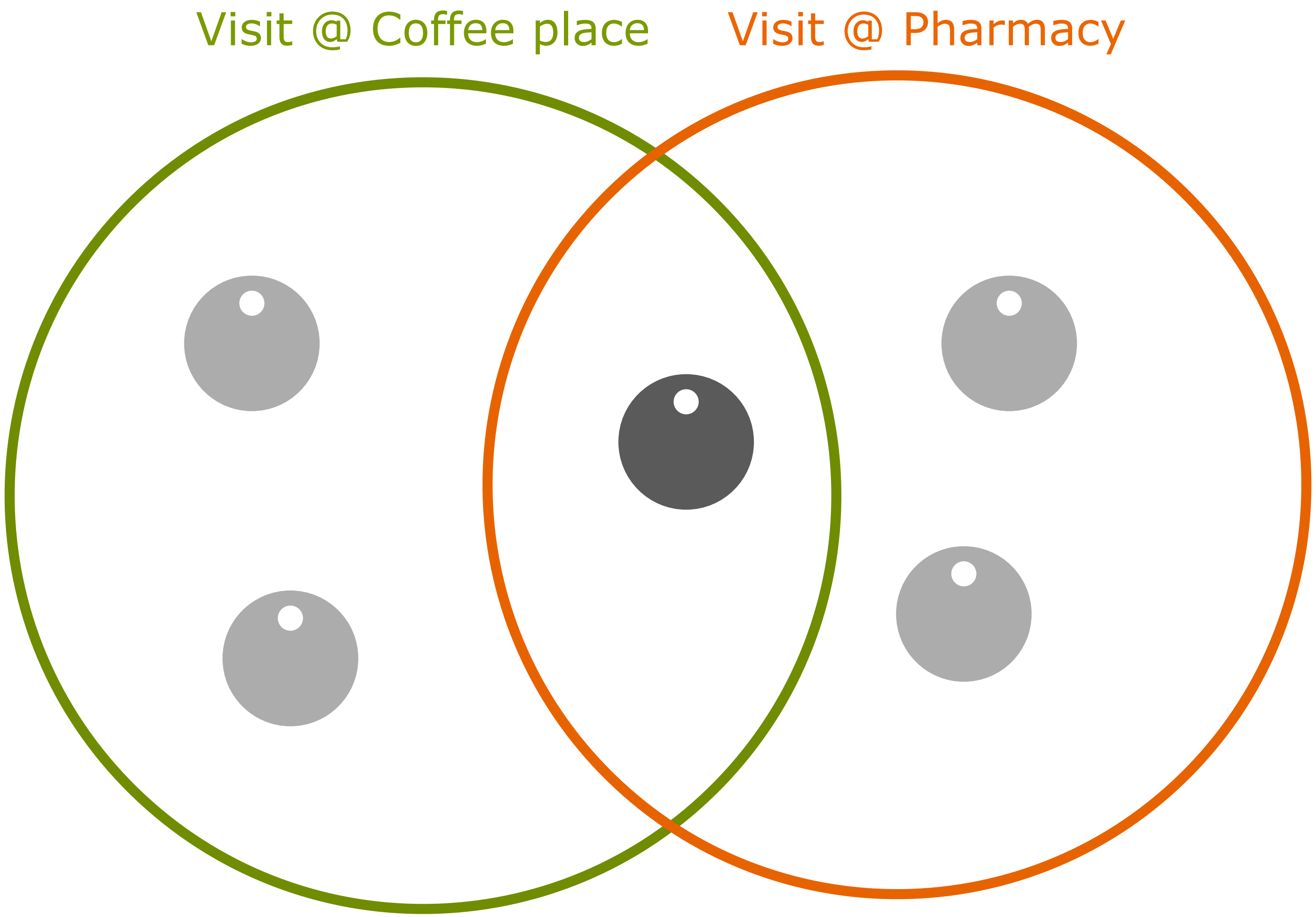
Event collection



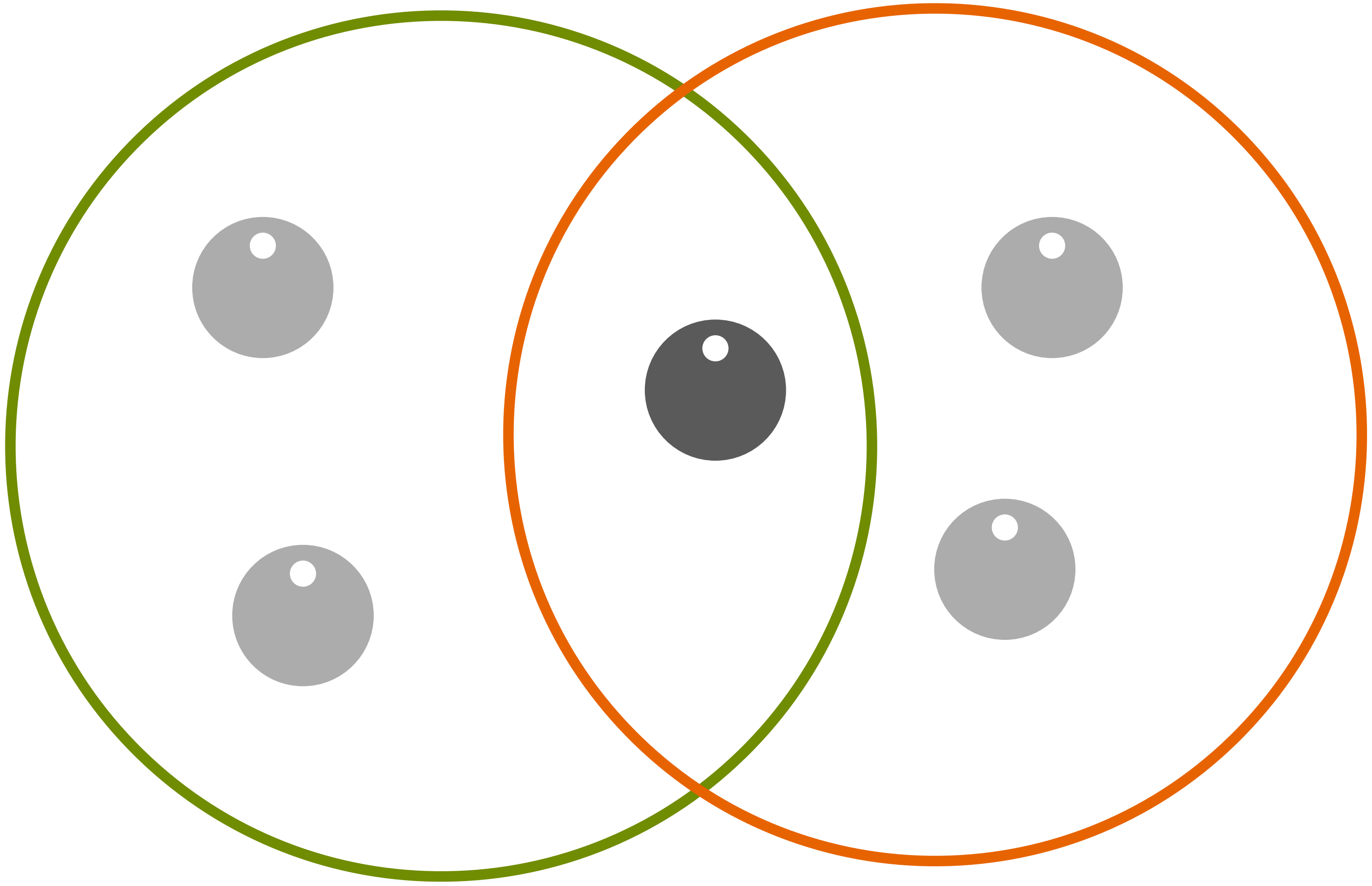
Detection Algorithms



Detection Algorithms



Detection Algorithms

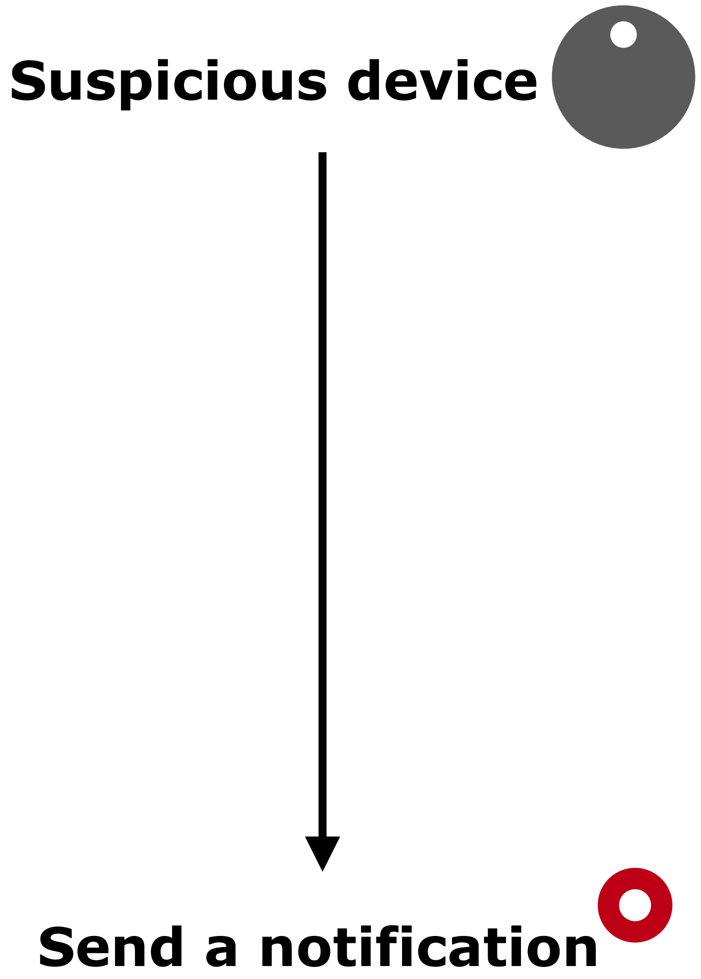


1. Has the tracker been seen in the last 5min

2. Did the tracker travel with the user for more than 420m

3. Did the tracker travel with the user for at least 5min

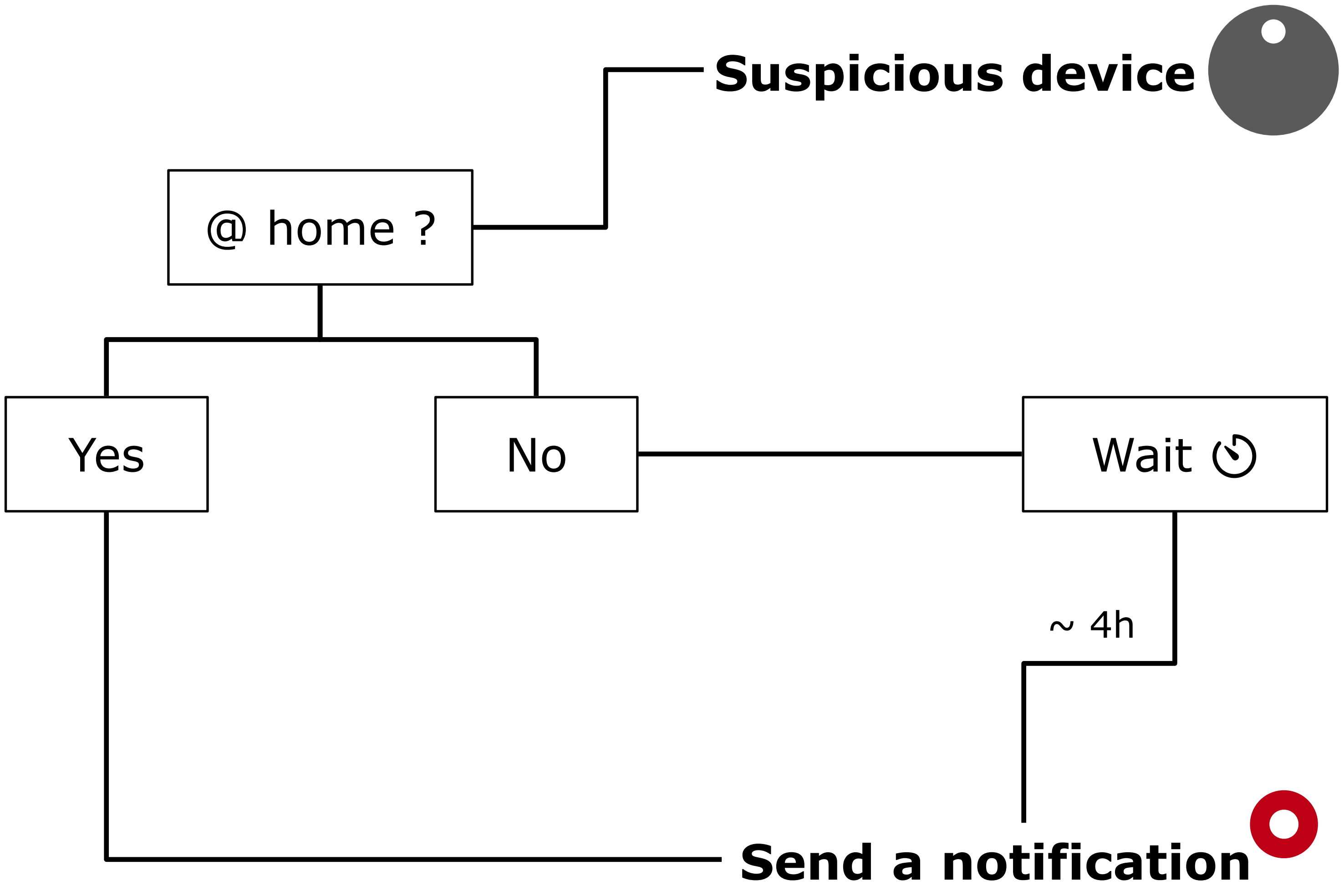
Suspicious Device = Notification?



Suspicious device

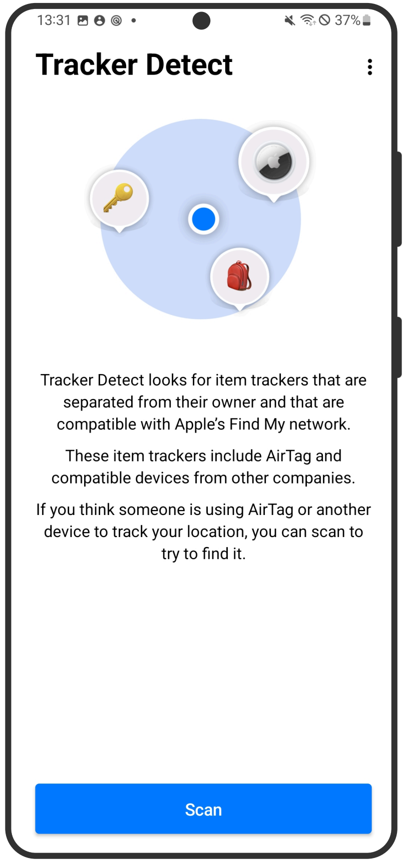
Send a notification

Suspicious Device = Notification?



AirGuard

Protection mechanisms for Android



13:31 37%

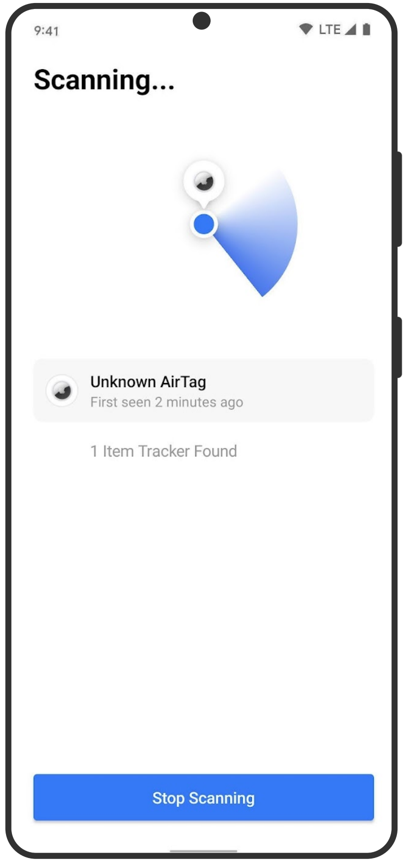
Tracker Detect

Tracker Detect looks for item trackers that are separated from their owner and that are compatible with Apple's Find My network.

These item trackers include AirTag and compatible devices from other companies.

If you think someone is using AirTag or another device to track your location, you can scan to try to find it.

Scan



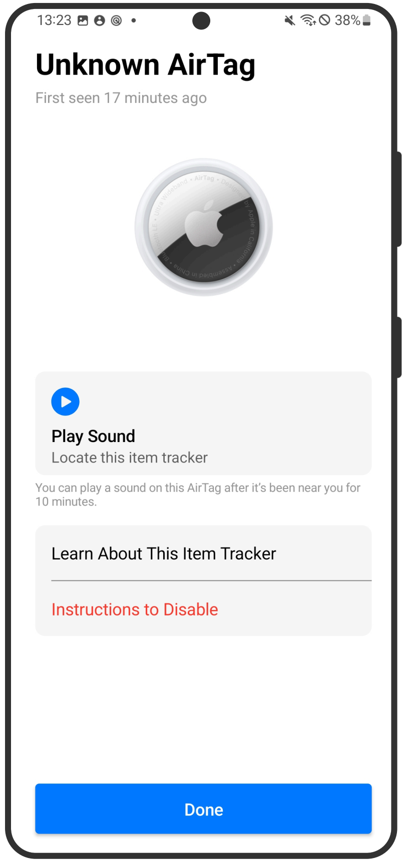
9:41 LTE

Scanning...

Unknown AirTag
First seen 2 minutes ago

1 Item Tracker Found

Stop Scanning



13:23 38%

Unknown AirTag

First seen 17 minutes ago

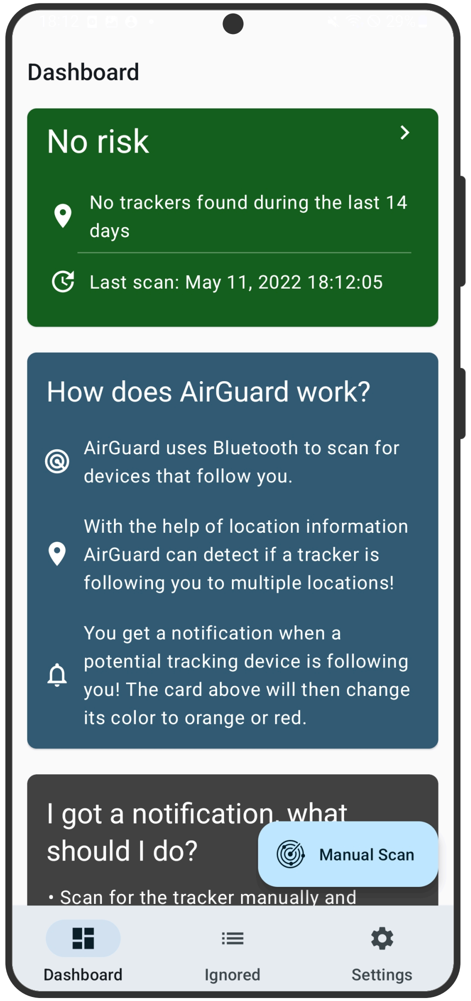
Play Sound
Locate this item tracker

You can play a sound on this AirTag after it's been near you for 10 minutes.

Learn About This Item Tracker

Instructions to Disable

Done



Dashboard

No risk

No trackers found during the last 14 days

Last scan: May 11, 2022 18:12:05

How does AirGuard work?

AirGuard uses Bluetooth to scan for devices that follow you.

With the help of location information AirGuard can detect if a tracker is following you to multiple locations!

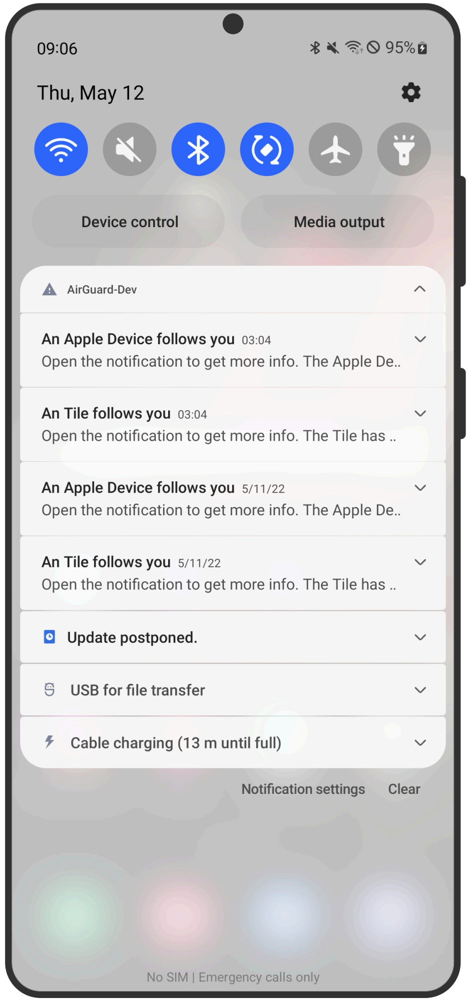
You get a notification when a potential tracking device is following you! The card above will then change its color to orange or red.

I got a notification, what should I do?

Manual Scan

• Scan for the tracker manually and

Dashboard Ignored Settings



09:06 95%

Thu, May 12

Device control Media output

AirGuard-Dev

An Apple Device follows you 03:04
Open the notification to get more info. The Apple De..

An Tile follows you 03:04
Open the notification to get more info. The Tile has ..

An Apple Device follows you 5/11/22
Open the notification to get more info. The Apple De..

An Tile follows you 5/11/22
Open the notification to get more info. The Tile has ..

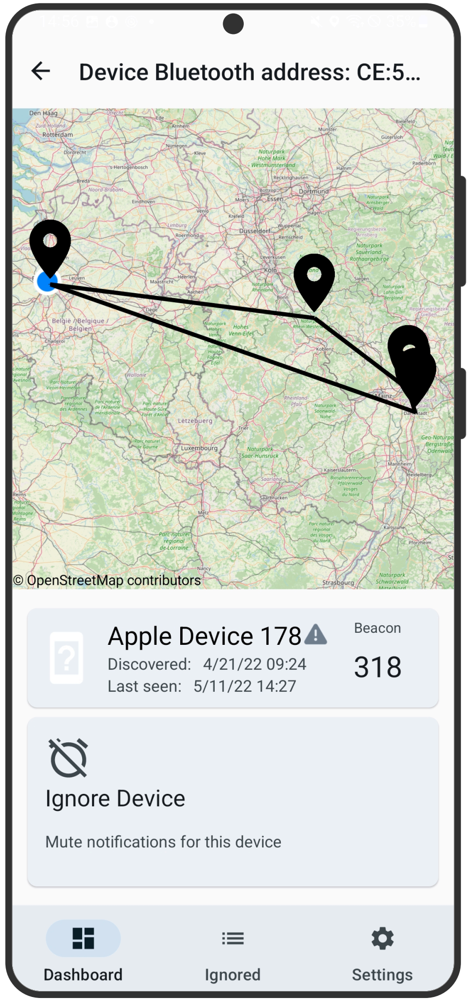
Update postponed.

USB for file transfer

Cable charging (13 m until full)

Notification settings Clear

No SIM | Emergency calls only



Device Bluetooth address: CE:5...

© OpenStreetMap contributors

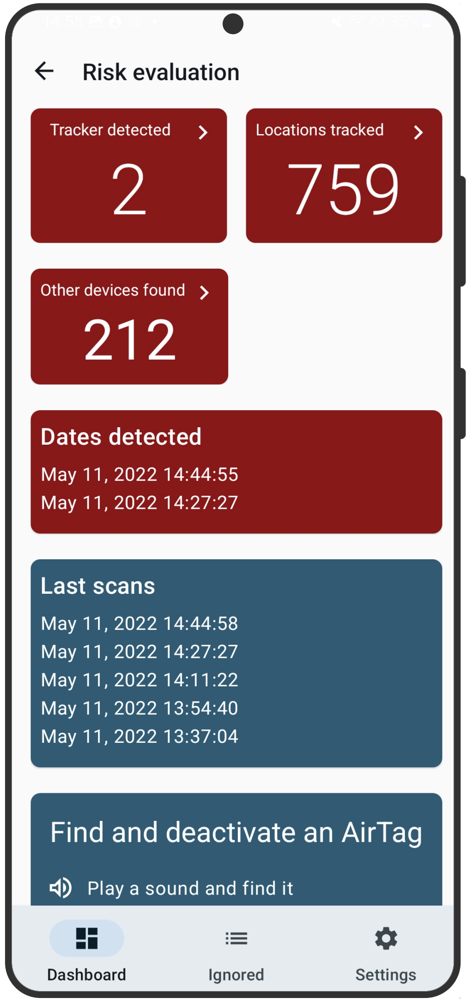
Apple Device 178
Discovered: 4/21/22 09:24
Last seen: 5/11/22 14:27

Beacon
318

Ignore Device

Mute notifications for this device

Dashboard Ignored Settings



Risk evaluation

Tracker detected
2

Locations tracked
759

Other devices found
212

Dates detected
May 11, 2022 14:44:55
May 11, 2022 14:27:27

Last scans
May 11, 2022 14:44:58
May 11, 2022 14:27:27
May 11, 2022 14:11:22
May 11, 2022 13:54:40
May 11, 2022 13:37:04

Find and deactivate an AirTag

Play a sound and find it

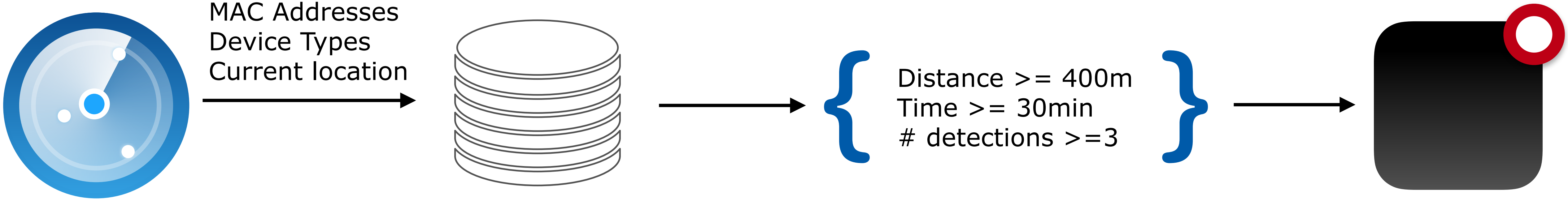
Dashboard Ignored Settings

280,000 downloads on Google Play

GET IT ON Google Play

GET IT ON F-Droid

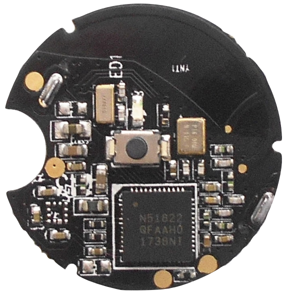
Tracking Detection



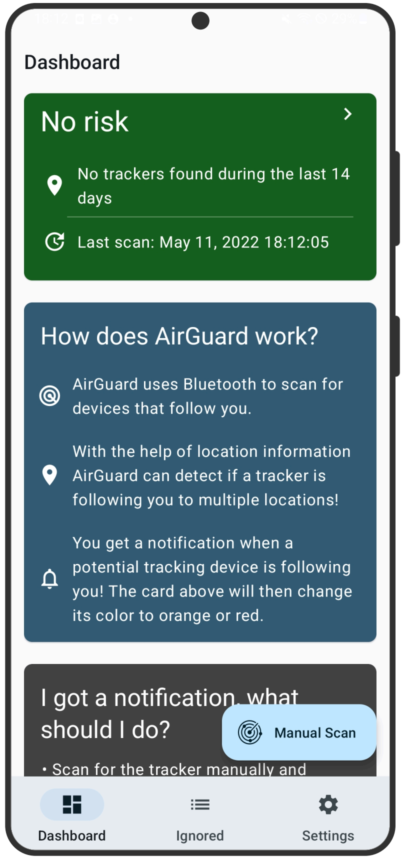
MAC Addresses
Device Types
Current location

Distance >= 400m
Time >= 30min
# detections >=3

Supported Trackers



Risk Levels


Dashboard

No risk

No trackers found during the last 14 days

Last scan: May 11, 2022 18:12:05

How does AirGuard work?

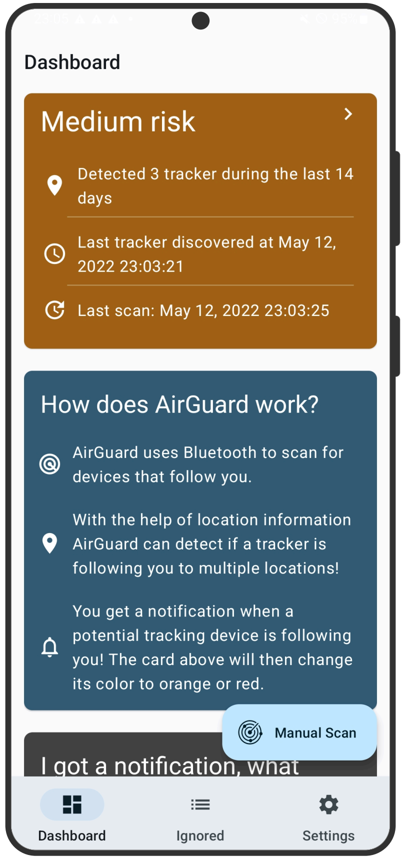
AirGuard uses Bluetooth to scan for devices that follow you.

With the help of location information AirGuard can detect if a tracker is following you to multiple locations!

You get a notification when a potential tracking device is following you! The card above will then change its color to orange or red.

I got a notification, what should I do?

• Scan for the tracker manually and


Dashboard

Medium risk

Detected 3 tracker during the last 14 days

Last tracker discovered at May 12, 2022 23:03:21

Last scan: May 12, 2022 23:03:25

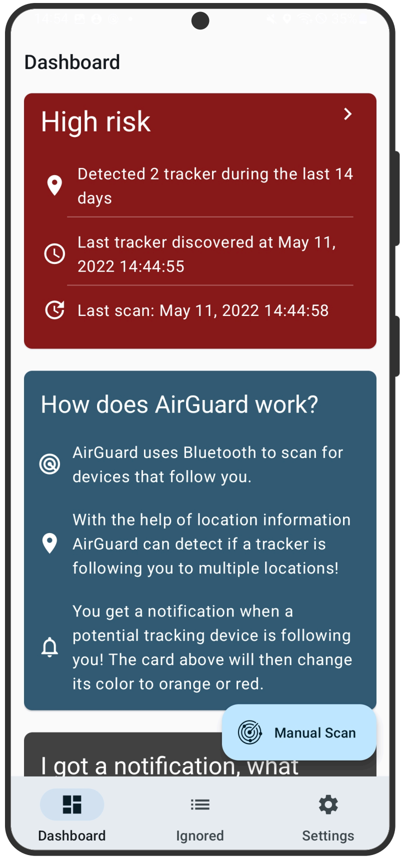
How does AirGuard work?

AirGuard uses Bluetooth to scan for devices that follow you.

With the help of location information AirGuard can detect if a tracker is following you to multiple locations!

You get a notification when a potential tracking device is following you! The card above will then change its color to orange or red.

I got a notification, what


Dashboard

High risk

Detected 2 tracker during the last 14 days

Last tracker discovered at May 11, 2022 14:44:55

Last scan: May 11, 2022 14:44:58

How does AirGuard work?

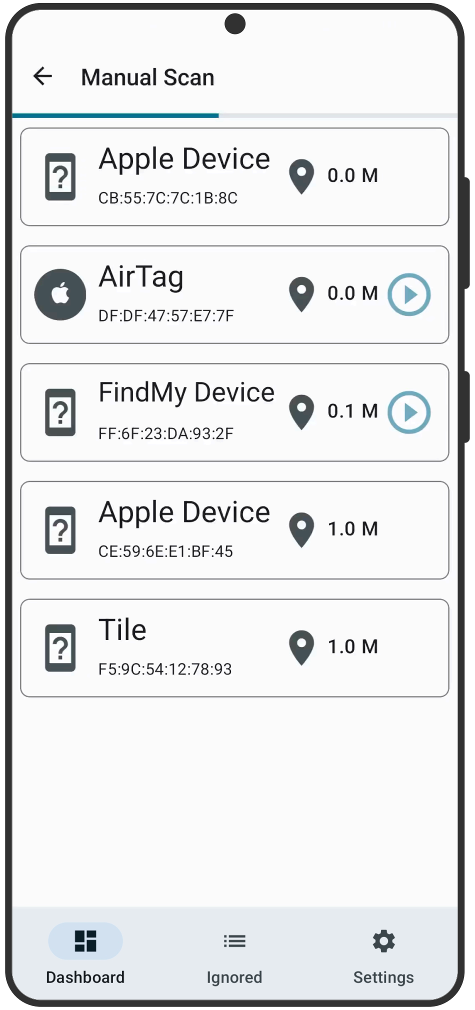
AirGuard uses Bluetooth to scan for devices that follow you.

With the help of location information AirGuard can detect if a tracker is following you to multiple locations!

You get a notification when a potential tracking device is following you! The card above will then change its color to orange or red.

I got a notification, what

Manual scans



Manual Scan

Apple Device
CB:55:7C:7C:1B:8C
0.0 M

AirTag
DF:DF:47:57:E7:7F
0.0 M

FindMy Device
FF:6F:23:DA:93:2F
0.1 M

Apple Device
CE:59:6E:E1:BF:45
1.0 M

Tile
F5:9C:54:12:78:93
1.0 M

Evaluation and Observations

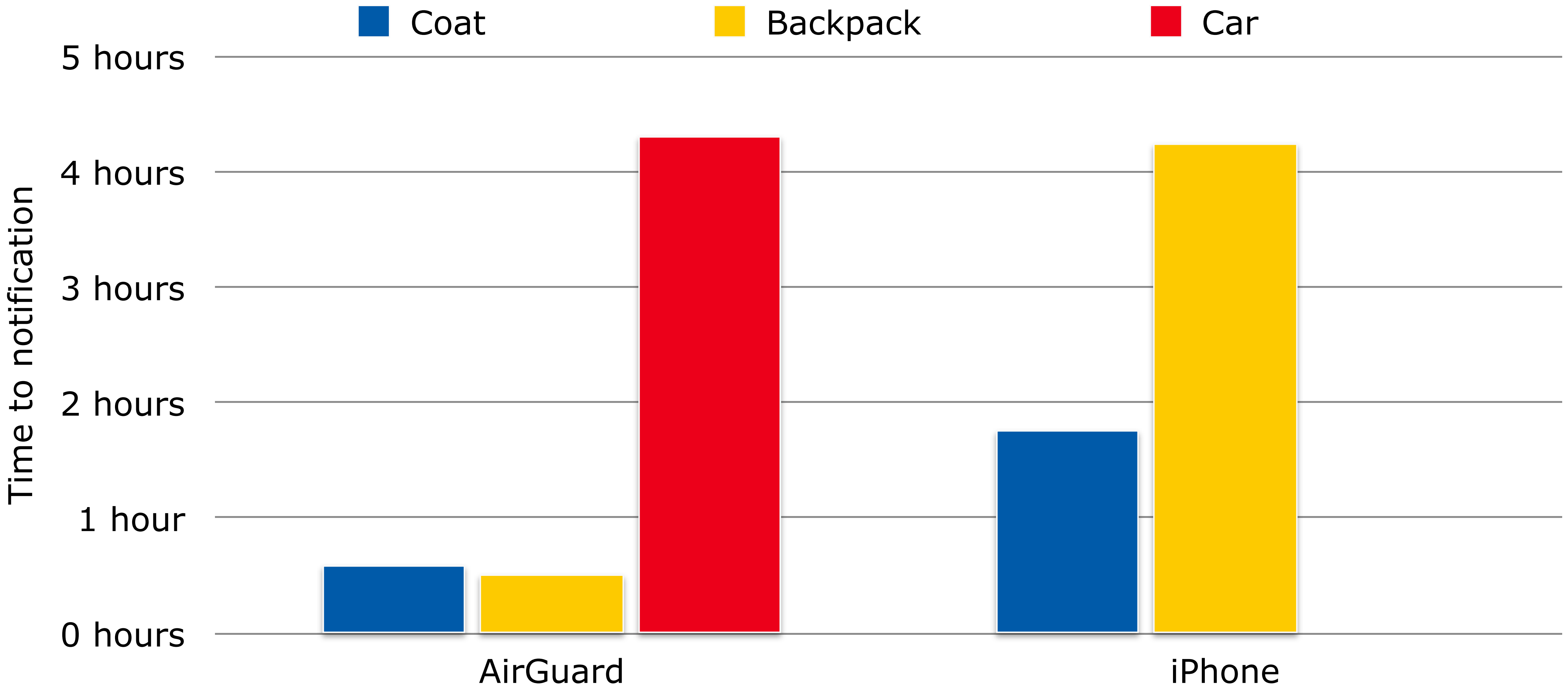
Evaluation

Coat

Backpack

Car

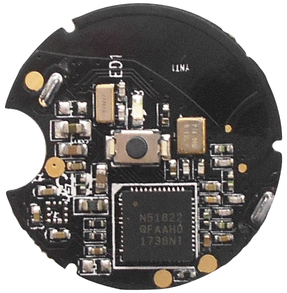
Evaluation



Coat
Backpack
Car
5 hours
4 hours
3 hours
2 hours
1 hour
0 hours
Time to notification
AirGuard
iPhone

Self-made trackers

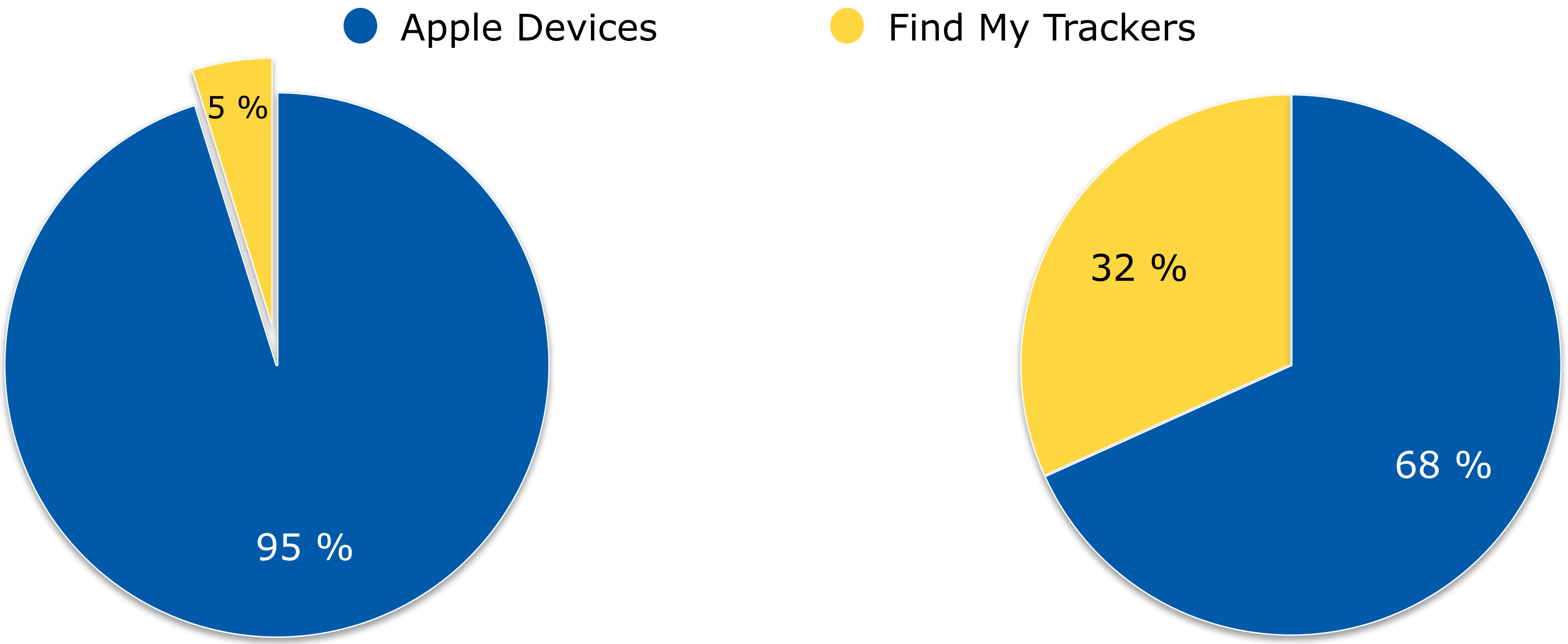
- Self-made trackers may not be detected by iOS
- Replicate the Offline Finding of Apple Devices
- Actively ignored for tracking detection in iOS
- Generally easy do detect



Real-World Observations

- Voluntarily share anonymous data with us
- 38,000 participants until March 2022
- About 11 million BLE advertisements

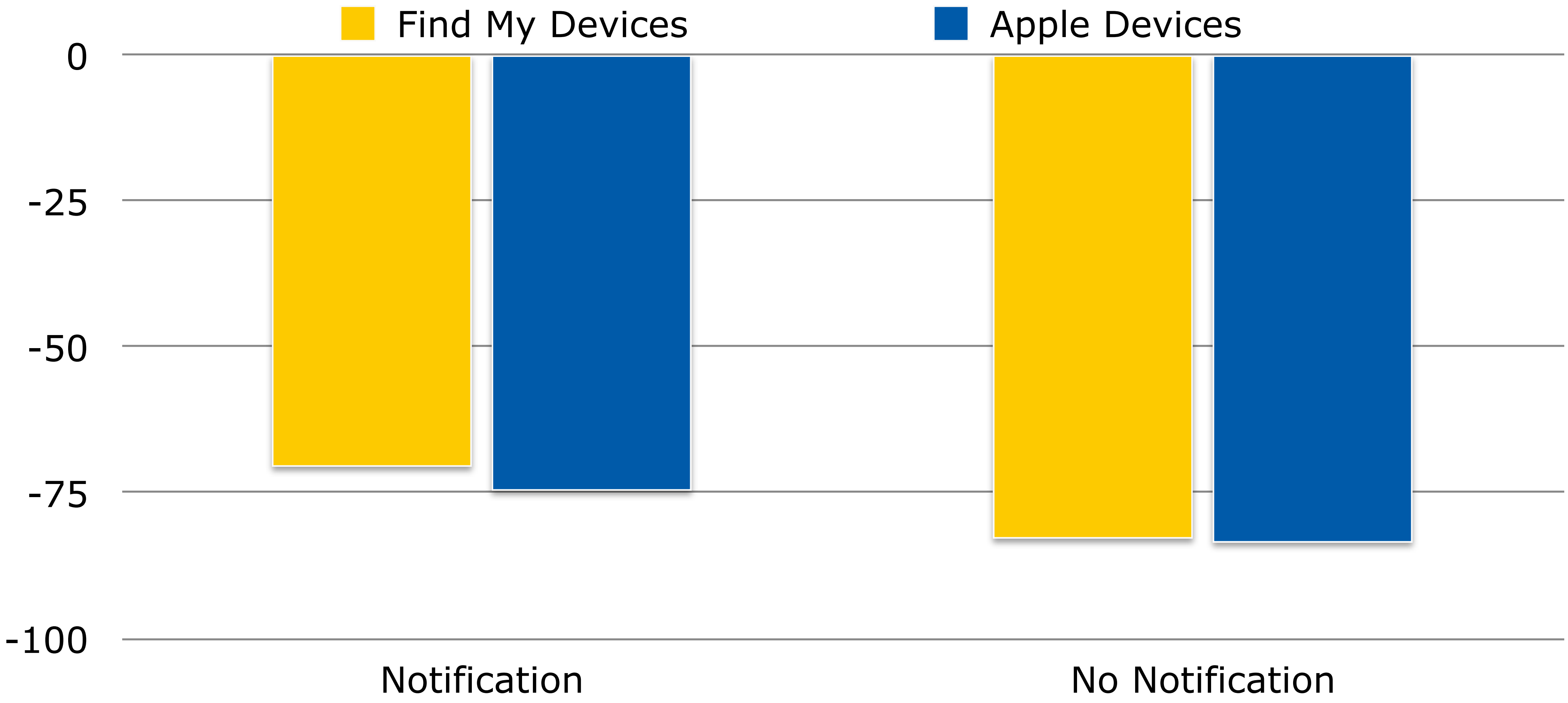
Device Distribution



All devices found

Devices with a tracking notification

RSSI Levels


Find My Devices
Apple Devices
0
-25
-50
-75
-100
Notification
No Notification

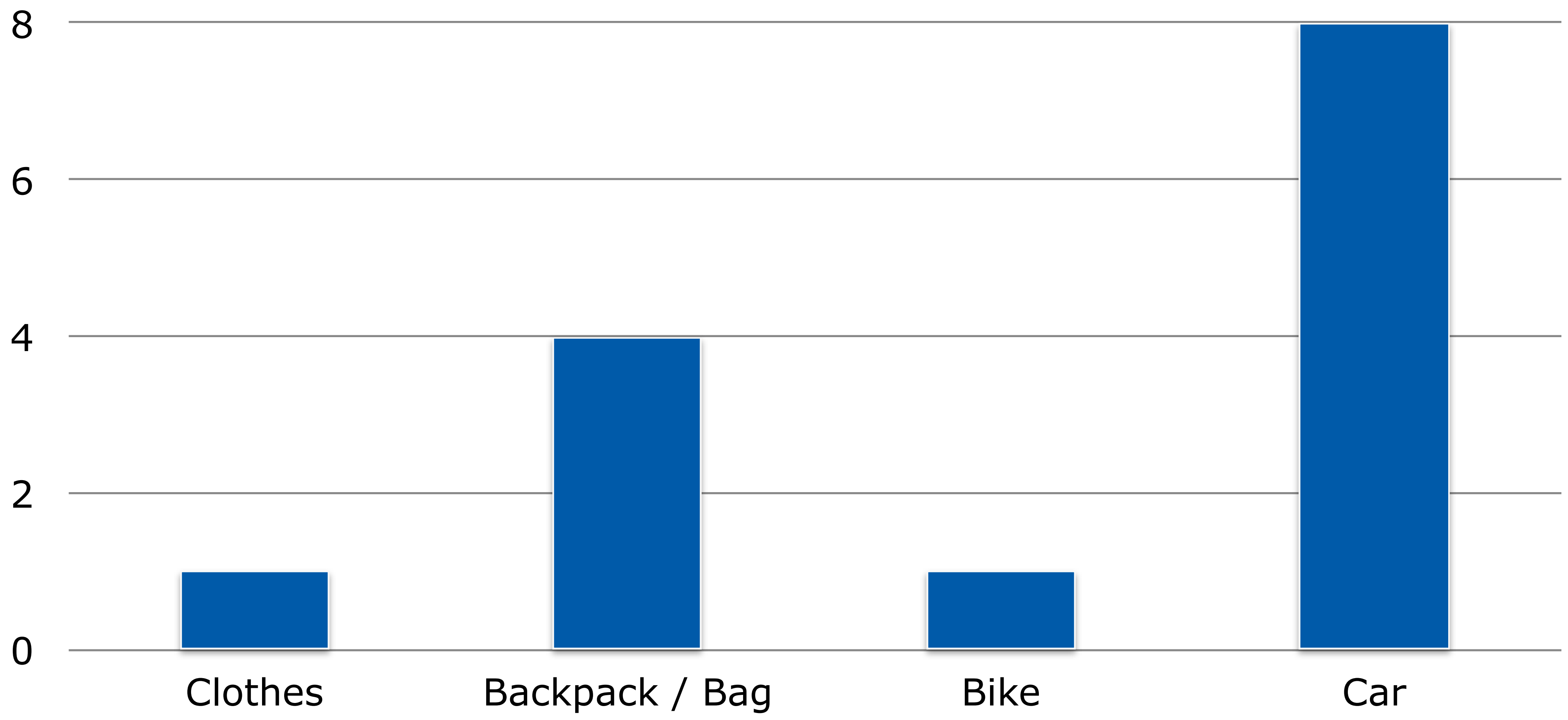
Real world observations

Did exactly what it was supposed to do!!! I used this app today to locate the air tag my ex put in my car to track me…

It took a little while though, like a day, but it detected an Apple Air tag 5 that was hid in my car. Fortunately the app allowed me the capability of playing a sound from within it and locating it.

Somone had my location and I even found it in my bag!!!

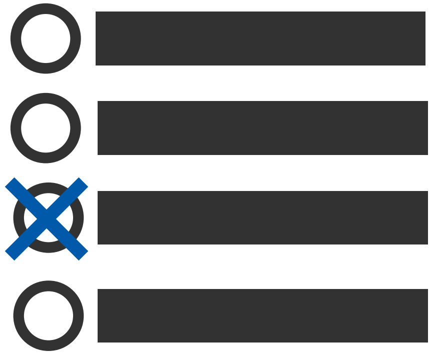
Feedback over the app



The Solution?

- Apps cannot be the solution
- OS-level integration necessary
- Support for all trackers
- Minimum standards for trackers

What comes next?



Thanks to…

Milan Stute	Jiska Classen	Niklas Bittner	Tim Kornhuber
PostDoc @ SEEMOO	PostDoc @ SEEMOO	Student	Student

Q&A

https://github.com/seemoo-lab

@Sn0wfreeze

aheinrich@seemoo.de