Schwachstelle iPhone?

Sicherheitsrisiken im Apple Ökosystem

Matthias Hollick und Team
FG Sichere Mobile Netze, SEEMOO, TU Darmstadt

Outline

Who Can „Find My“ Devices

Selected Research Highlights

Questions & Answers

Where is my ***? Oh no, it is offline!

Where is my ***? Oh no, it is offline!

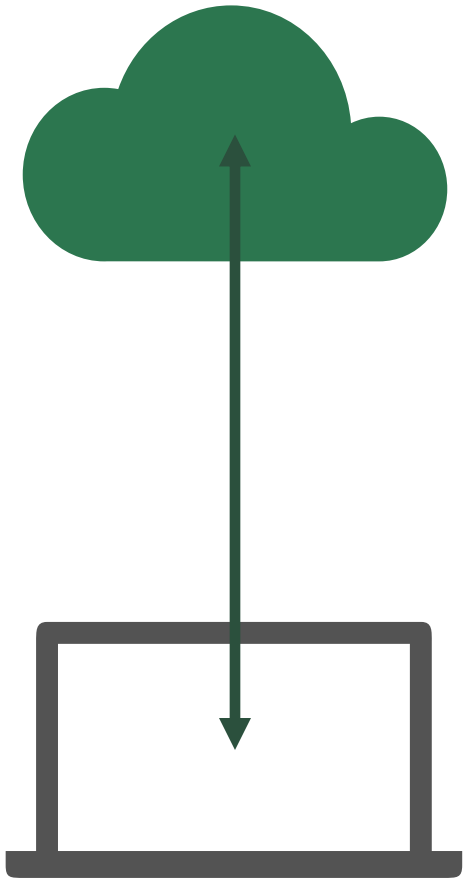
- You could try to find it alone
- You could try to ask friends and family

- Why not asking a crowd

- Best make it a few hundred million and let them cover the entire planet

Offline finding: when items know their location, and can tell you where they are, even if offline

What is offline finding?



What is offline finding?

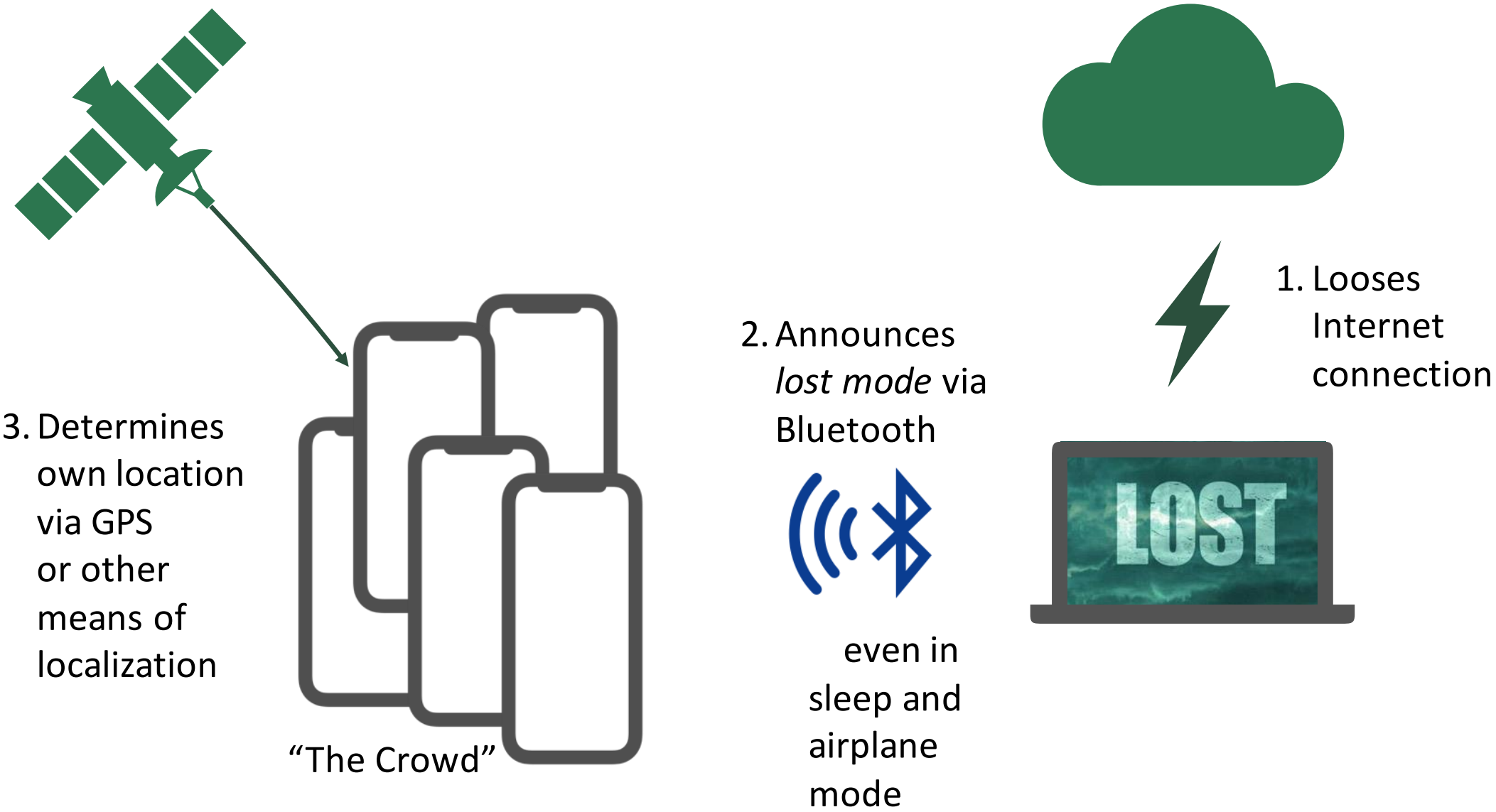
What is offline finding?

1. Looses Internet connection

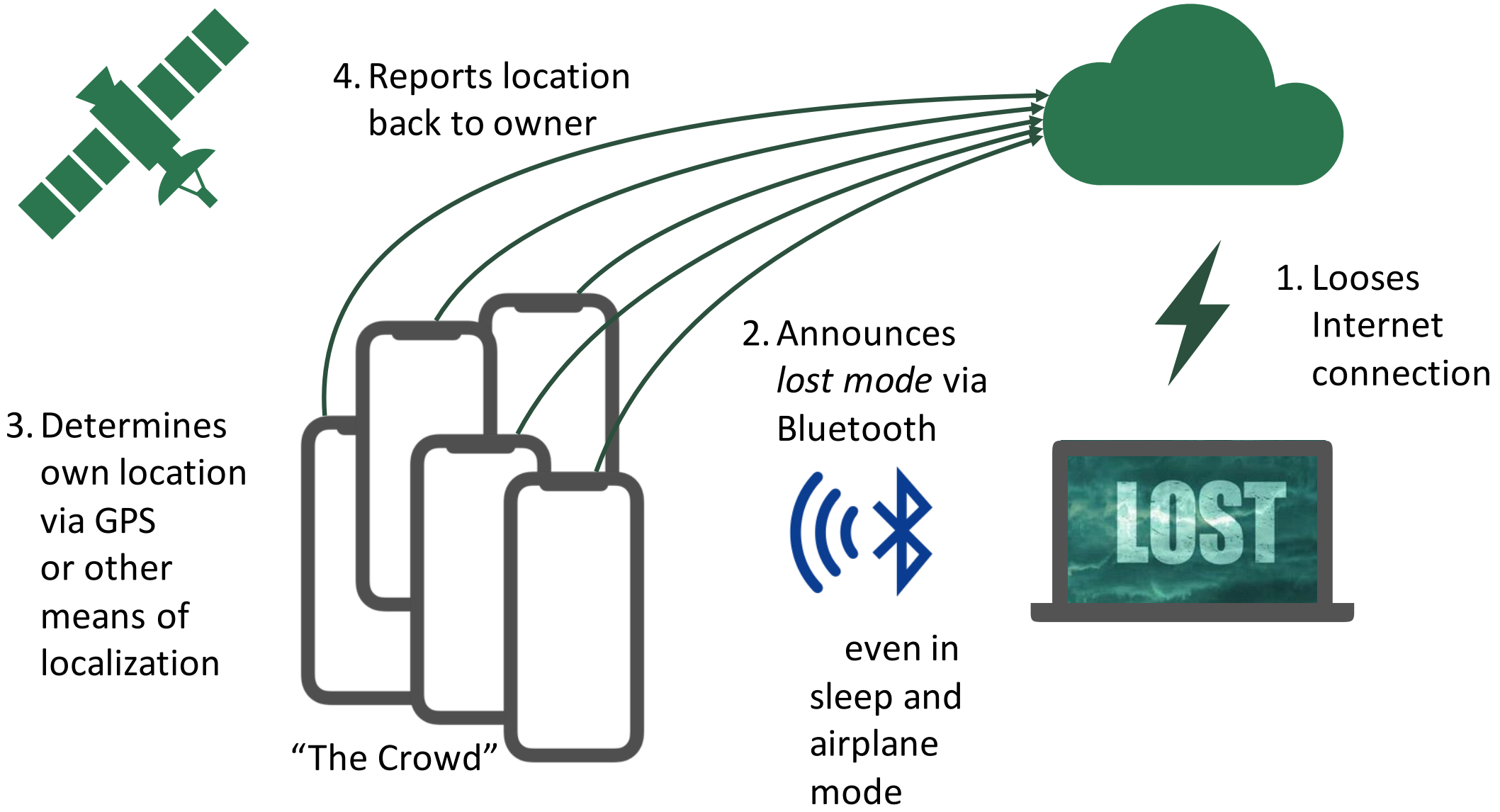
2. Announces *lost mode* via Bluetooth

even in sleep and airplane mode

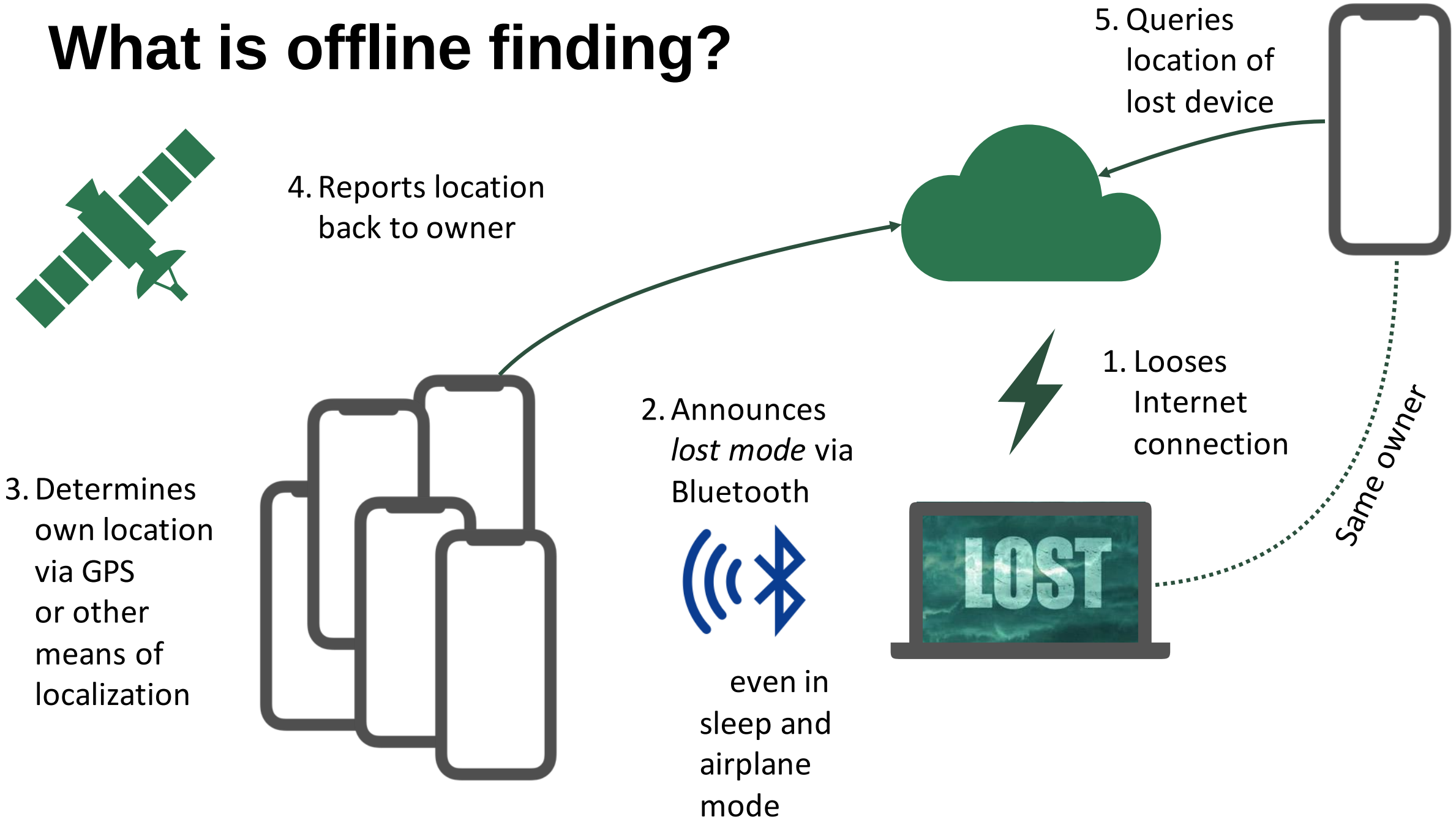
What is offline finding?



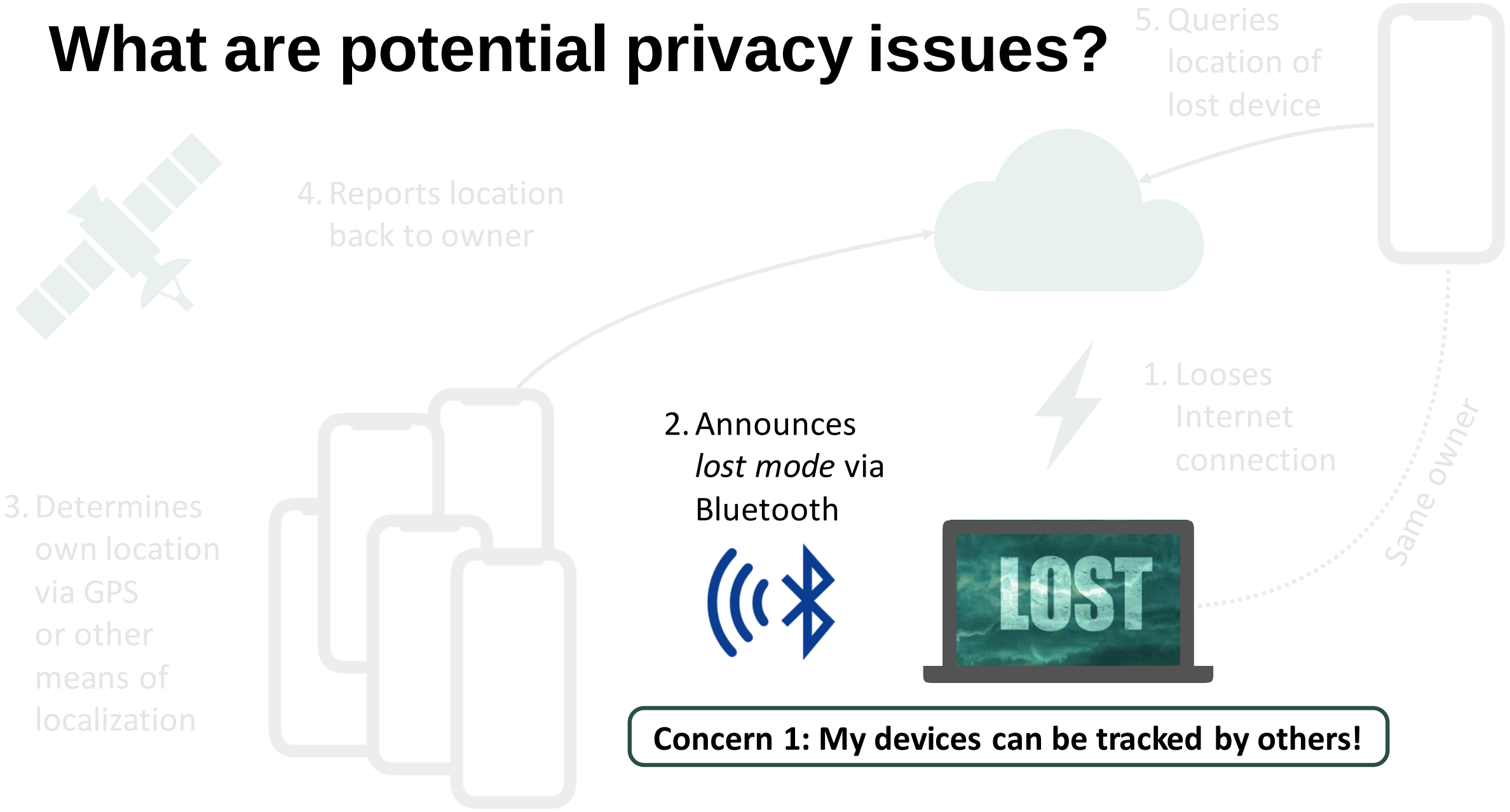
What is offline finding?



What is offline finding?

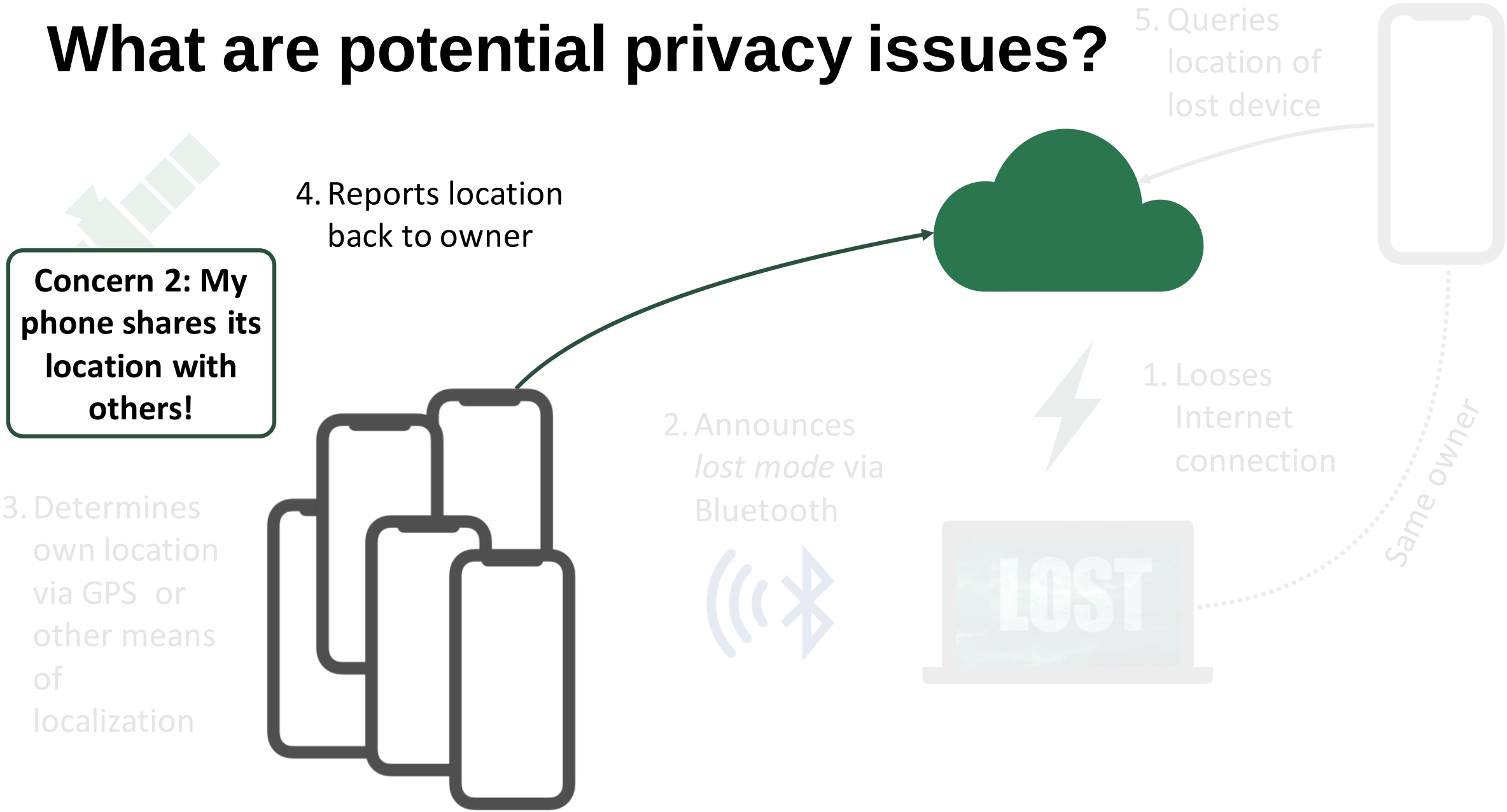


What are potential privacy issues?

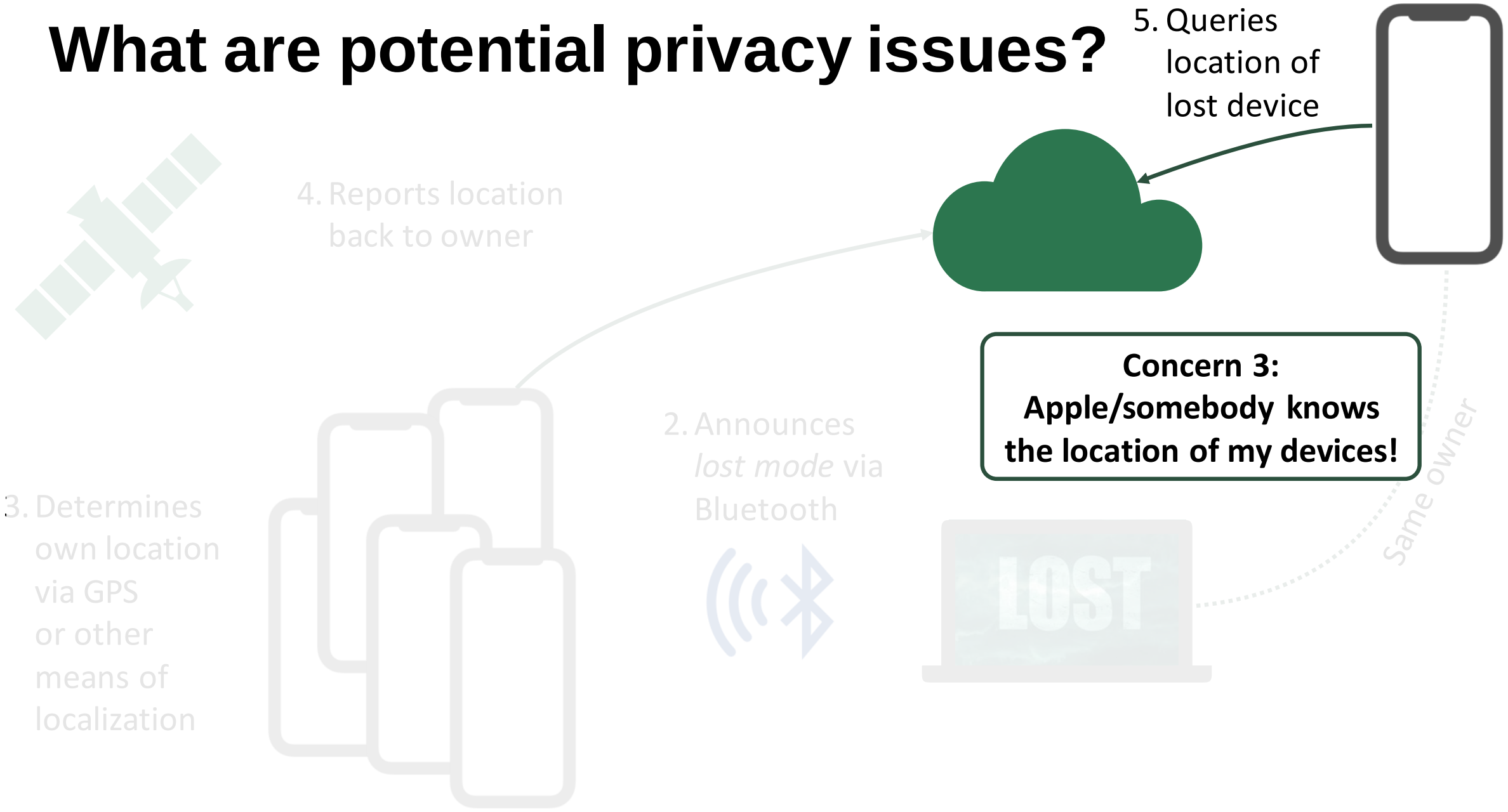


Concern 1: My devices can be tracked by others!

What are potential privacy issues?

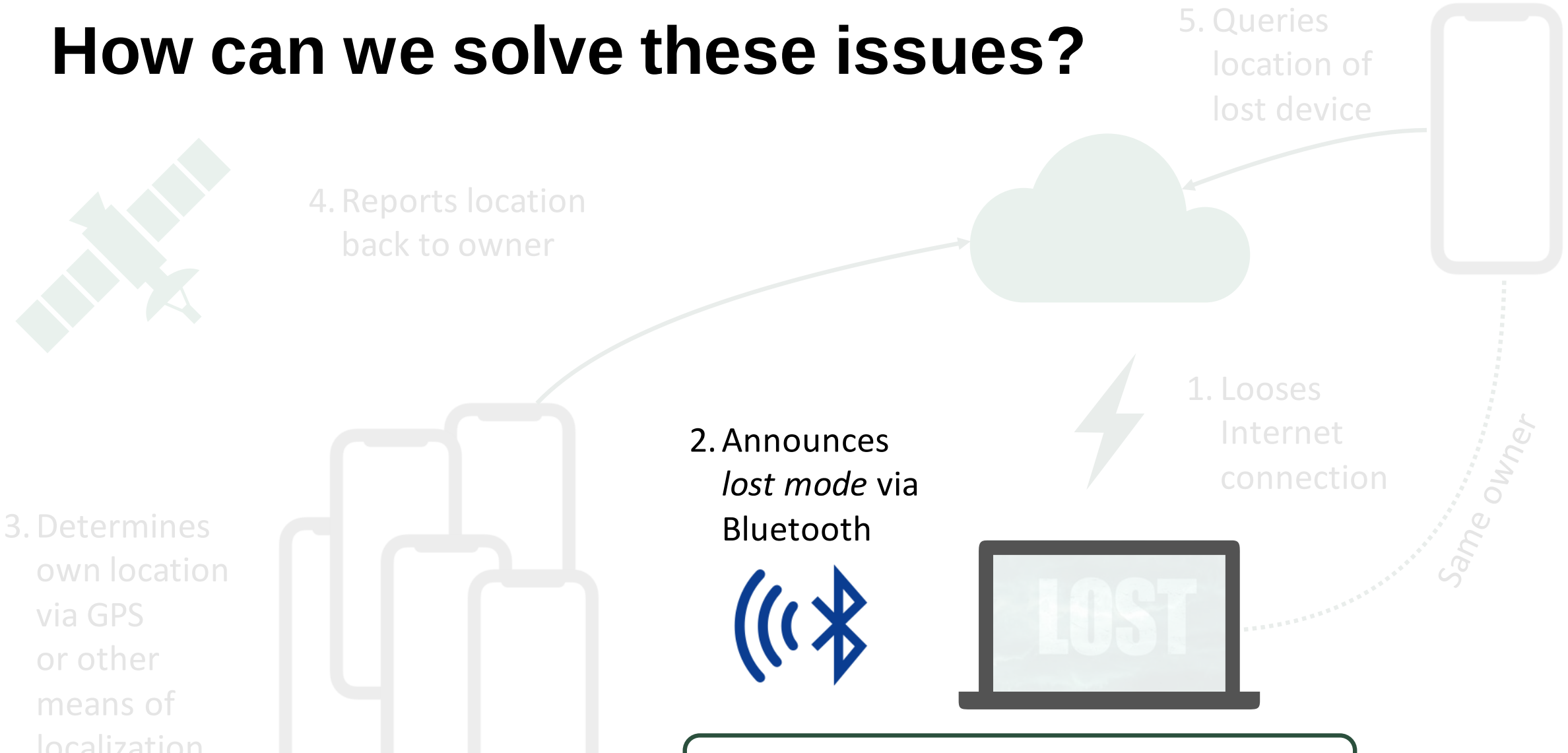


What are potential privacy issues?



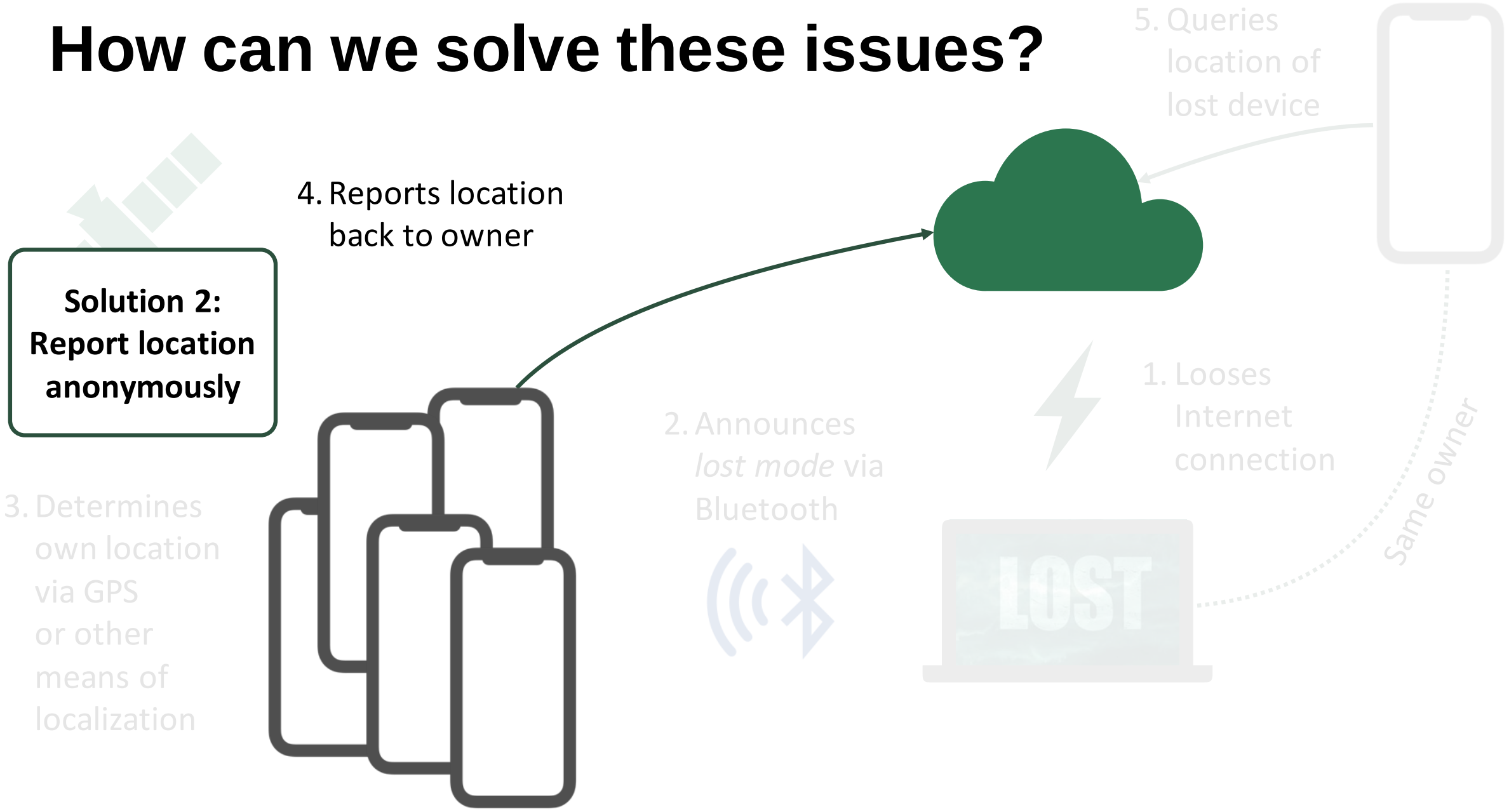
Concern 3: Apple/somebody knows the location of my devices!

How can we solve these issues?

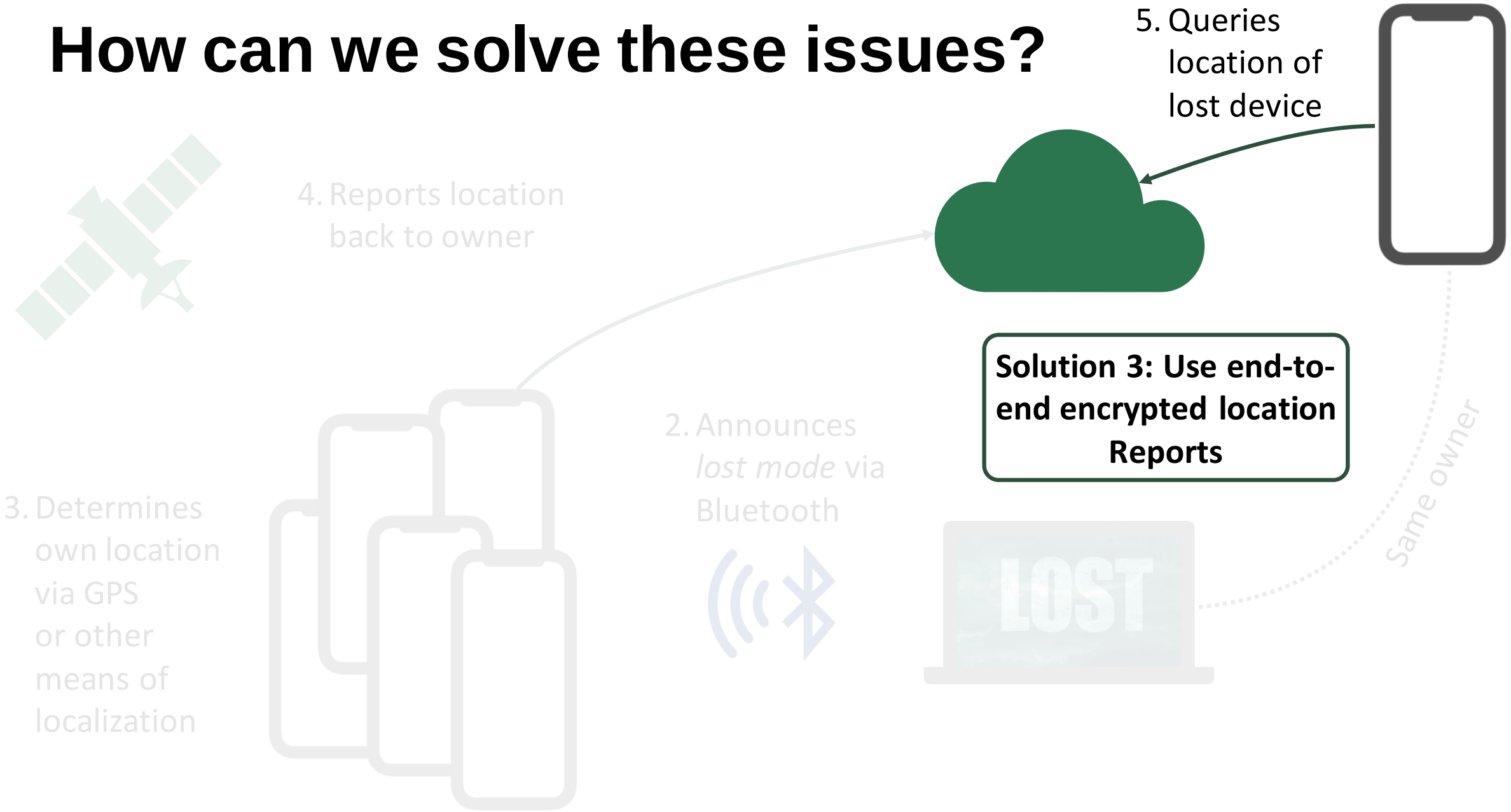


Solution 1: Use unlinkable pseudonyms

How can we solve these issues?



How can we solve these issues?



Solution 3: Use end-to-end encrypted location Reports

Security and Privacy Analysis

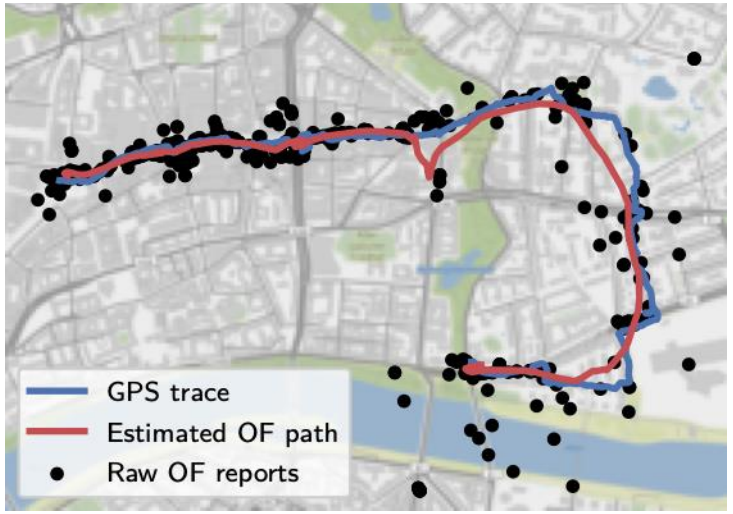
- "Find My" has a sophisticated **privacy-first** design
  - Encrypts reports end-to-end
  - Advertised public keys prevent long-term tracking of lost devices
  - Finder devices remain anonymous

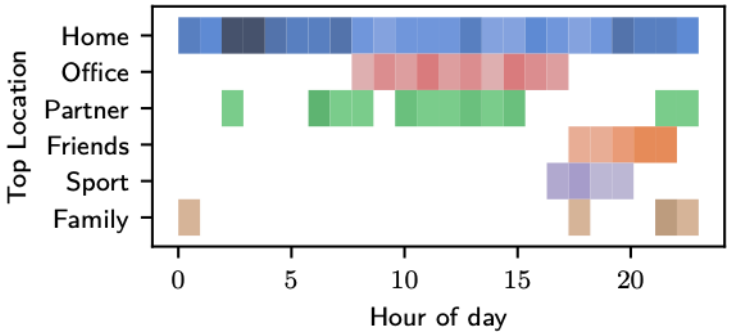
- **Best** finder system in terms of security and privacy out there **today**

- But: **rather complex** and only **partial specification** is publicly available
- Things can still go wrong …

What can (still) go wrong? Unauthorized Access of Location History

- All Apple services use a secure system keychain to store secrets
- Offline finding derives advertisement keys from master secret
- Derivation process is computationally heavy
- Store master secret in keychain but cache advertisement keys on disk
  - **Directory can be read by user applications**
- Allows for precise **user tracking** and **profiling**
- Apple adopted our proposed mitigation in September 2020





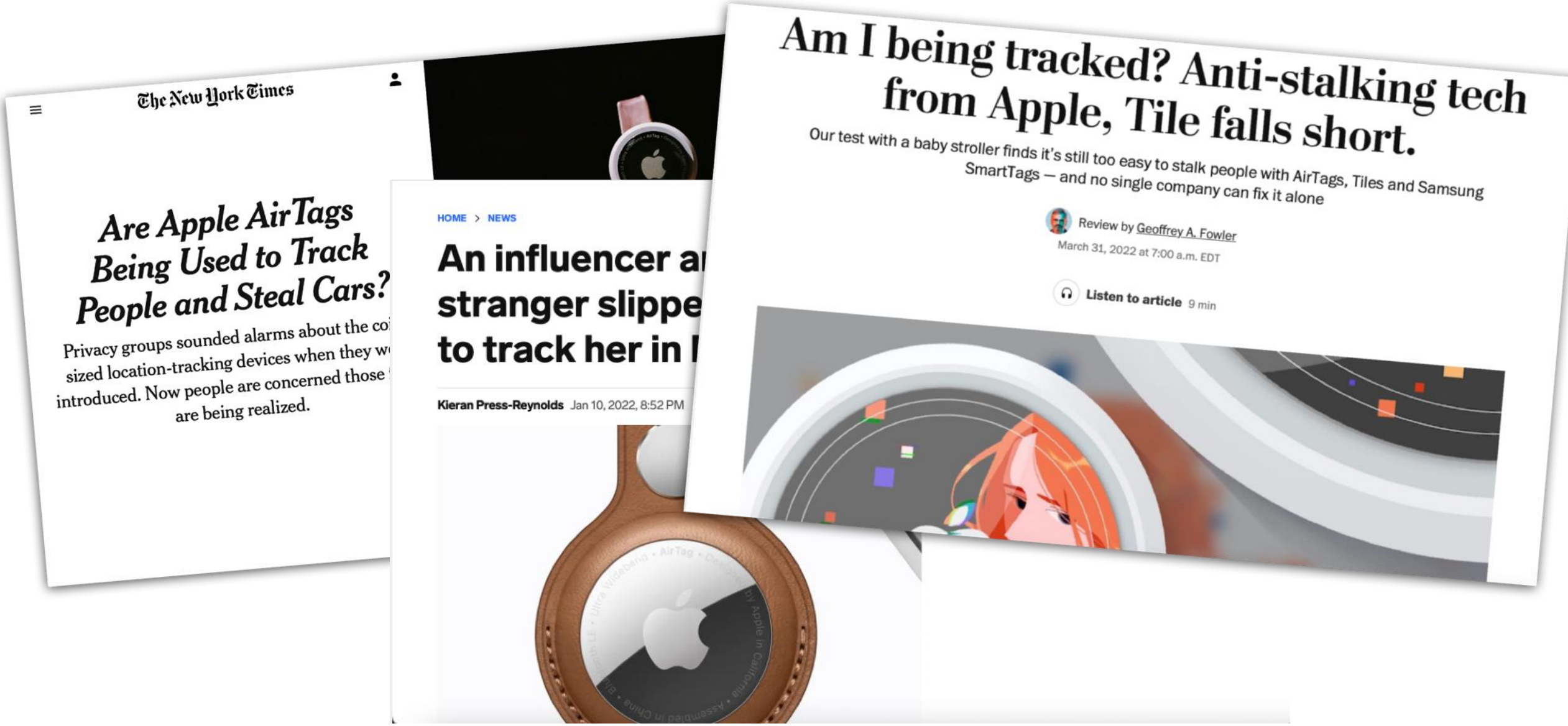
Outline

Who Can „Find My“ Devices

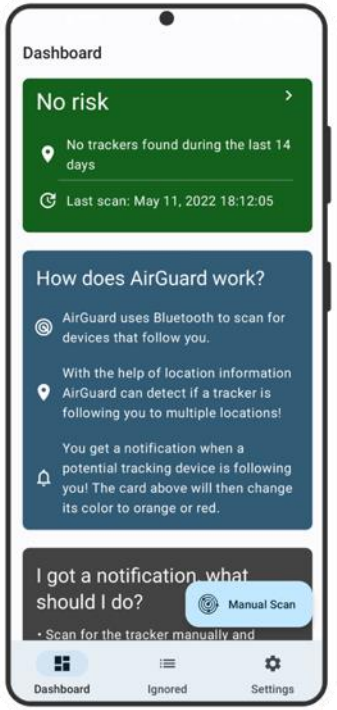
Selected Research Highlights

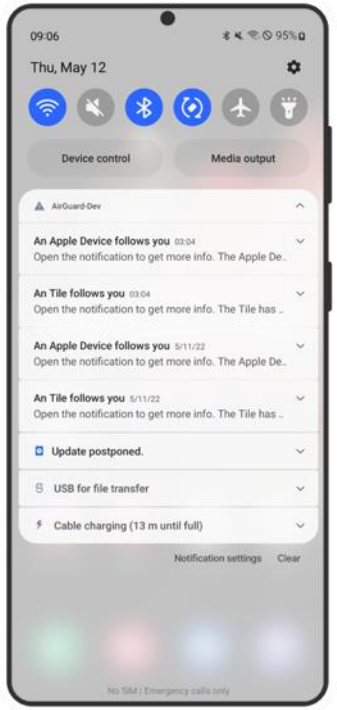
Questions & Answers

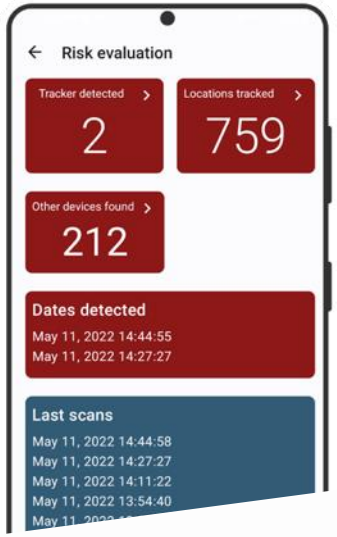
Protecting Against Stalking

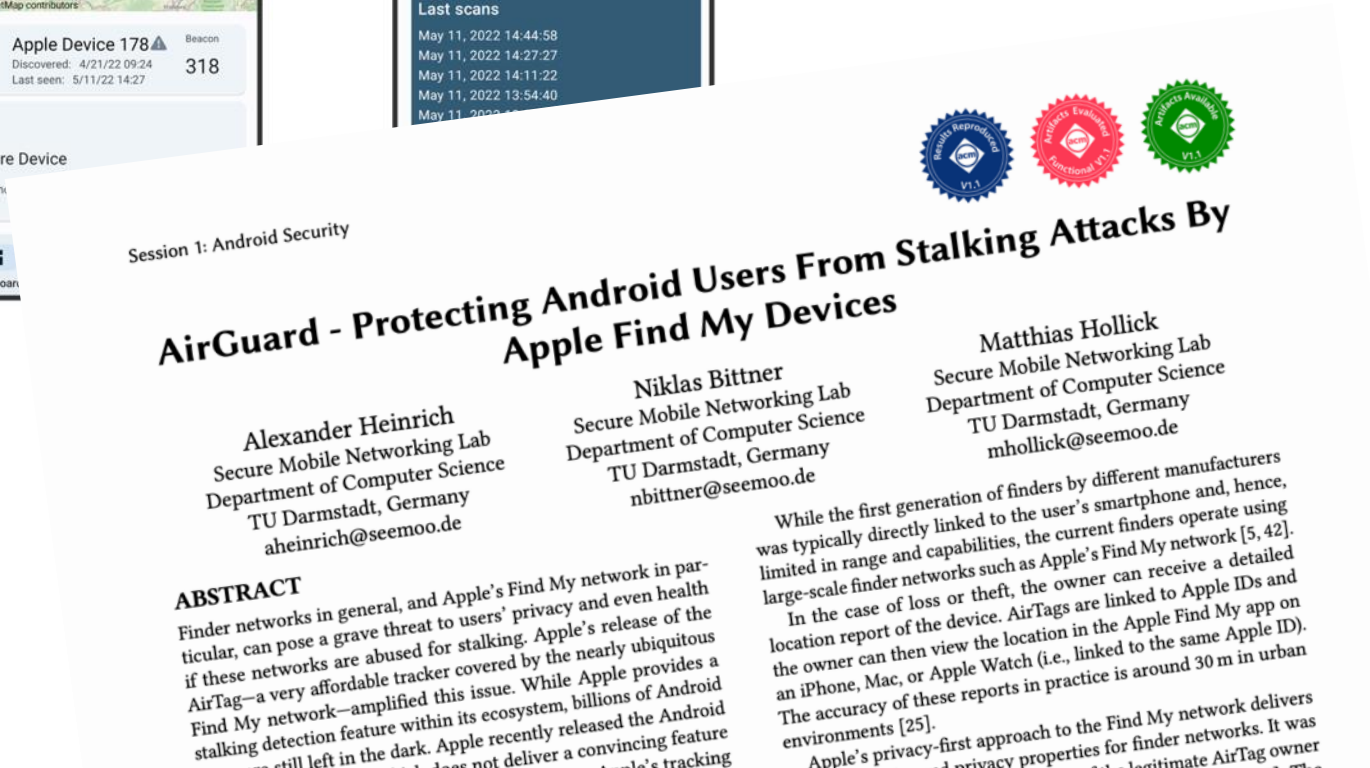


Protecting Against Stalking also on Android?!









Session 1: Android Security

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

Alexander Heinrich
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
aheinrich@seemoo.de

Niklas Bittner
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
nbittner@seemoo.de

Matthias Hollick
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
mhollick@seemoo.de

ABSTRACT

Finder networks in general, and Apple's Find My network in particular, can pose a grave threat to users' privacy and even health if these networks are abused for stalking. Apple's release of the AirTag—a very affordable tracker covered by the nearly ubiquitous Find My network—amplified this issue. While Apple provides a stalking detection feature within its ecosystem, billions of Android

While the first generation of finders by different manufacturers was typically directly linked to the user's smartphone and, hence, limited in range and capabilities, the current finders operate using large-scale finder networks such as Apple's Find My network [5, 42].

In the case of loss or theft, the owner can receive a detailed location report of the device. AirTags are linked to Apple IDs and the owner can then view the location in the Apple Find My app on an iPhone, Mac, or Apple Watch (i.e., linked to the same Apple ID). The accuracy of these reports in practice is around 30 m in urban environments [25].

Apple's privacy-first approach to the Find My network delivers

GET IT ON Google Play

GET IT ON F-Droid

280,000 downloads on Google Play

Privacy – Advertisement vs. Reality

The Register® OFF-PREM ON-PREM SOFTWARE SECURITY OFFBEAT VENDOR VOICE

{* SECURITY *}

Apple, you've AirDrop'd the ball: Academics detail ways to leak contact info of nearby iThings for spear-phishing

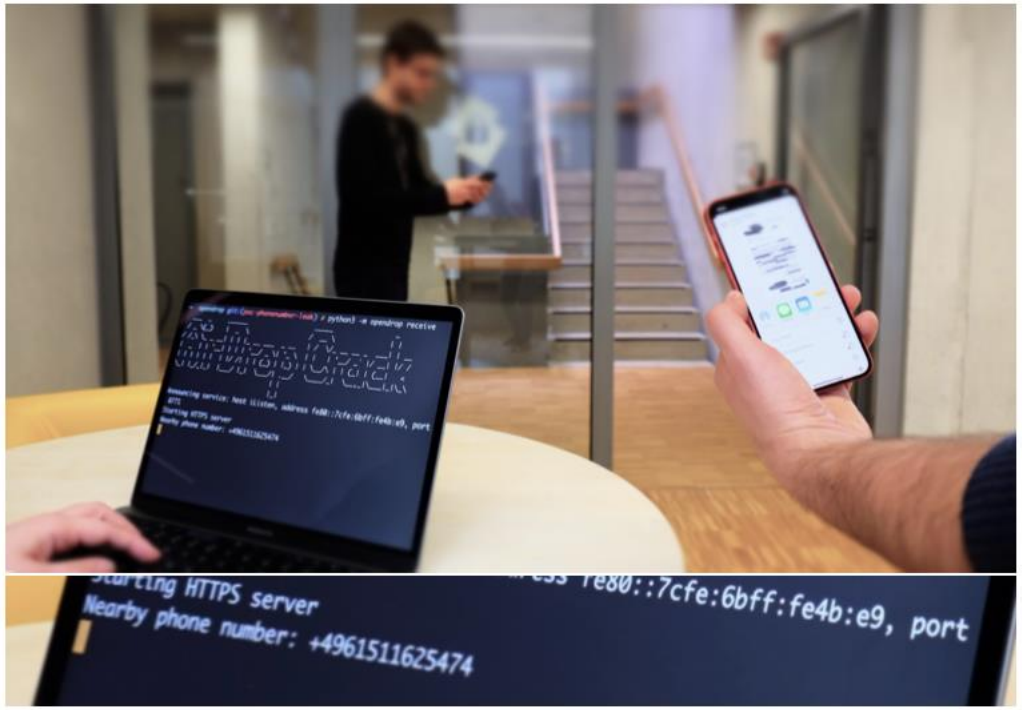
Too bad there's no suggested solution... oh, wait

Iain Thomson in San Francisco Thu 22 Apr 2021 // 08:16 UTC SHARE

Apple's AirDrop has a couple of potentially annoying privacy weaknesses that Cupertino is so far refusing to address even though a solution has been offered.

A bug-hunting team at Technische Universität Darmstadt in Germany reverse engineered AirDrop – iOS and macOS's ad-hoc over-the-air file-sharing service – and found that senders and receivers may leak their contact details in the process. More than a billion people are said to be at risk of this, in that there are now more than a billion active iPhones at any one time. Despite the team alerting Apple to the oversight in May 2019, and suggesting ways to address it last October, the iGiant hasn't issued a fix.

"We started looking at the protocols in 2017," Dr Milan Stute at the uni's Secure Mobile Networking Lab told *The Register* on Wednesday. "We reverse engineered a lot of stuff and found two major issues."



PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop

Alexander Heinrich Matthias Hollick Thomas Schneider
Milan Stute Christian Weinert

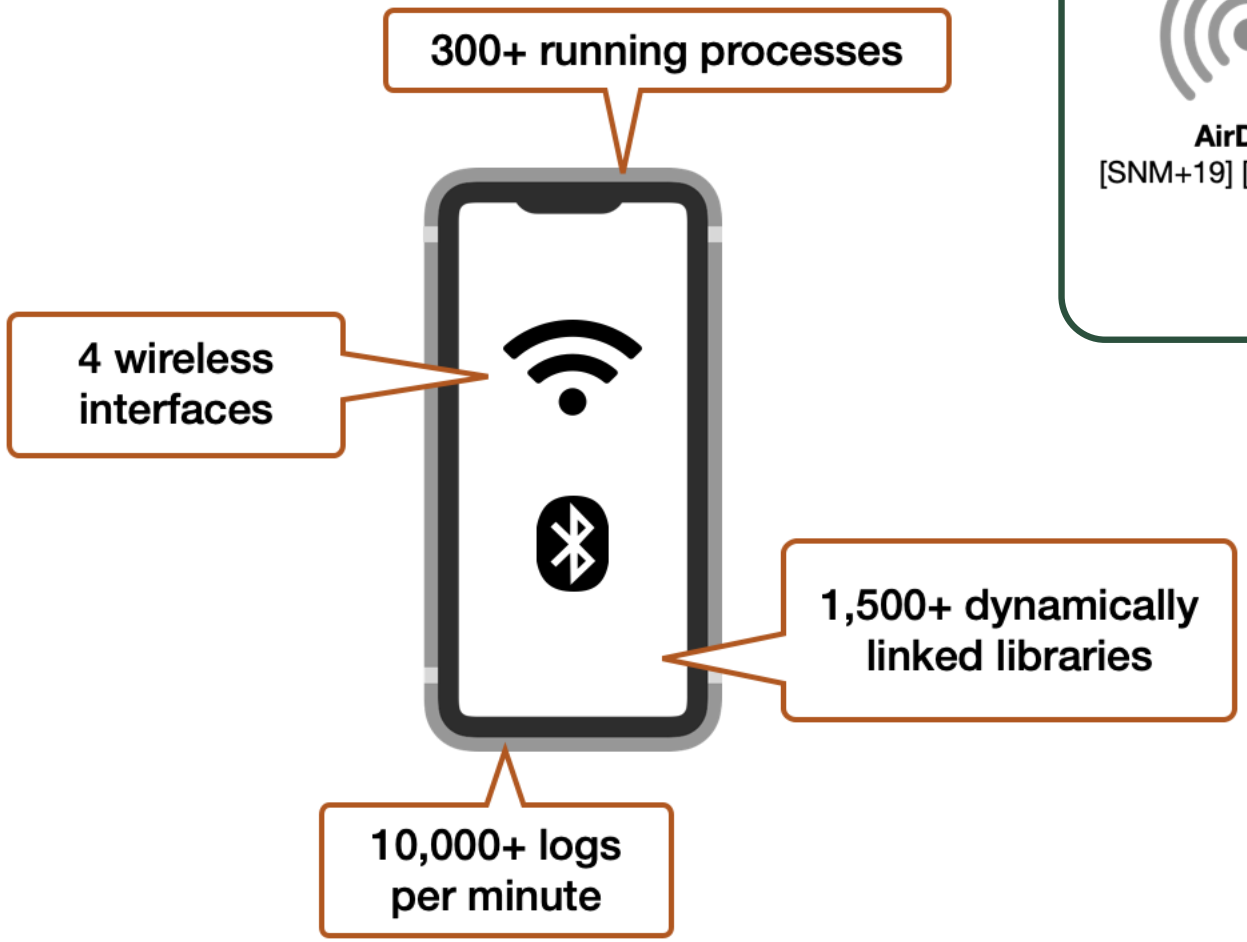
Technical University of Darmstadt, Germany

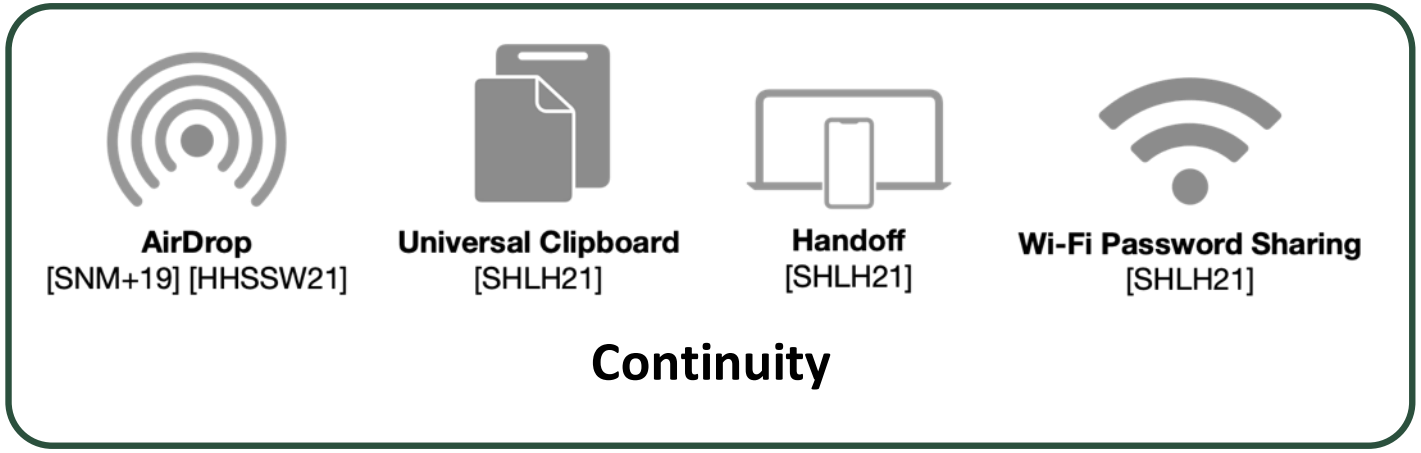
Abstract

Apple's offline file-sharing service AirDrop is integrated into devices worldwide. We dis-

Privacy-preserving contact discovery is commonly addressed via private set intersection (PSI) in the literature (e.g., [55, 59]). PSI protocols, in general, are cryptographic protocols that allow two interacting parties to securely intersection of their respective input sets without

Apple Ecosystem – Behind The Scenes of „Just Works“





Disrupting *Continuity* of Apple's Wireless Ecosystem Security: New Tracking, DoS, and MitM Attacks on iOS and macOS Through Bluetooth Low Energy, AWDL, and Wi-Fi

ARTIFACT EVALUATED usenix ASSOCIATION PASSED

Milan Stute Alexander Heinrich Jannik Lorenz Matthias Hollick

Secure Mobile Networking Lab, Technical University of Darmstadt, Germany

Abstract

Apple controls one of the largest mobile ecosystems, with 1.5 billion active devices worldwide, and offers twelve proprietary wireless *Continuity* services. Previous works have unveiled several security and privacy issues

improve the user experience, wireless protocol designs and implementations offer a large surface for attacks. This has been demonstrated via numerous attacks against standardized protocols, e.g.

Ghost Peak

Ghost Peak:
Practical Distance Reduction Attacks Against HRP UWB Ranging

Patrick Leu[1,*], Giovanni Camurati[1,*], Alexander Heinrich[2], Marc Roeschlin[1], Claudio Anliker[1], Matthias Hollick[2], Srdjan Capkun[1], and Jiska Classen[2]

[1]ETH Zurich
[2]TU Darmstadt
[*]Authors contributed equally to this research

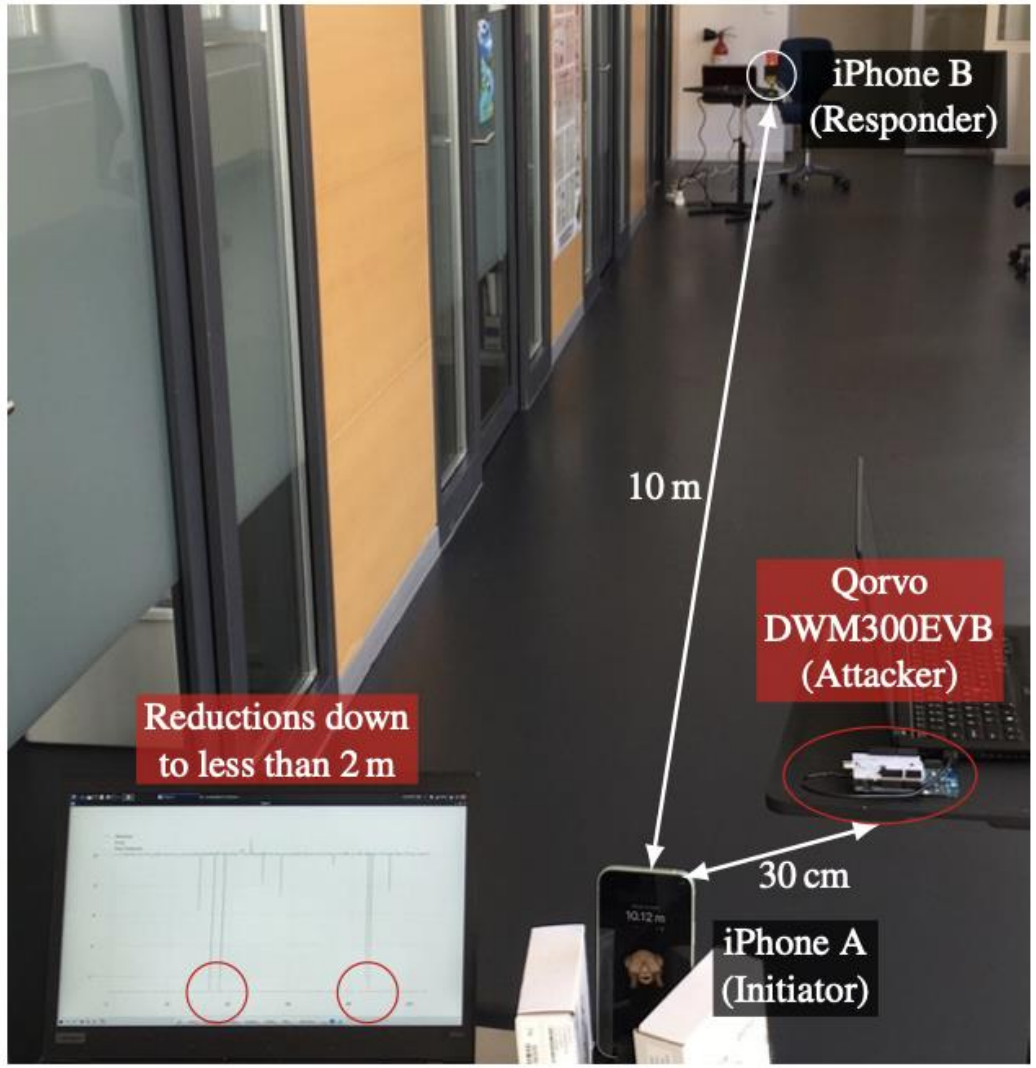
Abstract

We present the first over-the-air attack on IEEE 802.15.4z High-Rate Pulse Repetition Frequency (HRP) Ultra-Wide Band (UWB) distance measurement systems. Specifically, we demonstrate a practical distance reduction attack against pairs of Apple U1 chips (embedded in iPhones and AirTags), as well as against U1 chips inter-operating with NXP and Qorvo UWB chips. These chips have been deployed in a wide range of phones and cars to secure car entry and start and are projected for secure contactless payments, home locks, and contact tracing systems. Our attack operates without any knowledge of cryptographic material, results in distance reductions from 12 m (actual distance) to 0 m (spoofed distance) with attack success probabilities of up to 4 %, and requires only an inexpensive (USD 65) off-the-shelf device. Access control can only tolerate sub-second latencies to not inconvenience the user, leaving little margin to perform time-consuming verifications. These distance reductions bring into question the use of UWB HRP in security-critical applications.

as Samsung phones and SmartTags [10, 51, 55]. Despite its standardization and deployment, no public example implementations or standardized algorithms for security-relevant functionality exist. IEEE 802.15.4z focuses on message formats without mandating in detail how ranging is done and protected at the endpoints.

This paper demonstrates the first practical over-the-air distance reduction attack against the UWB IEEE 802.15.4z HRP mode. Even though HRP security has been recently studied, these studies were done in simulations [58]. We refine existing attacks, introduce a new one, and demonstrate their feasibility in practical settings with Apple U1 (iPhone/AirTag/HomePod), NXP Trimension SR040/SR150, and Qorvo DWM3000 chips. Our attack enabled a successful distance reduction of up to 12 m with an overall success rate of 4 %, which is higher than what is generally accepted for relevant applications. Typically, false acceptance rates are $1/2^{20}$ for gate access control and $1/2^{48}$ for mobile payments, such that it would take days to years until a fake measurement gets accepted.

Manufacturers advertise some of the evaluated chips as



New “Security” Feature (iOS 15)

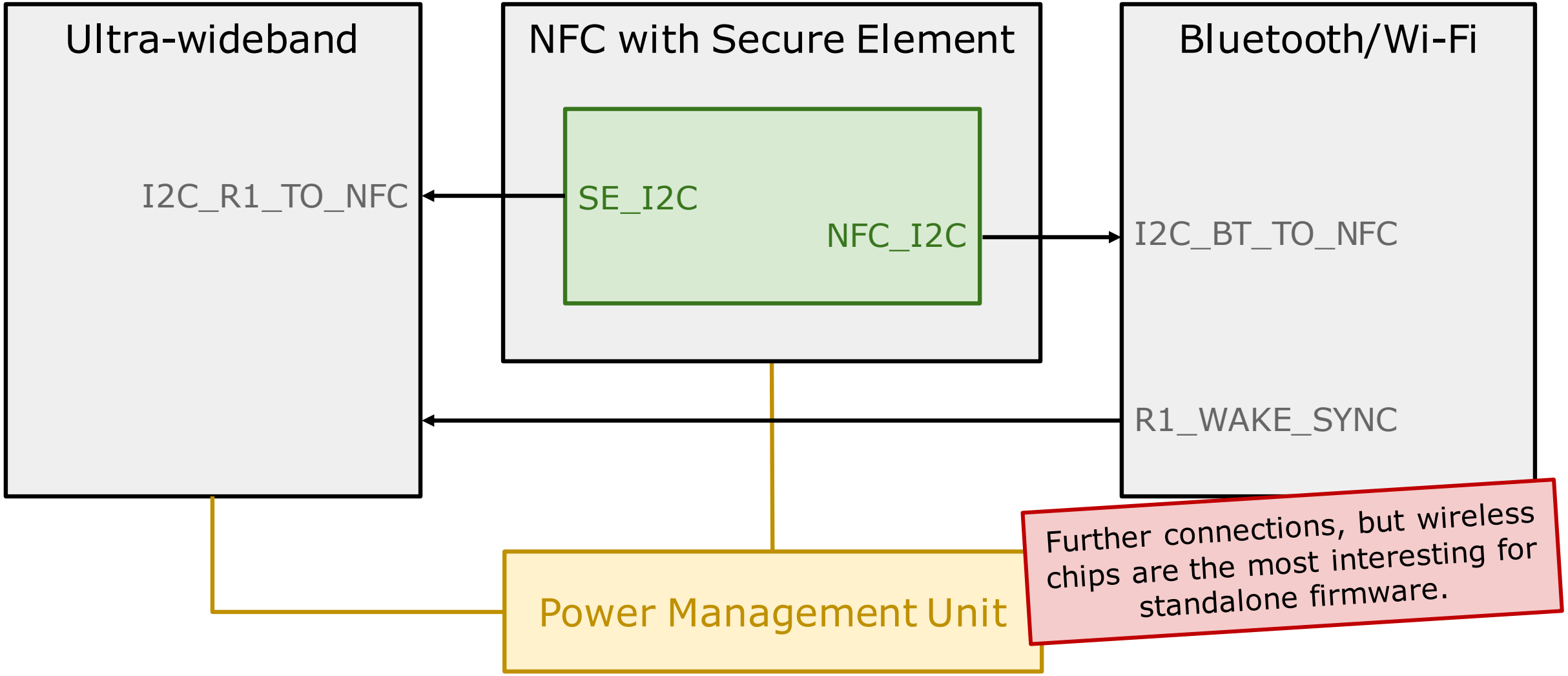
heise online heise+

iPhone aus, Funk bleibt an: Sicherheitsforscher sehen neue Angriffsfläche

Auf einem abgeschalteten iPhone kann Malware laufen, warnt ein Forschungsteam der TU Darmsta
Low-Power-Mode fehlen Schutzvorkehrungen.

Lesezeit: 3 Min. speichern

Hardware Changes (iPhone 11 and Newer)



Apple Platform Security

Communities Contact Support

Table of Contents ⊕

Express Cards with power reserve

If iOS isn't running because iPhone needs to be charged, there may still be enough power in the battery to support Express Card transactions. Supported iPhone devices automatically support this feature with:

- A payment or transit card designated as the Express Transit card
- Student ID cards with Express Mode turned on
- Car keys with Express Mode turned on
- Home keys with Express Mode turned on
- Hospitality or Corporate access cards with Express Mode turned on

Pressing the side button (or on iPhone SE 2nd generation, the Home button) displays the low-battery icon as well as text indicating that Express Cards are available to use. The NFC controller performs Express Card transactions under the same conditions as when iOS is running, except that transactions are indicated only with haptic notification (no visible notification is shown). On iPhone SE 2nd generation, completed transactions may take a few seconds to appear on screen. This feature isn't available when a standard user-initiated shutdown is performed.

Digital Car Key 3.0 supports power reserve and is based on Bluetooth & Ultra-wideband

We showed how to replace the Bluetooth firmware with malware that is powered by PMU

https://support.apple.com/guide/security/express-cards-with-power-reserve-sec90cd29d1f/web

Secure Mobile Networking Lab

Darmstadt, Germany | https://seemoo.de | Verified

Overview | Repositories 80 | Projects | Packages | People 12

Pinned

nexmon Public
The C-based Firmware Patching Framework for Broadcom/Cypress WiFi Chips that enables Monitor Mode, Frame Injection and much more
C | 1.9k | 397

opendrop Public
An open Apple AirDrop implementation written in Python
Python | 7k | 213

openhaystack Public
Build your own 'AirTags' 🏷️ today! Framework for tracking personal Bluetooth devices via Apple's massive Find My network.
Swift | 5.1k | 261

internalblue Public
Bluetooth experimentation framework for Broadcom and Cypress chips.
Python | 514 | 62

frankenstein Public
Broadcom and Cypress firmware emulation for fuzzing and further full-stack debugging
C | 349 | 55

AirGuard Public
Protect yourself from being tracked 🌍 by AirTags 🏷️ and Find My accessories 📍
Kotlin | 1.2k | 63

THE VERGE TECH SCIENCE ENTERTAINMENT MORE

APPLE \ APPS \ TECH

OpenHaystack is a new open-source tool that lets you create DIY AirTags on Apple's Find My network

You'll need a Mac, a BBC micro:bit, and some determination

By Dieter Bohn | @backlon | Mar 4, 2021, 12:07pm EST

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

SHARE

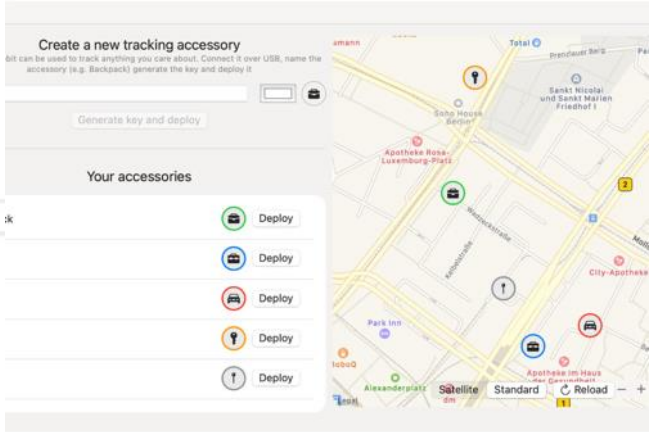


Image: OpenHaystack

Many Thanks For Your Attention

- For further information
  - https://seemoo.de
  - https://github.com/seemoo-lab

Time for Discussion

- For further information
  - https://seemoo.de
  - https://github.com/seemoo-lab

- Or contact me via eMail
  - mhollick@seemoo.tu-darmstadt.de