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?

1. Looses Internet connection
What is offline finding?

1. Looses Internet connection
2. Announces *lost mode* via Bluetooth even in sleep and airplane mode
What is offline finding?

1. Looses Internet connection
2. Announces *lost mode* via Bluetooth even in sleep and airplane mode
3. Determines own location via GPS or other means of localization

“The Crowd”
What is offline finding?

1. Loses Internet connection
2. Announces *lost mode* via Bluetooth even in sleep and airplane mode
3. Determines own location via GPS or other means of localization
4. Reports location back to owner

“The Crowd”
What is offline finding?

1. Looses Internet connection
2. Announces *lost mode* via Bluetooth even in sleep and airplane mode
3. Determines own location via GPS or other means of localization
4. Reports location back to owner
5. Queries location of lost device
What are potential privacy issues?

Concern 1: My devices can be tracked by others!
What are potential privacy issues?

Concern 2: My phone shares its location with others!

3. Determines own location via GPS or other means of localization

4. Reports location back to owner

5. Queries location of lost device

1. Loose Internet connection

2. Announces lost mode via Bluetooth

Concern 3: My phone shares its location with others!
What are potential privacy issues?

1. Looses Internet connection
2. Announces lost mode via Bluetooth
3. Determines own location via GPS or other means of localization
4. Reports location back to owner
5. Queries location of lost device

Concern 3: Apple/somebody knows the location of my devices!
How can we solve these issues?

1. Loose Internet connection

2. Announces lost mode via Bluetooth

3. Determines own location via GPS or other means of localization

4. Reports location back to owner

5. Queries location of lost device

Solution 1: Use unlinkable pseudonyms
How can we solve these issues?

Solution 2: Report location anonymously

1. Looses Internet connection
2. Announces lost mode via Bluetooth
3. Determines own location via GPS or other means of localization
4. Reports location back to owner
5. Queries location of lost device
How can we solve these issues?

1. Looses Internet connection
2. Announces lost mode via Bluetooth
3. Determines own location via GPS or other means of localization
4. Reports location back to owner
5. Queries location of lost device

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 also on Android?

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

Alexander Heyrich
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
alexander@securhoc.de

Nikolas Bittker
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
nibtker@securhoc.de

Matthias Holleck
Secure Mobile Networking Lab
Department of Computer Science
TU Darmstadt, Germany
mail@holleck.de

ABSTRACT
Finders networks is basically said Apple’s Find My network in particular, can pose a privacy threat to users’ privacy and even health if those networks are abused for stalking. Apple’s release of the Find My network—amplified this issue. While Apple provides a tool to detect, this approach cannot be implemented within Android. In the dark, Apple recently released the Android app “AirGuard” which allows users to detect and block tracking notifications on their devices.
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

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."
Apple Ecosystem – Behind The Scenes of „Just Works“

- 300+ running processes
- 4 wireless interfaces
- 1,500+ dynamically linked libraries
- 10,000+ logs per minute

Continuous Interfaces:
- AirDrop [SNM+19] [HHSSW21]
- Universal Clipboard [SHLH21]
- Handoff [SHLH21]
- Wi-Fi Password Sharing [SHLH21]
Ghost Peak:
Practical Distance Reduction Attacks Against HRP UWB Ranging

Patrick Leu\textsuperscript{1,}\textsuperscript{*}, Giovanni Camurati\textsuperscript{1,}\textsuperscript{*}, Alexander Heinrich\textsuperscript{2}, Marc Roeschlin\textsuperscript{3}, Claudio Anliker\textsuperscript{1}, Matthias Hollick\textsuperscript{2}, Srđan Capkun\textsuperscript{1}, and Jiska Classen\textsuperscript{2}

\textsuperscript{1}ETH Zurich
\textsuperscript{2}TU Darmstadt
\textsuperscript{*}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 \cite{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 \cite{59}. 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 DW43000 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 \$\Psi_{off}$ for gate access control and \$\Psi_{off}$ 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)
Hardware Changes (iPhone 11 and Newer)

Ultra-wideband
- I2C_R1_TO_NFC

NFC with Secure Element
- SE_I2C
- NFC_I2C

Bluetooth/Wi-Fi
- I2C_BT_TO_NFC
- R1_WAKE_SYNC

Power Management Unit

Further connections, but wireless chips are the most interesting for standalone firmware.
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 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

Secure Mobile Networking Lab

Pinned

- **nexmon** (Public)
  The C-based Firmware Patching Framework for Broadcom/Cypress WiFi Chips that enables Monitor Mode, Frame Injection and much more
  - **C**
  - GitHub stars: 1.9k
  - Issues: 397

- **open Haystack** (Public)
  Build your own AirTags today! Framework for tracking personal Bluetooth devices via Apple's massive Find My network.
  - **Swift**
  - GitHub stars: 5.1k
  - Issues: 261

- **opendrop** (Public)
  An open Apple AirDrop implementation written in Python
  - **Python**
  - GitHub stars: 7k
  - Issues: 213

- **internalblue** (Public)
  Bluetooth experimentation framework for Broadcom and Cypress chips.
  - **Python**
  - GitHub stars: 514
  - Issues: 62

- **frankenstein** (Public)
  Broadcom and Cypress firmware emulation for fuzzing and further full-stack debugging
  - **C**
  - GitHub stars: 349
  - Issues: 55

- **AirGuard** (Public)
  Protect yourself from being tracked by AirTags and Find My accessories
  - **Kotlin**
  - GitHub stars: 1.2k
  - Issues: 63

---

**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.

---

Create a new tracking accessory

Your accessories

1. Display
2. Display
3. Display
4. Display
5. Display
6. Display
7. Display
8. Display
9. Display
10. Display

---

Image: OpenHaystack

---

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