Breaking the Mirror

A Look at Apple’s New iPhone Remote Control Feature

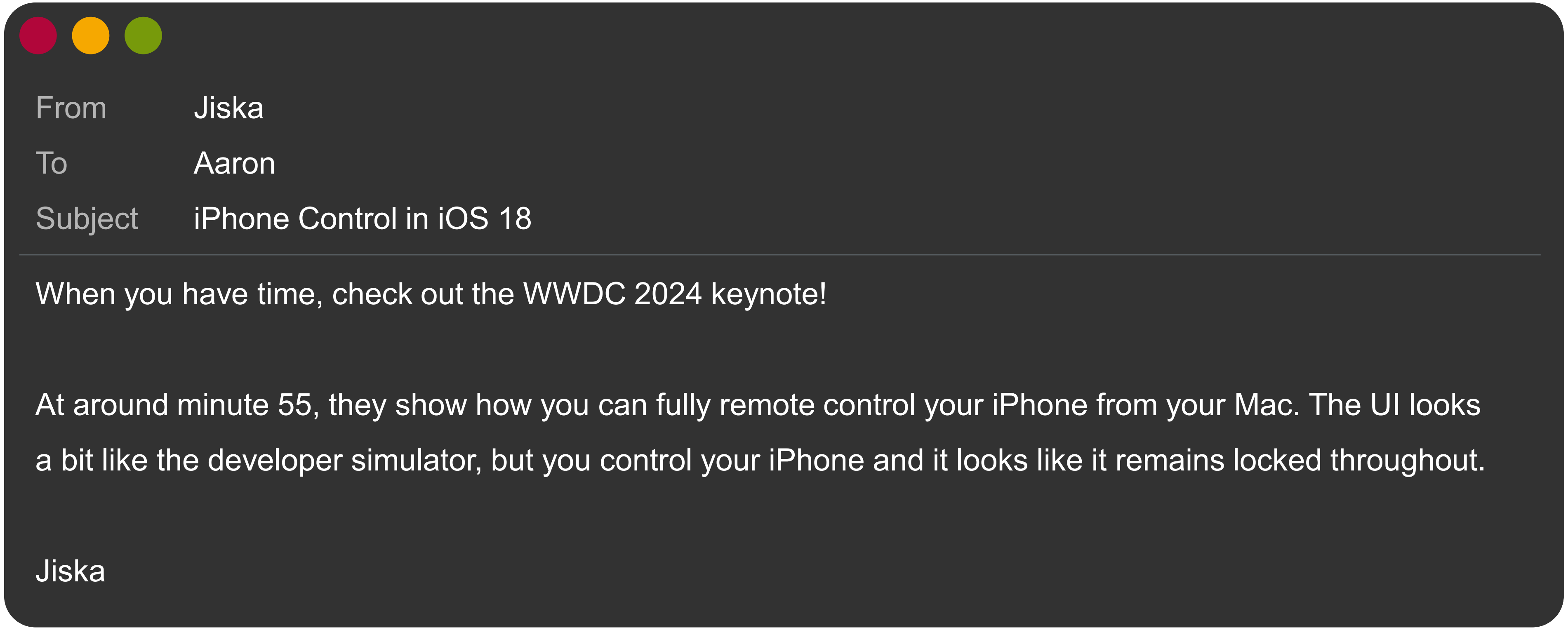
Aaron Schlitt
Cybersecurity – Mobile Security
Hasso Plattner Institute, University of Potsdam

Who am I

- Aaron Schlitt
- Cybersecurity M.Sc. Student at Hasso Plattner Institute, Uni Potsdam
- Researcher at *Cybersecurity – Mobile Security* chair of Jiska Classen

How It Started

*approximately



From Jiska

To Aaron

Subject iPhone Control in iOS 18

When you have time, check out the WWDC 2024 keynote!

At around minute 55, they show how you can fully remote control your iPhone from your Mac. The UI looks a bit like the developer simulator, but you control your iPhone and it looks like it remains locked throughout.

Jiska

User Experience

iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health
Notification
11m ago

Journal
Notification
41m ago

User Experience

TIME SENSITIVE
Medications Reminder
Time to log your 9:30 AM medications

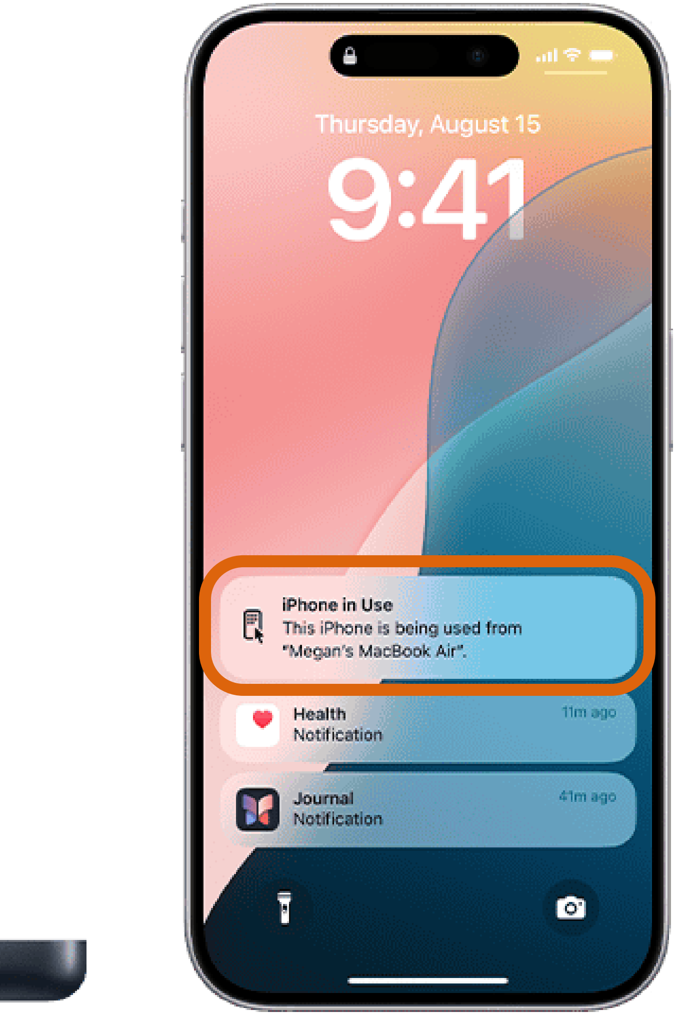
Time to Write
Take a moment to reflect in your journal.

iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health
Notification
11m ago

Journal
Notification
41m ago

Awareness Features in iOS



Thursday, August 15

9:41

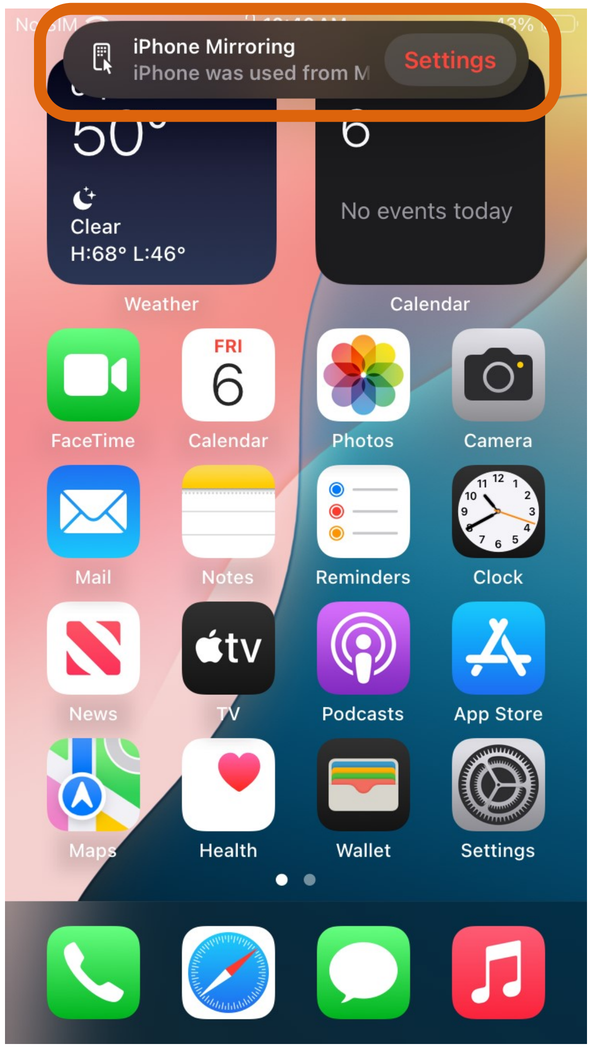
iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health
Notification
11m ago

Journal
Notification
41m ago

Permanent notification on lock screen

Notification after next unlock



iPhone Mirroring
iPhone was used from M

AirDrop

Handoff

Continuity Camera

Sidecar

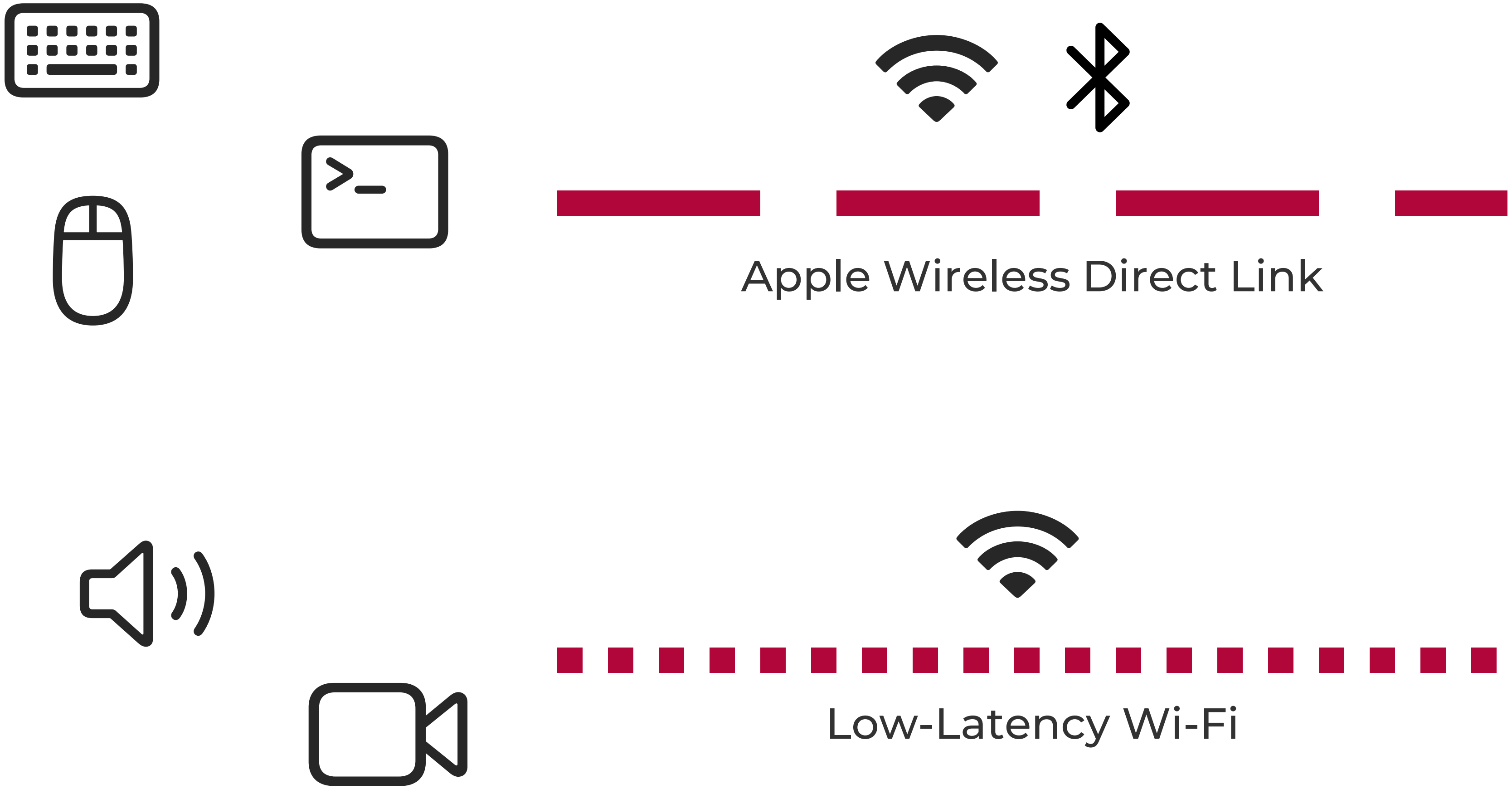
Apple Continuity

Universal Clipboard

What’s behind this?

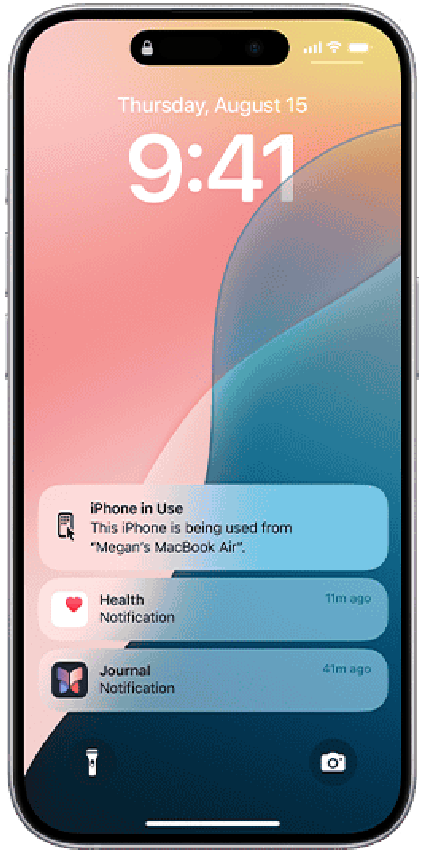
(with a lot of knowledge from Inga Dischinger’s work)

AWDL and LLW



Apple Wireless Direct Link

Low-Latency Wi-Fi



Thursday, August 15

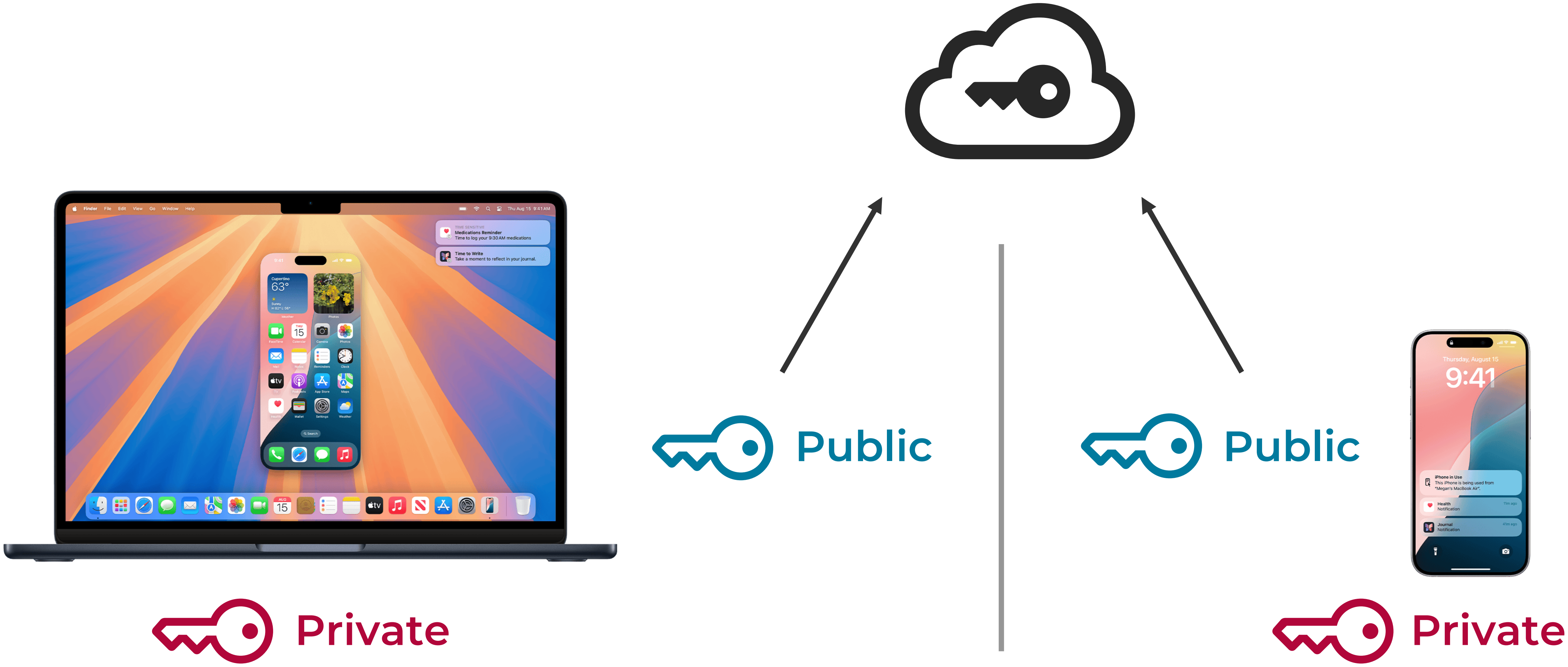
9:41

iPhone in Use
This iPhone is being used from
"Megan's MacBook Air".

Health
Notification
11m ago

Journal
Notification
41m ago

AWDL Key Management



Public

Public

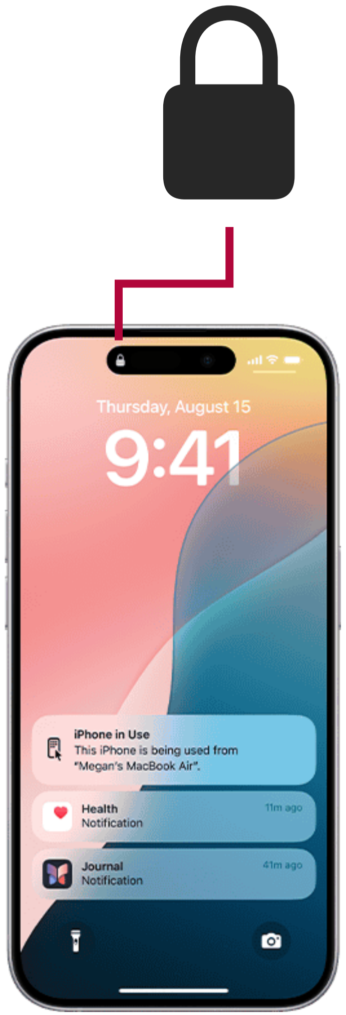
Private

Private

Threat Model

Finder File Edit View Go Window Help
Mon Jun 10 9:41 AM
iPhone Mirroring

Is my iPhone Locked?



Thursday, August 15

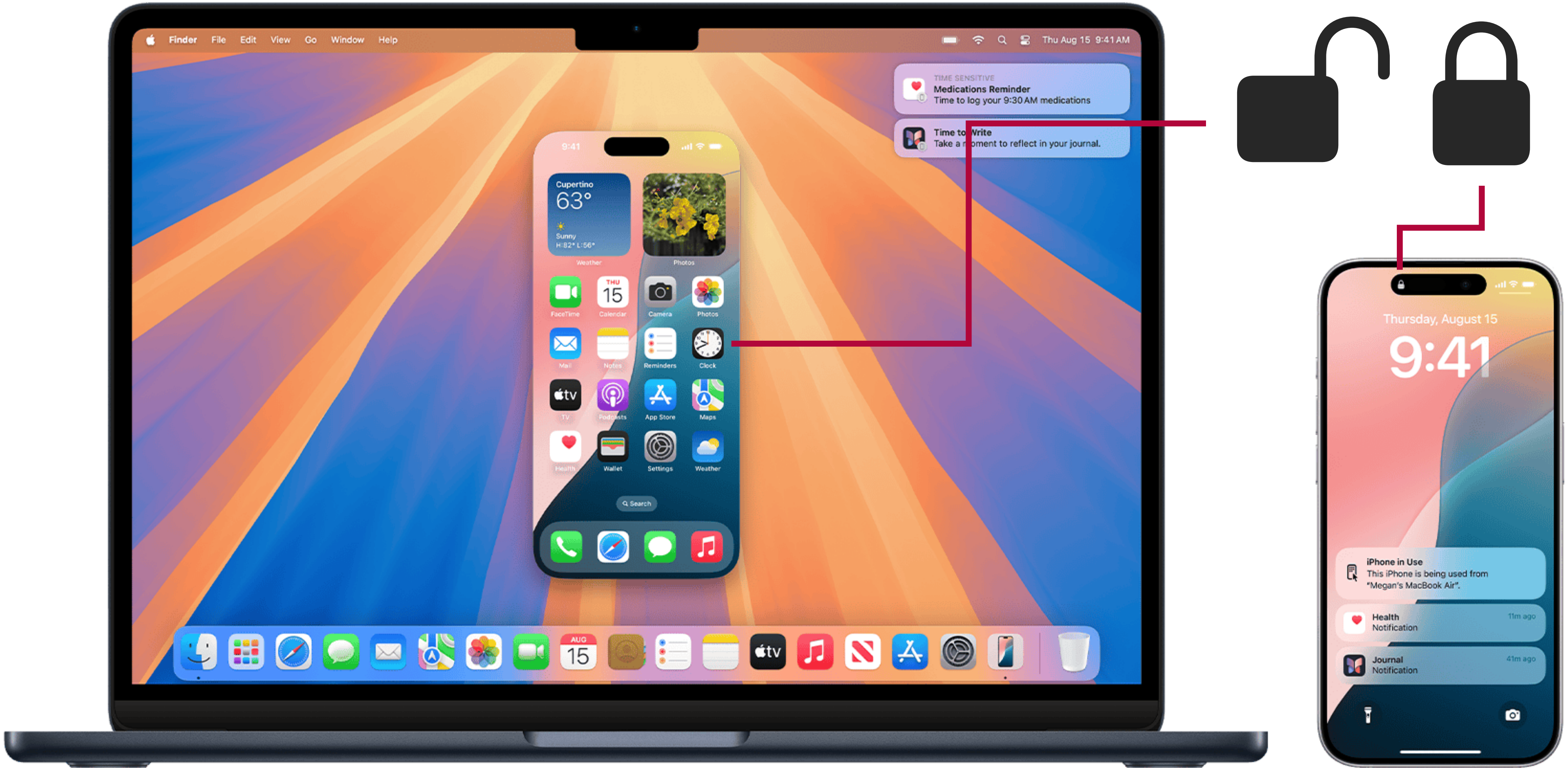
9:41

iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health 11m ago
Notification

Journal 41m ago
Notification

Is my iPhone Locked?



TIME SENSITIVE
Medications Reminder
Time to log your 9:30 AM medications

Time to Write
Take a moment to reflect in your journal.

iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health
Notification

Journal
Notification

Threat Model of iPhone Mirroring

No camera access

No microphone access

No PIN/Biometrics settings Access

No app/data access

Remote control is obvious to users

iPhones must remain secure while they are remote controlled.

iPhones might be accessed unwantedly and should provide safeguards against misuse in this case.

macOS as Attack Surface for iOS

- Previously: Very limited access to iOS devices from macOS
- Mainly via data shared over iCloud

- macOS: Far more open approach than iOS
  - Can run unsigned software
  - Can disable security features (SIP)

→Higher risk for malware and abuse

iPhone Mirroring could create a direct path from macOS compromise to iPhone compromise

Swapping AWDL Keys with FRIDA

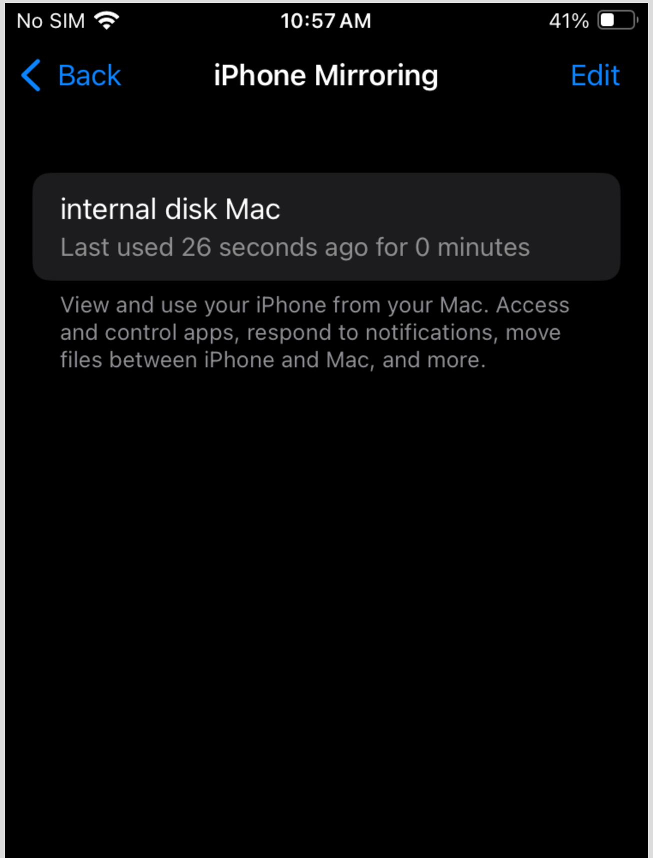
- Requires (multiple) SIP-disabled Macs
- Hook signing functions in rapportd on Mac

FRIDA

- Extract keys on Mac 1
- Insert keys into RAM on Mac 2 before signing function runs

→ iPhone Mirroring still works on a Mac that was previously paired

→ **iPhone Mirroring cannot be tricked into talking to an unpaired Mac**



internal disk Mac
Last used 26 seconds ago for 0 minutes

View and use your iPhone from your Mac. Access and control apps, respond to notifications, move files between iPhone and Mac, and more.

Future Work: Additional Cryptography in iPhone Mirroring

?

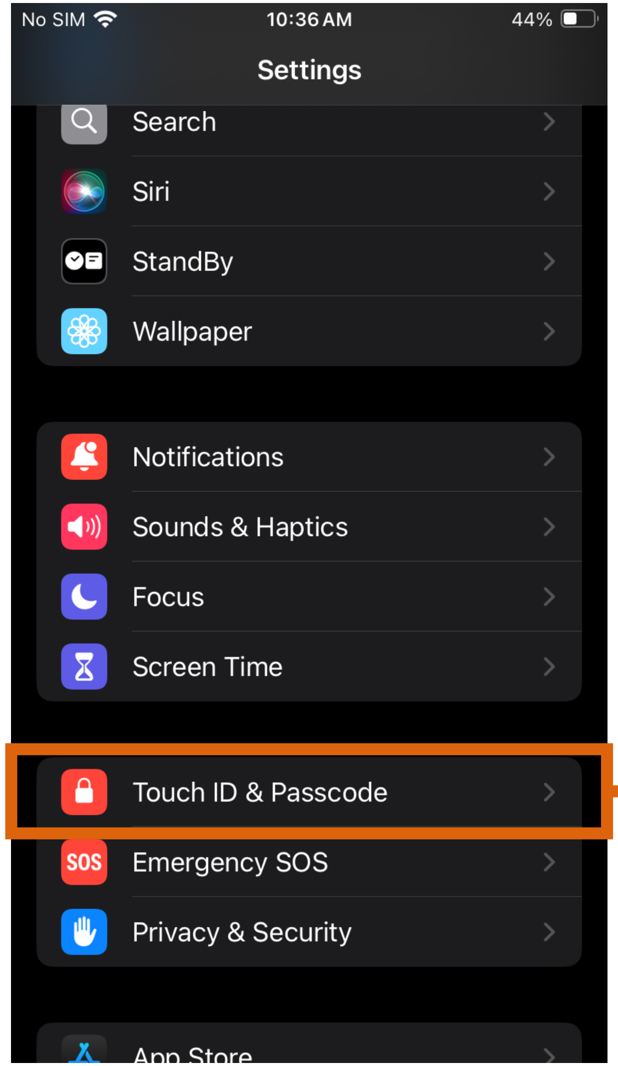
- Security Hardware might be used
- Very hardware-dependent firmware

Implementation Issues

Schrödinger’s iPhone

iPhone Mirroring Effects in iOS

On the iPhone



No SIM 10:36 AM 44%

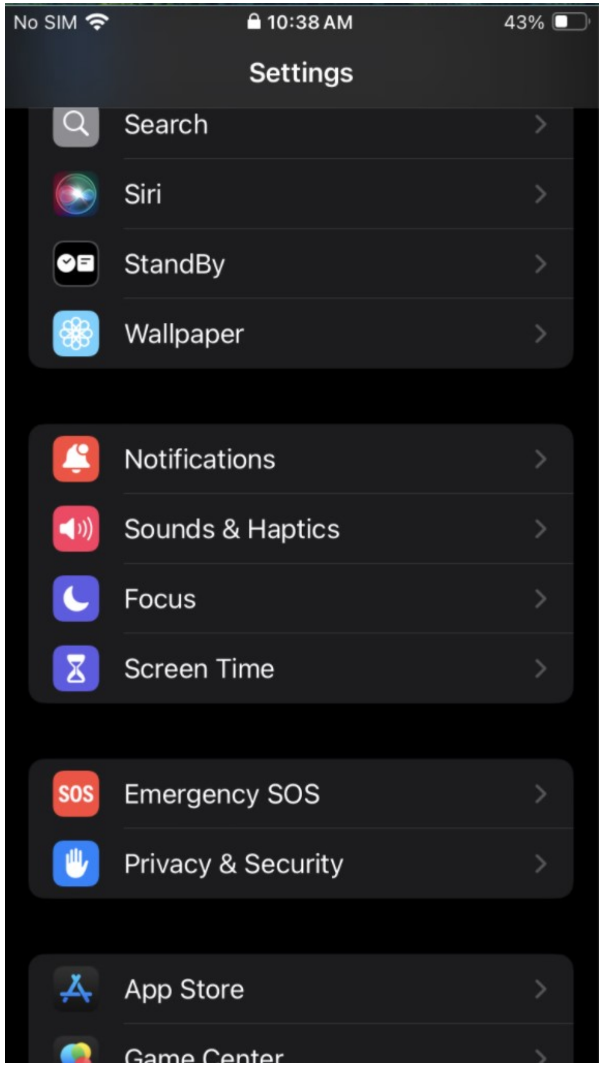
Settings

- Search
- Siri
- StandBy
- Wallpaper

- Notifications
- Sounds & Haptics
- Focus
- Screen Time

- Touch ID & Passcode
- Emergency SOS
- Privacy & Security

- App Store



No SIM 10:38 AM 43%

Settings

- Search
- Siri
- StandBy
- Wallpaper

- Notifications
- Sounds & Haptics
- Focus
- Screen Time

- Emergency SOS
- Privacy & Security

- App Store
- Game Center

Via iPhone Mirroring

iMac

macOS 15 Beta 2

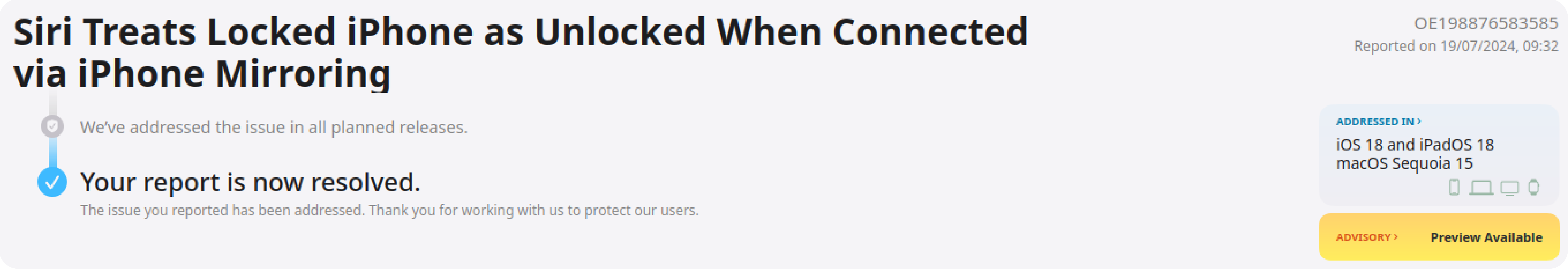
iPhone SE (2020)

iOS 18 Beta 2

Paired to Mac for iPhone Mirroring

Hey Siri!

- iOS 18 Beta 2: Siri treated iPhone as unlocked when connected via Mirroring
- Attackers were able to send and read messages from the lock screen
- Fixed in public release of iOS 18



Siri Treats Locked iPhone as Unlocked When Connected via iPhone Mirroring

OE198876583585
Reported on 19/07/2024, 09:32

We've addressed the issue in all planned releases.

✓ Your report is now resolved.

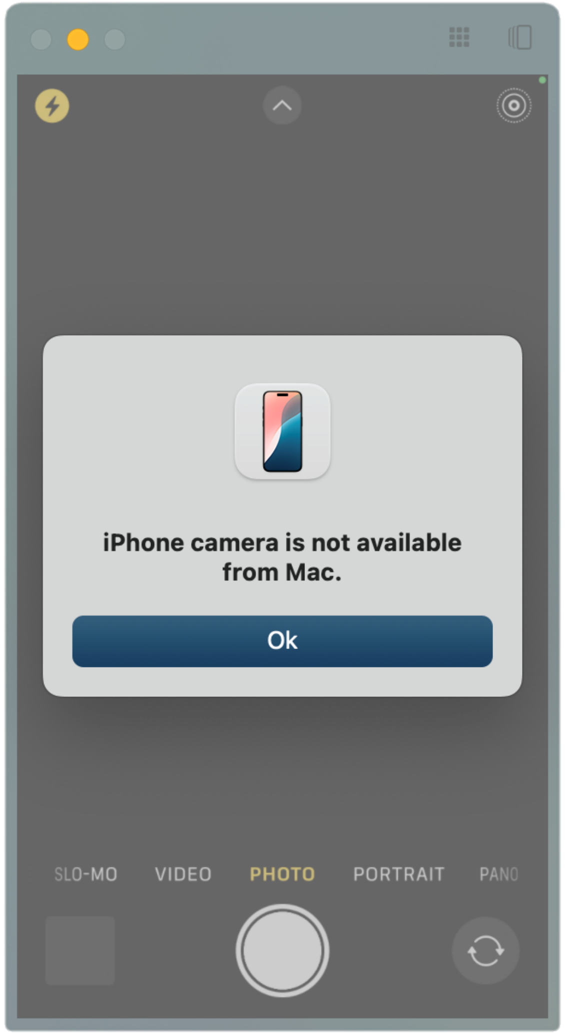
The issue you reported has been addressed. Thank you for working with us to protect our users.

ADDRESSED IN ›

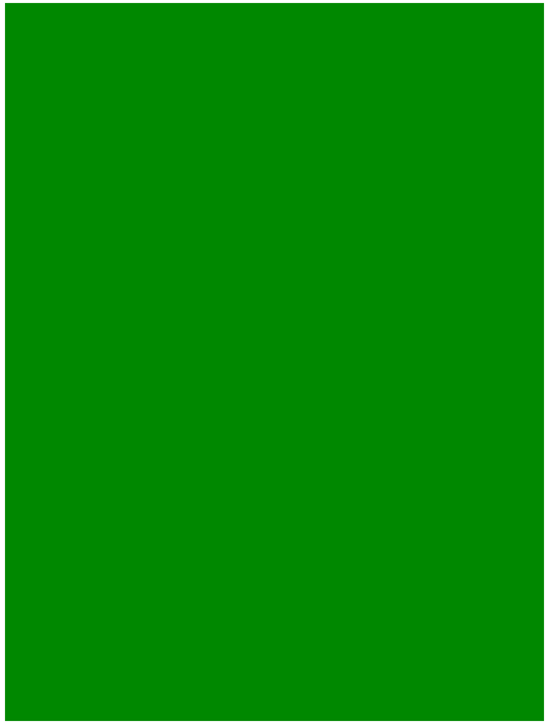
iOS 18 and iPadOS 18
macOS Sequoia 15

ADVISORY › Preview Available

Camera and Microphone Access



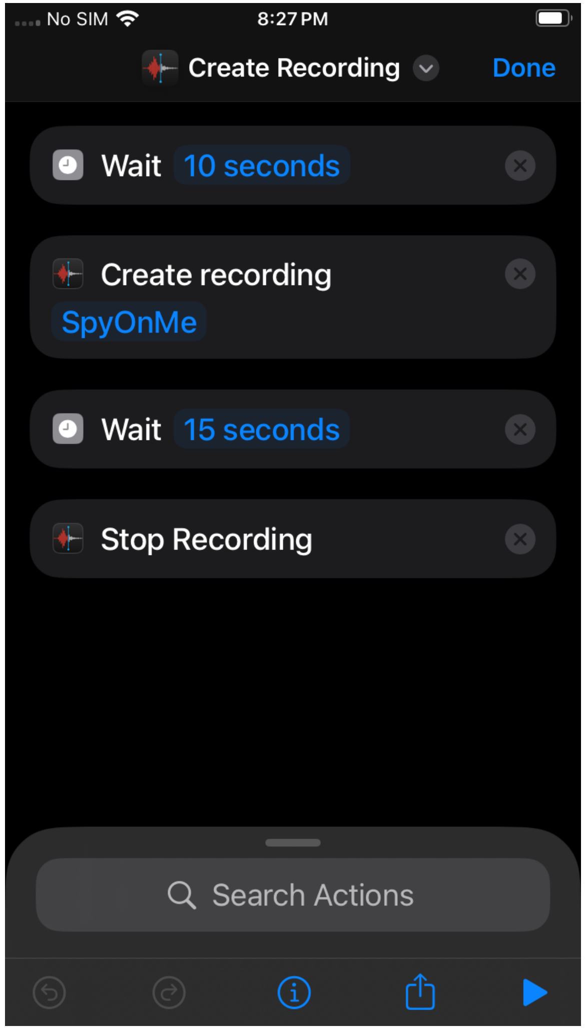
iPhone camera is not available from Mac.



(No, this is not a placeholder)

Prevent Spying using iPhone Mirroring?

Shortcuts to the Rescue!



Create Recording

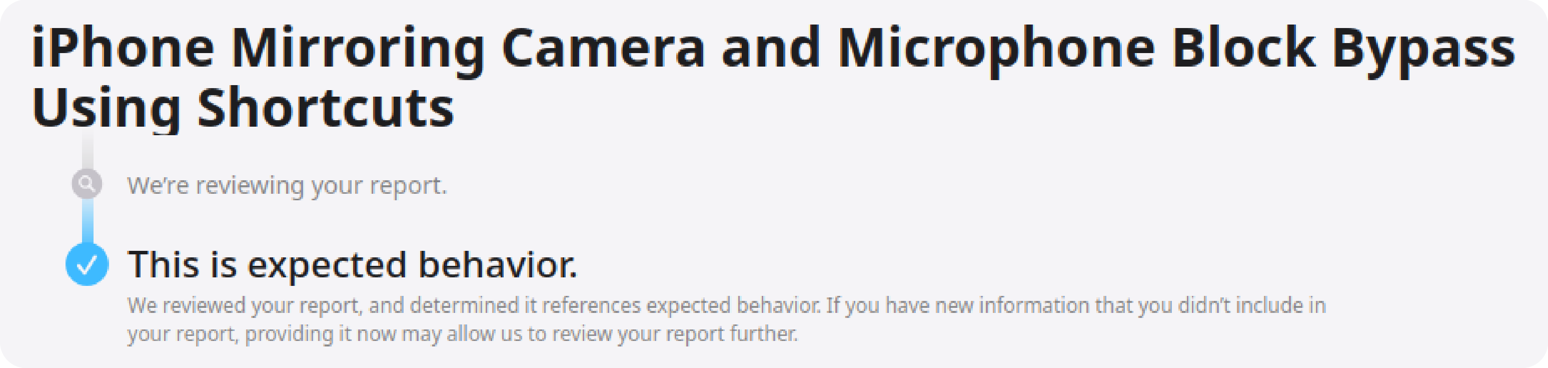
Wait 10 seconds

Create recording SpyOnMe

Wait 15 seconds

Stop Recording

- Create Shortcut with a delay
- Trigger shortcut and disconnect
- Can make recordings and upload them, initiate FaceTime calls



iPhone Mirroring Camera and Microphone Block Bypass Using Shortcuts

We're reviewing your report.

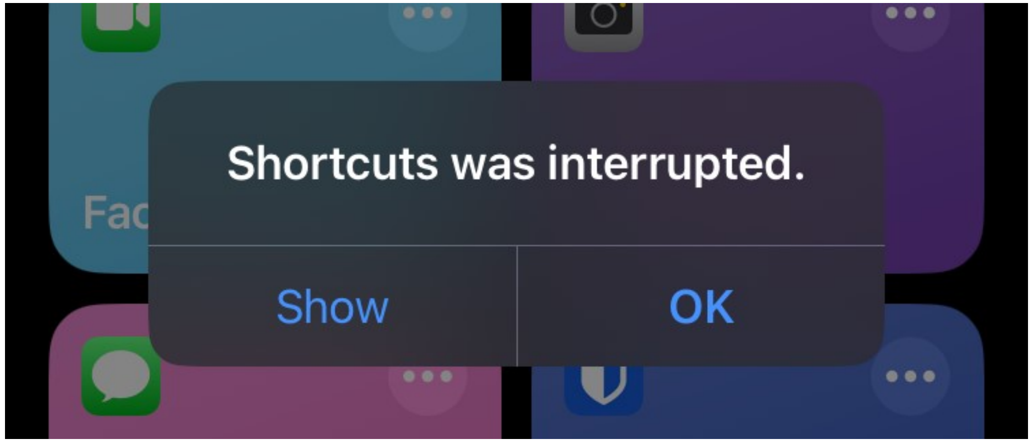
This is expected behavior.

We reviewed your report, and determined it references expected behavior. If you have new information that you didn't include in your report, providing it now may allow us to review your report further.

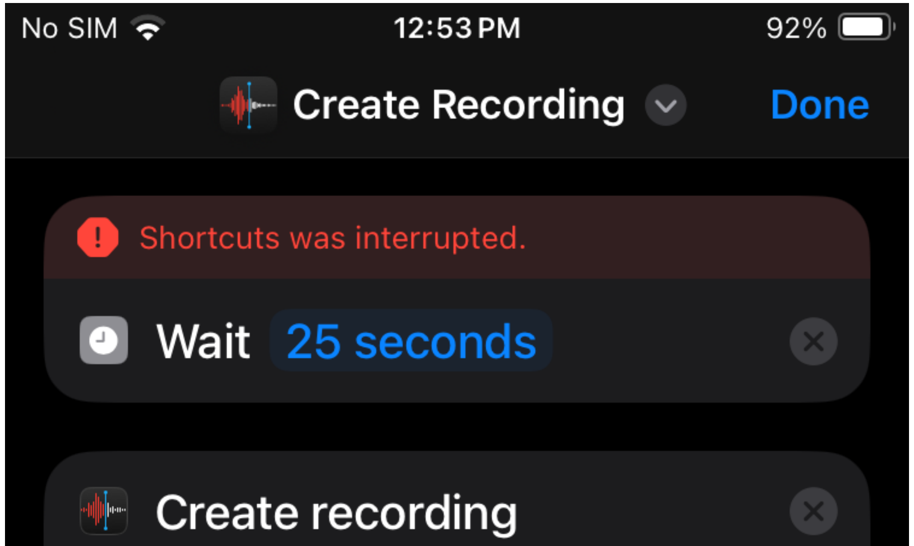
Or So I Thought…

- Reported in July 2024; Closed as *expected behaviour* four days later

- Retesting in December (iOS 18.2) shows that issue has in fact been fixed: All running shortcuts are interrupted when iPhone Mirroring disconnects.



Shortcuts was interrupted.



Shortcuts was interrupted.

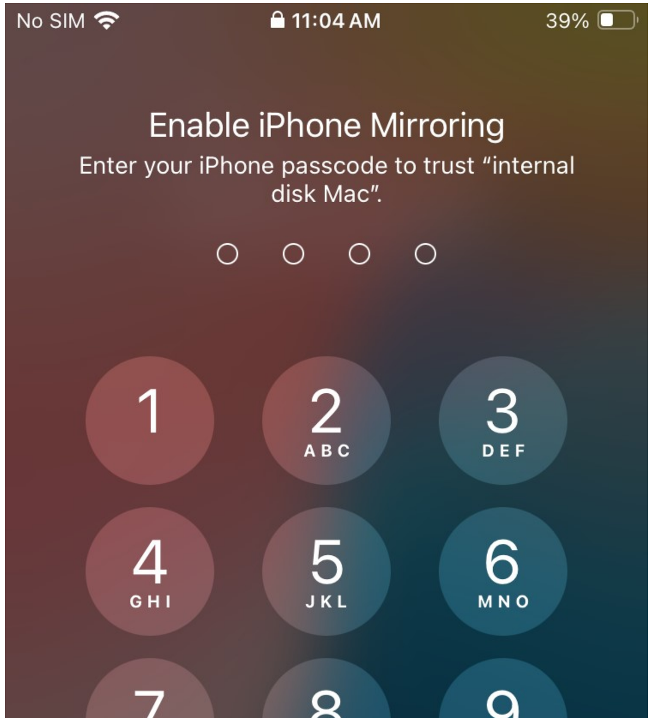
Wait 25 seconds

Create recording

Persisting and Hiding Access

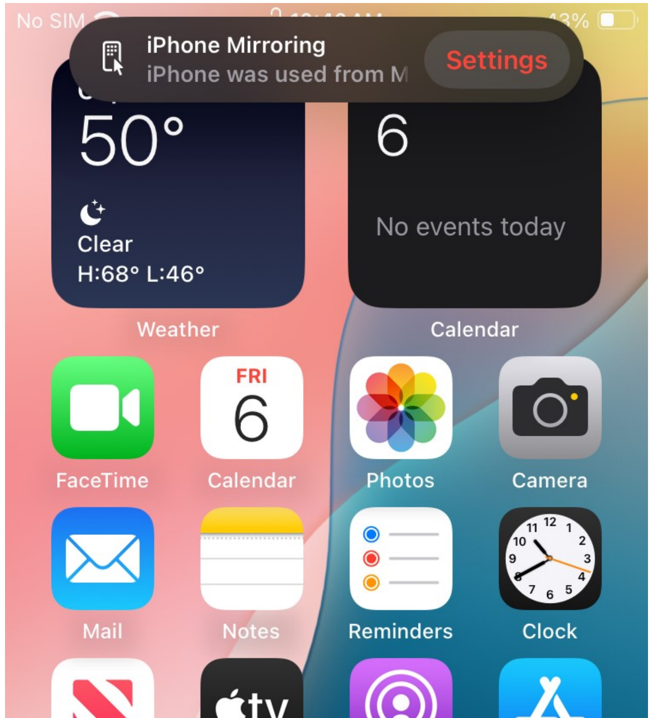
iPhone Mirroring Access is Temporary and Evident

- Regularly re-enter PIN on iPhone
- Notifications for current and past connections
- Connection History

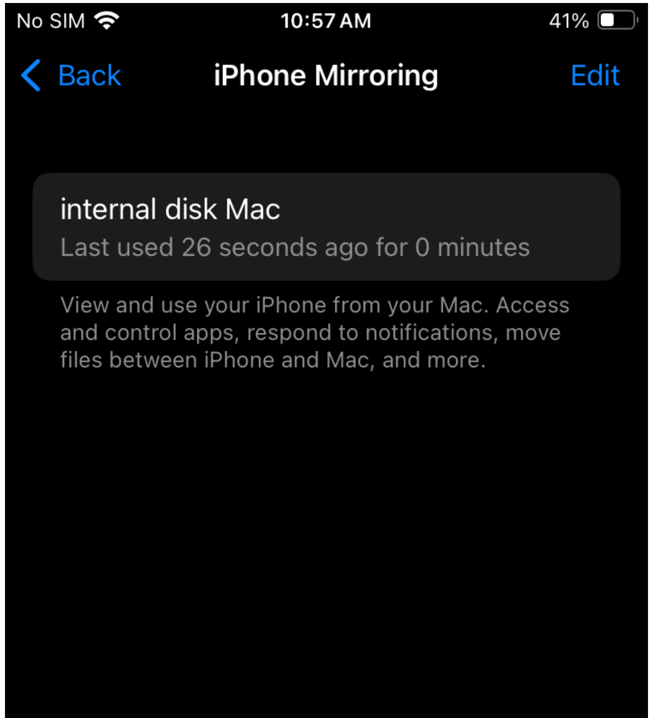


Enable iPhone Mirroring

Enter your iPhone passcode to trust “internal disk Mac”.



iPhone Mirroring
iPhone was used from M



internal disk Mac
Last used 26 seconds ago for 0 minutes

View and use your iPhone from your Mac. Access and control apps, respond to notifications, move files between iPhone and Mac, and more.

iMac

macOS 15

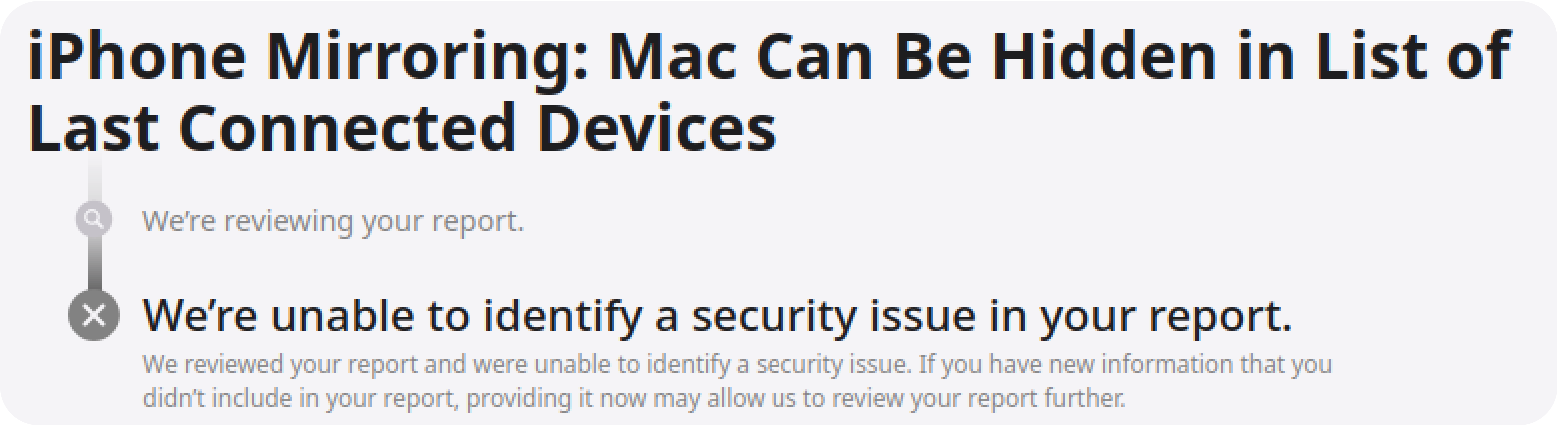
iPhone SE (2020)

iOS 18

Paired to Mac for iPhone Mirroring

Hiding Access

- iPhone Mirroring settings can be accessed from mirroring connection
- Removing all Macs hides the corresponding settings entry and history



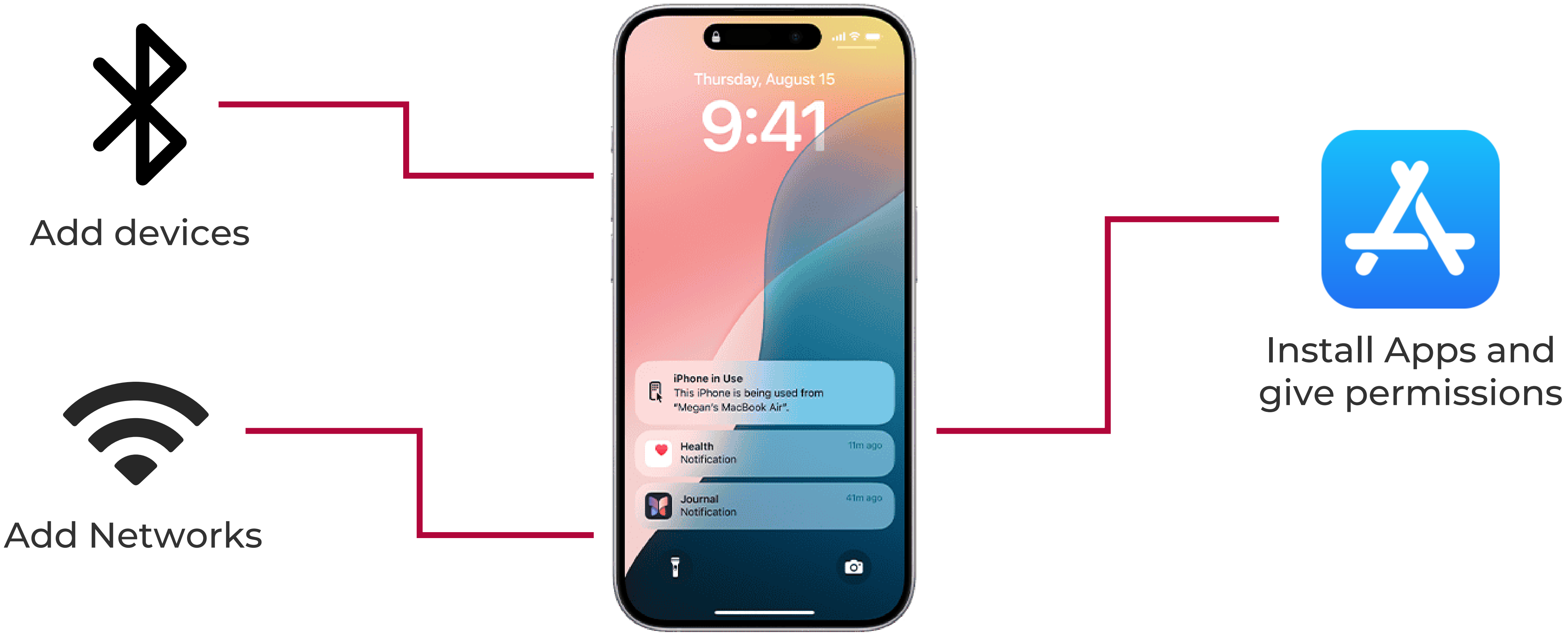
iPhone Mirroring: Mac Can Be Hidden in List of Last Connected Devices

We're reviewing your report.

We're unable to identify a security issue in your report.

We reviewed your report and were unable to identify a security issue. If you have new information that you didn't include in your report, providing it now may allow us to review your report further.

Gaining Persistence



Add devices

Add Networks

Install Apps and give permissions

Thursday, August 15

9:41

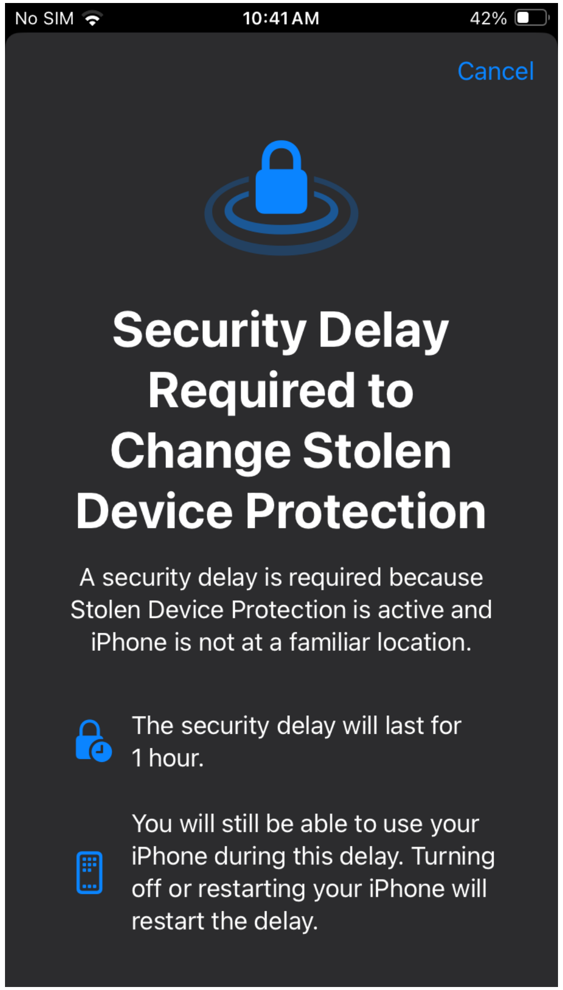
iPhone in Use
This iPhone is being used from "Megan's MacBook Air".

Health
Notification
11m ago

Journal
Notification
41m ago

Stolen Device Protection

Stolen Device Protection



Security Delay Required to Change Stolen Device Protection

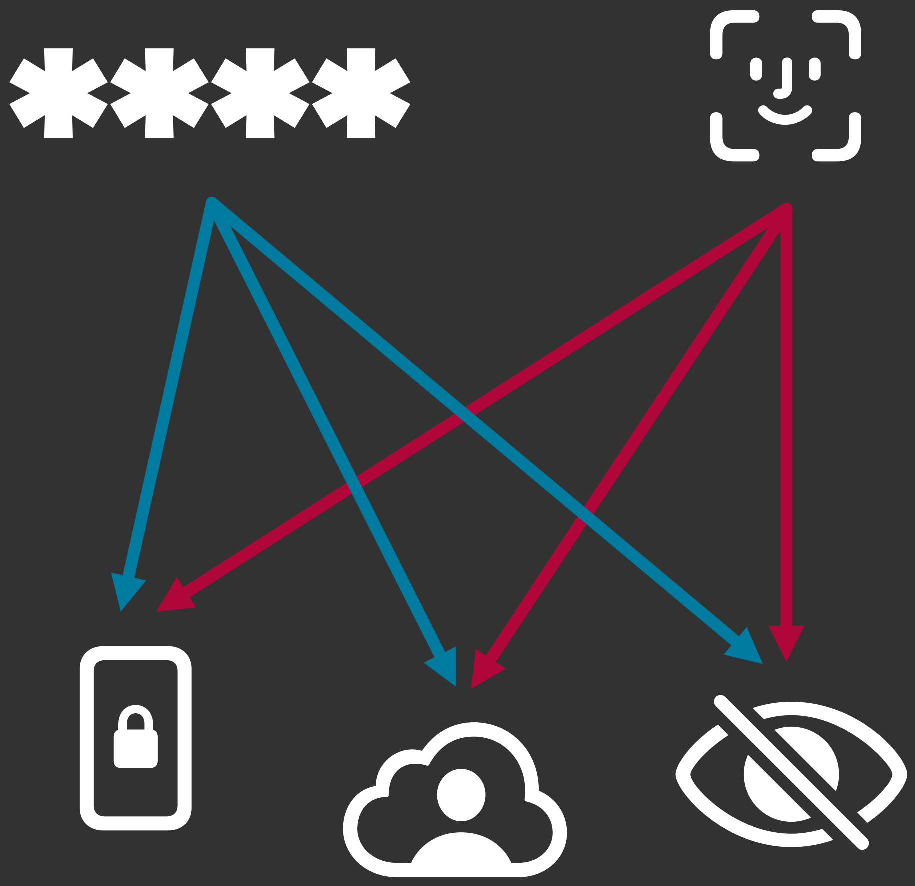
A security delay is required because Stolen Device Protection is active and iPhone is not at a familiar location.

The security delay will last for 1 hour.

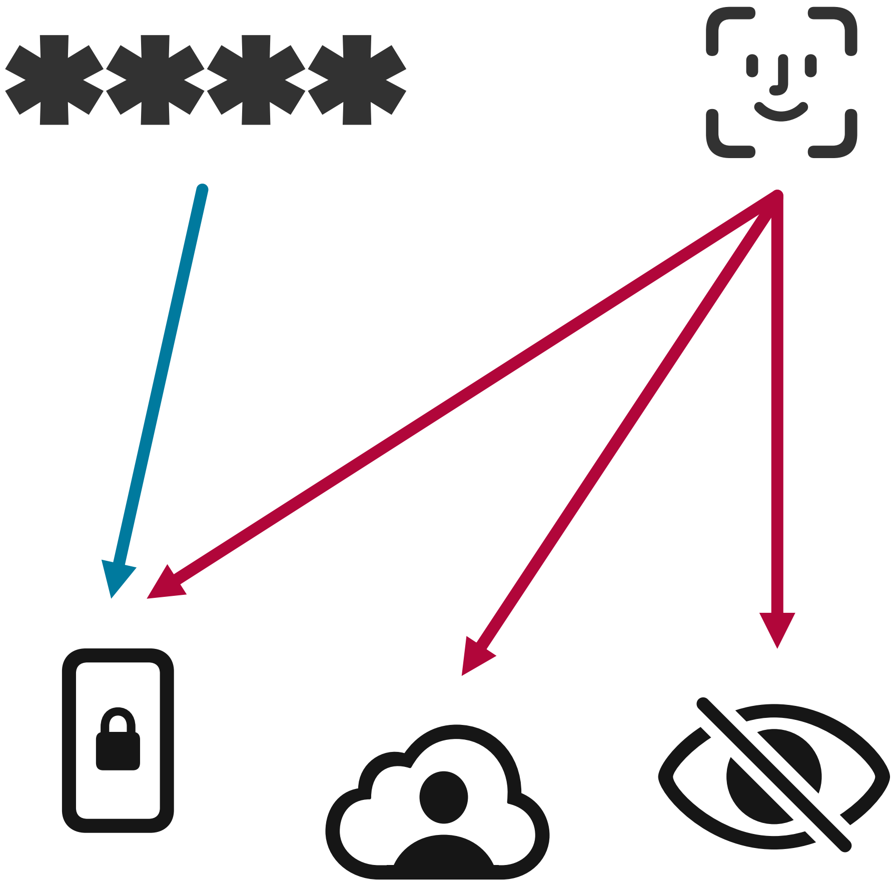
You will still be able to use your iPhone during this delay. Turning off or restarting your iPhone will restart the delay.

- Protects against device theft where PIN might be acquired as well
- Biometrics as the highest-security authentication
  - Required for iCloud password change
  - Required to access locked apps
- Further security features
  - Reboot iPhone after 72h when not unlocked
  - Change iCloud settings only after a timeout

SDP Access Vectors

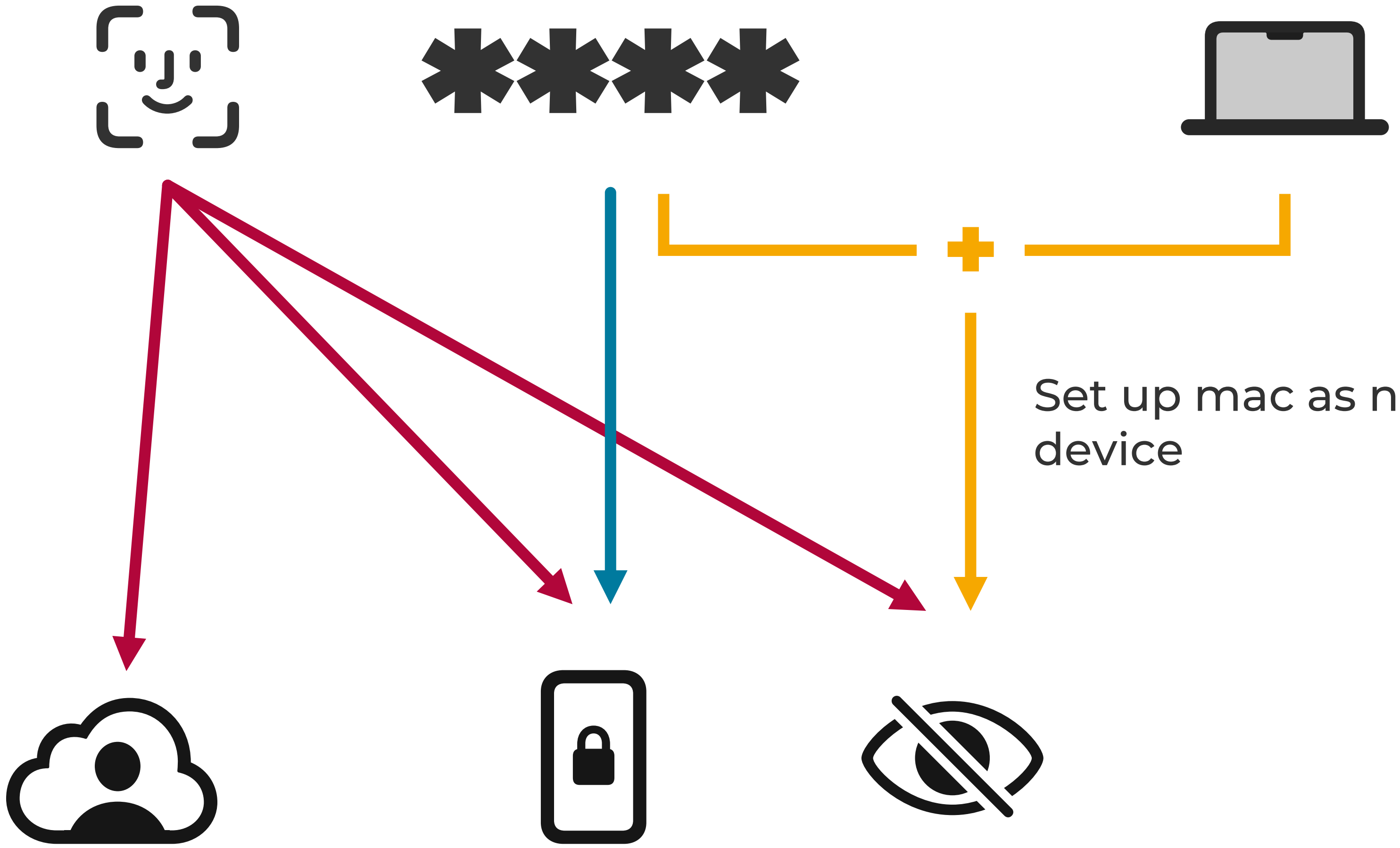


Without SDP



With SDP

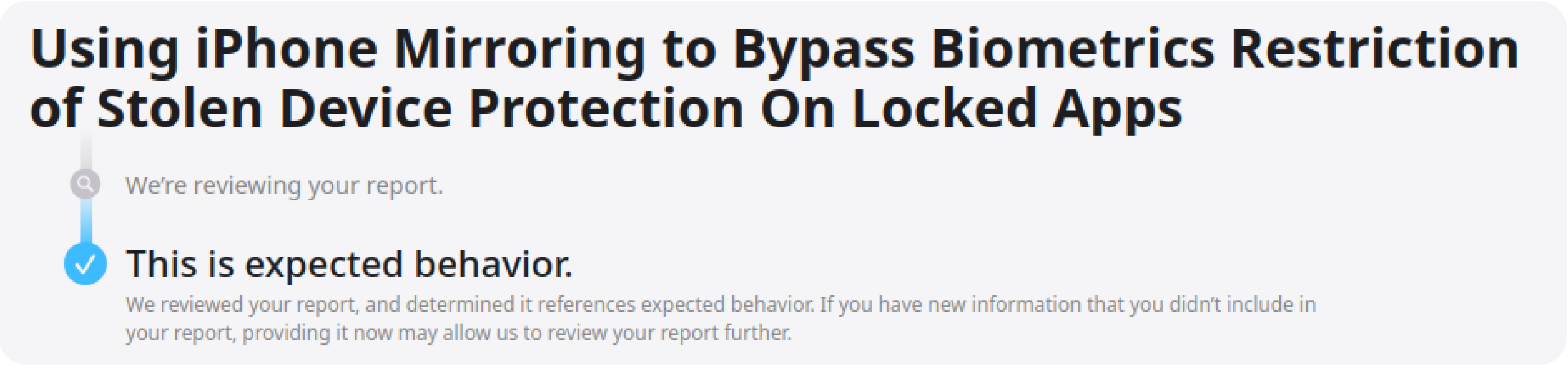
SDP with iPhone Mirroring



Mac signed into same Apple ID

Set up mac as new trusted device

SDP Authentication

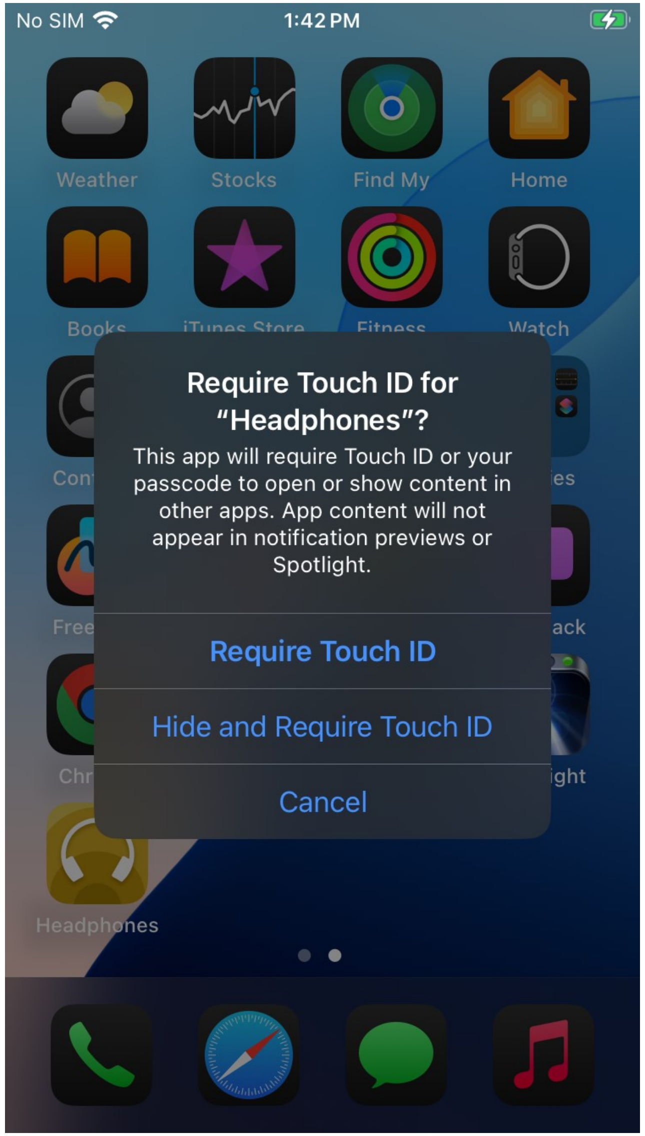


Using iPhone Mirroring to Bypass Biometrics Restriction of Stolen Device Protection On Locked Apps

We're reviewing your report.

✓ This is expected behavior.

We reviewed your report, and determined it references expected behavior. If you have new information that you didn't include in your report, providing it now may allow us to review your report further.



Require Touch ID for “Headphones”?

This app will require Touch ID or your passcode to open or show content in other apps. App content will not appear in notification previews or Spotlight.

Summary

- iPhone Mirroring is a complex and unprecedented feature from a security perspective
- Apple attempted to introduce a number of safeguards

- Initial implementations contained critical bugs
- Apparent threat Model is not implemented consistently

→ **Officially define threat model**

→ **Protect critical resources and don’t allow remote access**

→ **Properly assess reports by researchers**

Questions?

aaronschlitt.de
38c3@aaronschlitt.de
chaos.social/@aaron_els