

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

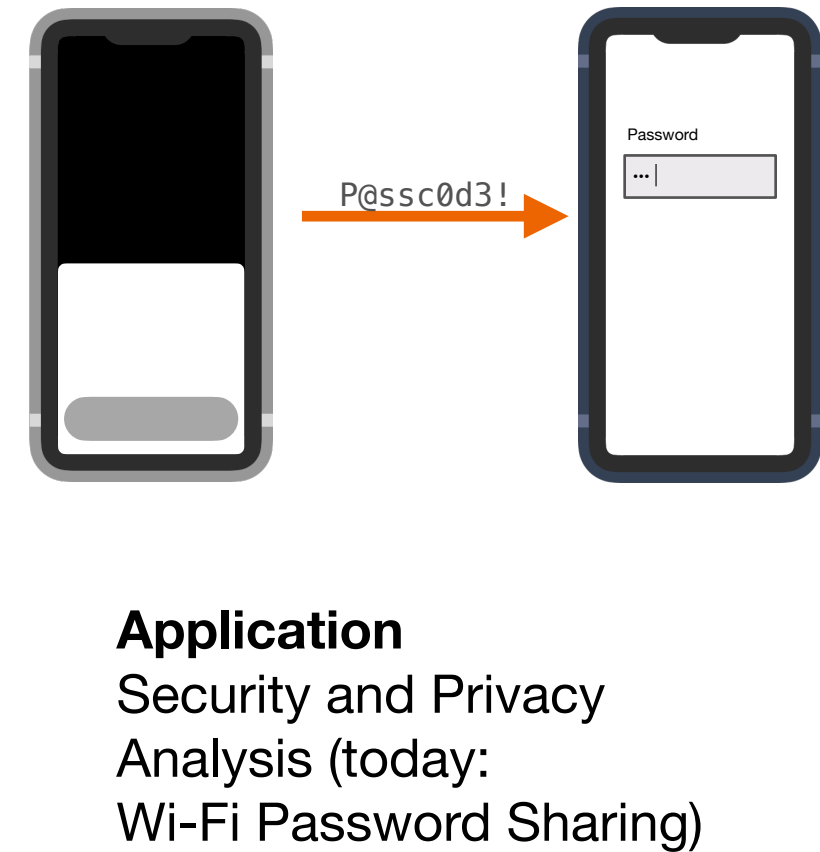
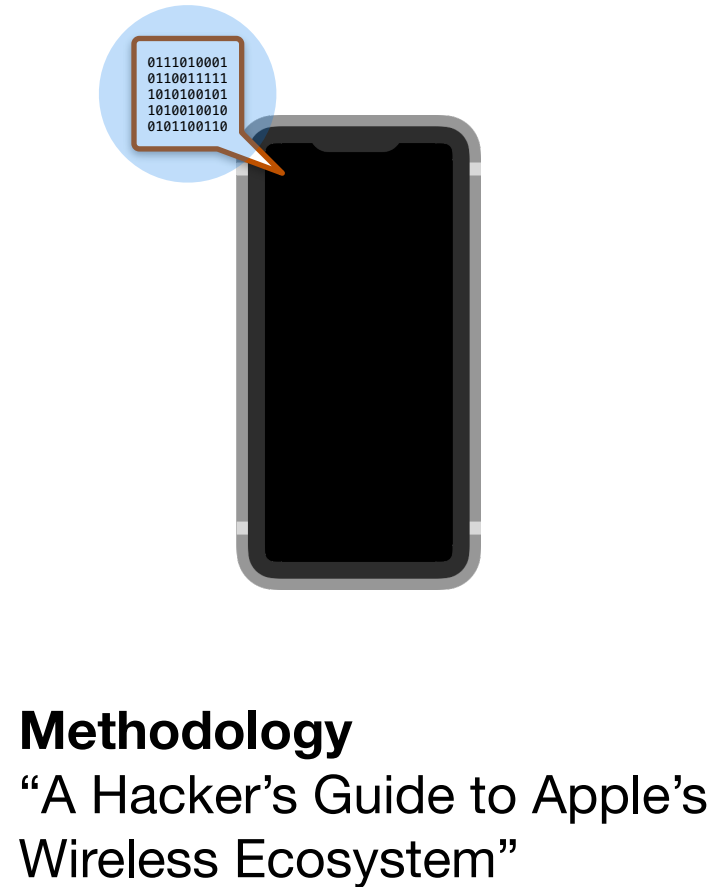
Milan Stute, Alexander Heinrich, Jannik Lorenz, and Matthias Hollick



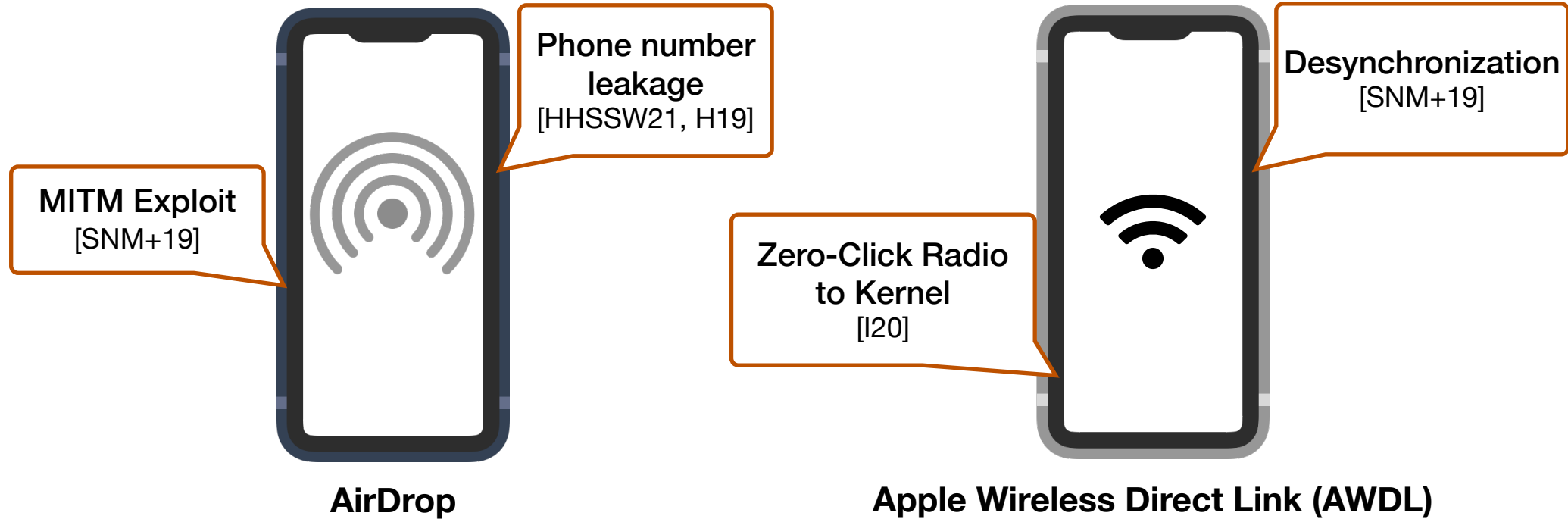
TECHNISCHE
UNIVERSITÄT
DARMSTADT



Roadmap



How secure are proprietary wireless protocols?



Goals

1. Define a structured approach on how to reverse-engineer proprietary wireless protocols in the Apple ecosystem
2. Apply our method on multiple protocols to uncover new security and privacy vulnerabilities

The ecosystem is complex

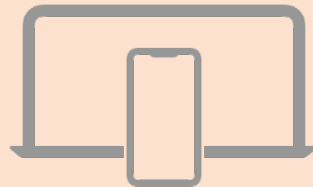
Continuity



AirDrop
[SNM+19] [HHSSW21]



Universal Clipboard
[SHLH21]



Handoff
[SHLH21]



Wi-Fi Password Sharing
[SHLH21]

The ecosystem is complex

Continuity

Continuity Markup

Sidecar

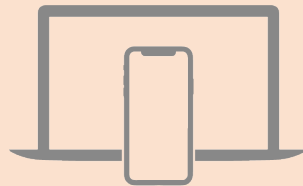
Continuity Sketch

iPhone Cellular
calls on Mac



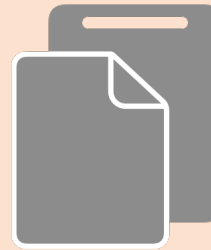
AirDrop

[SNM+19] [HHSSW21]



Handoff

[SHLH21]



Universal Clipboard

[SHLH21]



Wi-Fi Password Sharing

[SHLH21]

Auto Unlock

Continuity Camera

Apple Pay

Text Message
Forwarding

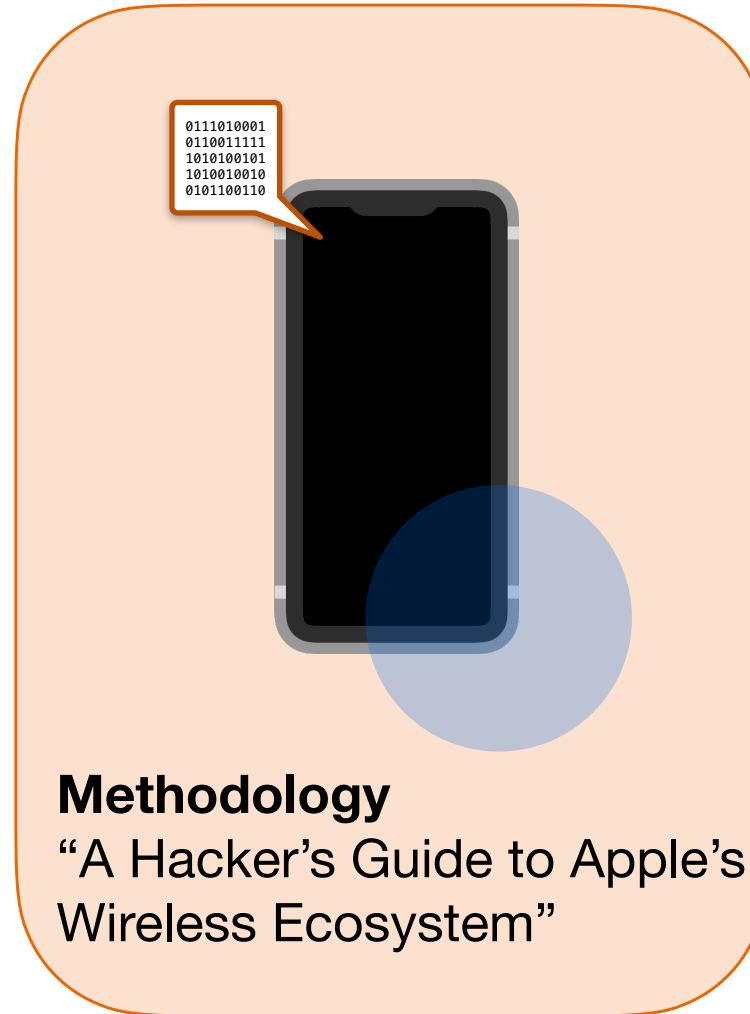
Instant Hotspot

Roadmap



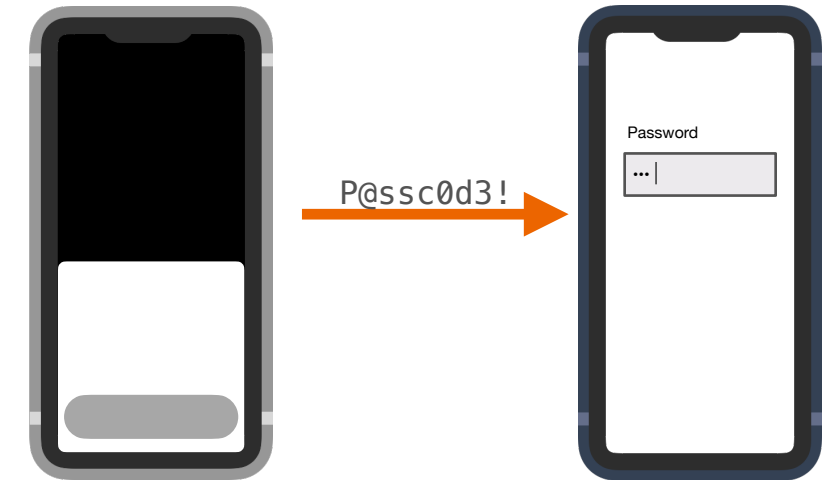
Problem

Complex and proprietary wireless protocols



Methodology

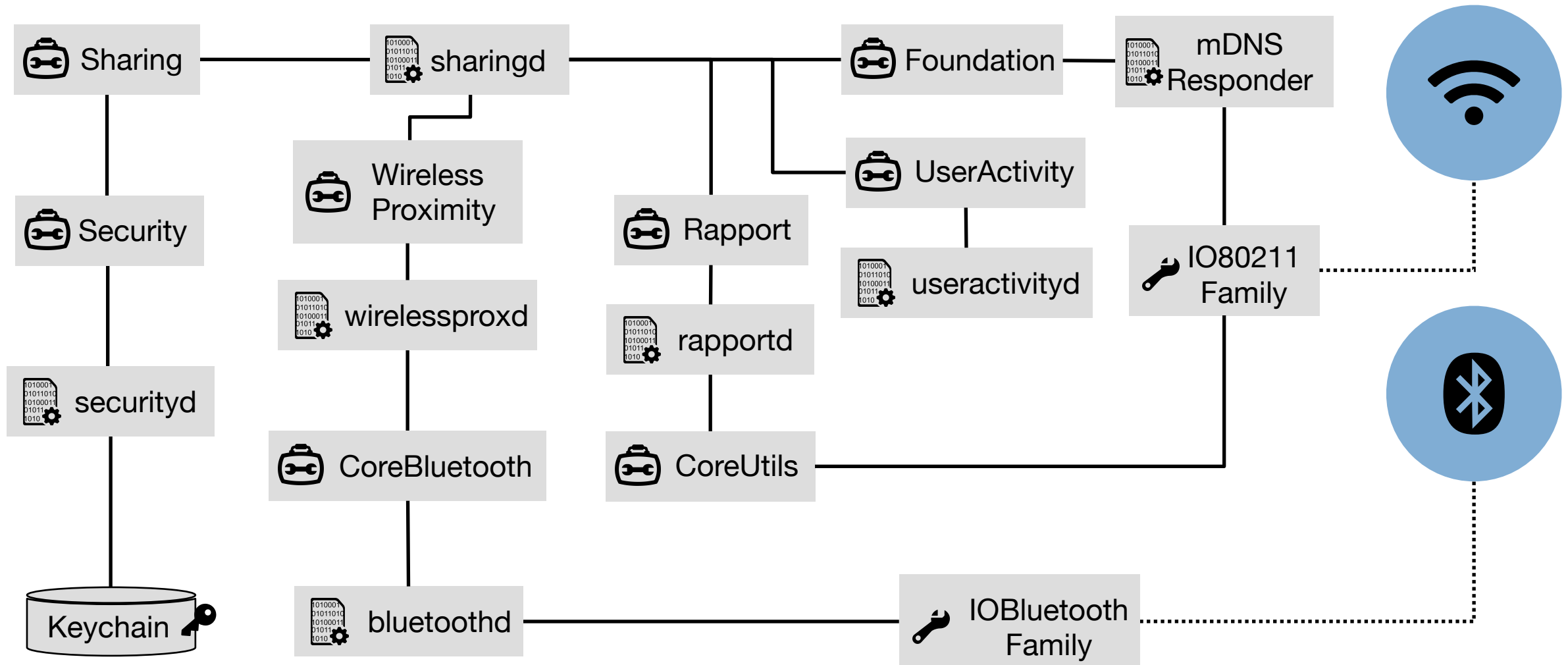
“A Hacker’s Guide to Apple’s Wireless Ecosystem”



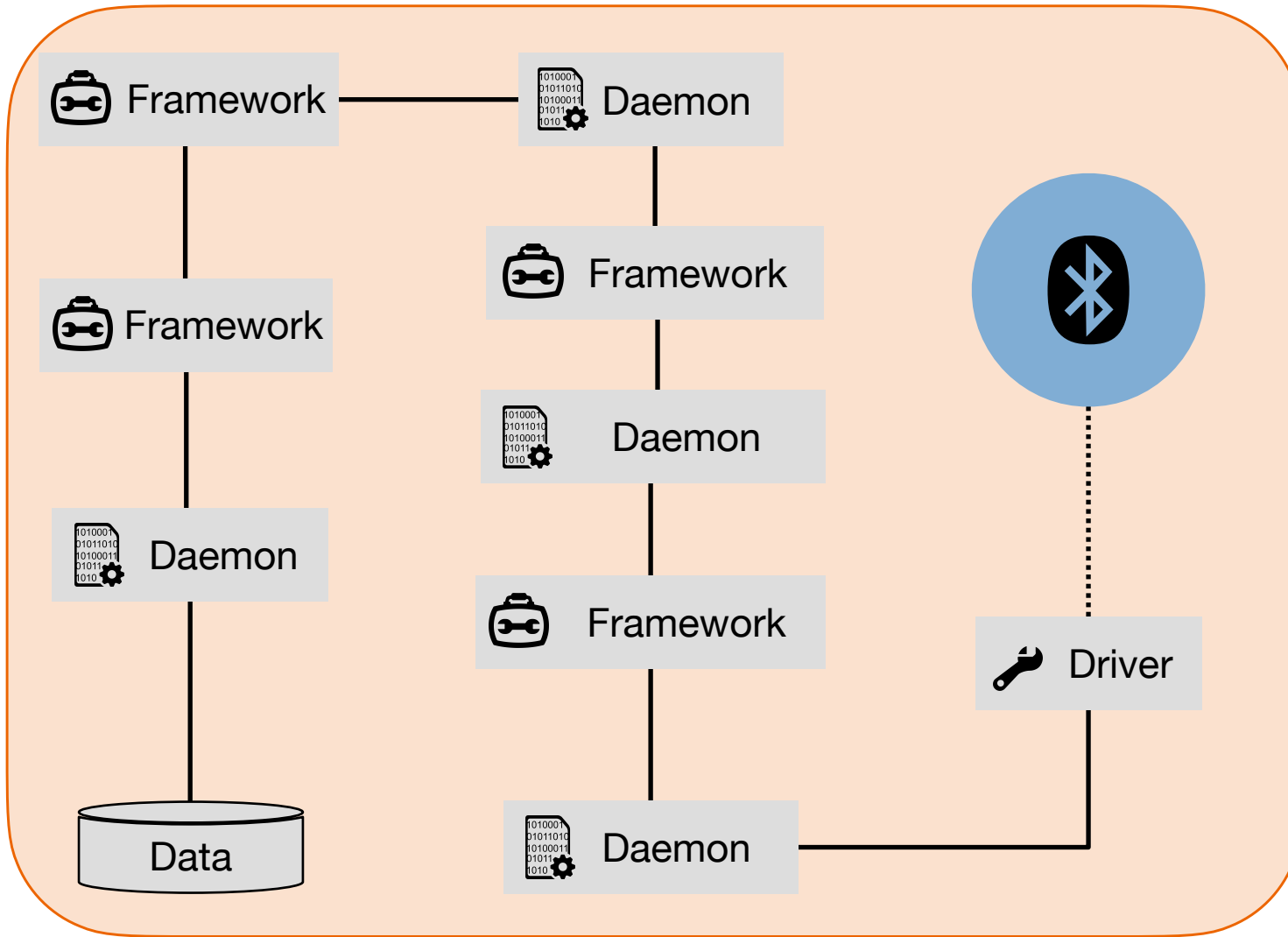
Application

Security and Privacy Analysis (today: Wi-Fi Password Sharing)

Universal Clipboard System Architecture



Hacker's Guide to Apple's Wireless Ecosystem



Vantage Point 1 **System**

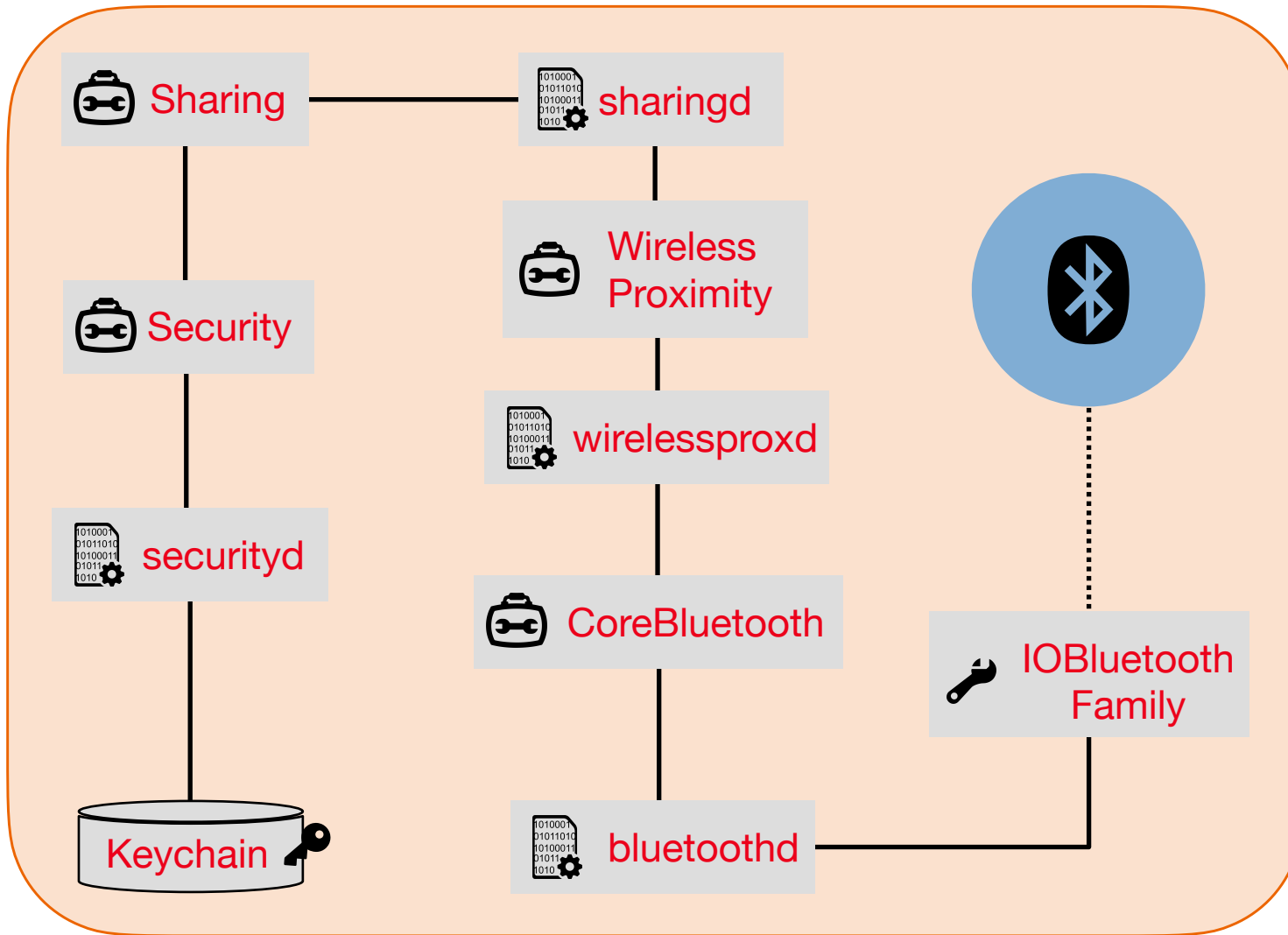
Tools

- System logs
- ioctl

Information

- Processes
- Frameworks
- Log Strings

Hacker's Guide to Apple's Wireless Ecosystem



Vantage Point 1 **System**

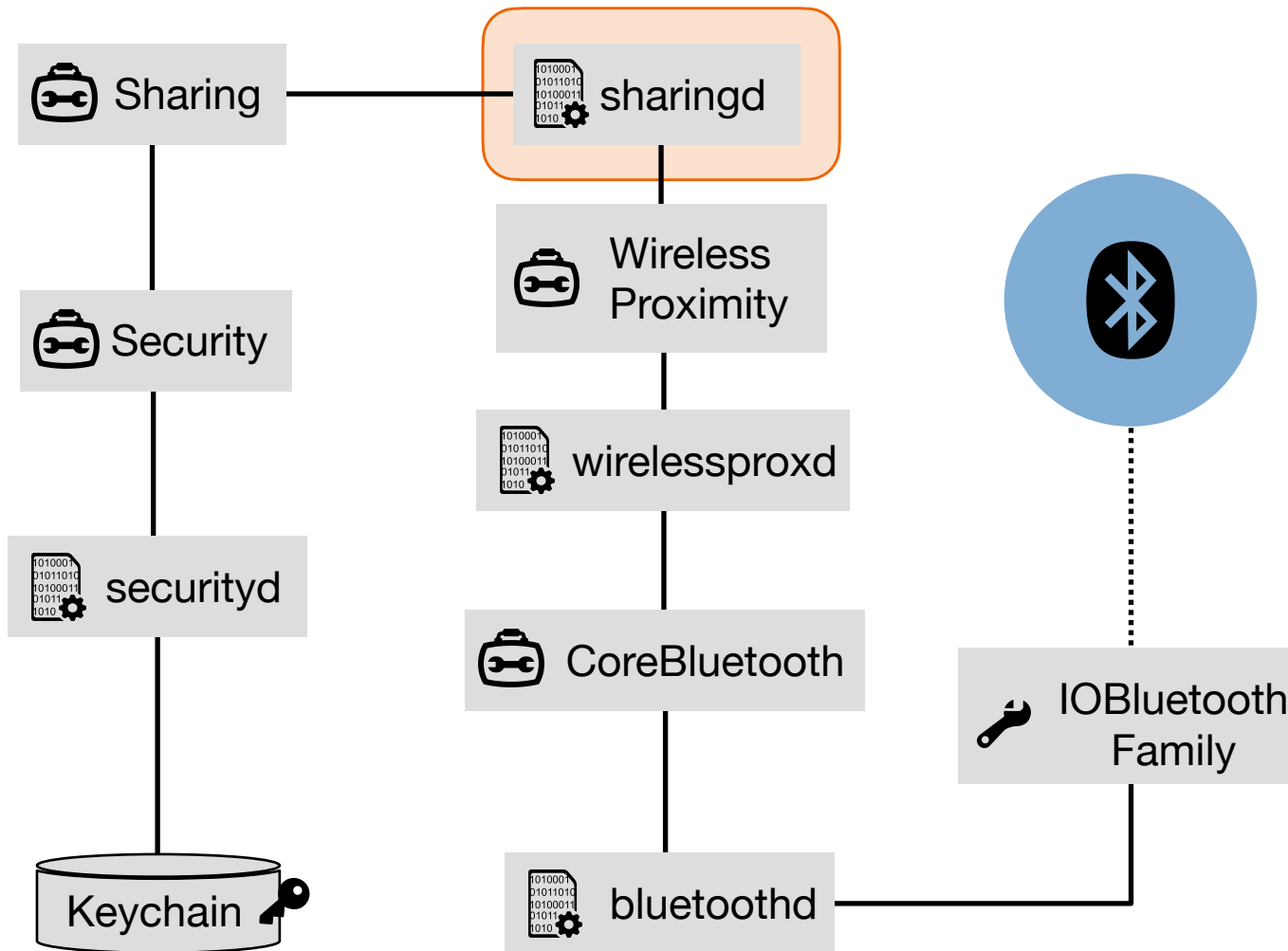
Tools

- System logs
- `ioctl`

Information

- Processes
- Frameworks
- Log Strings

Hacker's Guide to Apple's Wireless Ecosystem



Vantage Point 2

Binary Analysis

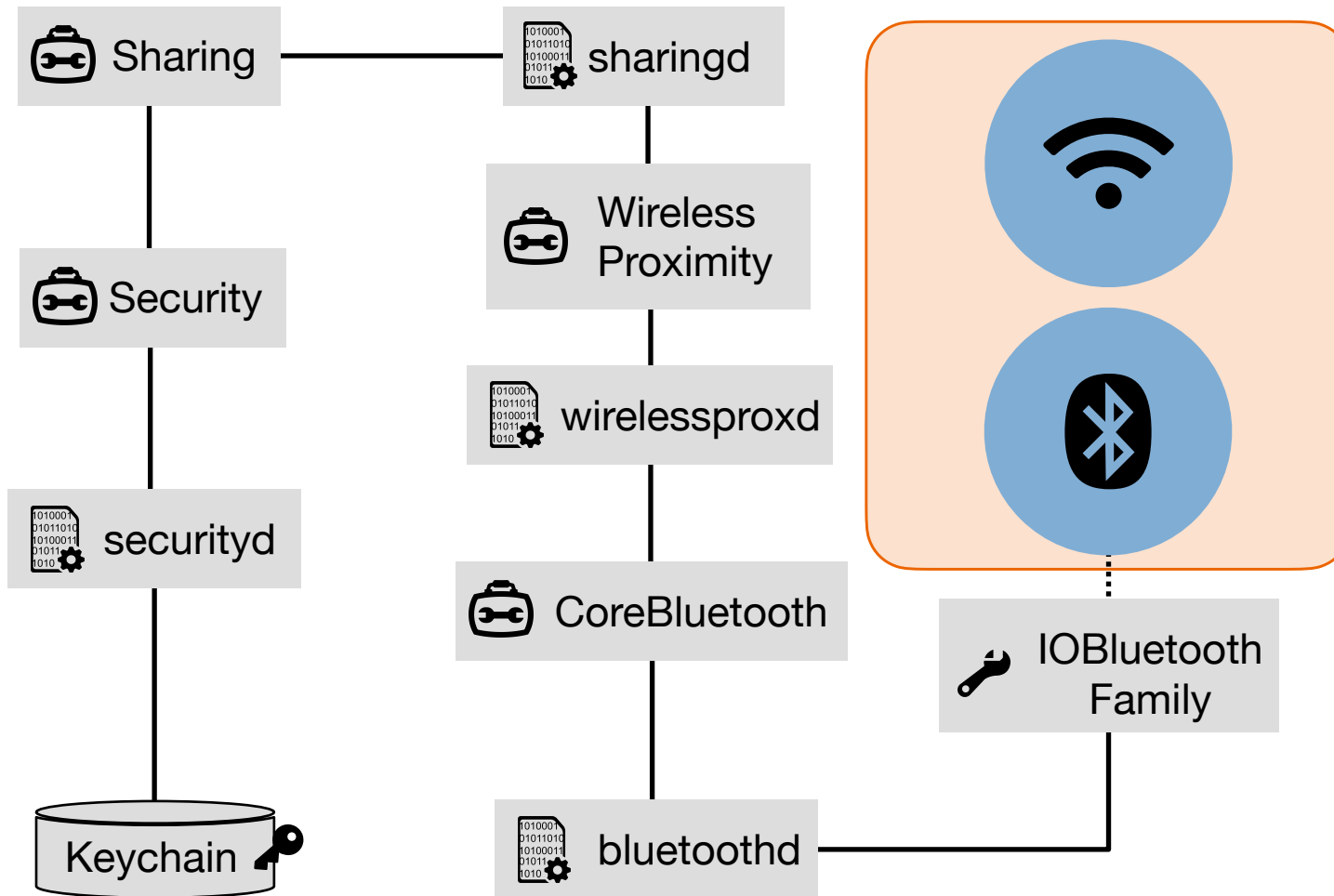
Tools

- Disassembler
- otool
- strings
- Frida

Information

- Message structure
- Encoding/Decoding
- Encryption Algorithms

Hacker's Guide to Apple's Wireless Ecosystem



Vantage Point 3

Network Interfaces

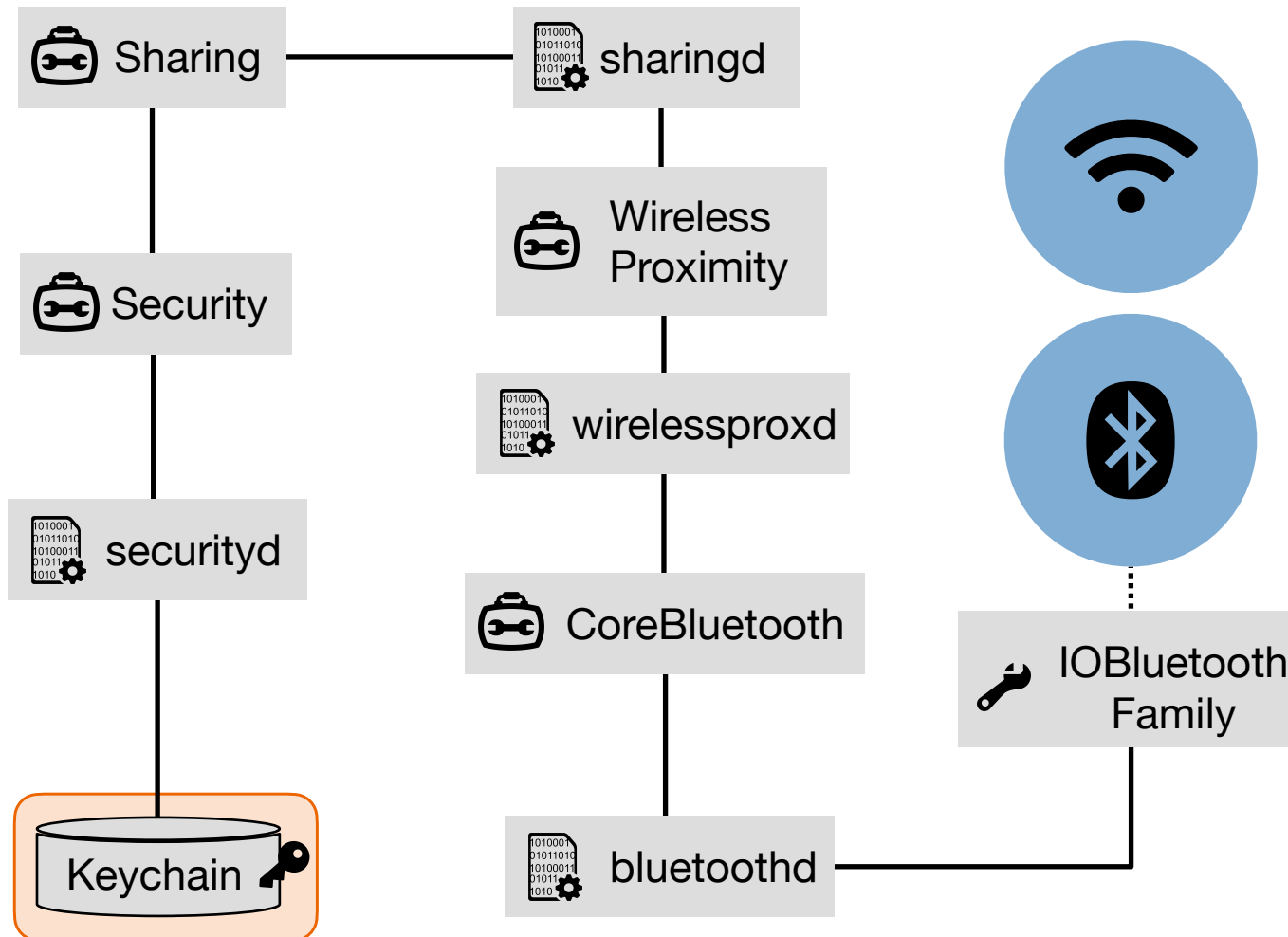
Tools

- Wireshark
- PacketLogger
- BTLEmap

Information

- (Public) Keys
- Certificates
- Static identifiers

Hacker's Guide to Apple's Wireless Ecosystem



Vantage Point 4

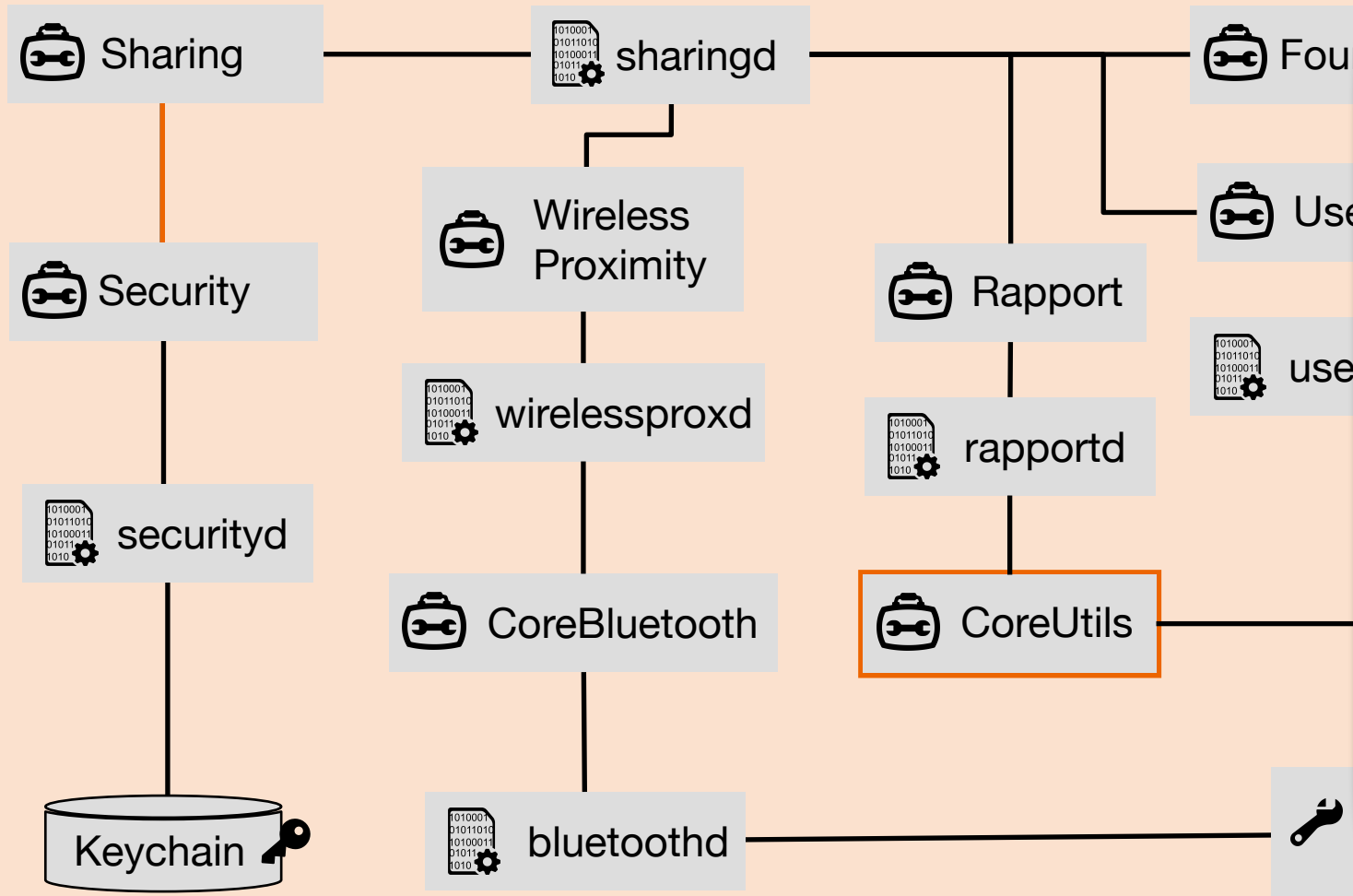
Keychain

Tools

- Security framework

Information

- Public & Private Keys
- Certificates
- Shared Keys



Automated Reverse Engineering Toolkit

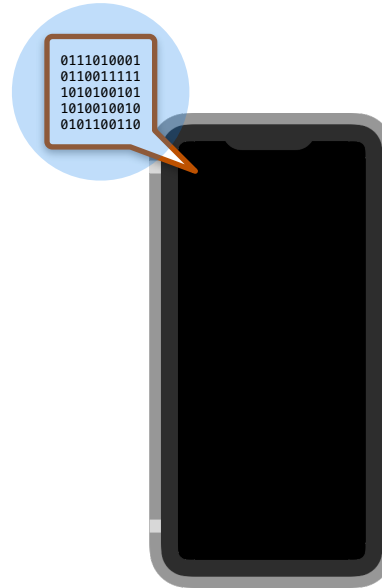
Identifying Interesting Binaries
Reading Continuity Messages
Accessing Relevant Keychain Items

Roadmap



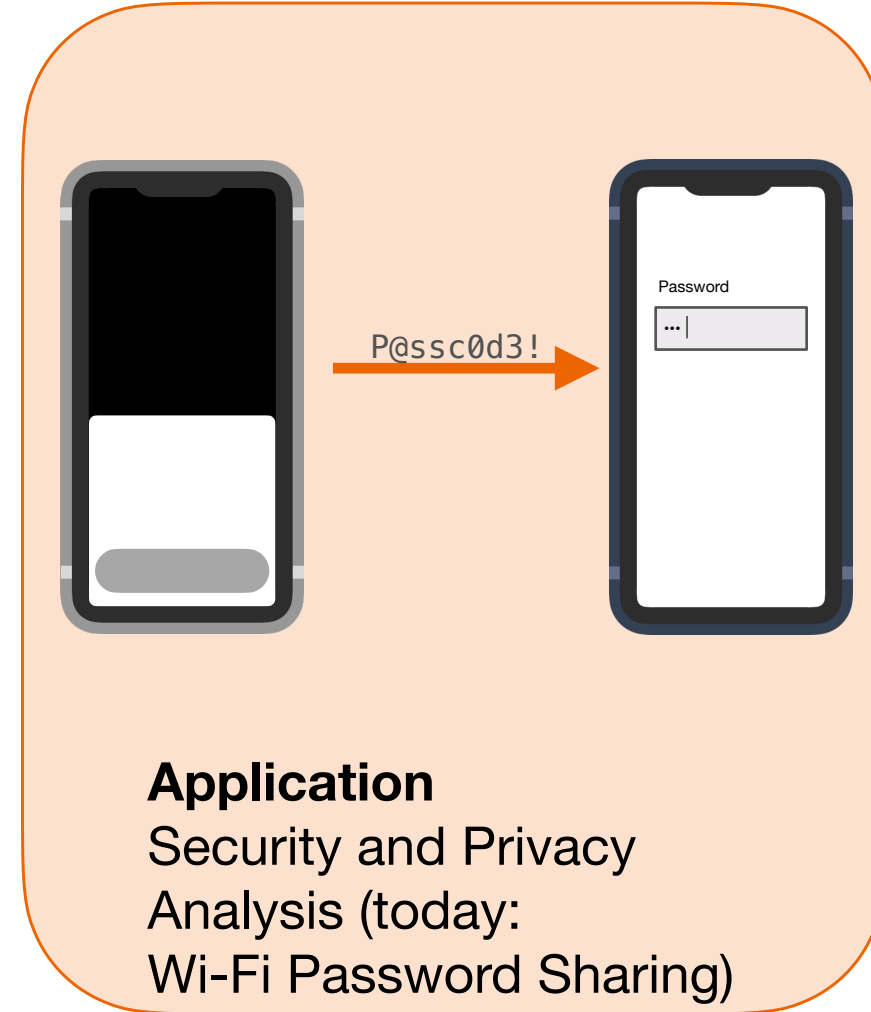
Problem

Complex and proprietary wireless protocols



Methodology

“A Hacker’s Guide to Apple’s Wireless Ecosystem”

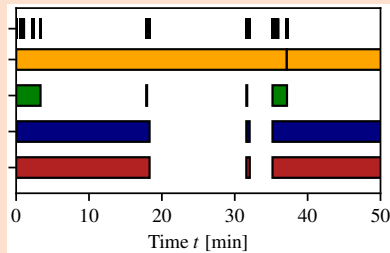


Application

Security and Privacy Analysis (today: Wi-Fi Password Sharing)

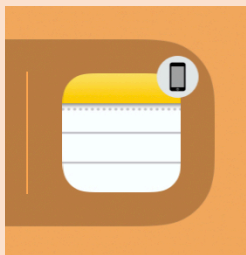
Vulnerabilities, Attacks, and Mitigations

Handoff + Universal Clipboard



Tracking

via asynchronous
identifier randomization
*fixed in iOS 13.4 and
macOS 10.15.4*



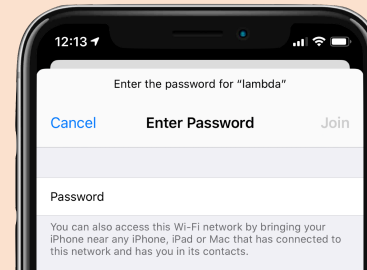
Denial-of-Service

via IV desynchronization
not fixed (yet)

Tracking [MAB+19]

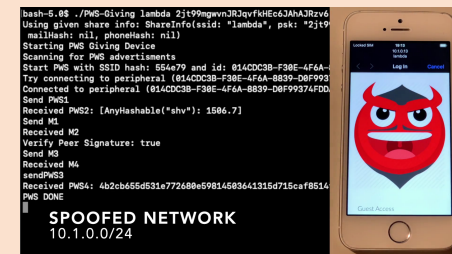
via linear IV
not fixed (yet)

Wi-Fi Password Sharing



Denial-of-Service

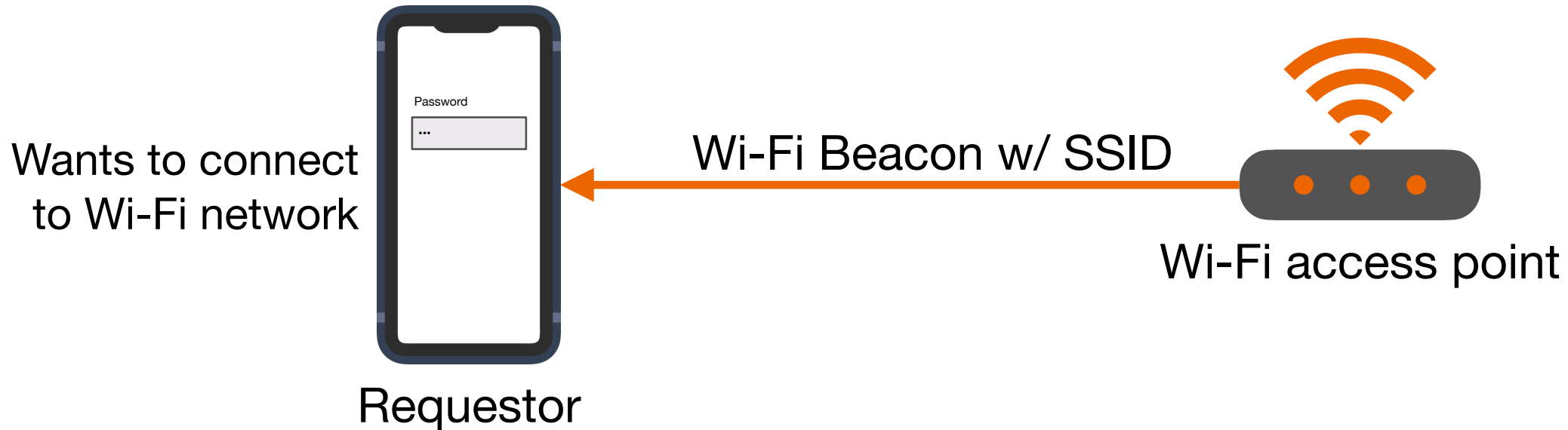
via settings app crash
CVE-2020-9827



Machine-in-the-Middle

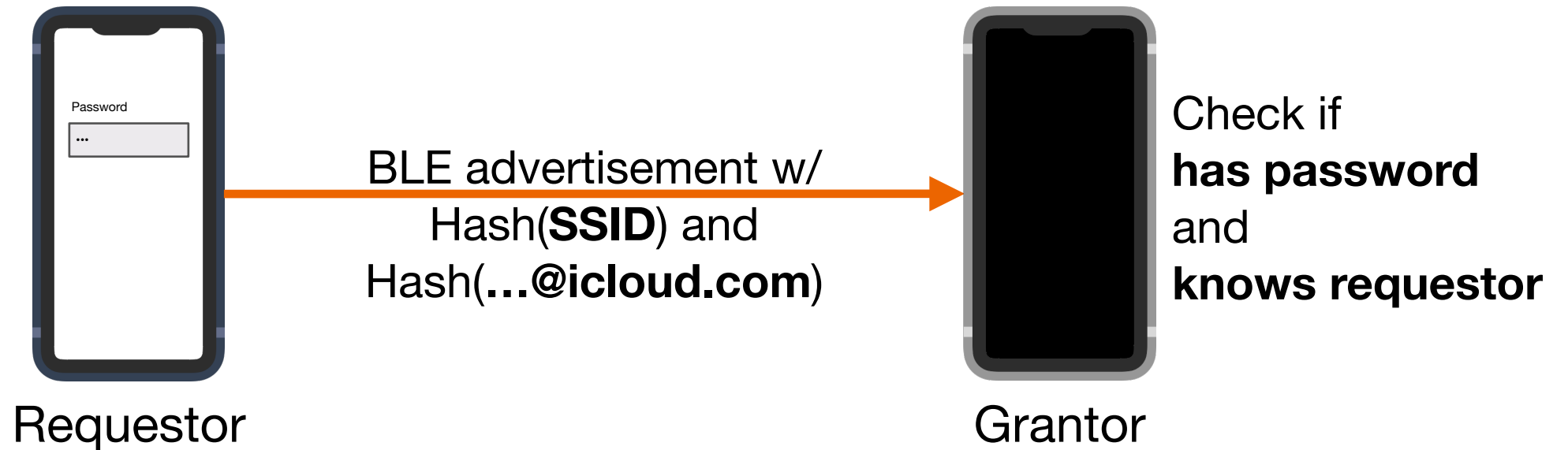
via Wi-Fi password
auto-fill
not fixed (yet)

Wi-Fi Password Sharing



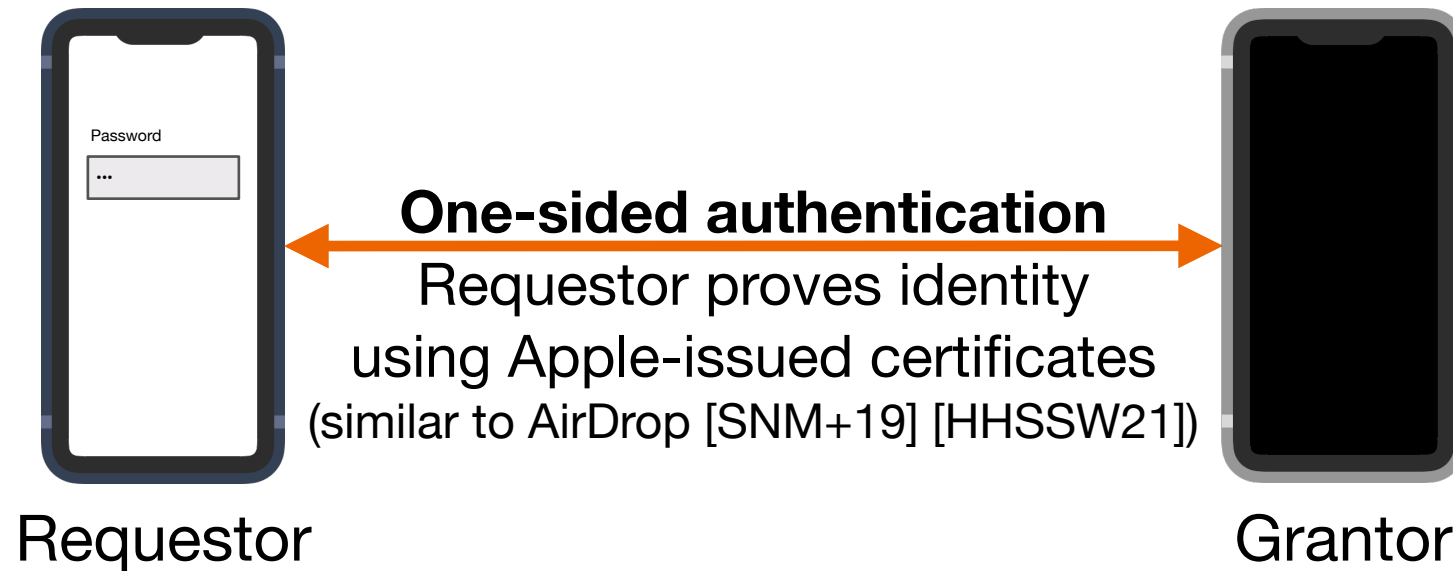
Simplified version of the protocol

Wi-Fi Password Sharing



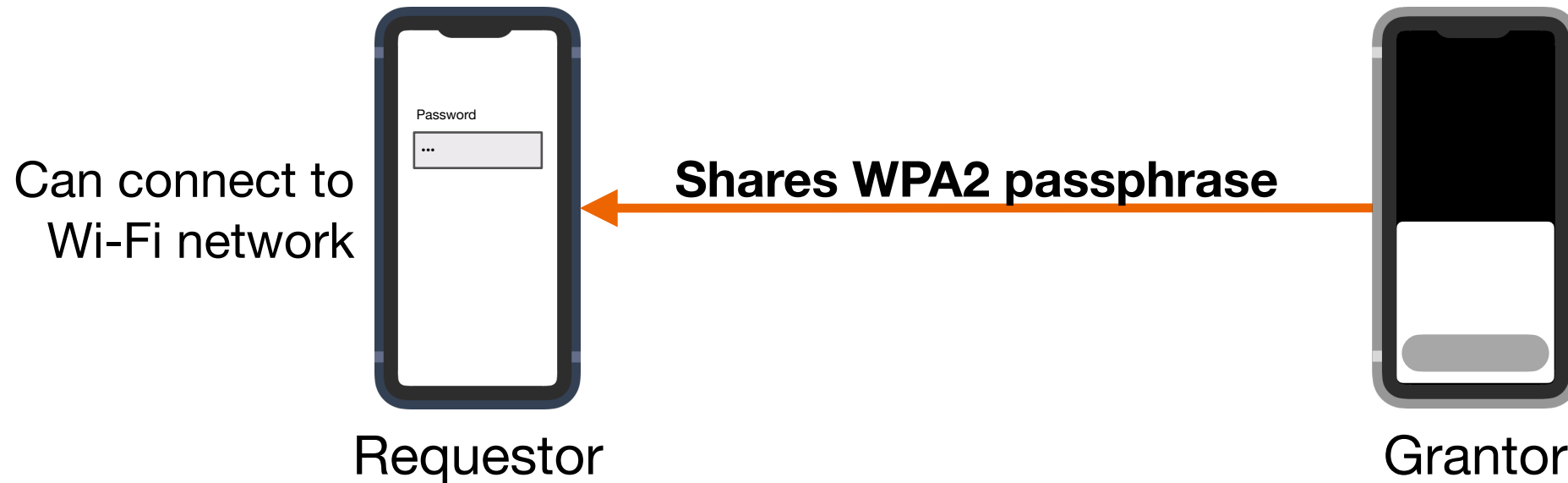
Simplified version of the protocol

Wi-Fi Password Sharing



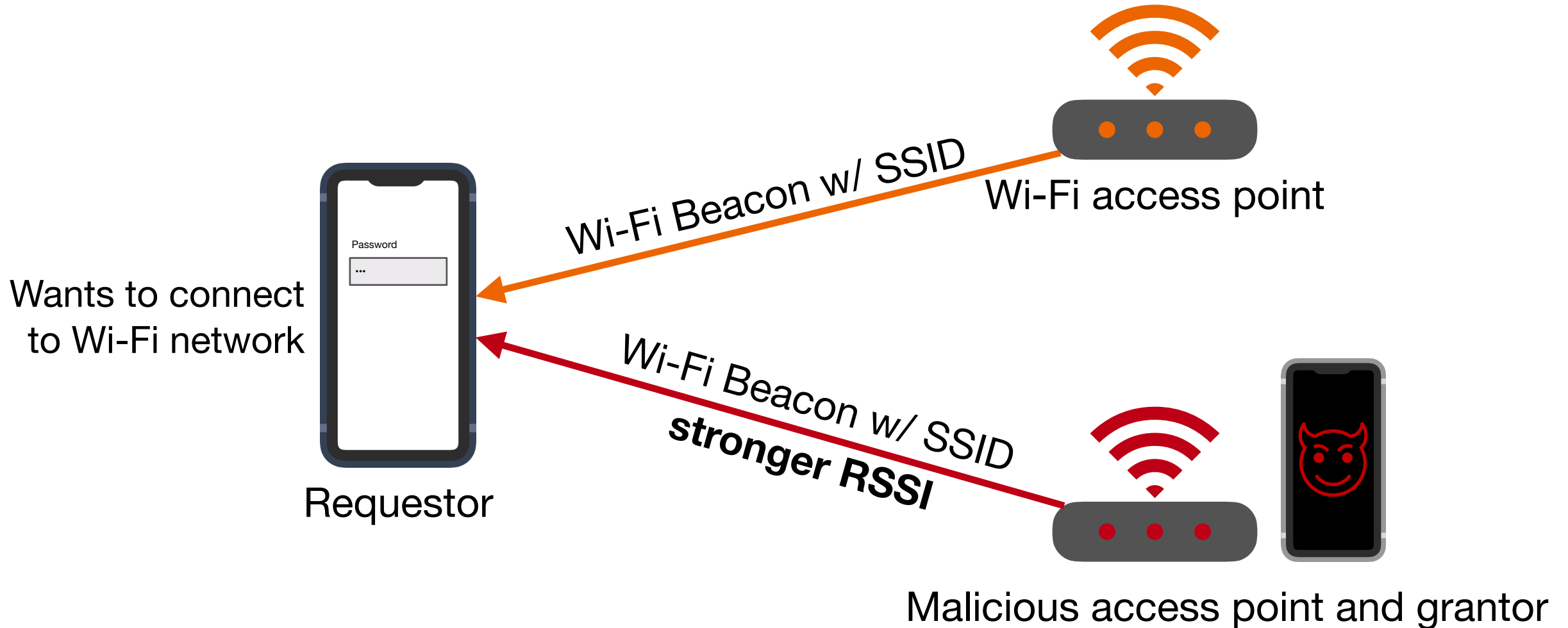
Simplified version of the protocol

Wi-Fi Password Sharing

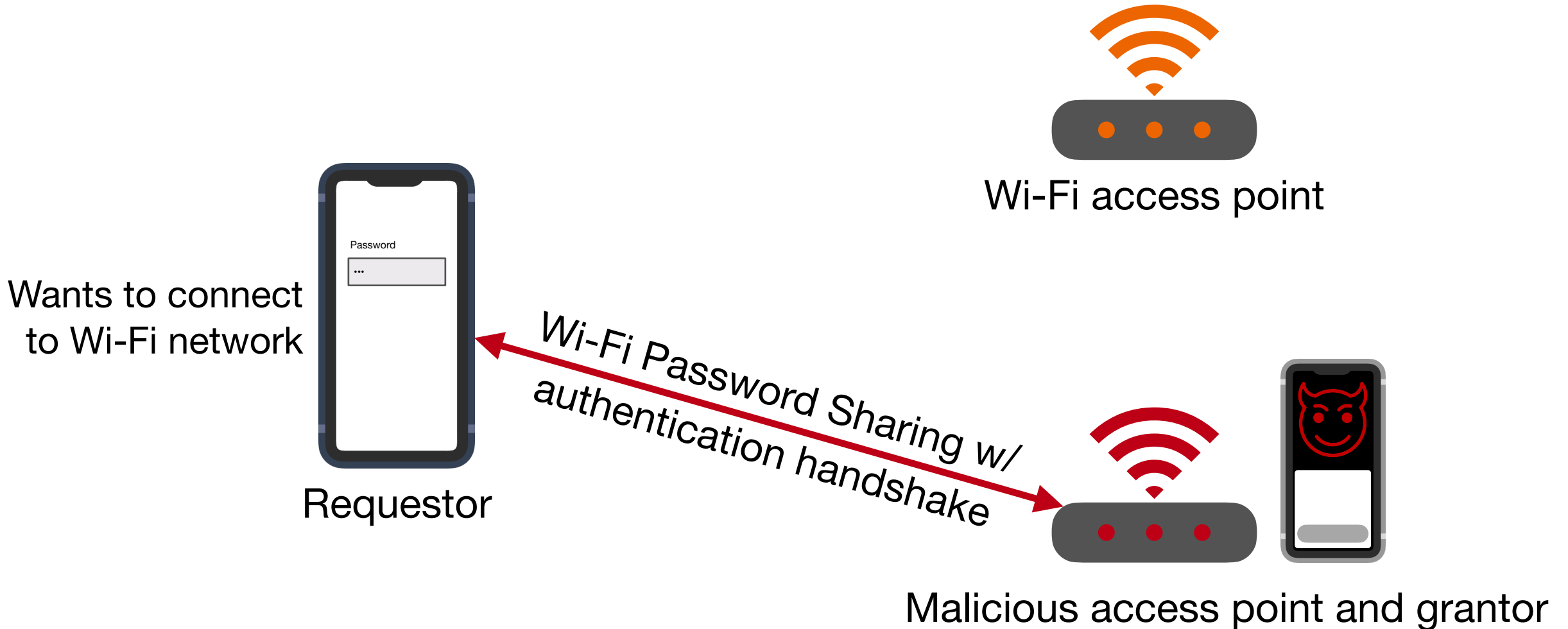


Simplified version of the protocol

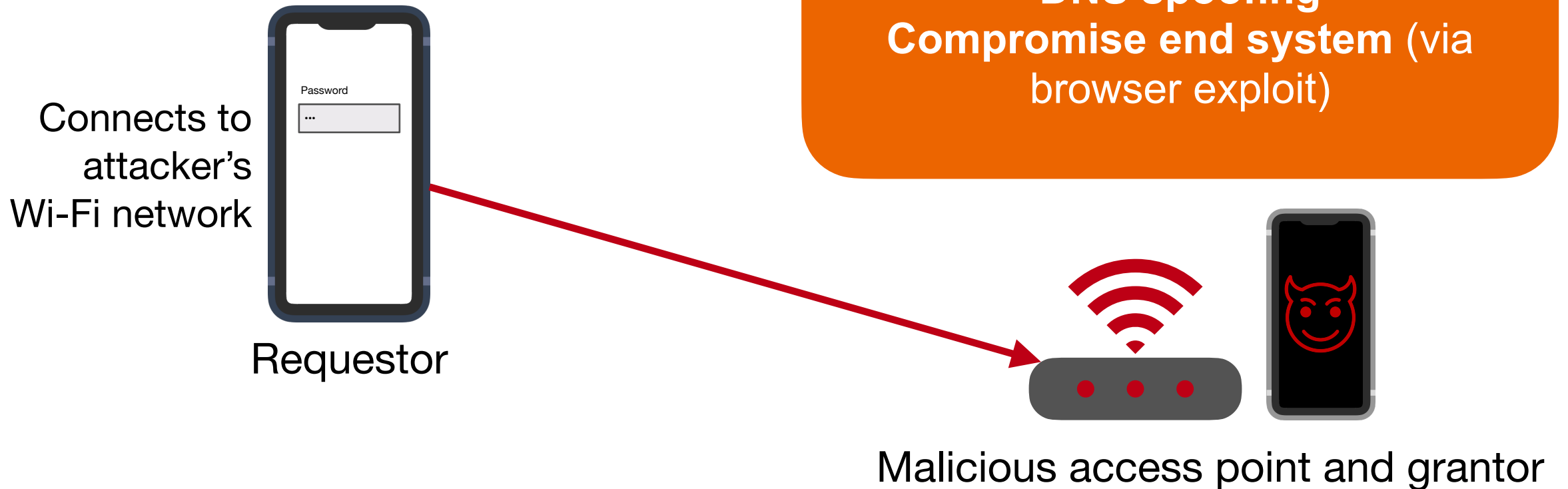
Attacking Wi-Fi Password Sharing



Attacking Wi-Fi Password Sharing



Attacking Wi-Fi Password Sharing




Simplified version of the protocol

Software

 **apple-continuity-tools** 

Reverse engineering toolkit for Apple's wireless ecosystem

 **openwifipass** 

An open source implementation of Apple's Wi-Fi Password Sharing protocol in Python.

 Python  621  21

... and several more at
<https://owlink.org>

Disclosure



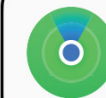
Discovered 4 distinct vulnerabilities and proposed **1** mitigation for a previously discovered flaw

Apple **fixed 2** so far...

... but **3 remain unfixed** (including MitM)

Outlook

Crowd-sourced Bluetooth-based **location tracking** [HSKH21]



Works with

Apple Find My

Graphics from apple.com

References

- **[HHSSW21]** Alexander Heinrich, Matthias Hollick, Thomas Schneider, Milan Stute, Christian Weinert. **PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop.** *USENIX Security*, 2021.
- **[HSKH21]** Alexander Heinrich, Milan Stute, Tim Kornhuber, and Matthias Hollick. **Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System.** *PoPETs*, 2021.
- **[MAB+19]** Jeremy Martin, Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske, Lucas Foppe, Travis Mayberry, Erik Rye, Brandon Sipes, and Sam Teplov. **Handoff All Your Privacy – A Review of Apple's Bluetooth Low Energy Continuity Protocol.** *PoPETs*, 2019.
- **[SHLH21]** Milan Stute, Alexander Heinrich, Jannik Lorenz, and Matthias Hollick. **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.** *USENIX Security*, 2021.
- **[SNM+19]** Milan Stute, Sashank Narain, Alex Mariotto, Alexander Heinrich, David Kreitschmann, Guevara Noubir, Matthias Hollick. **A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link.** *USENIX Security*, 2019.

References

- **[SKH18]** Milan Stute, David Kreitschmann, Matthias Hollick. **One Billion Apples' Secret Sauce: Recipe for the Apple Wireless Direct Link Ad hoc Protocol.** *MobiCom*, 2018.
- **[I20]** Ian Beer, **An iOS zero-click radio proximity exploit odyssey**, *Google Project Zero*, 2020.
- **[H19]** Hexway.io, **Apple bleee**, *Hexway.io*, 2019.

Icons

- **Icons** are part of the IcoFont, available at: icofont.com