Handoff All Your Privacy

A Review of Apple's Bluetooth Low Energy Continuity Protocol

JEREMY MARTIN, DOUGLAS ALPUCHE, KRISTINA BODEMAN, LAMONT BROWN, ELLIS FENSKE, LUCAS FOPPE, TRAVIS MAYBERRY, ERIK RYE, BRANDON SIPES, AND **SAM TEPLOV**

July 18, 2019

MITRE

Background

- Every wireless radio possesses a globally unique MAC address
- MAC addresses are crucial to communication as they are included in every link-layer frame
- **This poses a blatant privacy issue**
- Some manufacturers use temporary randomized MAC addresses to fix this
- Most published research has focused on defeating Wi-Fi MAC address randomization, with varied success

In this work, we analyze Apple's Continuity protocol and expose multiple privacy concerns that enable tracking, as well as defeat MAC address randomization

Inherent Problem

- Manufacturers implement MAC address randomization to improve privacy
- Application layer protocols still leak sensitive information
- This enables tracking and poses a large privacy concern
- Completely defeats the point of MAC address randomization

Apple Continuity

- Allows for seamless communication between devices
- Resume browsing sessions, auto unlock, instant hotspot
- Proprietary protocol; no open-source documentation
- Reverse engineering required

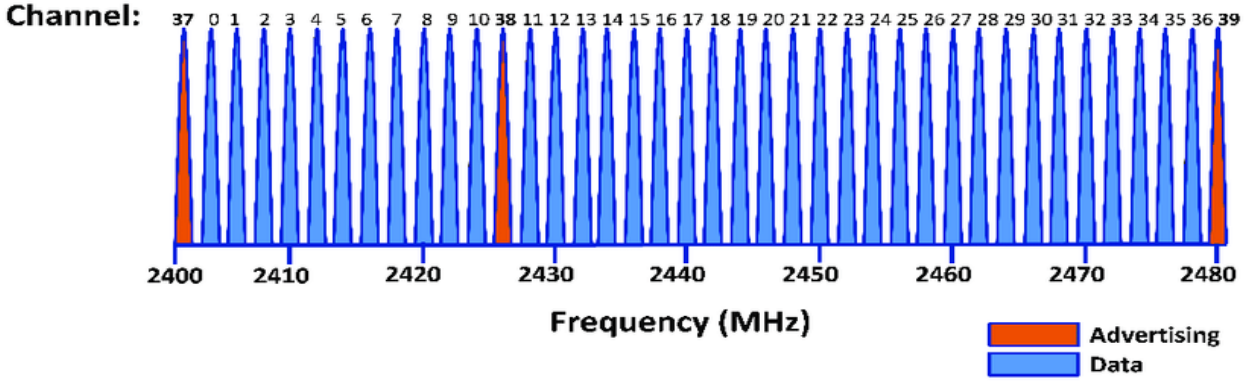



Why Apple?

- Devices are widespread
- Apple prides itself on privacy
- Continuity Ecosystem relies heavily on BLE

Bluetooth Low Energy

- Bluetooth Classic vs Bluetooth Low Energy (BLE)
- Advertising and Data channels
- Bluetooth Classic and BLE rated to 100m; BLE 5.0 capable of 400m

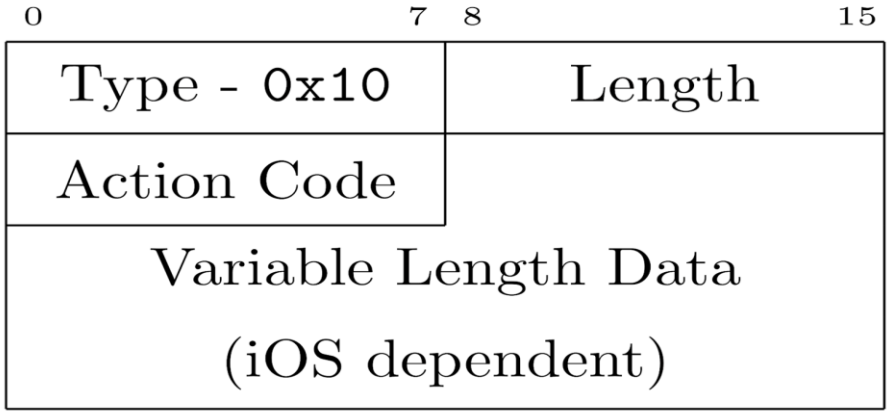


Apple BLE Advertisement Frame

0	7	8	15	16	23	24	31
Access Address - `0x8E89BED6`							
Packet Header							
Advertising Address - `xx:xx:xx:xx:xx:xx`							
Length / Type - `0x01` / Flags (Optional)							Length
Type - `0xFF`		Company ID - `0x004C`					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

Nearby Messages

- Indicate device state based off of user (in)action
- Allows for OS detection based off data field
- Messages never stop sending as of iOS 12



Action Codes

Type	Action Code
3	Locked Screen
7	Transition Phase
10	Locked Screen, Inform Watch
11	Active User
14	Phone Call or FaceTime

Correlating Random MAC Addresses

- Nearby messages include unknown data field
- This field changes when MAC addresses rotate, but not at the same time…

Time	Advertising Address	Unk (Nearby) Data
899.987876800	60:45:7a:bb:3f:2f	e77352
900.019127100	60:45:7a:bb:3f:2f	e77352
900.049127000	4b:80:5c:b1:92:2e	e77352
900.060377200	4b:80:5c:b1:92:2e	e77352
900.107877600	4b:80:5c:b1:92:2e	73b3f7
900.142877700	4b:80:5c:b1:92:2e	73b3f7

MacOS Breaks Itself

- In Mojave and High Sierra, globally unique BLE MAC address is leaked
- When Handoff and Nearby messages are sent concurrently, Nearby messages use the globally unique BLE MAC address
- Wi-Fi MAC is known when BLE MAC address is ± 1 from Wi-Fi MAC address

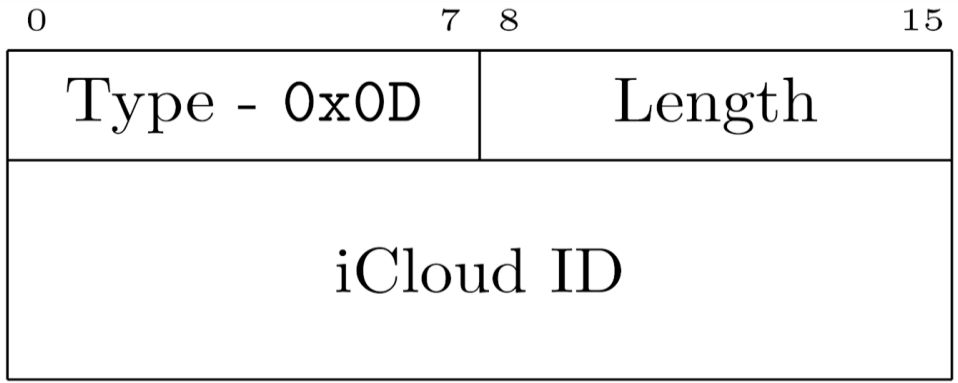
Time	Advertising Address	Type
84.300037100	54:8b:9e:87:5a:6f	Nearby
84.481289600	54:8b:9e:87:5a:6f	Nearby
84.513789800	54:8b:9e:87:5a:6f	Handoff
84.516292800	dc:a9:04:89:e8:95	Nearby
84.545040200	dc:a9:04:89:e8:95	Nearby

Apple Bluetooth Software Version: 6.0.11f4
Hardware, Features, and Settings:
Name: [redacted]
Address: DC-A9-04-89-E8-95

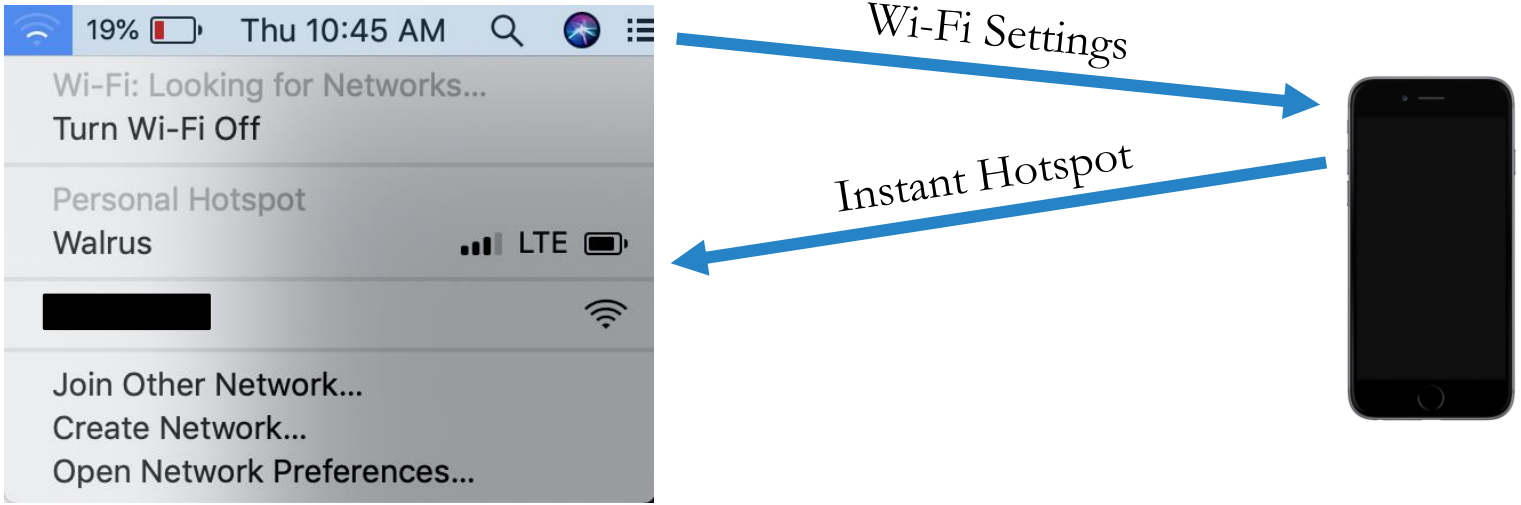
Device MAC Address

Wi-Fi Settings

- Triggered by navigating to Wi-Fi Settings page
- iCloud ID links together devices on the same iCloud
- Triggers instant hotspot messages from other devices



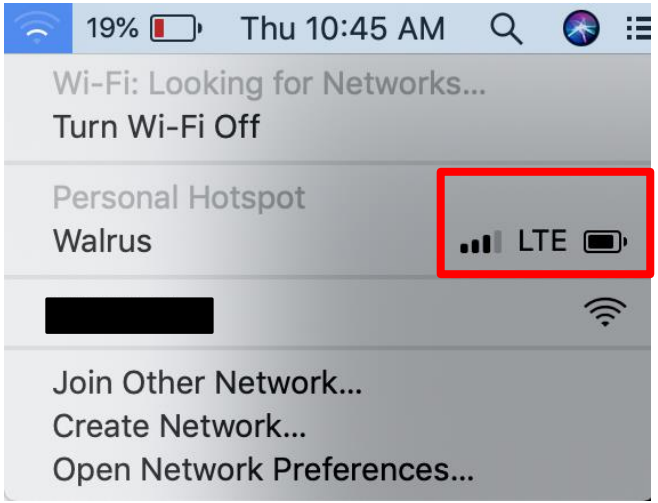
Wi-Fi Settings and Hotspot Messages



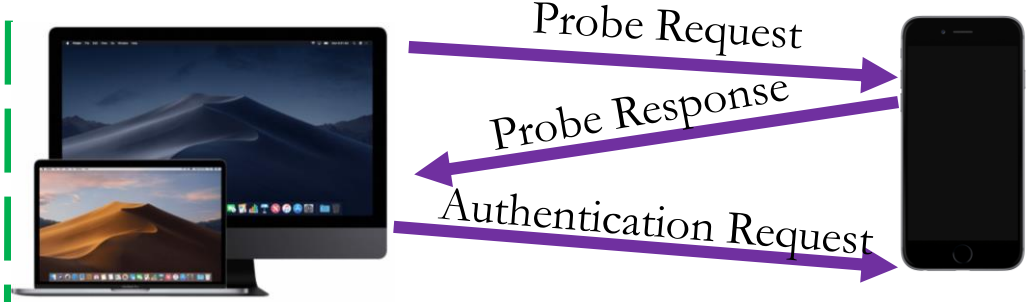
Instant Hotspot

- Triggered by Wi-Fi Settings page message
- Learn cellular service type, signal strength, battery life

0	7	8	15
Type - 0x0E		Length	
Data			
Battery Life		Data	
Cell Service		Cell Bars	



Defeat of MAC Address Randomization



Bluetooth Low Energy

Wi-Fi

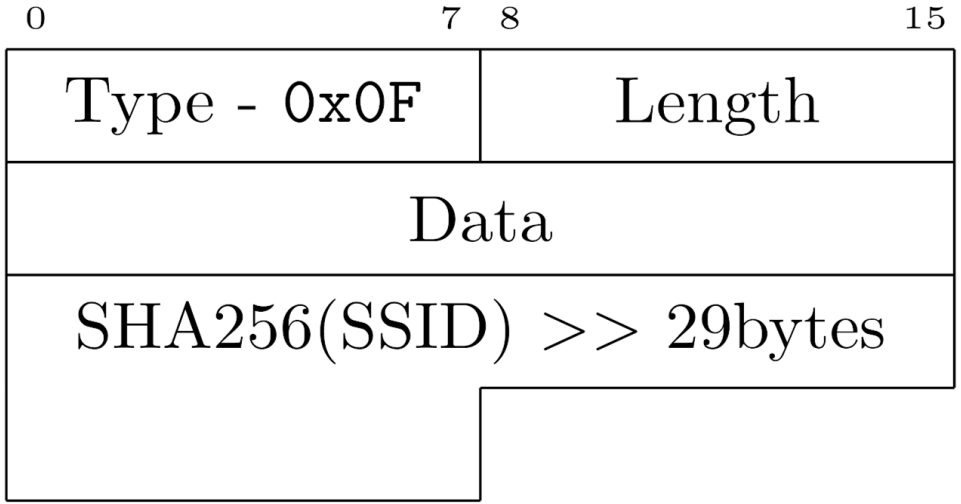
Hotspot Probe Response

No.	Time	Type/Subtype
7	0.093899787	Probe Response
9	0.099878777	Probe Response
10	0.105827993	Probe Response
11	0.119353348	Probe Response

```
▶ Tag: Vendor Specific: Apple, Inc.
▼ Tag: Vendor Specific: Apple, Inc.
    Tag Number: Vendor Specific (221)
    Tag length: 13
    OUI: 00:17:f2 (Apple, Inc.)
    Vendor Specific OUI-Type: 00:17:f2-6
    Vendor Specific OUI Type: 6
    Vendor Specific Data: 06020106a04ea72054dd
    Apple OUI Type: 6
  ▼ Apple Hotspot
      Apple Hostpot - WiFi MAC: a0:4e:a7:20:54:dc
      Apple Hostpot - Bluetooth MAC: a0:4e:a7:20:54:dd
    Vendor Specific Data: 06020106a04ea72054dd
▶ Tag: Vendor Specific: Broadcom
▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Wi-Fi Join

- Sent when user attempts to join a closed Wi-Fi network
- Message includes first 3 bytes of the SHA256 hash of the SSID



Defeat of MAC Address Randomization

Wi-Fi Settings

Wi-Fi Join

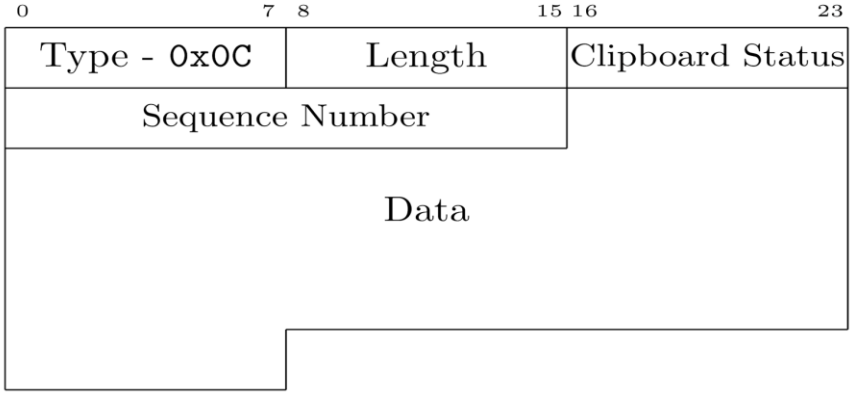
Authentication Request

Bluetooth Low Energy

Wi-Fi

Handoff

- Handoff messages sent whenever Handoff enabled apps are used
- Clipboard status
- Monotonically increasing sequence number (0-65535) based off user actions
- Data section seems to be encrypted



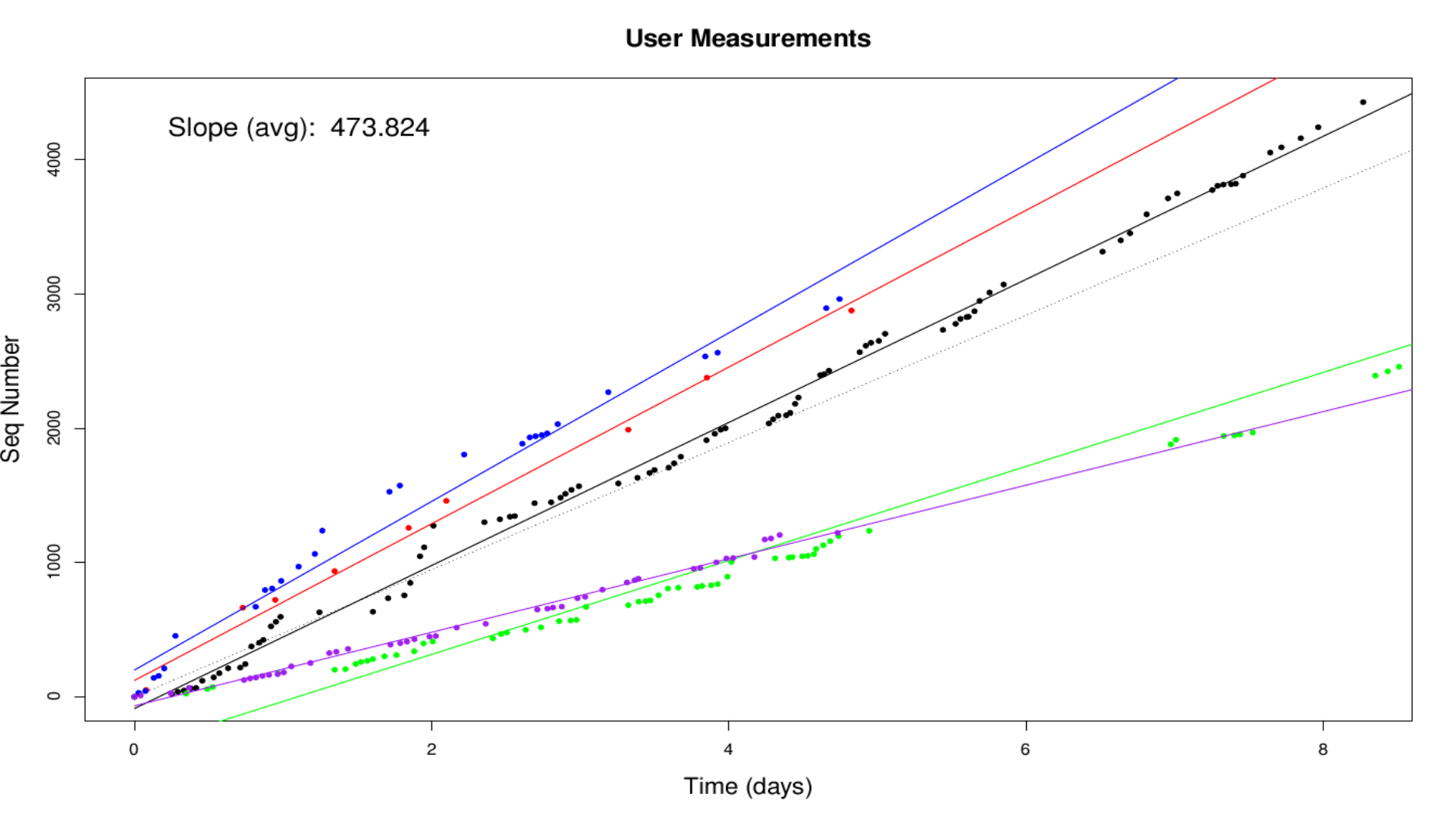
Correlating Random MAC Addresses

- MAC address changes can always be correlated since the sequence number will either stay the same or increment by 1
- The Handoff data field can also be used to correlate MAC address changes

Time	Advertising Address	Sequence Number ^	Unk (Handoff) Data
178.266725500	7e:07:ec:f0:aa:e8	45	a31238f908a24d517b6eb2
178.447977200	7e:07:ec:f0:aa:e8	45	a31238f908a24d517b6eb2
178.629233500	7e:07:ec:f0:aa:e8	45	a31238f908a24d517b6eb2
178.772989700	5e:3d:07:95:72:1a	45	a31238f908a24d517b6eb2
178.780489900	5e:3d:07:95:72:1a	45	a31238f908a24d517b6eb2
178.961741100	5e:3d:07:95:72:1a	45	a31238f908a24d517b6eb2

Sequence Number Trajectories

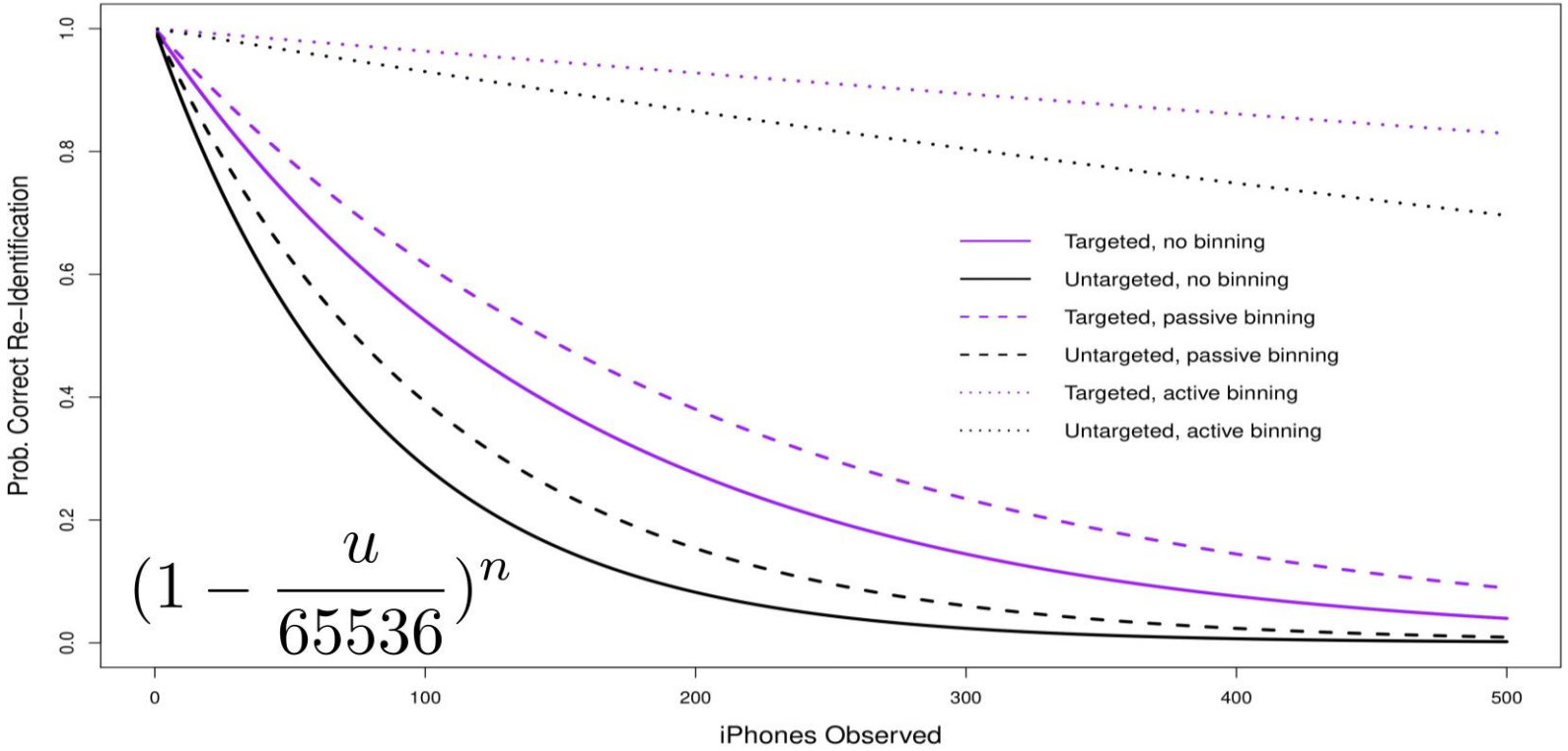
- Captured sequence numbers on 4 students and 1 faculty
- Data collected ~1 hour intervals for a week
- Data shows that sequence numbers increase slowly (~470/day)


User Measurements
Slope (avg): 473.824
Seq Number
0
1000
2000
3000
4000
0
2
4
6
8
Time (days)

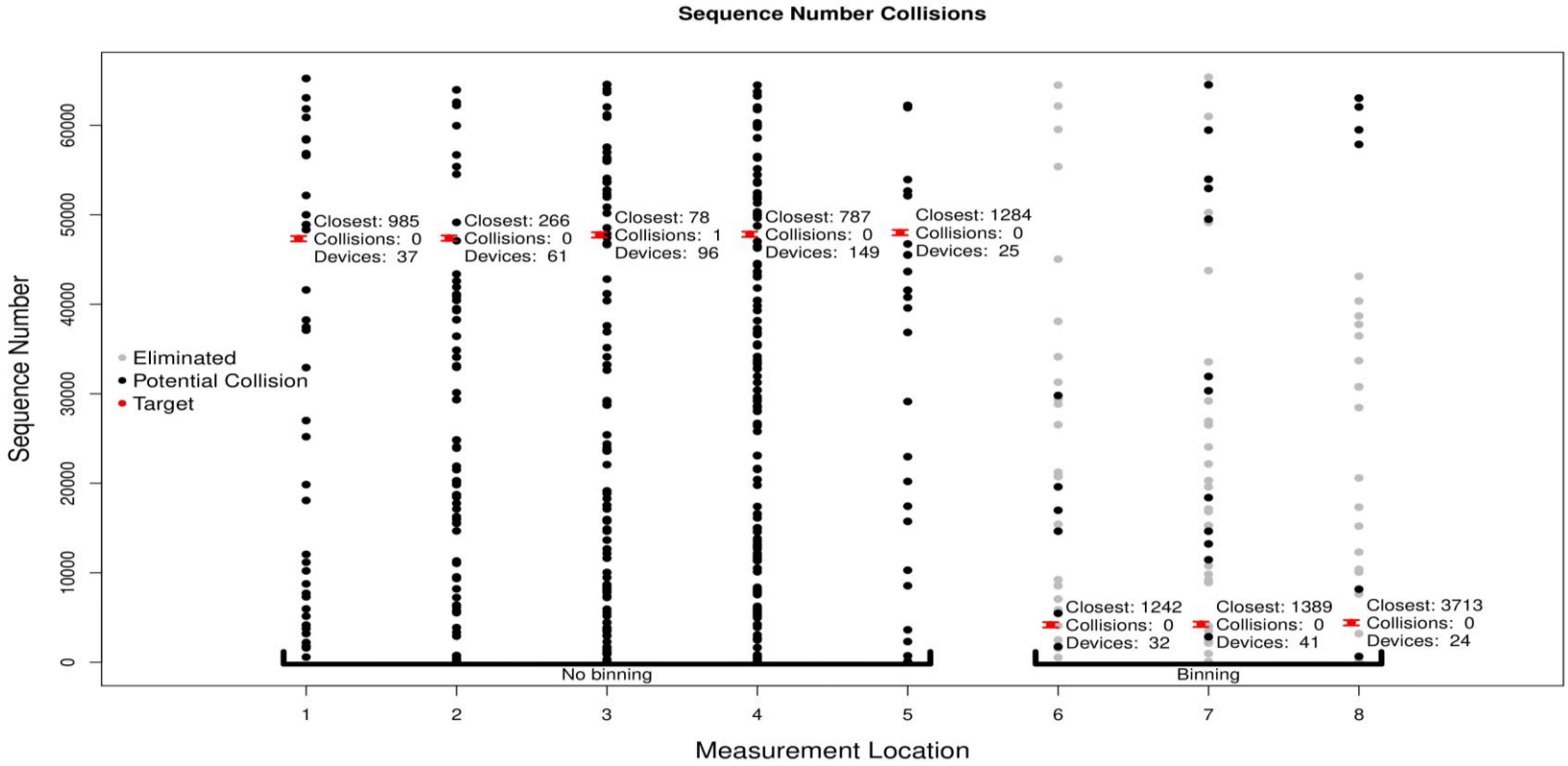
Attack Scenario

- **Goal: Identify a previously observed phone**
- Capture individual's random BLE MAC and sequence number
- Calculate trajectory and range of victim sequence number
- 1 week later, the victim's BLE MAC address has changed, but can reacquire by using difference in sequence numbers

Theoretical Results



Real Results



Remediation

- Fix MacOS bug
- Encrypt messages
- Rotate MAC addresses stochastically, more frequently, and change data
- Remove sequence numbers
- Disclosure to Apple

Final Thoughts

- Individually, each message leaks a small amount of data
- In aggregate, they can be used to identify and track devices
- Privacy vulnerabilities in one wireless domain can trivialize safeguards in another