Reverse Engineering Apple's BLE Continuity Protocol For Tracking, OS Fingerprinting, and Behavioral Profiling

FURIOUS MAC RESEARCH GROUP

SAM TEPLOV

January 31, 2020

Furious MAC

- Established at USNA in 2015
- Interested in hardware identifiers and privacy concerns associated with them
- Mostly focused on 802.11 MAC address randomization in past work
- BLE research was initially a "side project"…

Contributions

- Reverse engineer Apple BLE continuity messages
- See current activity of iPhones/MacBooks/AirPods/Watches
- Learn SSID of the network the user is connecting to
- OS fingerprinting for iOS 10-13 & MacOS
- Defeat MAC address randomization; enable user tracking & profiling

Release first ever public Wireshark dissector for Apple Continuity messages

Privacy Warning

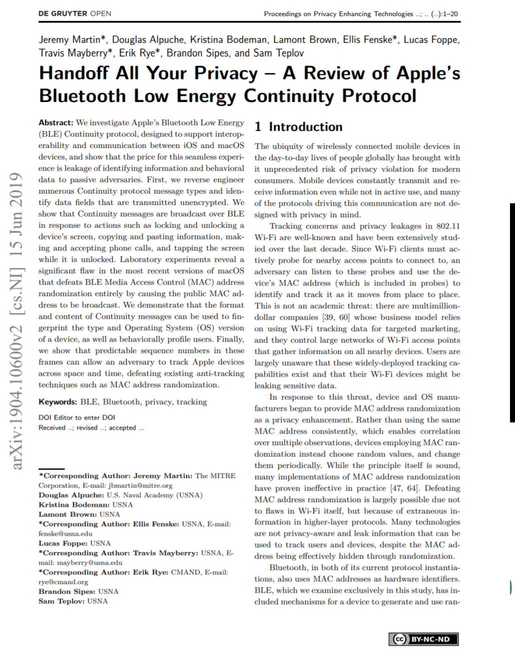
- We will be sniffing BLE traffic as part of our demo
- Please turn your Bluetooth OFF if you don’t want us sniffing your BLE traffic

Apple Continuity

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




Reverse Engineering Techniques



DE GRUYTER OPEN   Proceedings on Privacy Enhancing Technologies ..; .. (..):1–20

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

Abstract: We investigate Apple's Bluetooth Low Energy (BLE) Continuity protocol, designed to support interoperability and communication between iOS and macOS devices, and show that the price for this seamless experience is leakage of identifying information and behavioral data to passive adversaries. First, we reverse engineer numerous Continuity protocol message types and identify data fields that are transmitted unencrypted. We show that Continuity messages are broadcast over BLE in response to actions such as locking and unlocking a device's screen, copying and pasting information, making and accepting phone calls, and tapping the screen while it is unlocked. Laboratory experiments reveal a significant flaw in the most recent versions of macOS that defeats BLE Media Access Control (MAC) address randomization entirely by causing the public MAC address to be broadcast. We demonstrate that the format and content of Continuity messages can be used to fingerprint the type and Operating System (OS) version of a device, as well as behaviorally profile users. Finally, we show that predictable sequence numbers in these frames can allow an adversary to track Apple devices across space and time, defeating existing anti-tracking techniques such as MAC address randomization.

Keywords: BLE, Bluetooth, privacy, tracking

DOI Editor to enter DOI
Received ..; revised ..; accepted ...

***Corresponding Author: Jeremy Martin:** The MITRE Corporation, E-mail: jbmartin@mitre.org
Douglas Alpuche: U.S. Naval Academy (USNA)
Kristina Bodeman: USNA
Lamont Brown: USNA
***Corresponding Author: Ellis Fenske:** USNA, E-mail: fenske@usna.edu
Lucas Foppe: USNA
***Corresponding Author: Travis Mayberry:** USNA, E-mail: mayberry@usna.edu
***Corresponding Author: Erik Rye:** CMAND, E-mail: rye@cmand.org
Brandon Sipes: USNA
Sam Teplov: USNA

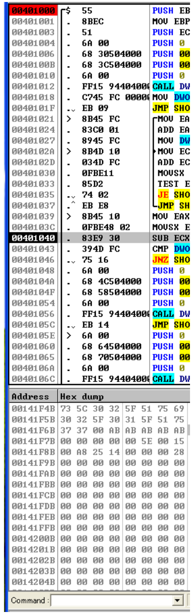
1 Introduction

The ubiquity of wirelessly connected mobile devices in the day-to-day lives of people globally has brought with it unprecedented risk of privacy violation for modern consumers. Mobile devices constantly transmit and receive information even while not in active use, and many of the protocols driving this communication are not designed with privacy in mind.

Tracking concerns and privacy leakages in 802.11 Wi-Fi are well-known and have been extensively studied over the last decade. Since Wi-Fi clients must actively probe for nearby access points to connect to, an adversary can listen to these probes and use the device's MAC address (which is included in probes) to identify and track it as it moves from place to place. This is not an academic threat: there are multimillion-dollar companies [39, 60] whose business model relies on using Wi-Fi tracking data for targeted marketing, and they control large networks of Wi-Fi access points that gather information on all nearby devices. Users are largely unaware that these widely-deployed tracking capabilities exist and that their Wi-Fi devices might be leaking sensitive data.

In response to this threat, device and OS manufacturers began to provide MAC address randomization as a privacy enhancement. Rather than using the same MAC address consistently, which enables correlation over multiple observations, devices employing MAC randomization instead choose random values, and change them periodically. While the principle itself is sound, many implementations of MAC address randomization have proven ineffective in practice [47, 64]. Defeating MAC address randomization is largely possible due not to flaws in Wi-Fi itself, but because of extraneous information in higher-layer protocols. Many technologies are not privacy-aware and leak information that can be used to track users and devices, despite the MAC address being effectively hidden through randomization.

Bluetooth, in both of its current protocol instantiations, also uses MAC addresses as hardware identifiers. BLE, which we examine exclusively in this study, has included mechanisms for a device to generate and use ran-



sciendo   Proceedings on Privacy Enhancing Technologies ; 2020 (1):26–46

Guillaume Celosia* and Mathieu Cunche

Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols

Abstract: Apple Continuity protocols are the underlying network component of *Apple Continuity* services which allow seamless nearby applications such as activity and file transfer, device pairing and sharing a network connection. Those protocols rely on Bluetooth Low Energy (BLE) to exchange information between devices: Apple Continuity messages are embedded in the payload of BLE advertisement packets that are periodically broadcasted by devices. Recently, Martin et al. identified [1] a number of privacy issues associated with Apple Continuity protocols; we show that this was just the tip of the iceberg and that Apple Continuity protocols leak a wide range of personal information.

In this work, we present a thorough reverse engineering of Apple Continuity protocols that we use to uncover a collection of privacy leaks. We introduce new artifacts, including identifiers, counters and battery levels, that can be used for passive tracking, and describe a novel active tracking attack based on Handoff messages. Beyond tracking issues, we shed light on severe privacy flaws. First, in addition to the trivial exposure of device characteristics and status, we found that HomeKit accessories betray human activities in a smarthome. Then, we demonstrate that AirDrop and Nearby Action protocols can be leveraged by passive observers to recover e-mail addresses and phone numbers of users. Finally, we exploit passive observations on the advertising traffic to infer Siri voice commands of a user.

Keywords: Bluetooth Low Energy; Privacy; Tracking; Activity inference; Inventory attacks; Perceptual hashing; Guesswork; Protocol.

DOI 10.2478/popets-2020-0003
Received 2019-05-31; revised 2019-09-15; accepted 2019-09-16.

***Corresponding Author: Guillaume Celosia:** Univ Lyon, INSA Lyon, Inria, CITI, F-69621 Villeurbanne, France, E-mail: guillaume.celosia@insa-lyon.fr
Mathieu Cunche: Univ Lyon, INSA Lyon, Inria, CITI, F-69621 Villeurbanne, France, E-mail: mathieu.cunche@insa-lyon.fr

1 Introduction

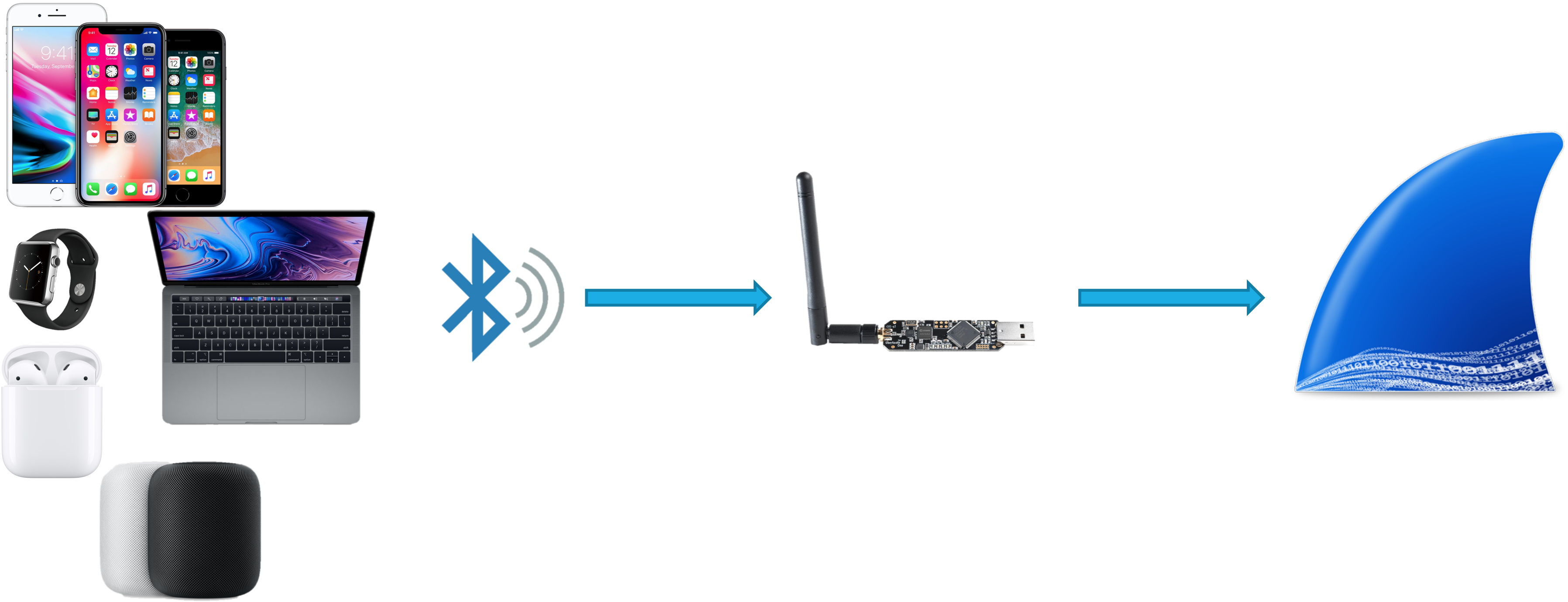
Smart devices interacting with each other are bringing new types of applications that simplify configuration procedures and enhance users experience. Those new applications include sending a file to a nearby device, transferring an activity to another device, network connection sharing, etc. Major vendors have developed protocols to enable those features: *Google Nearby* [2], *Microsoft Connected Devices Platform* (CDP) [3] and protocols developed by Apple, called *Apple Continuity protocols*, can be found in all Apple products but also in devices from third-party companies[1]. Thus, Apple Continuity protocols are embedded in more than one billion active devices [7], including smartphones, laptops, earphones, smartwatches and smarthome appliances. Within those devices, Apple Continuity protocols enable a range of services such as activity transfer, remote printing and smarthome monitoring.

Apple Continuity protocols rely on Bluetooth Low Energy (BLE) for the transport of information over the air: messages of continuity protocols are carried by BLE advertisement packets that are broadcasted and thus made available to all nearby devices.

Wireless communications functionalities of smart devices can represent privacy threats for users. In particular, Wi-Fi and Bluetooth/BLE signals can be used for users tracking [8, 9] and to infer other private attributes [10–12]. To remedy to the tracking issue, the Bluetooth Core Specification version 4.0 introduced the LE Privacy feature [13, Vol 3, Part C, sec. 10.7] that defines the use of temporary and random link layer identifiers. Several works [14, 15] have highlighted privacy issues associated with BLE showing that devices can still be tracked despite LE Privacy provisions. Furthermore, several serious issues have been recently discovered [1] in Apple Continuity protocols, allowing an attacker to track a device based on passive and active attacks.

1 Apple certified vendors [5] and HomeKit accessories manufacturers [6].

Methodology



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		

Types of Messages

Type	Message
3	AirPrint*
5	AirDrop
6	HomeKit*
7	AirPods (Proximity Pairing*)
8	"Hey Siri"*
9/10	AirPlay

Type	Message
11	Watch (Magic Switch*)
12	Handoff
13	Wi-Fi Settings (Tethering Target*)
14	Instant Hotspot (Tethering Source*)
15	Wi-Fi Join (Nearby Action*)
16	Nearby (Nearby Info*)

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

AirDrop*

- Transmitted when user attempts to AirDrop media
- Includes first 2 bytes of SHA256 of various user iCloud account data*

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Type=0x5</td><td colspan="8">Length</td><td colspan="16">0x00</td></tr>
<tr><td colspan="32">0x00</td></tr>
<tr><td colspan="16">0x00</td><td colspan="8">Version</td><td colspan="8">SHA256(AppleID)</td></tr>
<tr><td colspan="8">SHA256(AppleID)</td><td colspan="16">SHA256(Phone)</td><td colspan="8">SHA256(Email)</td></tr>
<tr><td colspan="8">SHA256(Email)</td><td colspan="16">SHA256(Email2)</td><td colspan="8">0x00</td></tr>
</table>

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

AirPod (Proximity Pairing*)

- Sent when user interacts with their AirPods
- Can observe current status of AirPods (in ear, in/out of case, etc.)

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="8">Type=0x7</td><td colspan="8">Length</td><td colspan="8">0x01</td><td colspan="8">Device Model</td></tr>
<tr><td colspan="8">Device Model</td><td colspan="8">Status</td><td colspan="4">Right Battery</td><td colspan="4">Left Battery</td><td></td><td>C</td><td>R</td><td>L</td><td colspan="4">Case Battery</td></tr>
<tr><td colspan="8">Lid Open Counter</td><td colspan="8">Device Color</td><td colspan="8">0x00</td><td colspan="8">Encrypted</td></tr>
<tr><td colspan="32">Encrypted</td></tr>
<tr><td colspan="32">Encrypted</td></tr>
<tr><td colspan="32">Encrypted</td></tr>
<tr><td colspan="24">Encrypted</td></tr>
</table>

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

Handoff

- Handoff messages sent whenever Handoff enabled apps are used
- Clipboard status
- Monotonically increasing IV (0-65535) based off user actions
- Data is encrypted

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="8">Type=0xC</td><td colspan="8">Length</td><td colspan="8">Clipboard Status</td><td colspan="8">IV (Seq num)</td></tr>
<tr><td colspan="8">IV (Seq num)</td><td colspan="8">GCM Auth</td><td colspan="16">Enc. Payload</td></tr>
<tr><td colspan="32">Encrypted Payload</td></tr>
<tr><td colspan="32">Encrypted Payload</td></tr>
</table>

Wi-Fi Settings (Tethering Target*)

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

0 – 7	8 – 15
Type - 0x0D	Length
iCloud ID	

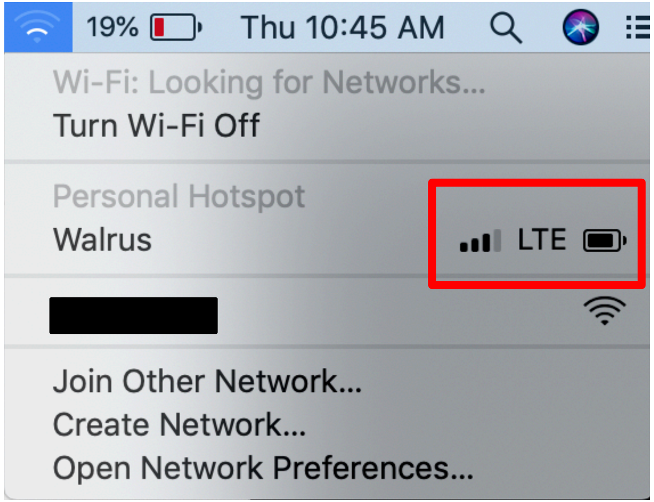
*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

Instant Hotspot (Tethering Source*)

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

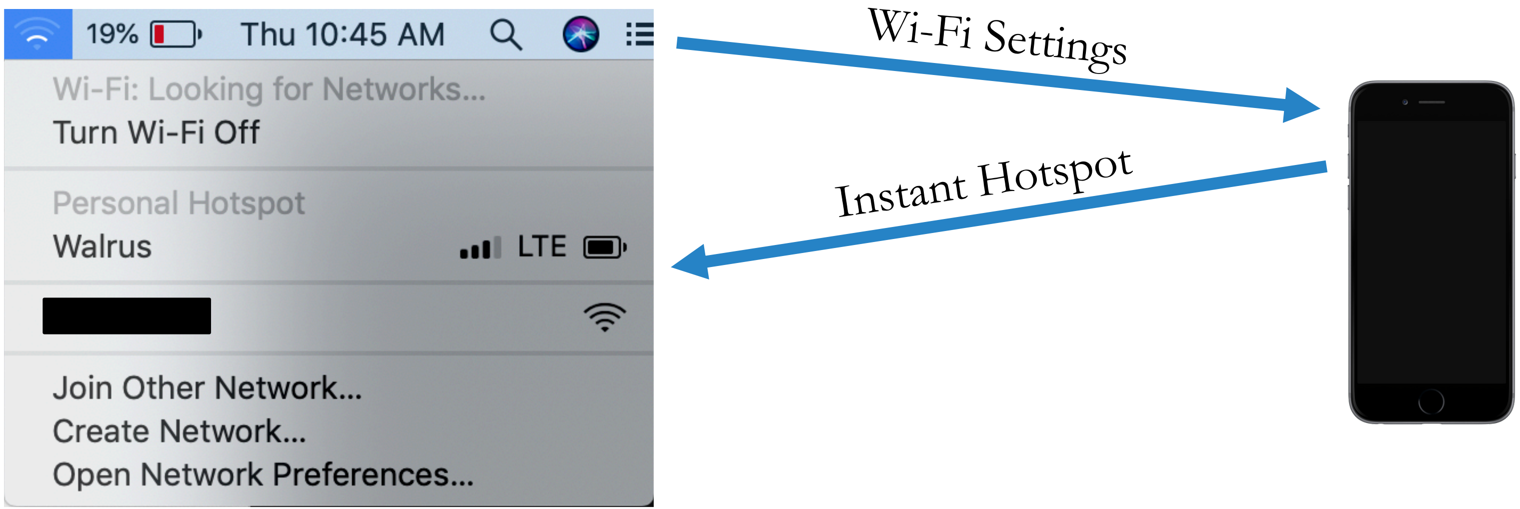
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

type=0xE	Length	Version	Flags
Battery Life	Data	Cell Type	Cell Signal



*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

Wi-Fi Settings and Hotspot Messages



Wi-Fi Joining (Nearby Action*)

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

0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Type=0x0F	Length	Action Flags	Action Type (0x08)
Auth Tag			SHA256(AppleID)
SHA256(AppleID)		SHA256(Phone #)	
SHA256(Phone #)	SHA256(Email)		
SHA256(SSID)			

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

Nearby (Nearby Info*)

- Indicate device state based off of user (in)action
- Allows for OS detection based off "iOS Dependent field"
- Messages never stop sending in iOS 12/13

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Type=0x10	Length	Status Flags	Action Code	iOS Dependent
Auth Tag				

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

Status Flags

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Type=0x10	Length	Status Flags	Action Code	iOS Dependent
Auth Tag				

Flag	Status
0001	Primary Device (Y/N)
0010	¯_(ツ)_/¯
0100	AirDrop Receiving (On/Off)
1000	Not Used

Action Codes

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Type=0x10	Length	Status Flags	Action Code	iOS Dependent
Auth Tag				

Value	Action
3	Locked Screen
7	Transition Phase
10	Locked Screen, Inform Watch
11	Active User
13	User is in a vehicle*
14	Phone Call or FaceTime

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

OS Fingerprinting

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Type=0x10	Length	Status Flags	Action Code	iOS Dependent
Auth Tag				

Data	iOS Version	Meaning
0x00	iOS 10	N/A
0x10	iOS 11	N/A
0x0C	iOS 12	Wi-Fi Join
0x18	iOS 12	Wi-Fi Off
0x1	iOS 12	Wi-Fi On

iOS 13 Fingerprinting

iOS 13

```
Access Address: 0x8e89bed6
Packet Header: 0x1740 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
Advertising Address: 68:8b:95:8c:bf:46
Advertising Data
  Flags
    Length: 2
    Type: Flags (0x01)
    Flag Value: 0x1a
    ...1 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): true (0x1)
    .... 1... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): true (0x1)
    .... .0.. = BR/EDR Not Supported: false (0x0)
    .... ..1. = LE General Discoverable Mode: true (0x1)
    .... ...0 = LE Limited Discoverable Mode: false (0x0)
  Tx Power Level
    Length: 2
    Type: Tx Power Level (0x0a)
    Power Level (dBm): 24
  Manufacturer Specific
    Length: 10
    Type: Manufacturer Specific (0xff)
    Company ID: Apple, Inc. (0x004c)
      Type: Nearby Info (16)
        Length: 5
        ...0 .... = Primary Device: N (0)
        ..0. .... = Watch State: Not Wearing Watch (0)
        .0.. .... = Screen State: Screen Off (0)
        .... 0001 = Action Code: Recently Updated/iPhone Setup (1)
        iOS Version: iOS 13.x
```

iOS 10, 11, 12

```
Access Address: 0x8e89bed6
Packet Header: 0x1440 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
Advertising Address: 46:71:73:d2:b9:66
Advertising Data
  Flags
    Length: 2
    Type: Flags (0x01)
    Flag Value: 0x1a
    ...1 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): true (0x1)
    .... 1... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): true (0x1)
    .... .0.. = BR/EDR Not Supported: false (0x0)
    .... ..1. = LE General Discoverable Mode: true (0x1)
    .... ...0 = LE Limited Discoverable Mode: false (0x0)
  Manufacturer Specific
    Length: 10
    Type: Manufacturer Specific (0xff)
    Company ID: Apple, Inc. (0x004c)
      Type: Nearby Info (16)
        Length: 5
        ...1 .... = Primary Device: Y (1)
        ..0. .... = Watch State: Not Wearing Watch (0)
        .0.. .... = Screen State: Screen Off (0)
        .... 1101 = Action Code: User is Driving a Vehicle (CarPlay) (13)
        iOS Version: iOS 12.x
        WiFi Status: WiFi Off (0x18)
        Auth Tag: ddba94
    Company ID: Apple, Inc. (0x004c)
CRC: 0xc4f950
```

macOS Fingerprinting

macOS

```
▼ Bluetooth Low Energy Link Layer
  ▶ Access Address: 0x8e89bed6
  ▶ Packet Header: 0x1440 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
    Advertising Address: 70:b1:87:12:a0:57
  ▼ Advertising Data
    ▼ Flags
        Length: 2
        Type: Flags (0x01)
        Flag Value: 0x06
        ...0 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x0)
        .... 0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x0)
        .... .1.. = BR/EDR Not Supported: true (0x1)
        .... ..1. = LE General Discoverable Mode: true (0x1)
        .... ...0 = LE Limited Discoverable Mode: false (0x0)
    ▼ Manufacturer Specific
        Length: 10
        Type: Manufacturer Specific (0xff)
      ▼ Company ID: Apple, Inc. (0x004c)
        ▼ Type: Nearby Info (16)
            Length: 5
            ...0 .... = Primary Device: N (0)
            ..0. .... = Watch State: Not Wearing Watch (0)
            .0.. .... = Screen State: Screen Off (0)
            .... 0111 = Action Code: Transition to Inactive User or from Locked Screen (7)
            iOS Version: macOS
            WiFi Status: WiFi On (0x1c)
            Auth Tag: 767a87
        Company ID: Apple, Inc. (0x004c)
  CRC: 0x540eb5
```

iPhones, watches, etc.

```
▼ Bluetooth Low Energy Link Layer
  ▶ Access Address: 0x8e89bed6
  ▶ Packet Header: 0x1440 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
    Advertising Address: 46:71:73:d2:b9:66
  ▼ Advertising Data
    ▼ Flags
        Length: 2
        Type: Flags (0x01)
        Flag Value: 0x1a
        ...1 .... = Simultaneous LE and BR/EDR to Same Device Capable (Host): true (0x1)
        .... 1... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): true (0x1)
        .... .0.. = BR/EDR Not Supported: false (0x0)
        .... ..1. = LE General Discoverable Mode: true (0x1)
        .... ...0 = LE Limited Discoverable Mode: false (0x0)
    ▼ Manufacturer Specific
        Length: 10
        Type: Manufacturer Specific (0xff)
      ▼ Company ID: Apple, Inc. (0x004c)
        ▼ Type: Nearby Info (16)
            Length: 5
            ...1 .... = Primary Device: Y (1)
            ..0. .... = Watch State: Not Wearing Watch (0)
            .0.. .... = Screen State: Screen Off (0)
            .... 1101 = Action Code: User is Driving a Vehicle (CarPlay) (13)
            iOS Version: iOS 12.x
            WiFi Status: WiFi Off (0x18)
            Auth Tag: ddba94
        Company ID: Apple, Inc. (0x004c)
  CRC: 0xc4f950
```

User Tracking via Static Fields

- Nearby & Handoff Data remain static during MAC address change
- This allows random MAC addresses to be correlated

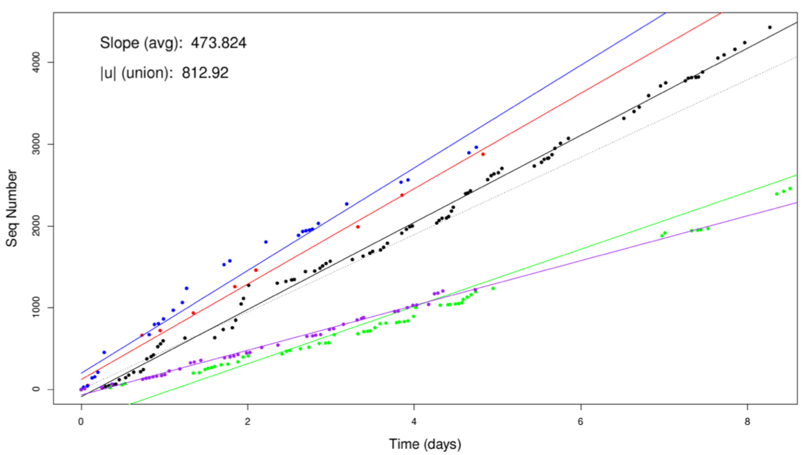
Time	Advertising Address	Unk (Nearby) Data
899.987876800	60:45:7a:bb:3f:2f	e77352
900.019127100	60:45:7a:bb:3f:2f	e77352
900.049127000	4b:80:5c:b1:92:2e	e77352
900.060377200	4b:80:5c:b1:92:2e	e77352
900.107877600	4b:80:5c:b1:92:2e	73b3f7

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

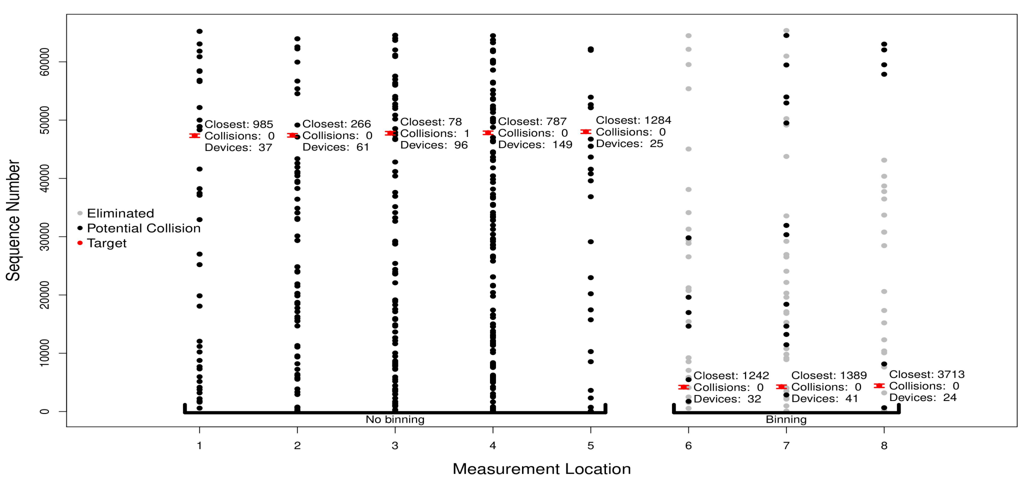
User Tracking via Handoff IV

- The IV in Handoff messages increments sequentially, based off user actions
- Can be used as a tracking mechanism, defeating MAC address randomization

User Measurements



Sequence Number Collisions



Live Demo

Disclosure & Remediation

- Disclosed to Apple in March, 2019
- Encrypt messages
- Rotate MAC addresses stochastically, more frequently, and change data
- Change IV generation

Wireshark Dissector

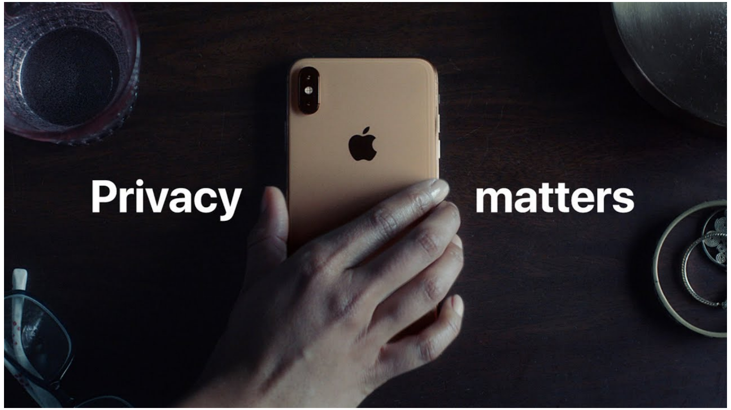
- https://github.com/furiousmac/continuity
- Supports:
  - Stable Release (3.2.1)
  - Old Stable Release (3.0.8)
- Still being updated with new message types

Final Thoughts

- Individually, each message leaks a small amount of data
- In aggregate, they can be used to conduct OS fingerprinting, behavioral profiling, and user tracking

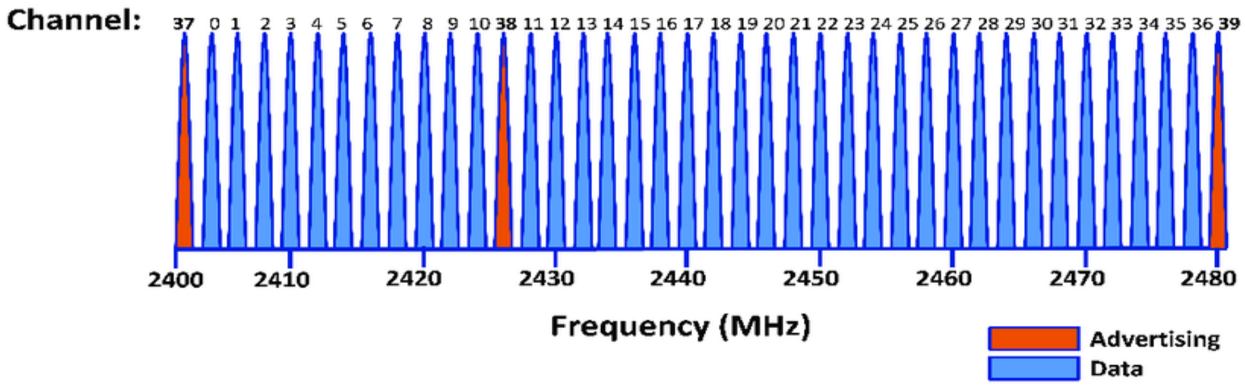
Why Apple?

- 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



Watch (Magic Switch*)

- Sent if Apple Watch loses connection to paired phone
- Contains confidence value for if watch is on wrist or not*

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Type=0xB	Length	Data
Confidence		

*Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 26-46.

MacOS Breaks Itself

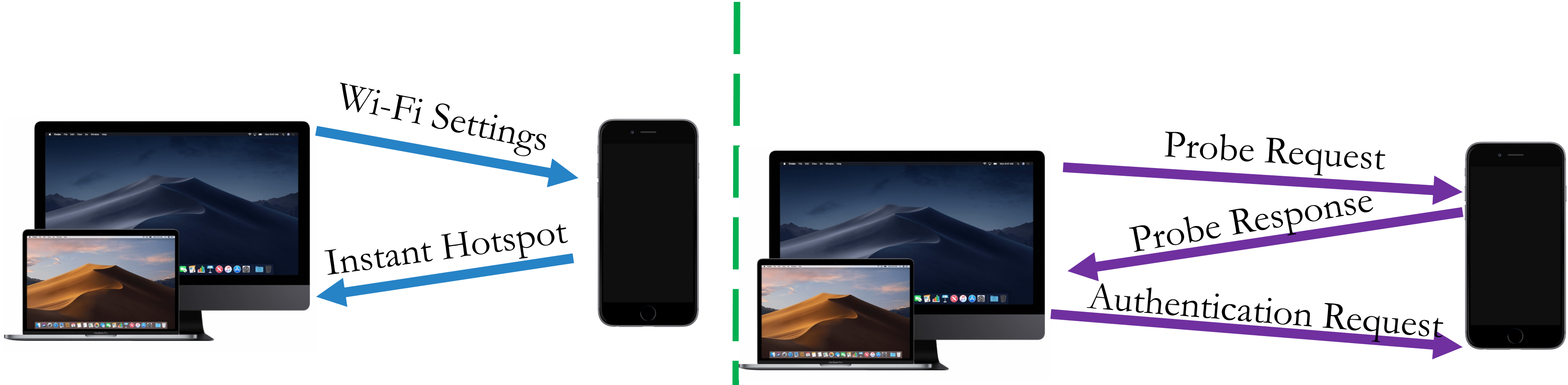
- In Mojave and High Sierra, globally unique BLE MAC address is leaked
- When Handoff and Nearby messages are sent concurrently, Nearby messages use the globally unique BLE MAC address
- Wi-Fi MAC is known when BLE MAC address is $\pm$ 1 from Wi-Fi MAC address

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

Defeat of MAC Address Randomization



Bluetooth Low Energy | **Wi-Fi**

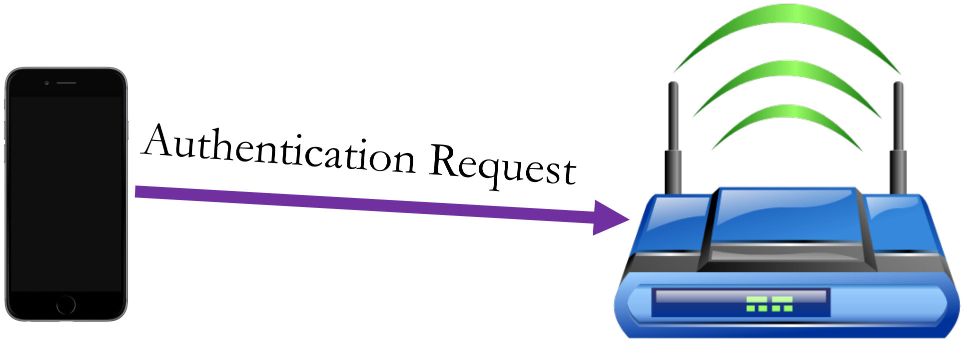
Hotspot Probe Response

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
```

Defeat of MAC Address Randomization

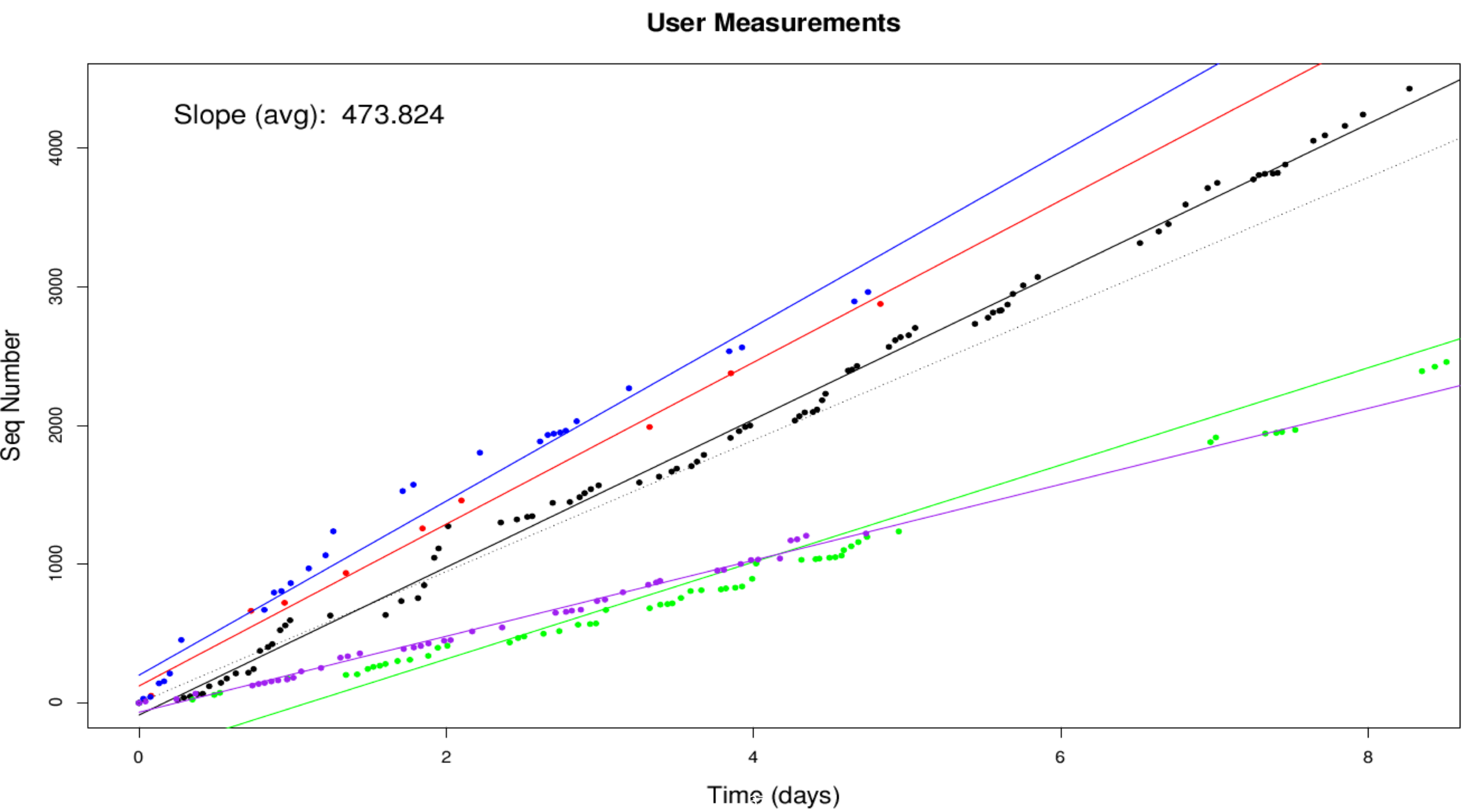
Bluetooth Low Energy



Wi-Fi

Sequence Number Trajectories

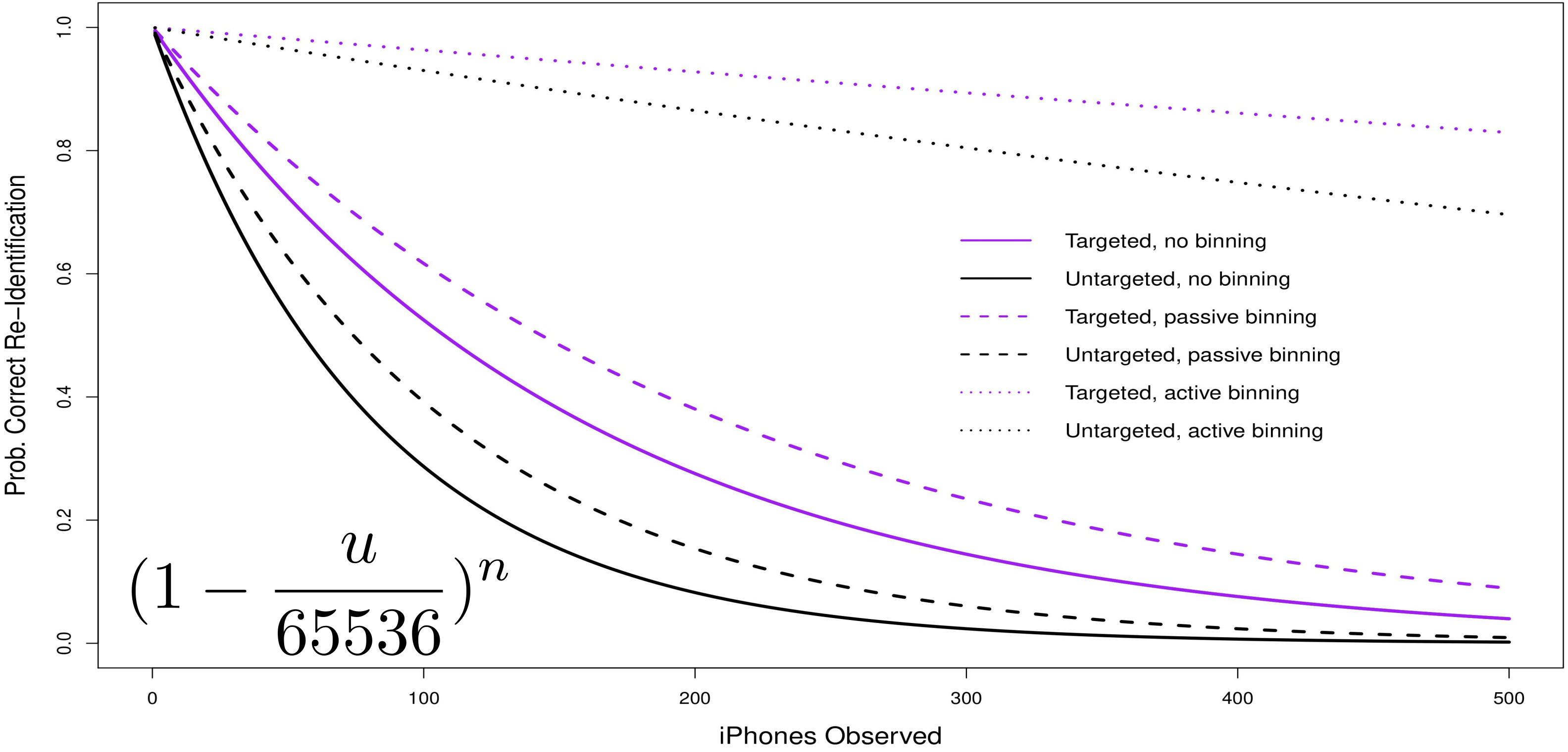
- Captured sequence numbers on 4 students and 1 faculty
- Data collected ~1 hour intervals for a week
- Data shows that sequence numbers increase slowly (~470/day)


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

Attack Scenario

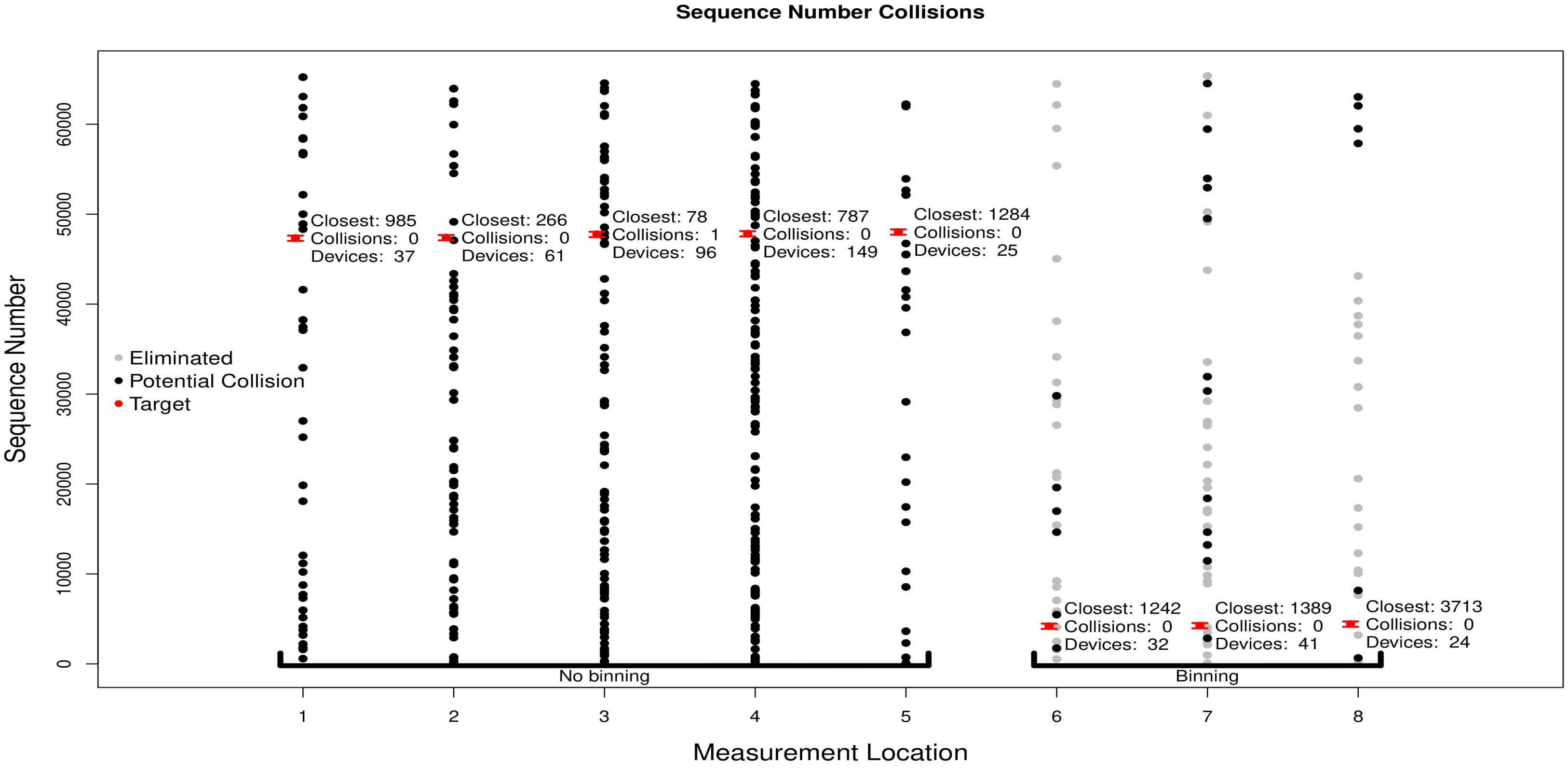
- **Goal: Identify a previously observed phone**
- Capture individual's random BLE MAC and sequence number
- Calculate trajectory and range of victim sequence number
- 1 week later, the victim's BLE MAC address has changed, but can reacquire by using difference in sequence numbers

Theoretical Results



$$\left(1 - \frac{u}{65536}\right)^n$$

Real Results



Apple’s Response

From: **product-security@apple.com** <product-security@apple.com>
Date: Mon, Jul 15, 2019, 15:41
Subject: Re: Re: Privacy Issues with Continuity and use of Bluetooth Low Energy; Follow-up:[redacted]
To: [redacted]

Hello FURIOUSMAC Team,

I apologize for the delay in getting back to you.

Thank you again for sharing your paper with us. The paper brought up many good points, and many of which we have been working on.

We are still working to address some of the points you raised and if will reach out for recognition once they are addressed. We appreciate your willingness to share your research with us.

Best regards,
[redacted]
Apple Product Security