# Rethinking the Security and Privacy of Bluetooth Low Energy

Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

04/14/2023

# Outline

1. Introduction

2. BLE Security

3. BLE Privacy

4. Takeaway

# Outline

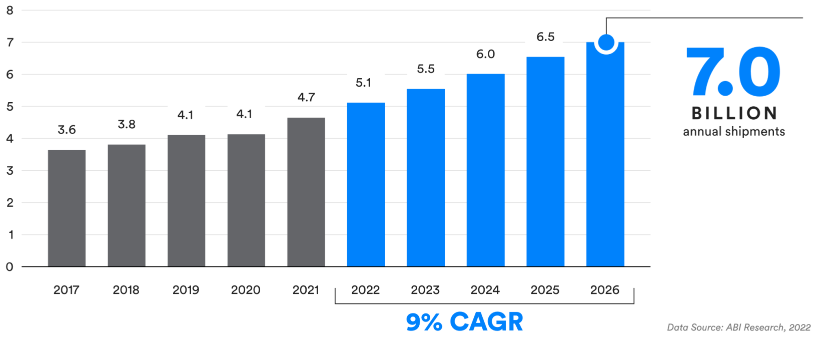
1. Introduction
2. BLE Security
3. BLE Privacy
4. Takeaway

# What is Bluetooth

# What is Bluetooth

## Total Annual Bluetooth® Device Shipments

NUMBERS IN BILLIONS



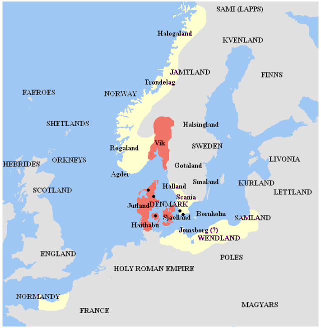
Data Source: ABI Research, 2022

# Why Named Bluetooth

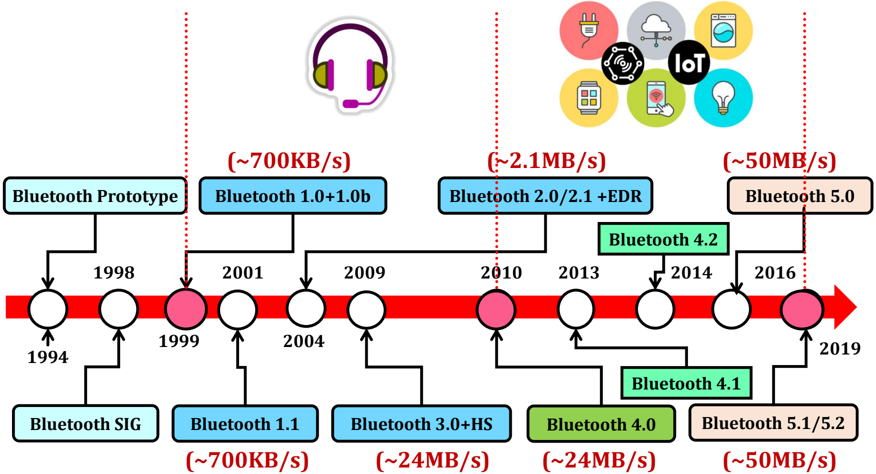
## Harald “Bluetooth” Gormsson

- King of Denmark 940-981.
- He was also known for his bad **tooth**, which had a very dark **blue-grey** shade.
- He united the Tribes of Denmark.

The technology was named after the king in 1997, based on an analogy **that the technology would unite devices the way Harald Bluetooth united the tribes of Denmark into a single kingdom**.



# History of Bluetooth



IoT

(~700KB/s) (~2.1MB/s) (~50MB/s)

Bluetooth Prototype

Bluetooth 1.0+1.0b

Bluetooth 2.0/2.1 +EDR

Bluetooth 5.0

Bluetooth 4.2

1998 2001 2009 2010 2013 2014 2016

1994 1999 2004 2019

Bluetooth 4.1

Bluetooth SIG

Bluetooth 1.1

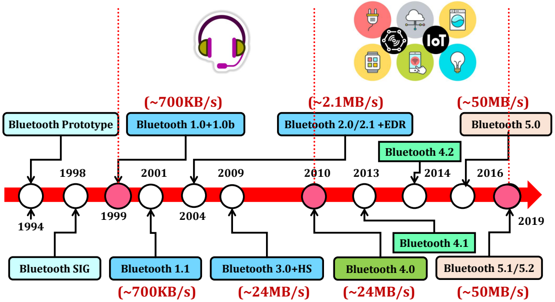
Bluetooth 3.0+HS

Bluetooth 4.0

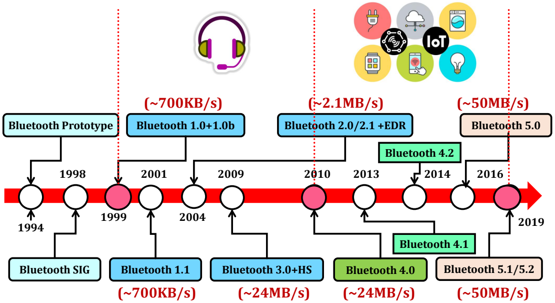
Bluetooth 5.1/5.2

(~700KB/s) (~24MB/s) (~24MB/s) (~50MB/s)

# Our Recent Works on Bluetooth Security and Privacy

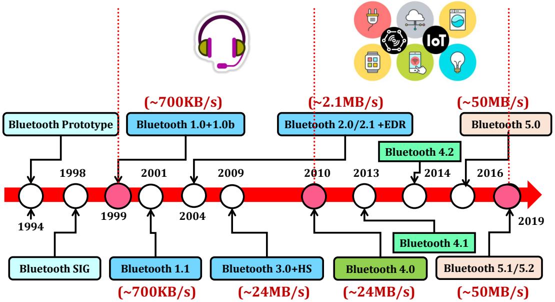


# Our Recent Works on Bluetooth Security and Privacy



1. **BLEScope: Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps**. In ACM CCS 2019
2. **FirmXRay: Detecting Bluetooth Link Layer Vulnerabilities From Bare-Metal Firmware**. In ACM CCS 2020.
3. **Breaking Secure Pairing of Bluetooth Low Energy in Mobile Devices Using Downgrade Attacks**. In USENIX Security 2020
4. **On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps**. In SECURECOMM. October 2020
5. **When Good Becomes Evil: Tracking Bluetooth Low Energy Devices via Allowlist-based Side Channel and Its Countermeasure"**. In ACM CCS 2022 (Best paper award honorable mention)
6. **Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing**. In NDSS 2023

# Our Recent Works on Bluetooth Security and Privacy



1. ~~BLEScope: Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps. In ACM CCS 2019~~
2. ~~FirmXRay: Detecting Bluetooth Link Layer Vulnerabilities From Bare-Metal Firmware. In ACM CCS 2020.~~
3. **Breaking Secure Pairing of Bluetooth Low Energy in Mobile Devices Using Downgrade Attacks**. In USENIX Security 2020
4. ~~On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps. In SECURECOMM. October 2020~~
5. **When Good Becomes Evil: Tracking Bluetooth Low Energy Devices via Allowlist-based Side Channel and Its Countermeasure”**. In ACM CCS 2022 (Best paper award honorable mention)
6. ~~Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing. In NDSS 2023~~

# Outline

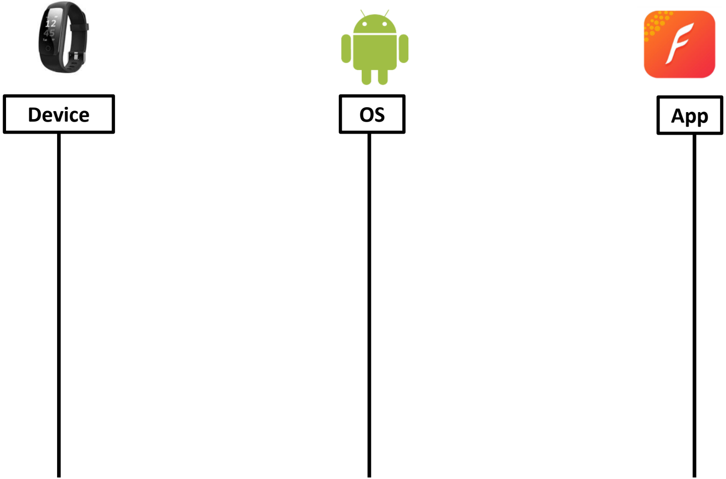
1. Introduction

2. BLE Security

3. BLE Privacy

4. Takeaway

# Pairing Workflow

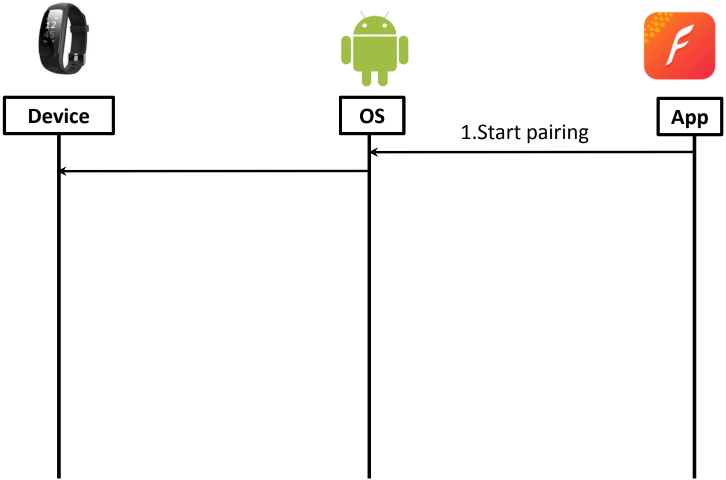


Device

OS

App

# Pairing Workflow



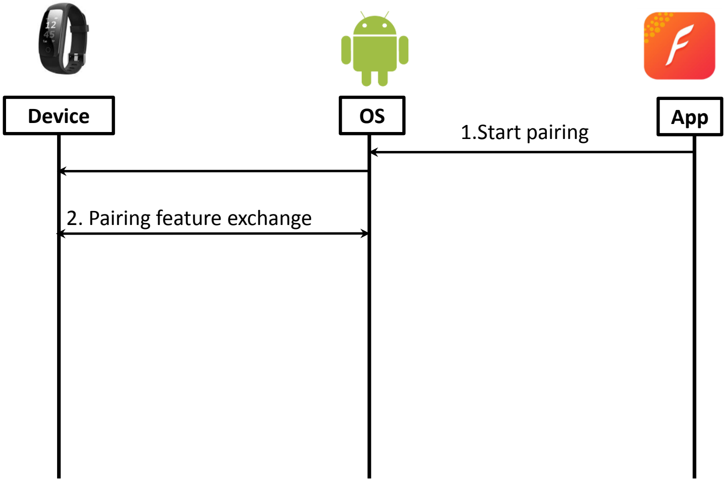
Device

OS

App

1.Start pairing

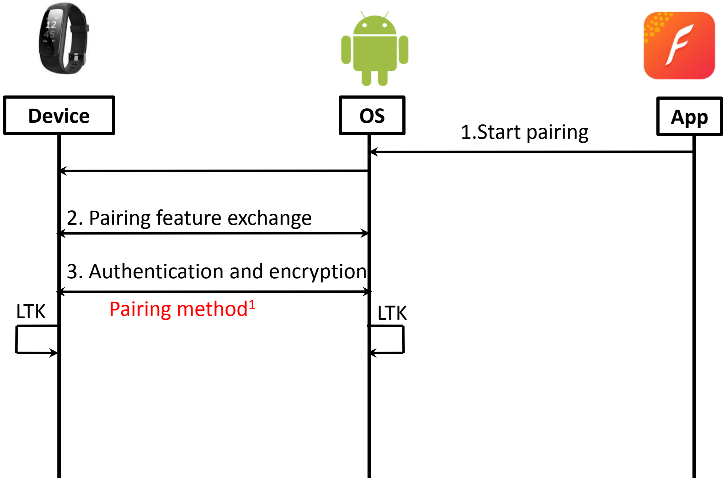
# Pairing Workflow



**I/O Features**

- Keypad
- Screen
- Out of band Channel

# Pairing Workflow



Device

OS

App

1.Start pairing

2. Pairing feature exchange

3. Authentication and encryption

Pairing method[1]

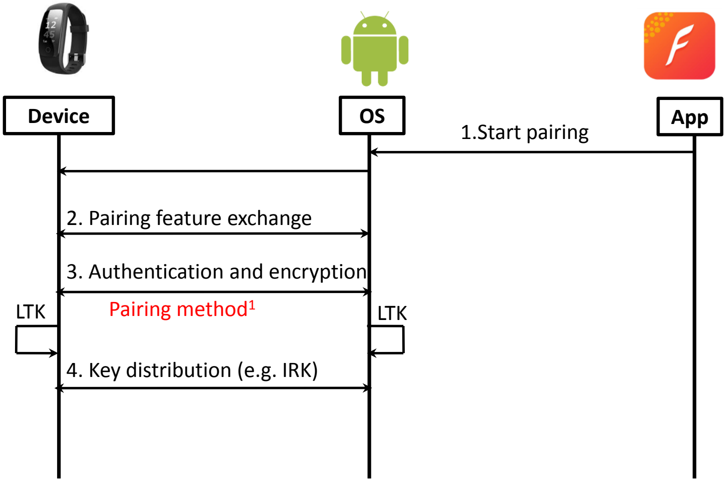
LTK

LTK

**Pairing Methods**

- Just Works
- Passkey Entry
- Out of band
- Numeric Comparison

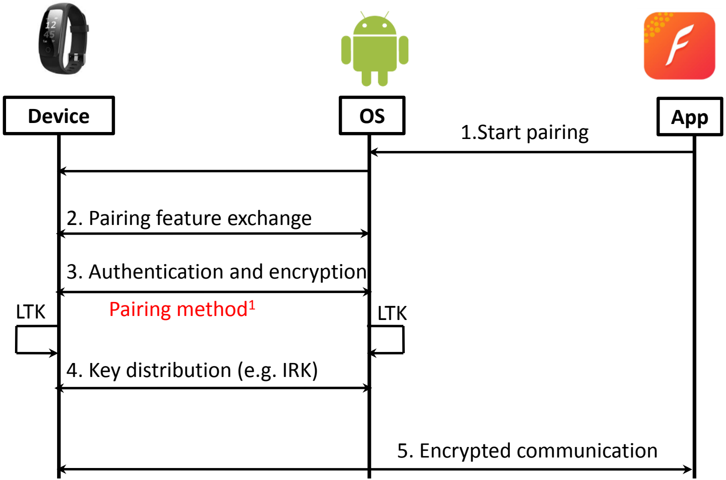
# Pairing Workflow


Device
OS
App
1.Start pairing
2. Pairing feature exchange
3. Authentication and encryption
Pairing method[1]
LTK
LTK
4. Key distribution (e.g. IRK)

**Pairing Methods**

- Just Works
- Passkey Entry
- Out of band
- Numeric Comparison

# Pairing Workflow


Device
OS
App
1.Start pairing
2. Pairing feature exchange
3. Authentication and encryption
Pairing method[1]
LTK
LTK
4. Key distribution (e.g. IRK)
5. Encrypted communication

**Pairing Methods**

- Just Works
- Passkey Entry
- Out of band
- Numeric Comparison

# Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$

# Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$
2. Bob generates a random ECC key pair: $\{Pri_B, PK_B = Pri_B$ * G$\}$

# Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$
2. Bob generates a random ECC key pair: $\{Pri_B, PK_B = Pri_B$ * G$\}$
3. Alice and Bob exchanges $PK_A$ and $PK_B$

# Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$
2. Bob generates a random ECC key pair: $\{Pri_B, PK_B = Pri_B$ * G$\}$
3. Alice and Bob exchanges $PK_A$ and $PK_B$
4. Alice calculates sharedKey: $K_A = Pri_A * PK_B$

## Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

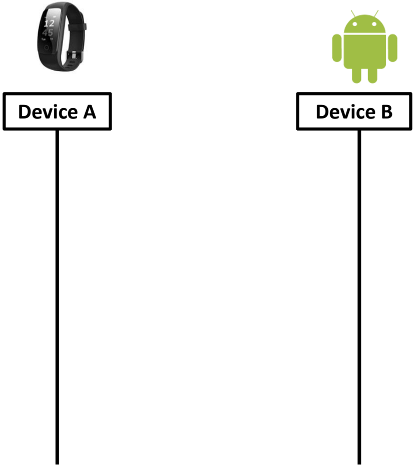
1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$
2. Bob generates a random ECC key pair: $\{Pri_B, PK_B = Pri_B$ * G$\}$
3. Alice and Bob exchanges $PK_A$ and $PK_B$
4. Alice calculates sharedKey: $K_A = Pri_A * PK_B$
5. Bob calculates sharedKey: $K_B = Pri_B * PK_A$

# Workflow of Pairing: Elliptic Curve Diffie–Hellman (**ECDH**) Key Exchange

1. Alice generates a random ECC key pair: $\{Pri_A, PK_A = Pri_A$ * G$\}$
2. Bob generates a random ECC key pair: $\{Pri_B, PK_B = Pri_B$ * G$\}$
3. Alice and Bob exchanges $PK_A$ and $PK_B$
4. Alice calculates sharedKey: $K_A = Pri_A * PK_B$
5. Bob calculates sharedKey: $K_B = Pri_B * PK_A$

$$Pri_A * (Pri_B * G) = Pri_B * (Pri_A * G)$$

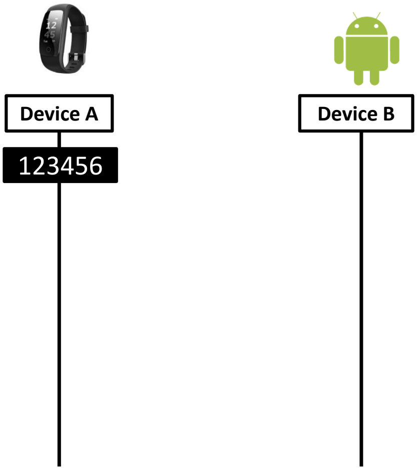
# Workflow of Passkey Entry



Device A

Device B

# Workflow of Passkey Entry

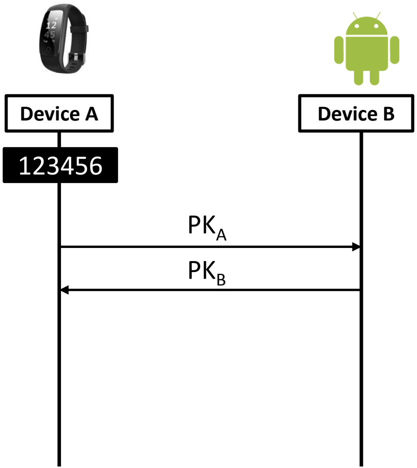


Device A

Device B

123456

# Workflow of Passkey Entry



Device A

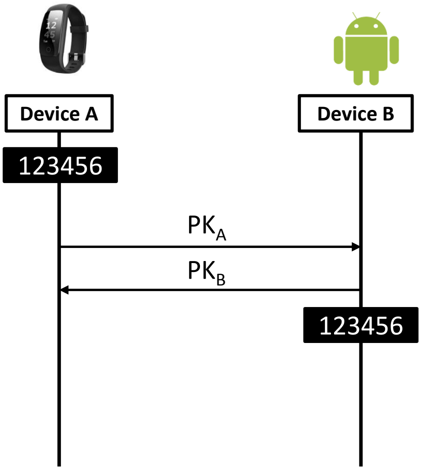
Device B

123456

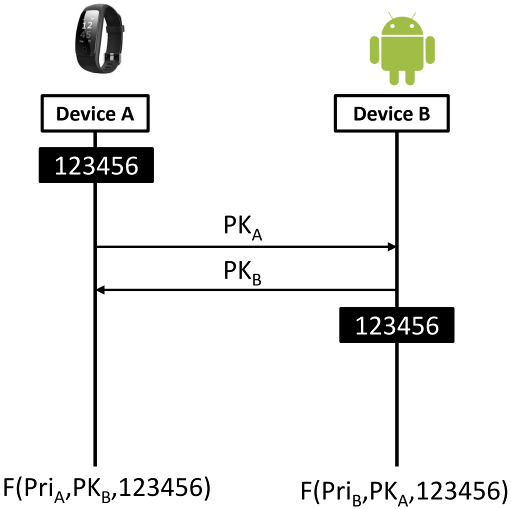
$PK_A$

$PK_B$

# Workflow of Passkey Entry



# Workflow of Passkey Entry



Device A

Device B

123456

$PK_A$

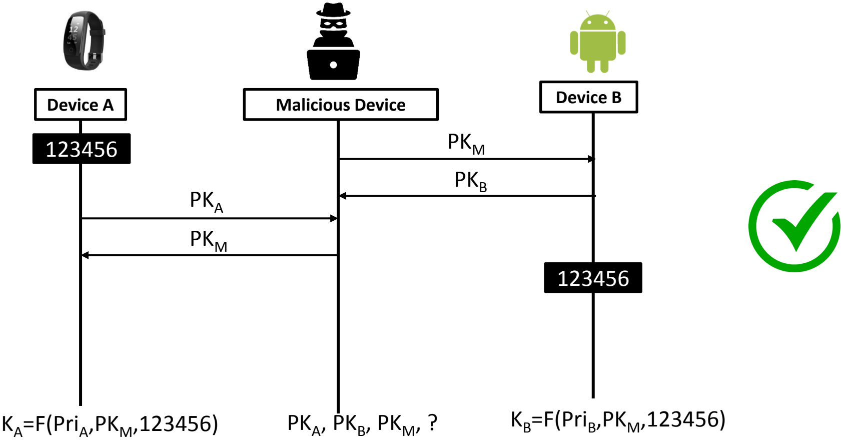
$PK_B$

123456

$F(Pri_A,PK_B,123456)$

$F(Pri_B,PK_A,123456)$

# Workflow of Passkey Entry



Device A

Malicious Device

Device B

123456

$PK_M$

$PK_B$

$PK_A$

$PK_M$

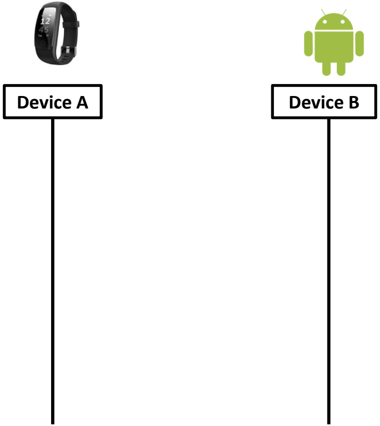
123456

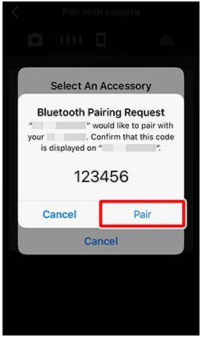
$K_A$=F($Pri_A$,$PK_M$,123456)

$PK_A$, $PK_B$, $PK_M$, ?

$K_B$=F($Pri_B$,$PK_M$,123456)

# Workflow of Numeric Comparison





Pair with camera

Select An Accessory

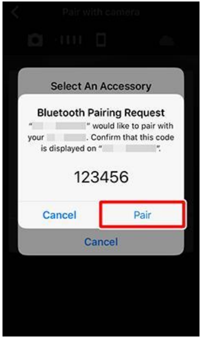
Bluetooth Pairing Request

“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456

Cancel | Pair

Cancel



Pair with camera

Select An Accessory

Bluetooth Pairing Request

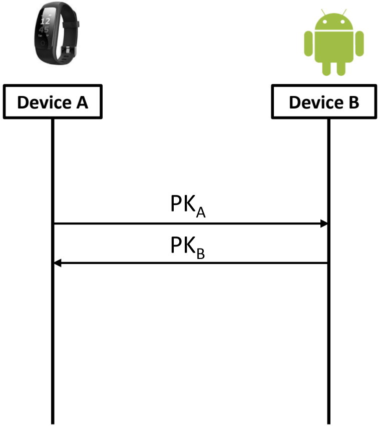
“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

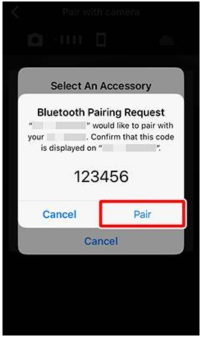
123456

Cancel | Pair

Cancel

# Workflow of Numeric Comparison



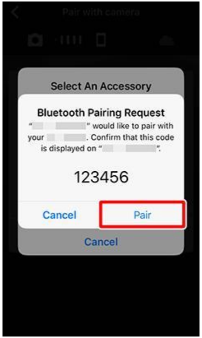


Select An Accessory

Bluetooth Pairing Request

“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456



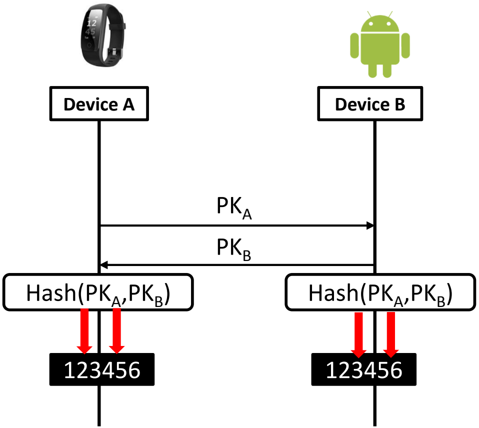
Select An Accessory

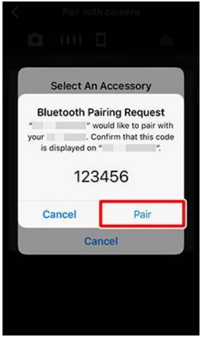
Bluetooth Pairing Request

“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456

# Workflow of Numeric Comparison




Pair with camera

Select An Accessory

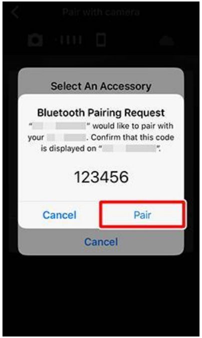
Bluetooth Pairing Request

“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456

Cancel Pair

Cancel


Pair with camera

Select An Accessory

Bluetooth Pairing Request

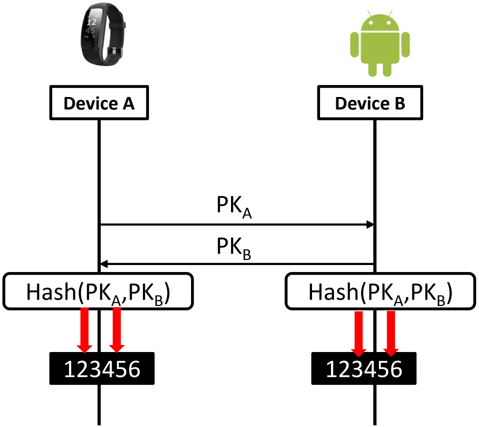
“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

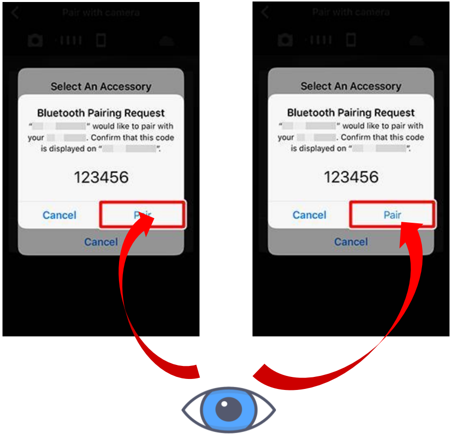
123456

Cancel Pair

Cancel

# Workflow of Numeric Comparison





Select An Accessory

Bluetooth Pairing Request

"[redacted]" would like to pair with your [redacted]. Confirm that this code is displayed on "[redacted]".

123456

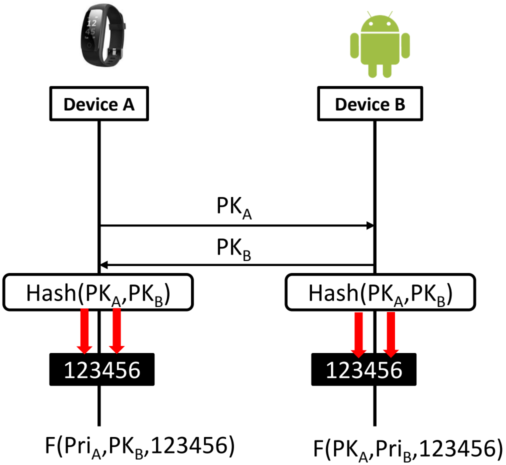
Select An Accessory

Bluetooth Pairing Request

"[redacted]" would like to pair with your [redacted]. Confirm that this code is displayed on "[redacted]".

123456

# Workflow of Numeric Comparison



Device A

Device B

$PK_A$

$PK_B$

$Hash(PK_A,PK_B)$

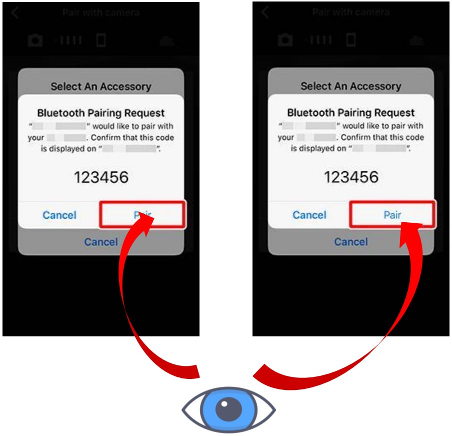
$Hash(PK_A,PK_B)$

123456

123456

$F(Pri_A,PK_B,123456)$

$F(PK_A,Pri_B,123456)$



Pair with camera

Select An Accessory

**Bluetooth Pairing Request**

“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456

Cancel | Pair

Cancel

Pair with camera

Select An Accessory

**Bluetooth Pairing Request**

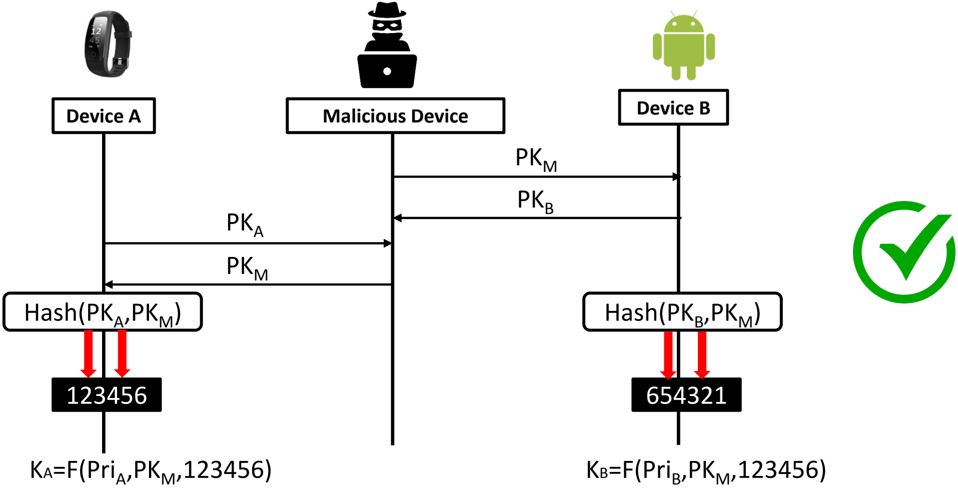
“[redacted]” would like to pair with your [redacted]. Confirm that this code is displayed on “[redacted]”.

123456

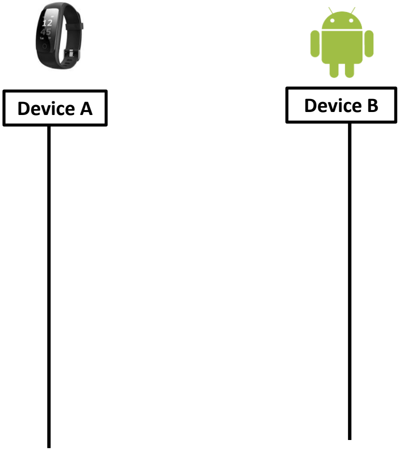
Cancel | Pair

Cancel

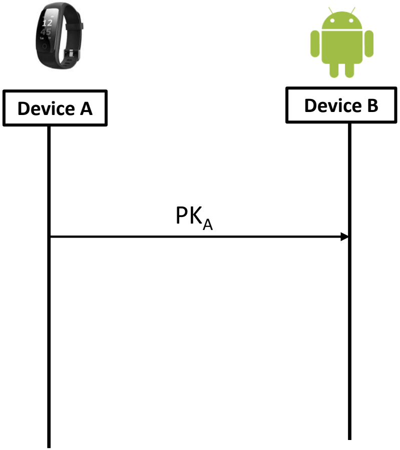
# Workflow of Numeric Comparison



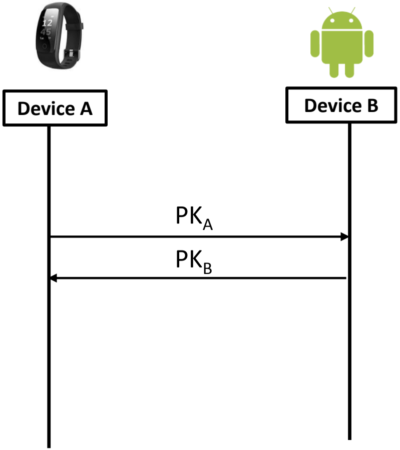
# Workflow of Out of Band



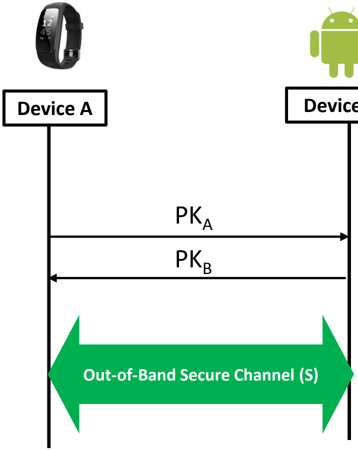
# Workflow of Out of Band



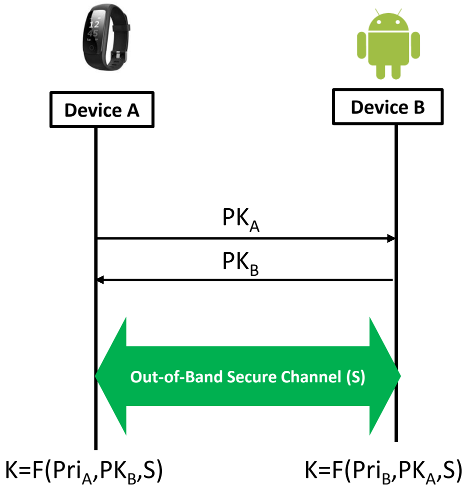
# Workflow of Out of Band



# Workflow of Out of Band



# Workflow of Out of Band



Device A

Device B

$PK_A$

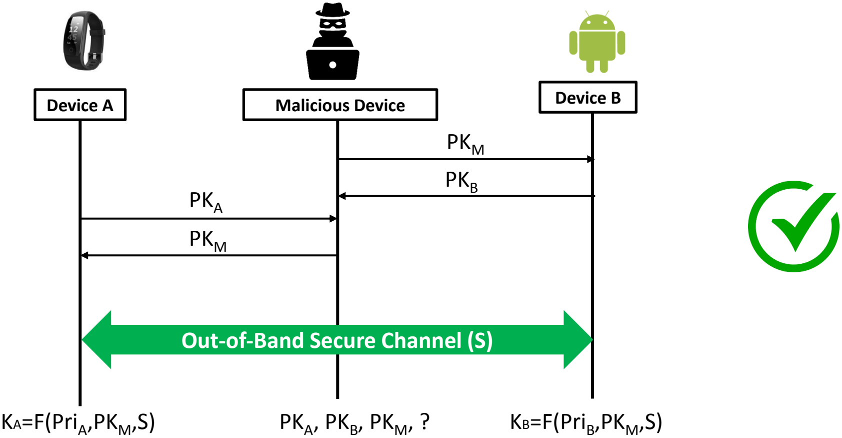
$PK_B$

Out-of-Band Secure Channel (S)

$K=F(Pri_A,PK_B,S)$

$K=F(Pri_B,PK_A,S)$

# Workflow of Out of Band



Device A

Malicious Device

Device B

$PK_M$

$PK_B$

$PK_A$

$PK_M$

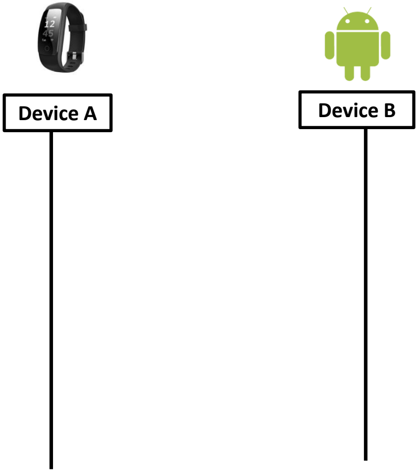
Out-of-Band Secure Channel (S)

$K_A=F(Pri_A,PK_M,S)$

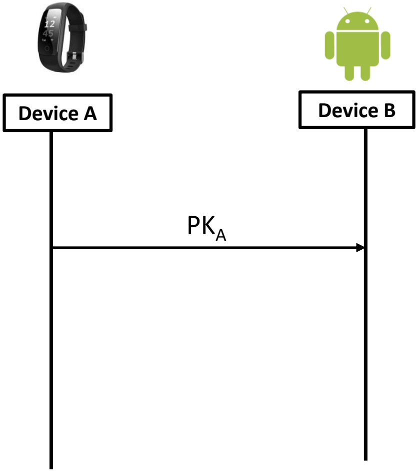
$PK_A$, $PK_B$, $PK_M$, ?

$K_B=F(Pri_B,PK_M,S)$

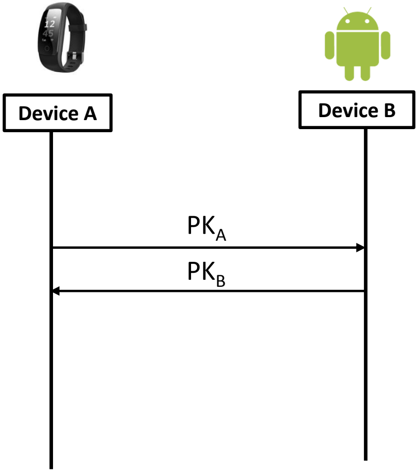
# Workflow of Justworks



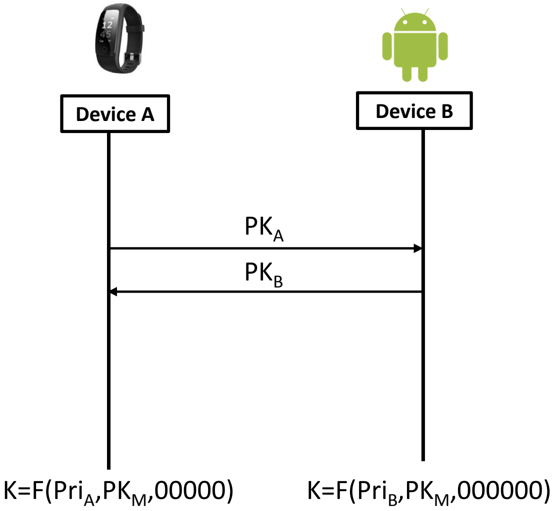
# Workflow of Justworks



# Workflow of Justworks



# Workflow of Justworks



Device A

Device B

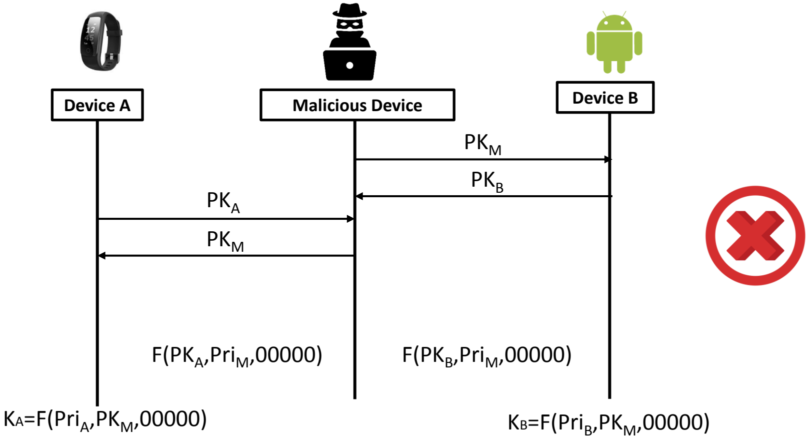
$PK_A$

$PK_B$

$K=F(Pri_A,PK_M,00000)$

$K=F(Pri_B,PK_M,000000)$

# Workflow of Justworks



Device A

Malicious Device

Device B

$PK_M$

$PK_B$

$PK_A$

$PK_M$

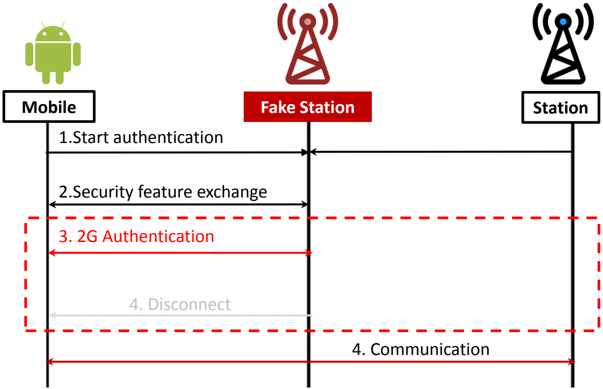
$F(PK_A,Pri_M,00000)$

$F(PK_B,Pri_M,00000)$

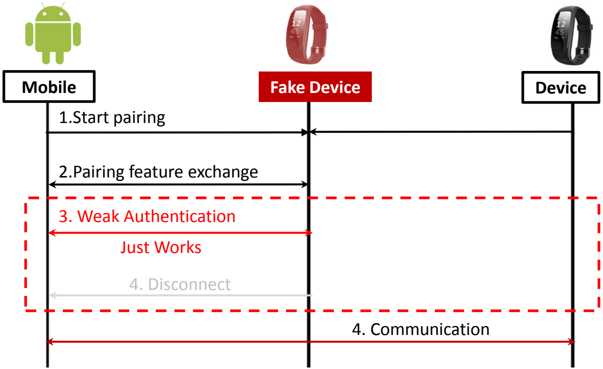
$K_A=F(Pri_A,PK_M,00000)$

$K_B=F(Pri_B,PK_M,00000)$

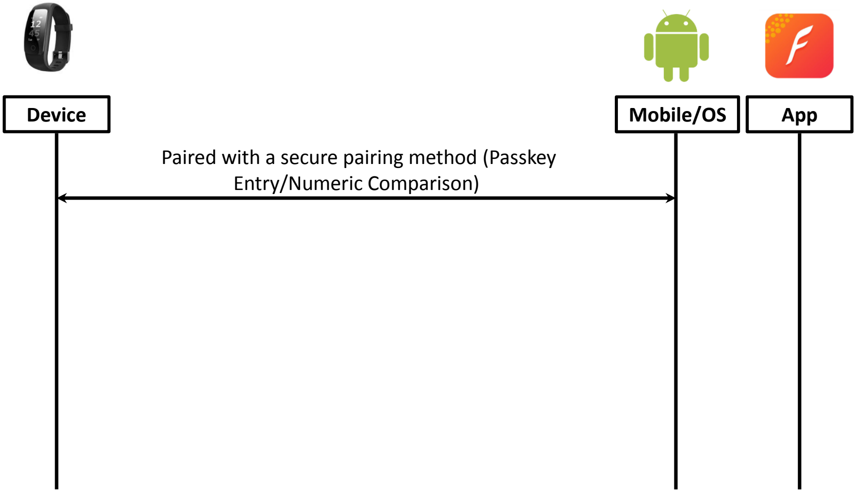
# Our Downgrade Attacks against Bluetooth Low Energy



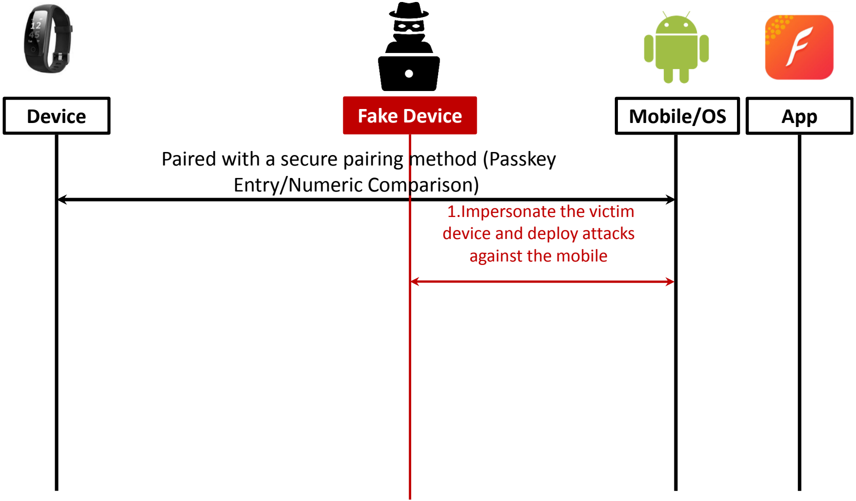
# Our Downgrade Attacks against Bluetooth Low Energy



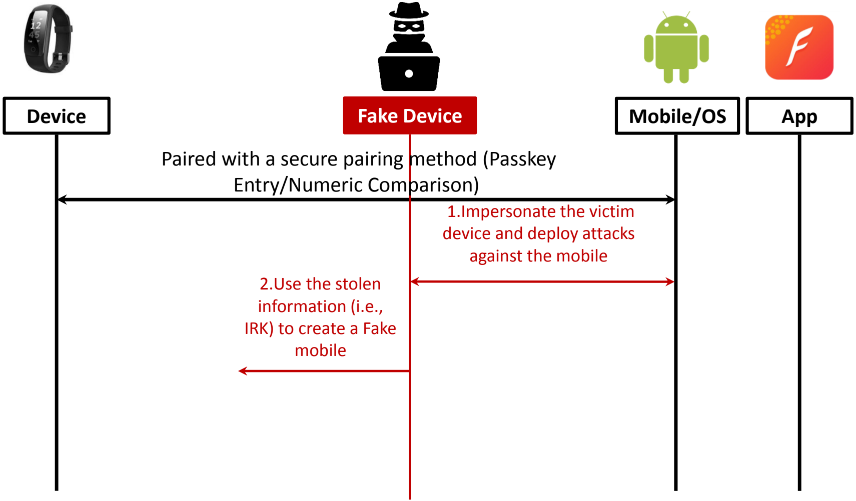
# Our Downgrade Attacks against Bluetooth Low Energy


Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)

# Our Downgrade Attacks against Bluetooth Low Energy


Device
Fake Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)
1.Impersonate the victim device and deploy attacks against the mobile

# Our Downgrade Attacks against Bluetooth Low Energy



Device

Fake Device

Mobile/OS

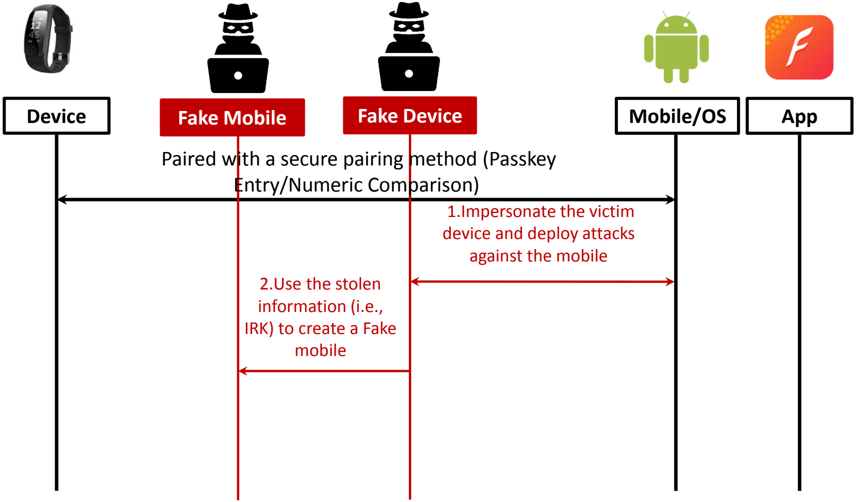
App

Paired with a secure pairing method (Passkey Entry/Numeric Comparison)

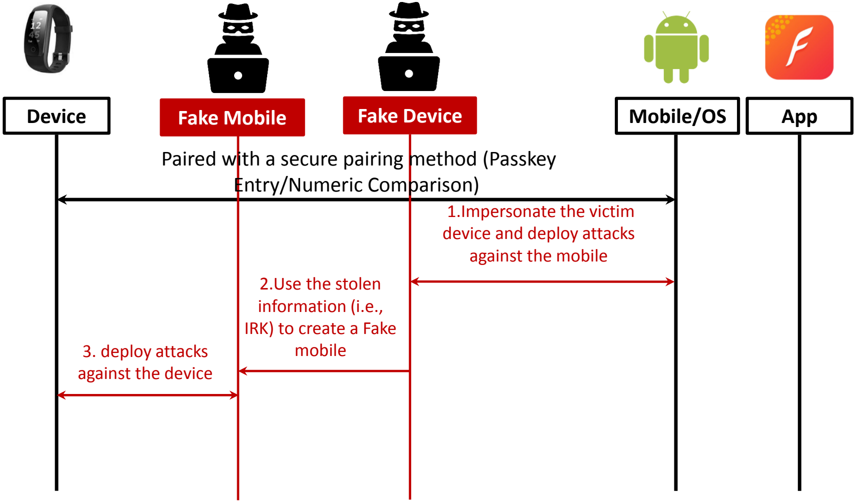
1.Impersonate the victim device and deploy attacks against the mobile

2.Use the stolen information (i.e., IRK) to create a Fake mobile

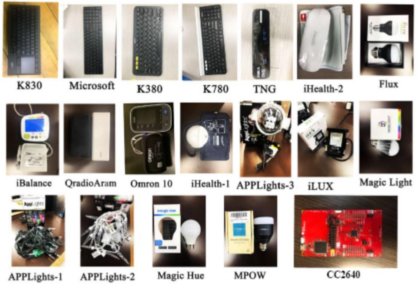
# Our Downgrade Attacks against Bluetooth Low Energy


Device
Fake Mobile
Fake Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)
1.Impersonate the victim device and deploy attacks against the mobile
2.Use the stolen information (i.e., IRK) to create a Fake mobile

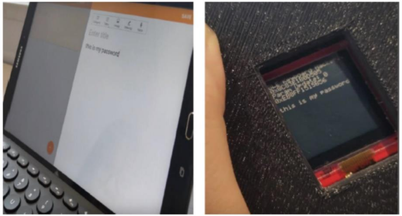
# Our Downgrade Attacks against Bluetooth Low Energy


Device
Fake Mobile
Fake Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)
1.Impersonate the victim device and deploy attacks against the mobile
2.Use the stolen information (i.e., IRK) to create a Fake mobile
3. deploy attacks against the device

# Our Downgrade Attacks against Bluetooth Low Energy



The Tested BLE devices

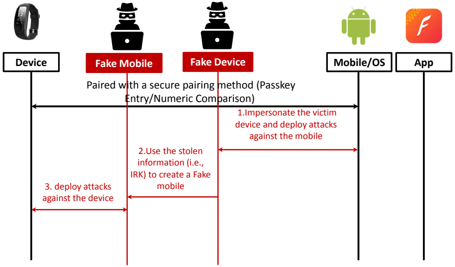

User

Attacker

MITM attack against BLE keyboards

**CVE-2020-9770**

# Our Downgrade Attacks against Bluetooth Low Energy

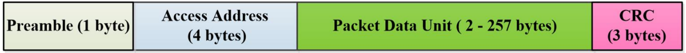

Device
Fake Mobile
Fake Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)
1.Impersonate the victim device and deploy attacks against the mobile
2.Use the stolen information (i.e., IRK) to create a Fake mobile
3. deploy attacks against the device

**"Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks"**, Yue Zhang, Jian Weng, Rajib Dey, Yier Jin, Zhiqiang Lin, and Xinwen Fu. *In Proceedings of the 29th USENIX Security Symposium*, Boston, MA. August 2020

# Outline

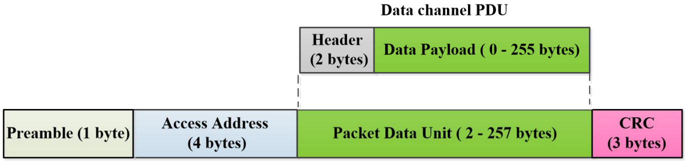
1. Introduction
2. BLE Security
3. BLE Privacy
4. Takeaway

# The Format of A Bluetooth Packet

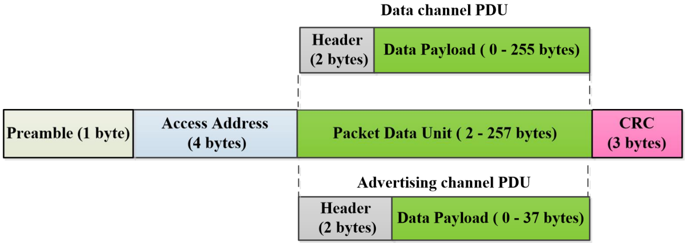


| | | | |
|---|---|---|---|
| Preamble (1 byte) | Access Address<br>(4 bytes) | Packet Data Unit ( 2 - 257 bytes) | CRC<br>(3 bytes) |

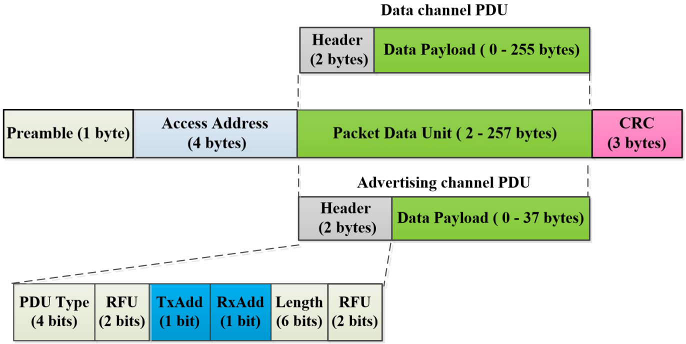
# The Format of A Bluetooth Packet



# The Format of A Bluetooth Packet



# The Format of A Bluetooth Packet



Data channel PDU

| Header (2 bytes) | Data Payload ( 0 - 255 bytes) |
|---|---|

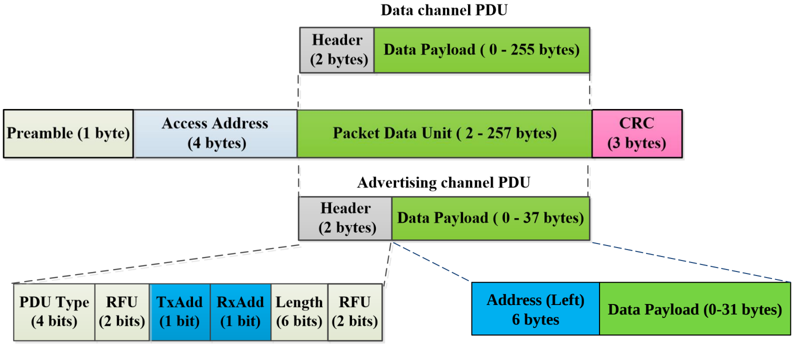
| Preamble (1 byte) | Access Address (4 bytes) | Packet Data Unit ( 2 - 257 bytes) | CRC (3 bytes) |
|---|---|---|---|

Advertising channel PDU

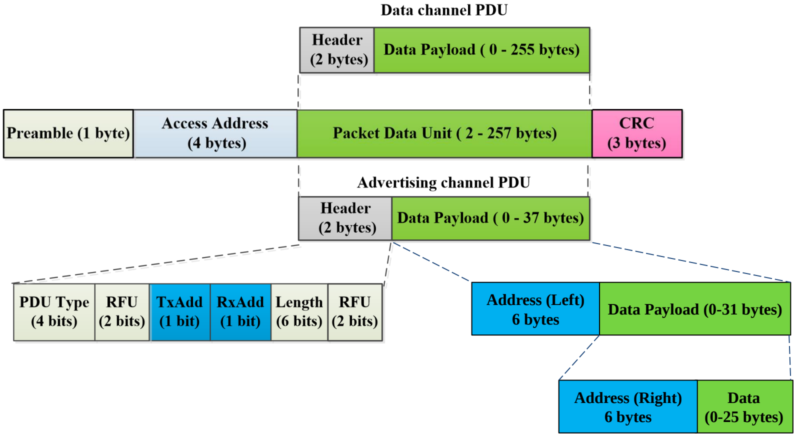
| Header (2 bytes) | Data Payload ( 0 - 37 bytes) |
|---|---|

| PDU Type (4 bits) | RFU (2 bits) | TxAdd (1 bit) | RxAdd (1 bit) | Length (6 bits) | RFU (2 bits) |
|---|---|---|---|---|---|

# The Format of A Bluetooth Packet



# The Format of A Bluetooth Packet



Data channel PDU

Header (2 bytes) | Data Payload ( 0 - 255 bytes)

Preamble (1 byte) | Access Address (4 bytes) | Packet Data Unit ( 2 - 257 bytes) | CRC (3 bytes)

Advertising channel PDU

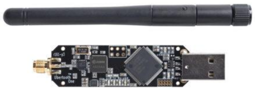
Header (2 bytes) | Data Payload ( 0 - 37 bytes)

PDU Type (4 bits) | RFU (2 bits) | TxAdd (1 bit) | RxAdd (1 bit) | Length (6 bits) | RFU (2 bits)

Address (Left) 6 bytes | Data Payload (0-31 bytes)

Address (Right) 6 bytes | Data (0-25 bytes)

# Bluetooth Sniffers

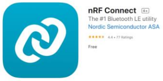


**Ubertooth One Sniffer**

**125 USD**

**Adafruit LE sniffer**

**25 USD**



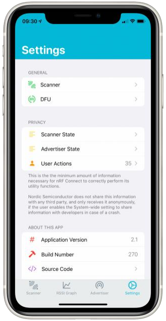
nRF Connect 4+

The #1 Bluetooth LE utility

Nordic Semiconductor ASA

★★★★★ 4.4 • 77 Ratings

Free



09:30

## Settings

GENERAL

- Scanner
- DFU

PRIVACY

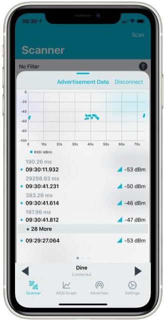
- Scanner State
- Advertiser State
- User Actions 35

This is the the minimum amount of information necessary for nRF Connect to correctly perform its utility functions.

Nordic Semiconductor does not share this information with any third party, and only receives it anonymously, if the user enables the System-wide setting to share information with developers in case of a crash.

ABOUT THIS APP

| | |
|---|---|
| Application Version | 2.1 |
| Build Number | 270 |
| Source Code | |



09:30

Scan

## Scanner

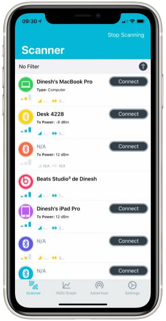
No Filter

Advertisement Data Disconnect

```
190.26 ms
• 09:30:11.932        -53 dBm
29298.93 ms
• 09:30:41.231        -50 dBm
383.26 ms
• 09:30:41.614        -46 dBm
197.96 ms
• 09:30:41.812        -47 dBm
+ 28 More
• 09:29:27.064        -53 dBm
```

Dine

Connected



09:30

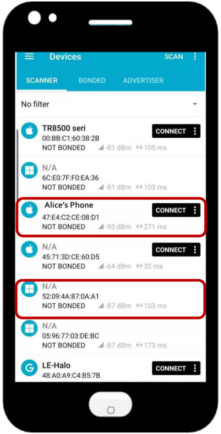
Stop Scanning

## Scanner

No Filter

- Dinesh's MacBook Pro — Type: Computer — Connect
- Desk 4228 — Tx Power: -8 dBm — Connect
- N/A — Tx Power: 12 dBm — N/A N/A — Connect
- Beats Studio$^{3}$ de Dinesh
- Dinesh's iPad Pro — Tx Power: 12 dBm — Connect
- N/A — Connect
- N/A — Connect

# Bluetooth Sniffers



Devices SCAN

SCANNER BONDED ADVERTISER

No filter

TR8500 seri
00:BB:C1:60:38:2B
NOT BONDED -81 dBm ↔105 ms
CONNECT

N/A
6C:E0:7F:F0:EA:36
NOT BONDED -81 dBm ↔103 ms

Alice's Phone
47:E4:C2:CE:08:D1
NOT BONDED -93 dBm ↔271 ms
CONNECT

N/A
45:71:3D:CE:60:D5
NOT BONDED -64 dBm ↔32 ms
CONNECT

N/A
52:09:4A:87:0A:A1
NOT BONDED -87 dBm ↔103 ms

N/A
05:96:77:03:DE:BC
NOT BONDED -87 dBm ↔173 ms

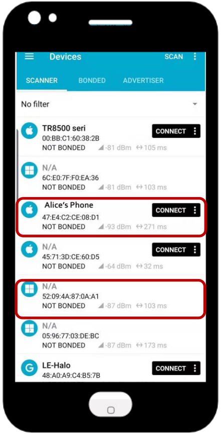
LE-Halo
48:A0:A9:C4:B5:7B
CONNECT

Alice's phone

Bob's phone

**T1: 52:09:4A:87:0A:A1**

# Bluetooth Sniffers



Devices SCAN

SCANNER BONDED ADVERTISER

No filter

TR8500 seri
00:BB:C1:60:38:2B
NOT BONDED -81 dBm ↔105 ms
CONNECT

N/A
6C:E0:7F:F0:EA:36
NOT BONDED -81 dBm ↔103 ms

Alice's Phone
47:E4:C2:CE:08:D1
NOT BONDED -93 dBm ↔271 ms
CONNECT

N/A
45:71:3D:CE:60:D5
NOT BONDED -64 dBm ↔32 ms
CONNECT

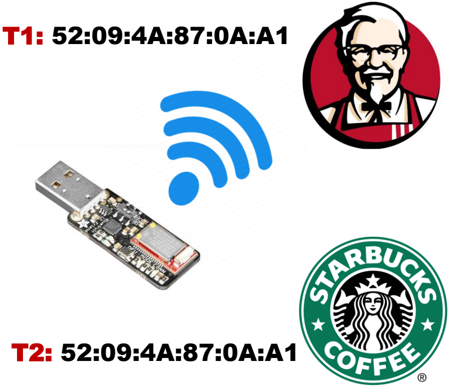
N/A
52:09:4A:87:0A:A1
NOT BONDED -87 dBm ↔103 ms

N/A
05:96:77:03:DE:BC
NOT BONDED -87 dBm ↔173 ms

LE-Halo
48:A0:A9:C4:B5:7B
CONNECT

Alice's phone

Bob's phone



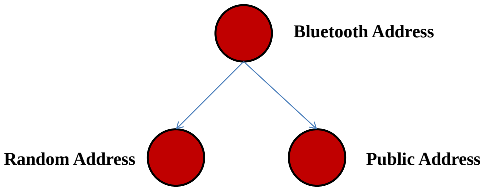
**T1: 52:09:4A:87:0A:A1**

**T2: 52:09:4A:87:0A:A1**

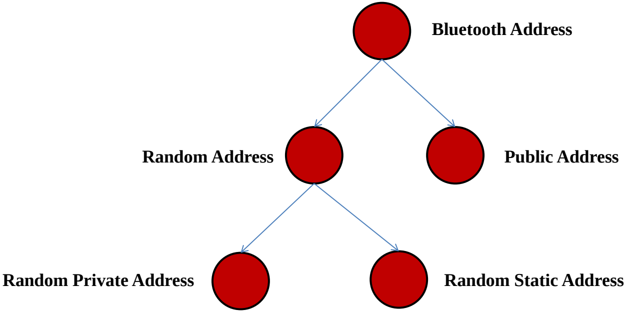
# Bluetooth Address Types

**Bluetooth Address**

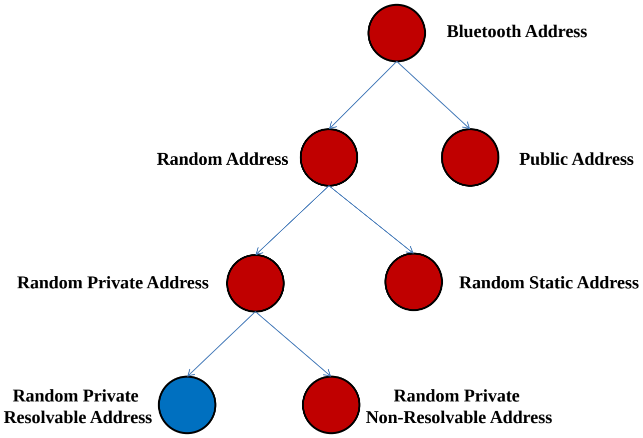
# Bluetooth Address Types



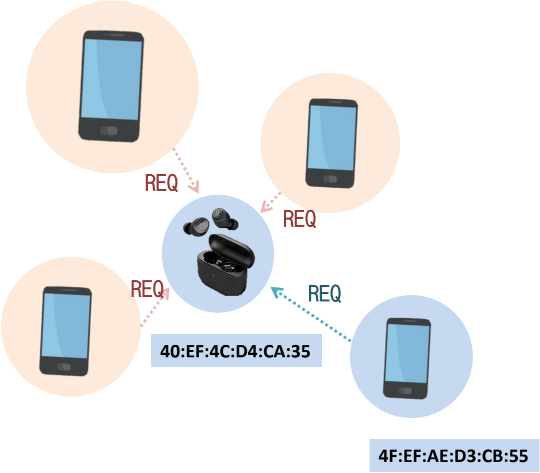
# Bluetooth Address Types



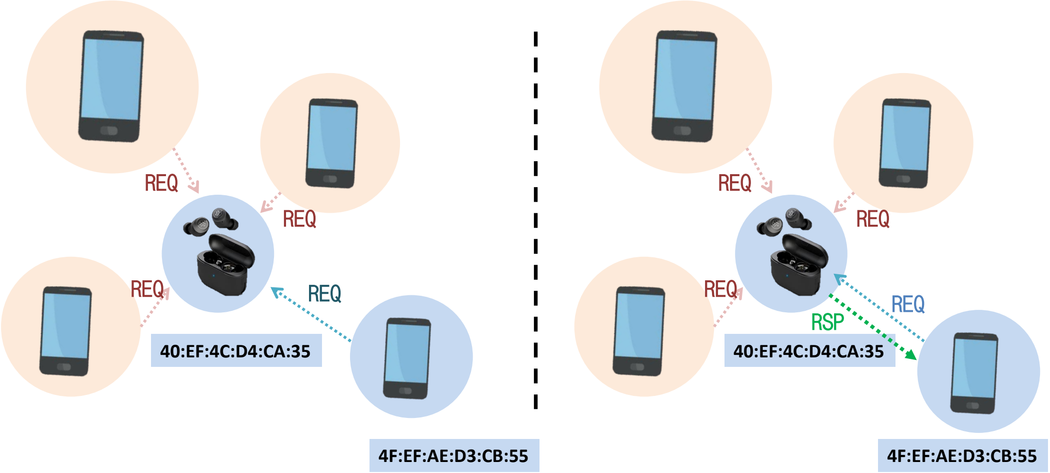
# Bluetooth Address Types



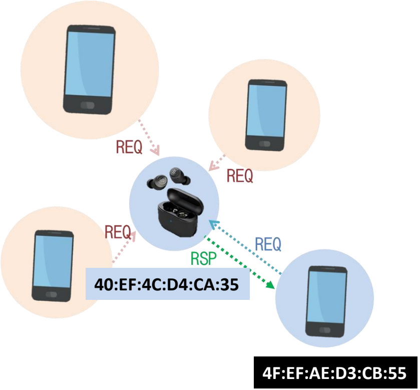
# Our First Finding: Allowlist-based Side Channel



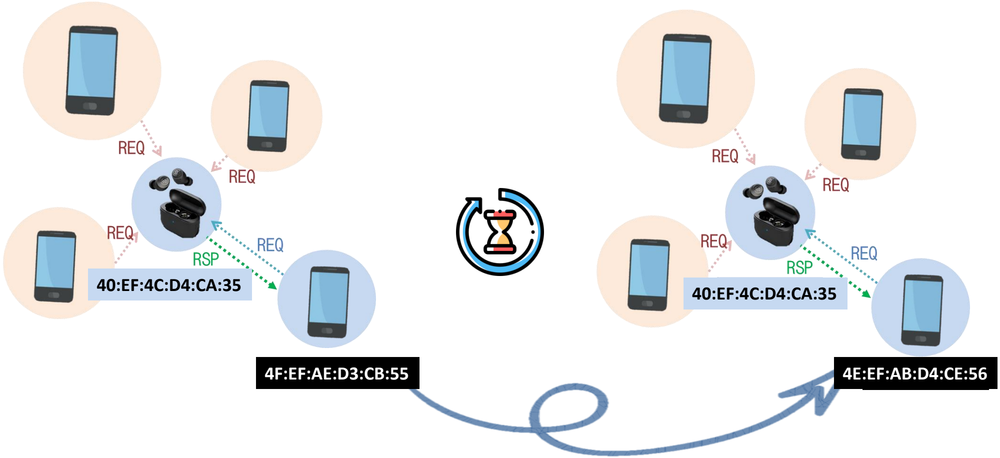
# Our First Finding: Allowlist-based Side Channel



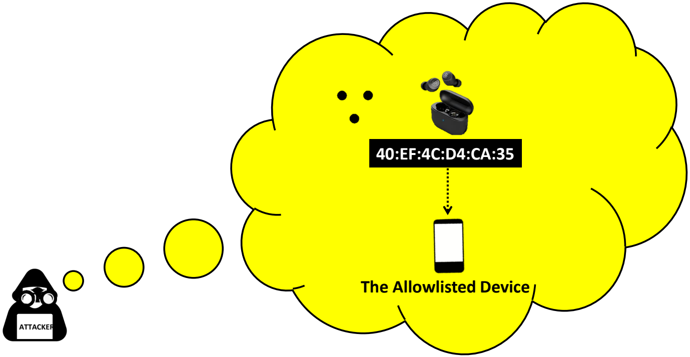
# Our First Finding: Allowlist-based Side Channel



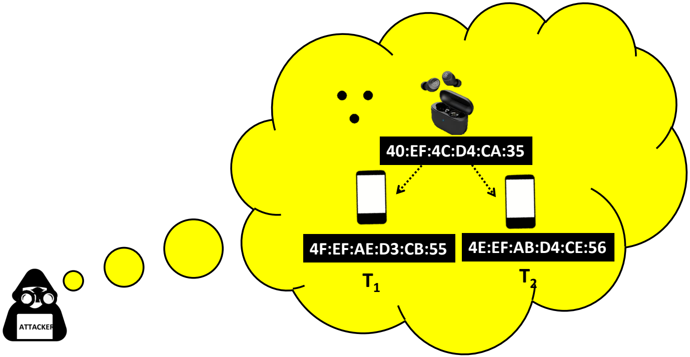
# Our First Finding: Allowlist-based Side Channel



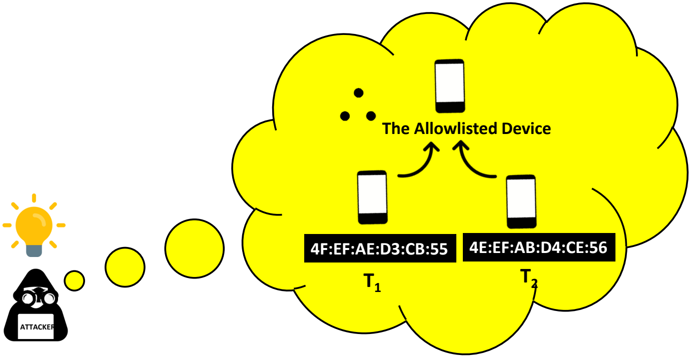
# Our First Finding: Allowlist-based Side Channel



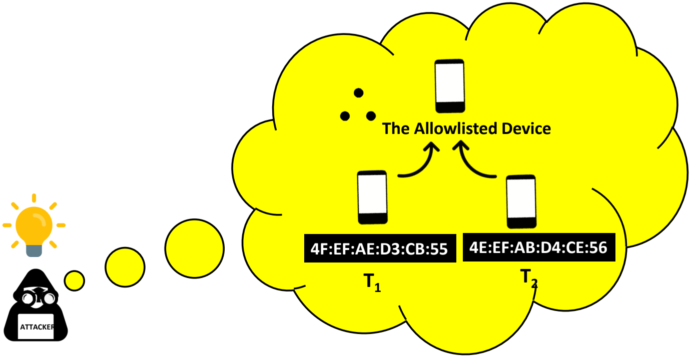
# Our First Finding: Allowlist-based Side Channel



# Our First Finding: Allowlist-based Side Channel

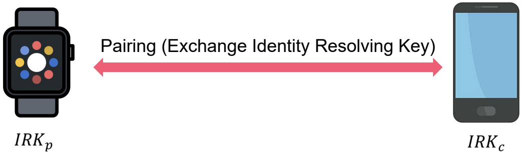


# Our First Finding: Allowlist-based Side Channel

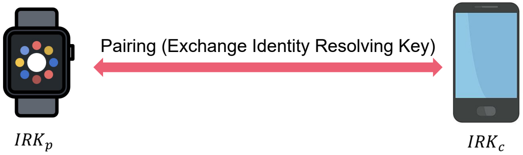


1. Cache
2. Timing
3. Power
4. Votage
5. Acoustic
6. **Allowlist**
7. ...

# Our Second Finding: MAC Address Can be Replayed



# Our Second Finding: MAC Address Can be Replayed


Pairing (Exchange Identity Resolving Key)

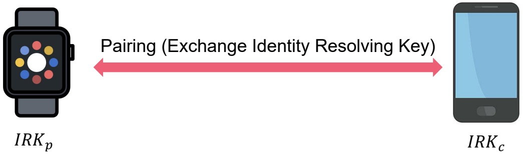
**Random Address (RA) Generation**

$$RA_p = prand_{24} \,||\, H_{24}(prand_{24} \,||\, IRK_p)$$

47:2B:3C:6F:1C:DE

**Random Address (RA) Resolution**

# Our Second Finding: MAC Address Can be Replayed



**Random Address (RA) Generation**

$$RA_p = prand_{24} \, || \, H_{24}(prand_{24} \, || \, IRK_p)$$

47:2B:3C:6F:1C:DE

**Random Address (RA) Resolution**

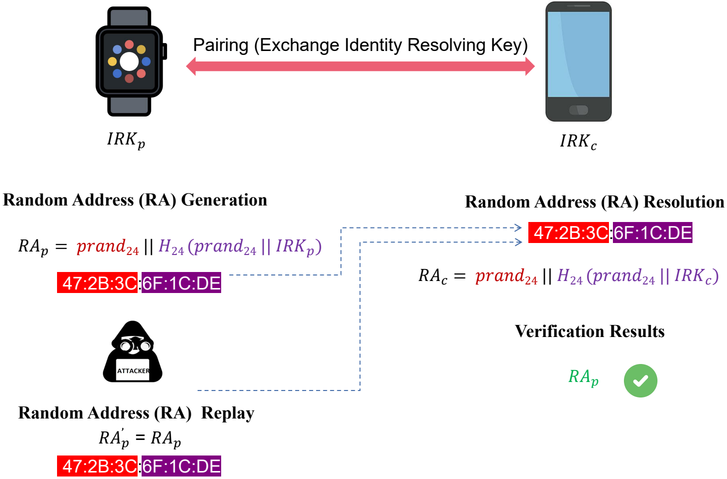
47:2B:3C:6F:1C:DE

$$RA_c = prand_{24} \, || \, H_{24}(prand_{24} \, || \, IRK_c)$$

**Verification Results**

$RA_p$ ✓

# Our Second Finding: MAC Address Can be Replayed



Pairing (Exchange Identity Resolving Key)

$IRK_p$

$IRK_c$

**Random Address (RA) Generation**

$RA_p = prand_{24} \,||\, H_{24}(prand_{24} \,||\, IRK_p)$

47:2B:3C:6F:1C:DE

**Random Address (RA) Replay**

$RA'_p = RA_p$

47:2B:3C:6F:1C:DE

**Random Address (RA) Resolution**

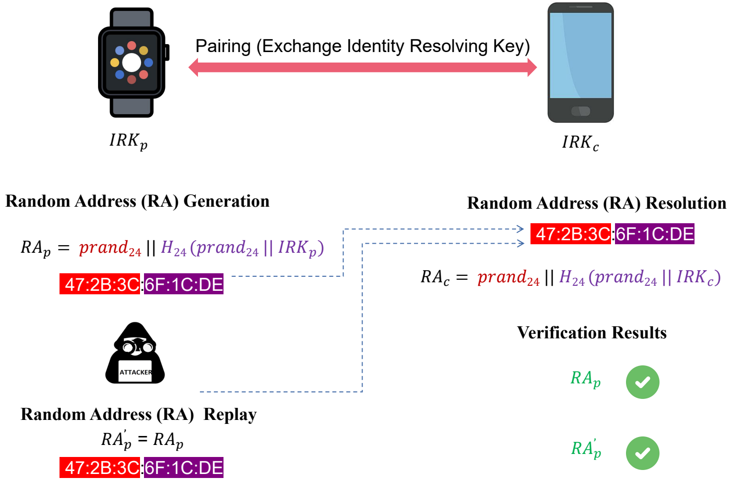
47:2B:3C:6F:1C:DE

$RA_c = prand_{24} \,||\, H_{24}(prand_{24} \,||\, IRK_c)$

**Verification Results**

$RA_p$ ✓

# Our Second Finding: MAC Address Can be Replayed



Pairing (Exchange Identity Resolving Key)

$IRK_p$

$IRK_c$

**Random Address (RA) Generation**

$RA_p = prand_{24} \,||\, H_{24}(prand_{24} \,||\, IRK_p)$

47:2B:3C:6F:1C:DE

**Random Address (RA) Replay**

$RA_p^{'} = RA_p$

47:2B:3C:6F:1C:DE

**Random Address (RA) Resolution**

47:2B:3C:6F:1C:DE

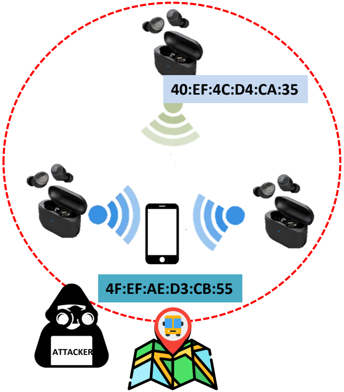
$RA_c = prand_{24} \,||\, H_{24}(prand_{24} \,||\, IRK_c)$

**Verification Results**

$RA_p$ ✓

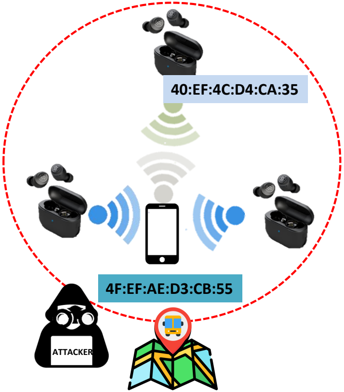
$RA_p^{'}$ ✓

# Attack Example



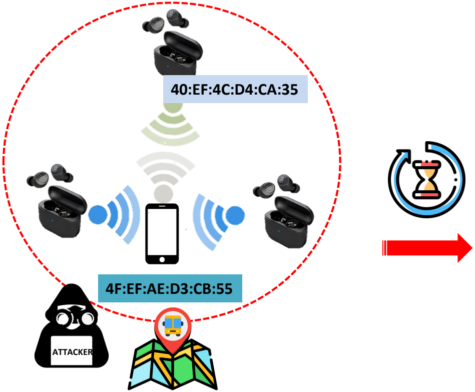
**Tracking a Victim's Real-time Location**

# Attack Example



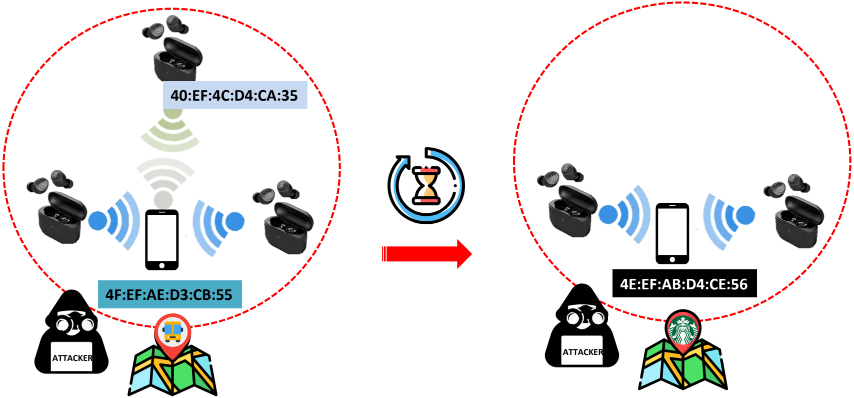
**Tracking a Victim's Real-time Location**

# Attack Example



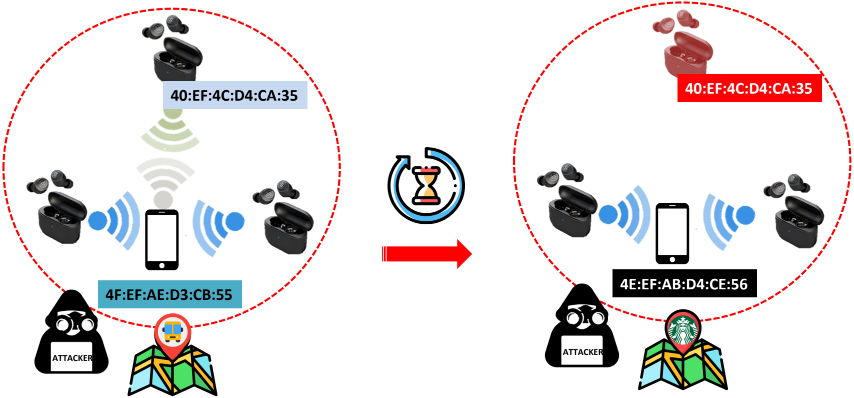
**Tracking a Victim's Real-time Location**

# Attack Example



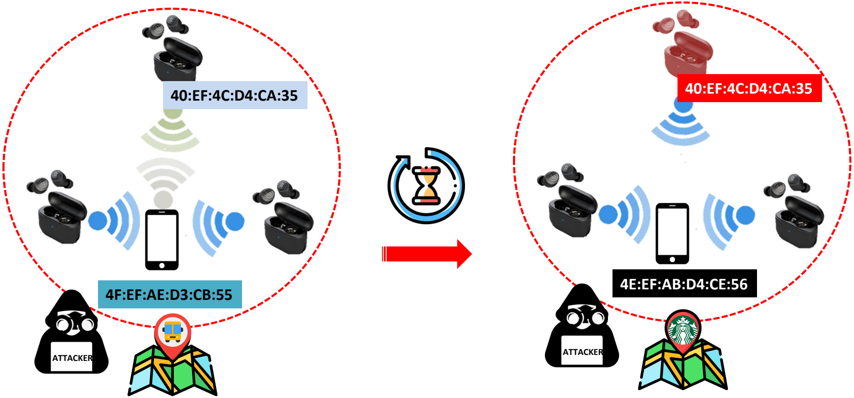
**Tracking a Victim's Real-time Location**

# Attack Example



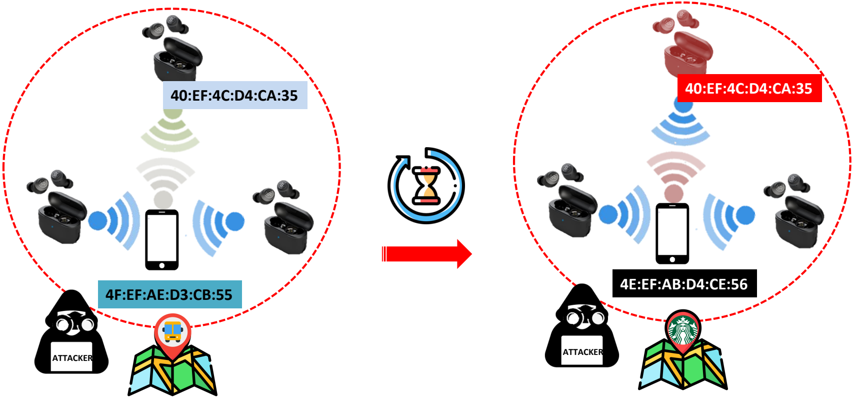
**Tracking a Victim's Real-time Location**

# Attack Example



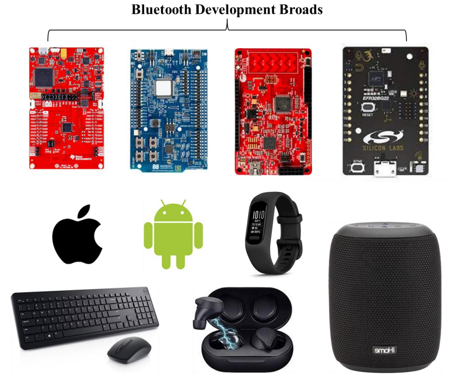
**Tracking a Victim’s Real-time Location**

# Attack Example



**Tracking a Victim's Real-time Location**

# Devices That are Subject to BAT Attacks



**CVE-2020-35473**

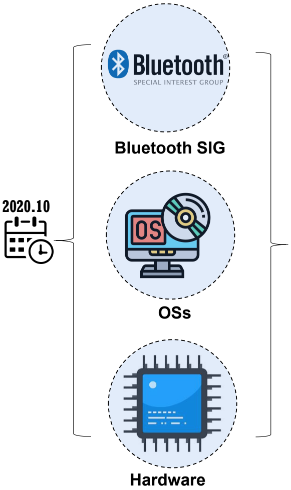
**Peripherals & Development Boards**

| Brand & Model | Allowlist | | Device Type | MAC Addr | Power Saving | Passive Attacks | | Active Attacks | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | From Malicious Central | | From Malicious Peripheral | |
| | Enabled by P | Used by C | | | | TC | TP | TC | TP | TC | TP |
| DRACONIC | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| JellyComb | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| iClever | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Microsoft (V1) | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Microsoft (V2) | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| byteblue | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Logitech K780 | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Logitech K830 | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Logitech K380 | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SXWL | ✓ | ✓ | Keyboard | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SXWL | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Inphic | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vogek | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| JellyComb (V1) | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| JellyComb (V2) | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SEENDA | ✓ | ✓ | Mouse | SRA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| MiBand 4C | ✓ | ✗ | Wristband | PA | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| i-Home Alexa | ✗ | ✓ | Speaker | PA | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TEZO | ✗ | ✓ | Earbuds | PA | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Boltune | ✗ | ✓ | Earbuds | PA | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SoundBot | ✗ | ✓ | Earbuds | PA | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Riitek | ✗ | ✓ | Keyboard | PA | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Cimetech | ✗ | ✓ | Mouse | SRA | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Ergonomic | ✗ | ✓ | Mouse | SRA | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| TI CC2640R2F | ✓ | ✓ | Dev Board | RPA | - | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Nordic NRF52 | ✓ | ✓ | Dev Board | RPA | - | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Silicon Labs 6101D | ✗ | ✓ | Dev Board | RPA | - | - | - | ✗ | ✗ | ✓ | ✓ |
| Crypess CY8kCIT | ✗ | ✓ | Dev Board | RPA | - | - | - | ✗ | ✗ | ✓ | ✓ |

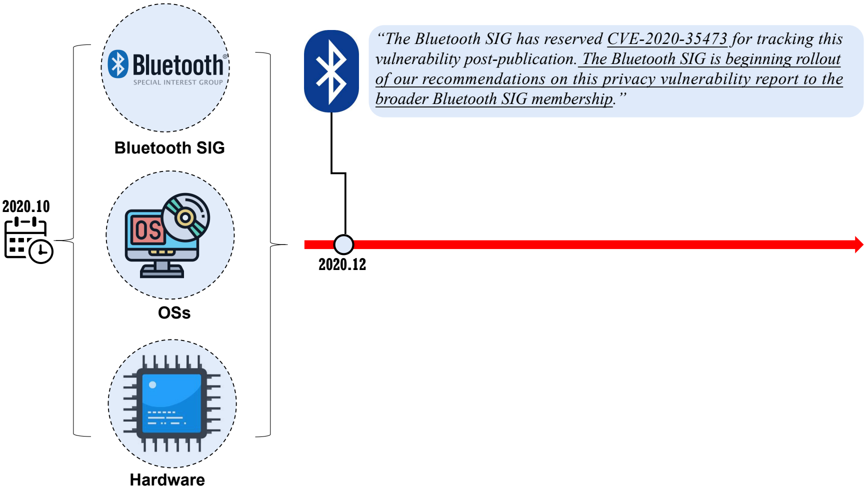
**Centrals**

| Brand & Model | Allowlist | | Type & OS | MAC Addr | Random Interval | Passive Attacks | | Active Attacks | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | From Malicious Central | | From Malicious Peripheral | |
| | Enabled by C | Used by P | | | | TP | TC | TP | TC | TP | TC |
| Google Pixel 4 | ✓ | ✓ | Phone (Android 11) | RPA | 5-15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Google Pixel 2 | ✓ | ✓ | Phone (Android 10) | RPA | 5-15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Samsung S10 | ✓ | ✓ | Phone (Android 10) | RPA | 5-15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Google Piexl 4 | ✓ | ✓ | Phone (Android 10) | RPA | 5-15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| iPhone 8 | ✓ | ✓ | Phone (iOS 13.2) | RPA | 15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| iPhone 11 | ✓ | ✓ | Phone (iOS 13.2) | RPA | 15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| iPad | ✓ | ✓ | Tablet (iOS 13.2) | RPA | 15 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Dell GD1H4KU | ✓ | ✓ | Laptop (Windows 10) | PA | $+\infty$ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Dell | ✓ | ✓ | Laptop (Ubuntu 20.02) | PA | $+\infty$ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Thinkpad T450s | ✓ | ✓ | Laptop (Windows 8) | PA | $+\infty$ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Surface Pro | ✓ | ✓ | Tablet (Windows 10) | PA | $+\infty$ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# Responsible Disclosure



# Responsible Disclosure



2020.10

Bluetooth SIG

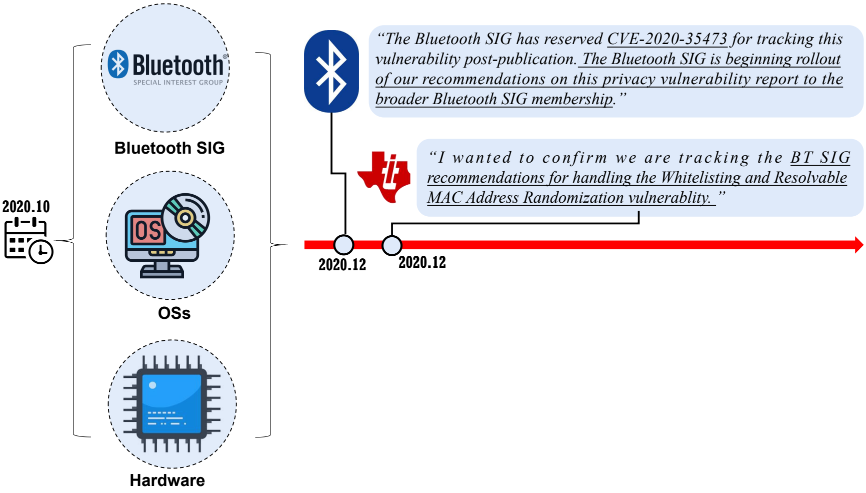
OSs

Hardware

2020.12

*"The Bluetooth SIG has reserved CVE-2020-35473 for tracking this vulnerability post-publication. The Bluetooth SIG is beginning rollout of our recommendations on this privacy vulnerability report to the broader Bluetooth SIG membership."*

# Responsible Disclosure



2020.10

Bluetooth SIG

OSs

Hardware

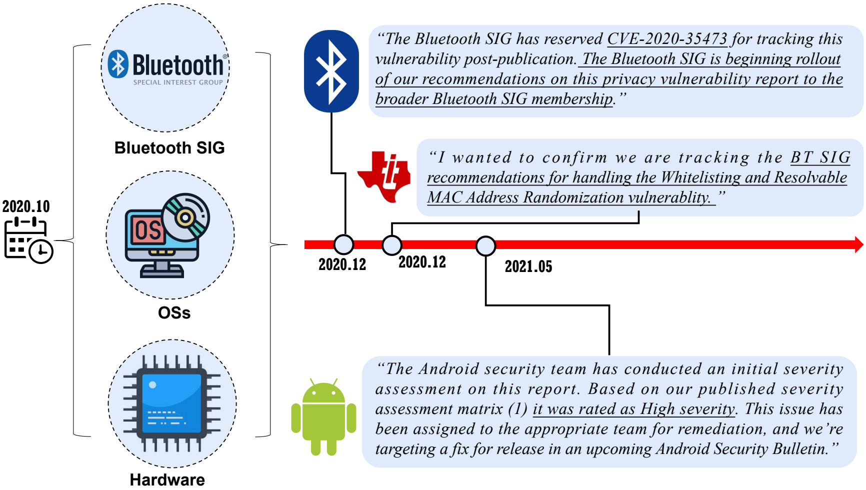
2020.12

*"The Bluetooth SIG has reserved CVE-2020-35473 for tracking this vulnerability post-publication. The Bluetooth SIG is beginning rollout of our recommendations on this privacy vulnerability report to the broader Bluetooth SIG membership."*

2020.12

*"I wanted to confirm we are tracking the BT SIG recommendations for handling the Whitelisting and Resolvable MAC Address Randomization vulnerablity. "*

# Responsible Disclosure

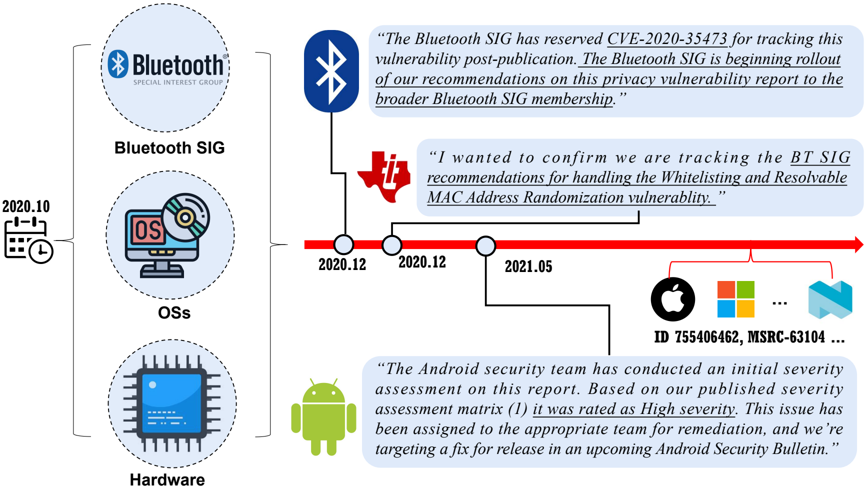


*"The Bluetooth SIG has reserved CVE-2020-35473 for tracking this vulnerability post-publication. The Bluetooth SIG is beginning rollout of our recommendations on this privacy vulnerability report to the broader Bluetooth SIG membership."*

*"I wanted to confirm we are tracking the BT SIG recommendations for handling the Whitelisting and Resolvable MAC Address Randomization vulnerablity. "*

*"The Android security team has conducted an initial severity assessment on this report. Based on our published severity assessment matrix (1) it was rated as High severity. This issue has been assigned to the appropriate team for remediation, and we're targeting a fix for release in an upcoming Android Security Bulletin."*

# Responsible Disclosure


2020.10
Bluetooth SPECIAL INTEREST GROUP
Bluetooth SIG
OS
OSs
Hardware
2020.12
2020.12
2021.05
...
ID 755406462, MSRC-63104 ...

*"The Bluetooth SIG has reserved CVE-2020-35473 for tracking this vulnerability post-publication. The Bluetooth SIG is beginning rollout of our recommendations on this privacy vulnerability report to the broader Bluetooth SIG membership."*

*"I wanted to confirm we are tracking the BT SIG recommendations for handling the Whitelisting and Resolvable MAC Address Randomization vulnerablity. "*

*"The Android security team has conducted an initial severity assessment on this report. Based on our published severity assessment matrix (1) it was rated as High severity. This issue has been assigned to the appropriate team for remediation, and we're targeting a fix for release in an upcoming Android Security Bulletin."*

# Our Countermeasure: Securing Address of BLE (SABLE)

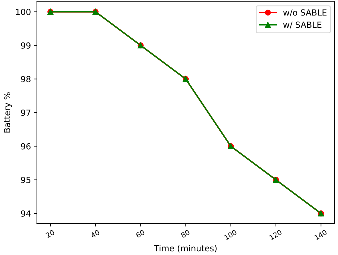
## Allowlist Side Channel (Mitigation)

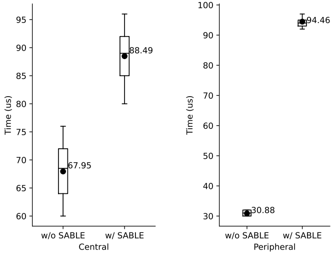
- We advocate the use of an interval unpredictable, central and peripheral synchronized RPA generation scheme to mitigate the side channel.

## MAC Address Replay (Prevention)

- We propose adding a sequence number (which could be a timestamp) when generating the RPA to ensure that each MAC address can only be used once to prevent the replay attack.

# Performance of SABLE



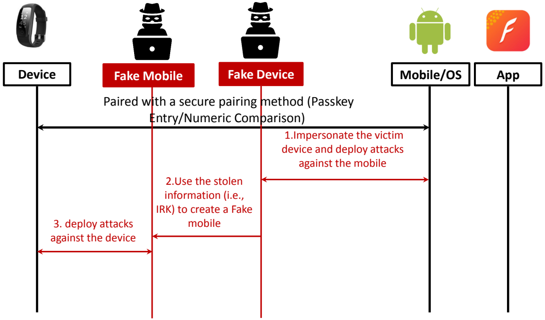


**"When Good Becomes Evil: Tracking Bluetooth Low Energy Devices via Allowlist-based Side Channel and Its Countermeasure"**. Yue Zhang, and Zhiqiang Lin. *In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS 2022)*. November 2022

# Outline

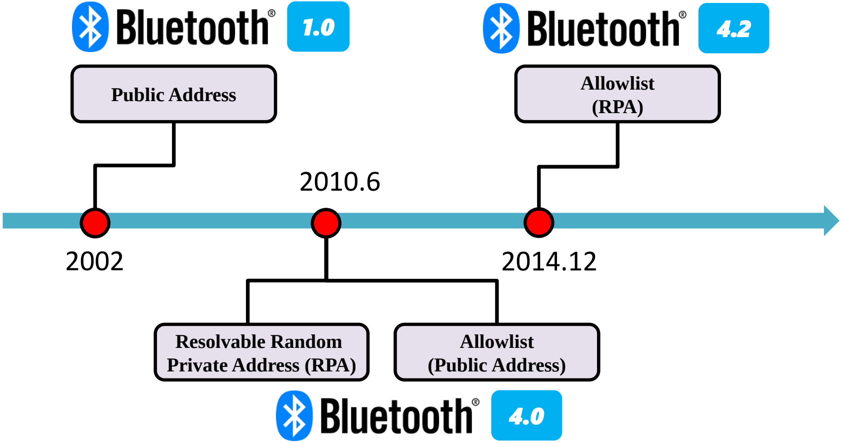
1. Introduction
2. BLE Security
3. BLE Privacy
4. Takeaway

# Lesson Learned (1/3): BLE Communication Can Be Downgraded

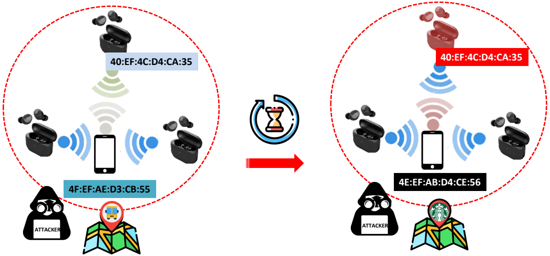

Device
Fake Mobile
Fake Device
Mobile/OS
App
Paired with a secure pairing method (Passkey Entry/Numeric Comparison)
1.Impersonate the victim device and deploy attacks against the mobile
2.Use the stolen information (i.e., IRK) to create a Fake mobile
3. deploy attacks against the device

- Bluetooth low energy (BLE) pairing can be **downgraded**
- There are many stages that are not part of the pairing process, but they are, in fact, closely related to pairing security.
- A systematic analysis of the pairing process, including the **error handling** of BLE communication, is needed.

# Lesson Learned (2/3): New Features Need Re-examinations

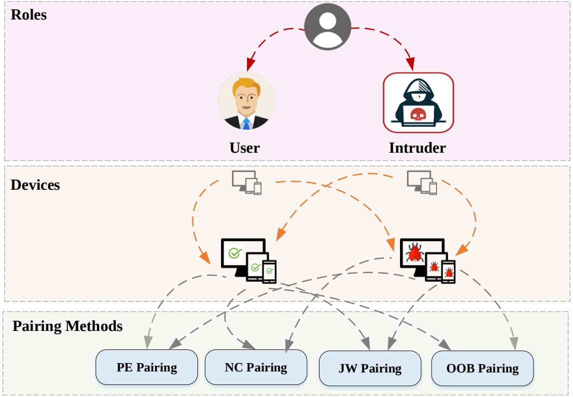


# Lesson Learned (2/3): New Features Need Re-examinations



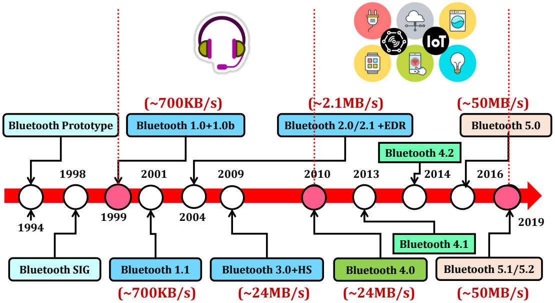
- BLE introduces multiple new features, some of which may **violate existing assumptions**
- Simliar to allowlist, those new features need to be **scrunitized**. For example, Cross-transport key derivation (CTKD); Authorization; The Connection Signature Resolving Key (CSRK).

# Lesson Learned (3/3): Formal Method Can Help Improve BLE Security



- The specification (3,000+ pages) is often confusing and inconsistent across chapters.
- The confusion may lead to different vendors implement BLE protocols in quite different ways, for example, for error handling, and IRK use.
- Converting the Bluetooth specification to formal model, and formally verify the entire protocol would help.
- See our NDSS'23 paper.

# Our Recent Work on Bluetooth Security and Privacy



(~700KB/s) (~2.1MB/s) (~50MB/s)

Bluetooth Prototype

Bluetooth 1.0+1.0b

Bluetooth 2.0/2.1 +EDR

Bluetooth 5.0

Bluetooth 4.2

1998 2001 2009 2010 2013 2014 2016

1994 1999 2004 2019

Bluetooth 4.1

Bluetooth SIG

Bluetooth 1.1

Bluetooth 3.0+HS

Bluetooth 4.0

Bluetooth 5.1/5.2

(~700KB/s) (~24MB/s) (~24MB/s) (~50MB/s)

1. ~~BLEScope: Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps. In ACM CCS 2019~~
2. ~~FirmXRay: Detecting Bluetooth Link Layer Vulnerabilities From Bare-Metal Firmware. In ACM CCS 2020.~~
3. **Breaking Secure Pairing of Bluetooth Low Energy in Mobile Devices Using Downgrade Attacks**. In USENIX Security 2020
4. ~~On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps. In SECURECOMM. October 2020~~
5. **When Good Becomes Evil: Tracking Bluetooth Low Energy Devices via Allowlist-based Side Channel and Its Countermeasure"**. In ACM CCS 2022 (Best paper award honorable mention)
6. ~~Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing. In NDSS 2023~~

# Thank You

## Rethinking the Security and Privacy of Bluetooth Low Energy

Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

04/14/2023