Rethinking the Security and Privacy of Bluetooth Low Energy

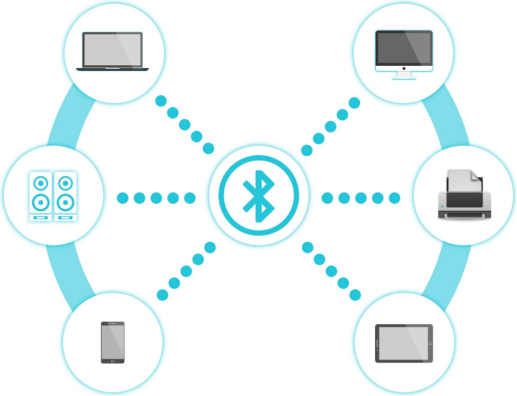
Zhiqiang Lin
Distinguished Professor of Engineering
zlin@cse.ohio-state.edu

09/30/2022

What is Bluetooth

Bluetooth wireless technology

- Low-cost, low-power
- Short-range radio
- For ad-hoc wireless communication
- For voice and data transmission



What is Bluetooth

Google

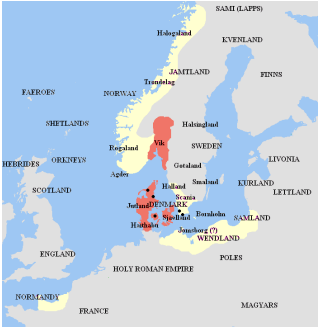
Contact tracing

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 Bluetooth wireless specification design 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**.

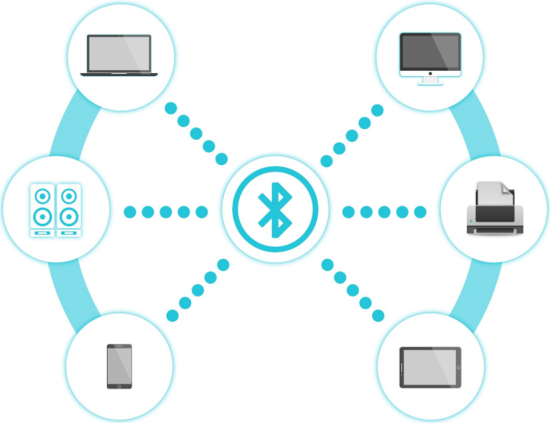


Why Named Bluetooth

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 Bluetooth wireless specification design 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**.



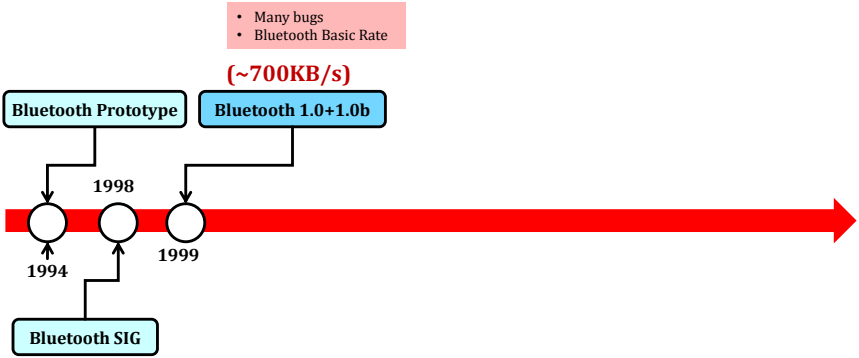
History of Bluetooth

History of Bluetooth

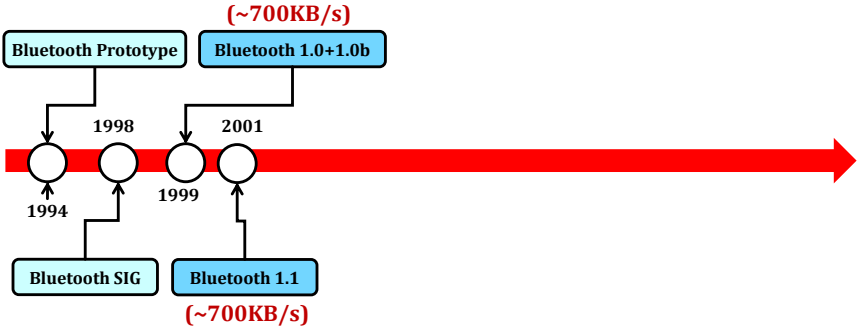
Dr. Jaap Haartsen started a project named Bluetooth.

History of Bluetooth

History of Bluetooth

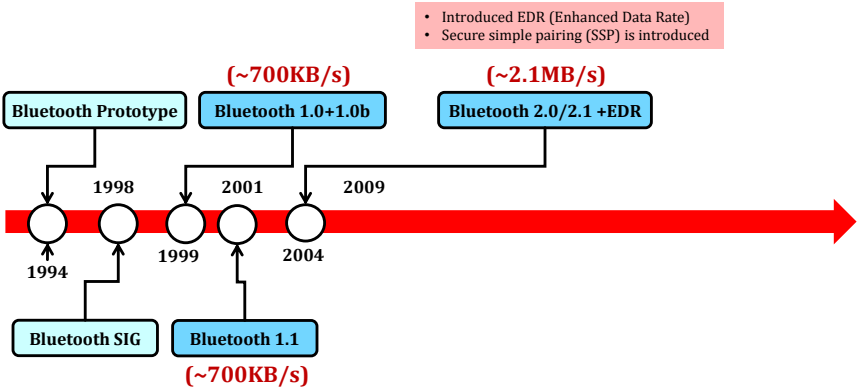


History of Bluetooth

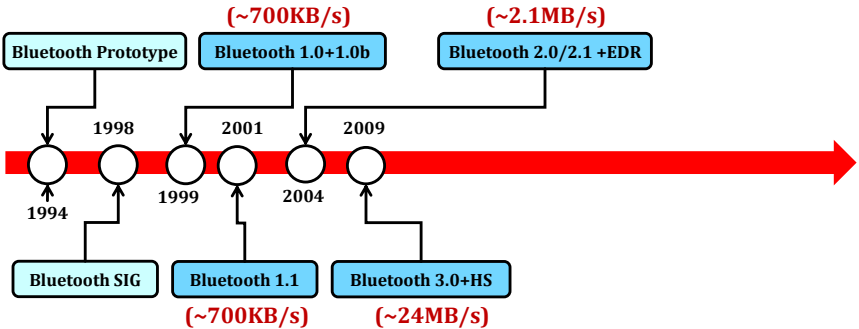


- Fixed security issues.
- First marketable product version.

History of Bluetooth

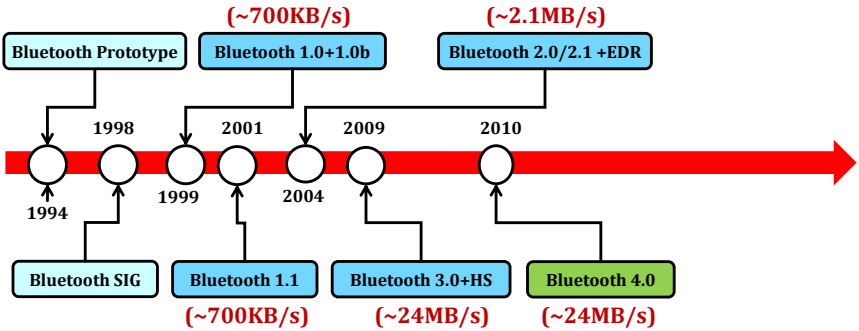


History of Bluetooth



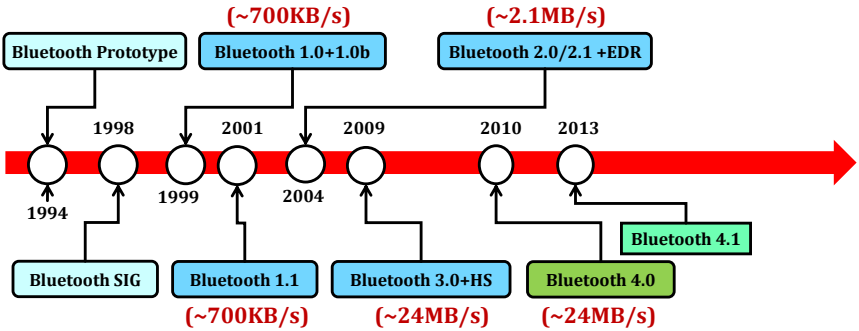
Introduced High-speed channel

History of Bluetooth



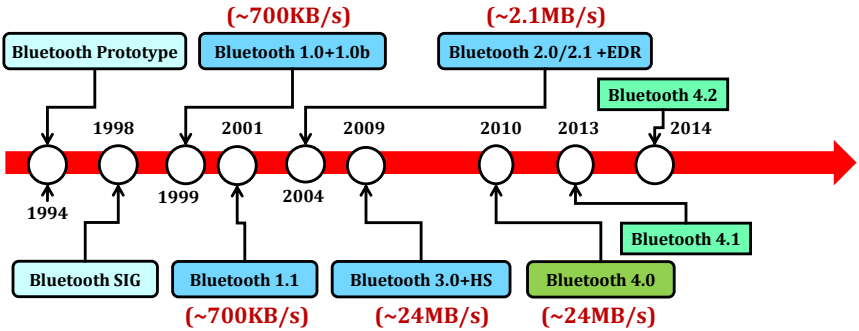
- Low energy (LE) protocol for IoT;
- 128-bit encryption/LE Privacy and Whitelisting

History of Bluetooth



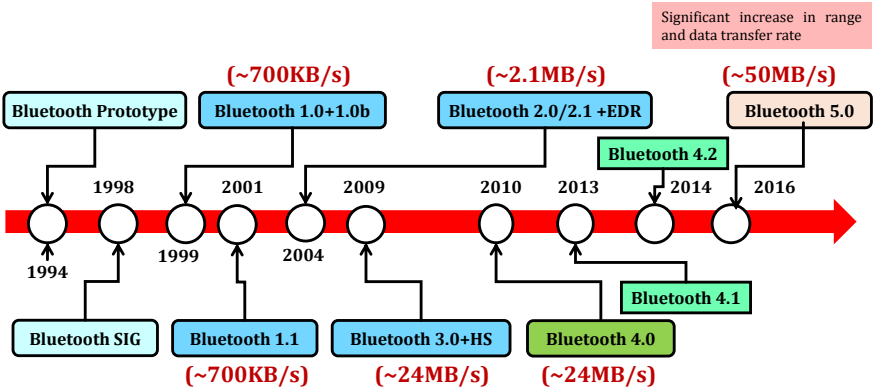
- Low energy (LE) protocol for IoT;
- 128-bit encryption/LE Privacy and Whitelisting

History of Bluetooth

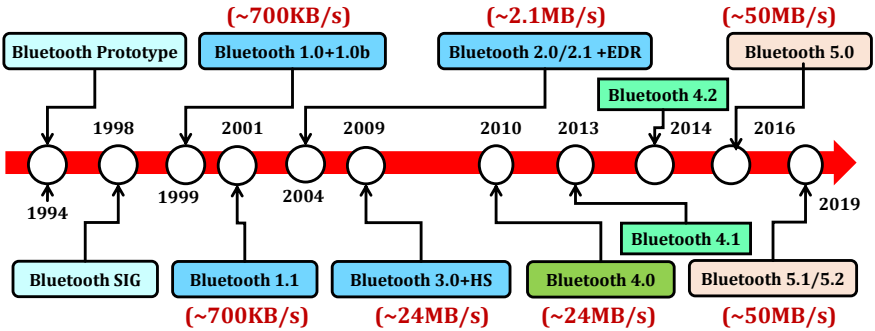


- Low energy (LE) protocol for IoT;
- 128-bit encryption/LE Privacy and Whitelisting

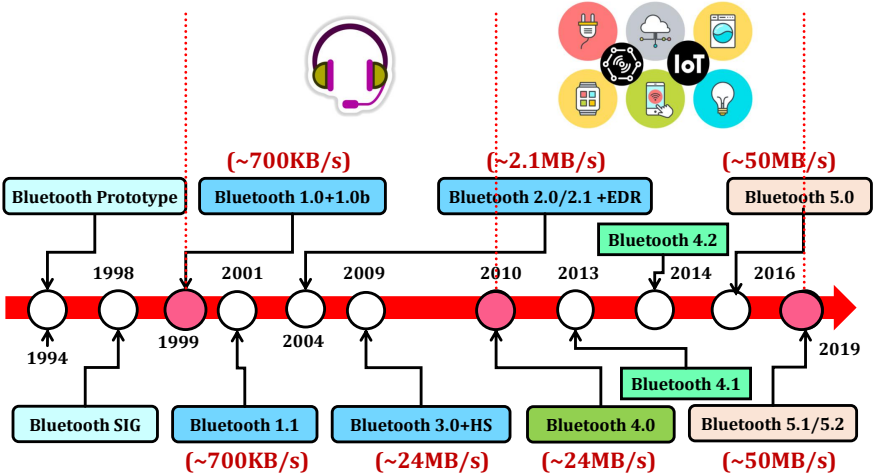
History of Bluetooth



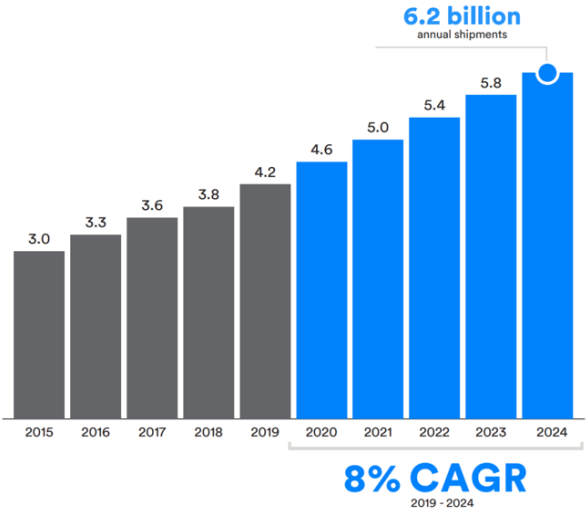
History of Bluetooth



History of Bluetooth

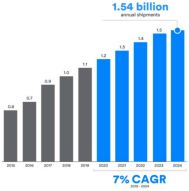


Total Annual Bluetooth Device Shipments



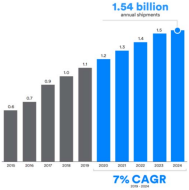
Total Annual Bluetooth Device Shipments

Annual Bluetooth Audio Streaming Device Shipments

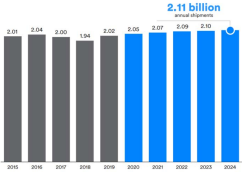


Total Annual Bluetooth Device Shipments

Annual Bluetooth Audio Streaming Device Shipments

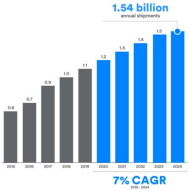


Annual Bluetooth Phone, Tablet & PC Shipments

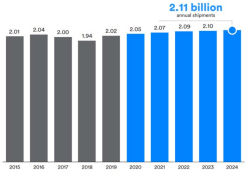


Total Annual Bluetooth Device Shipments

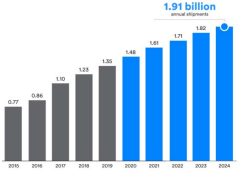
Annual Bluetooth Audio Streaming Device Shipments



Annual Bluetooth Phone, Tablet & PC Shipments

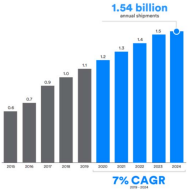


Annual Bluetooth Entertainments Shipments

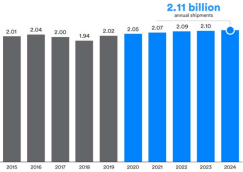


Total Annual Bluetooth Device Shipments

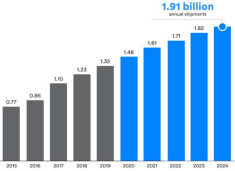
Annual Bluetooth Audio Streaming Device Shipments



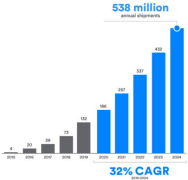
Annual Bluetooth Phone, Tablet & PC Shipments



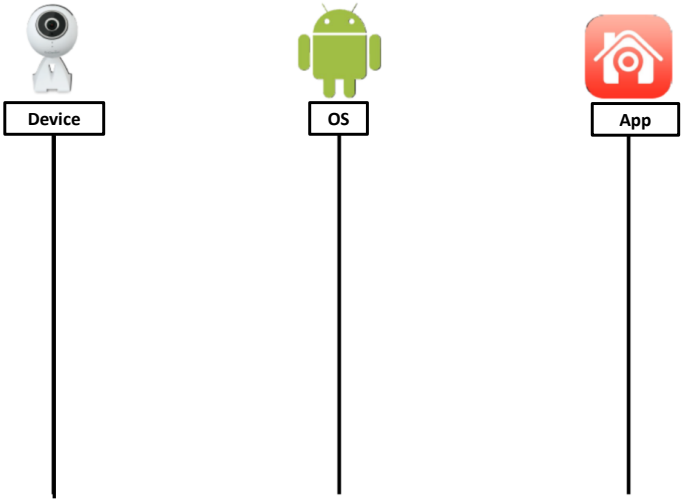
Annual Bluetooth Entertainments Shipments



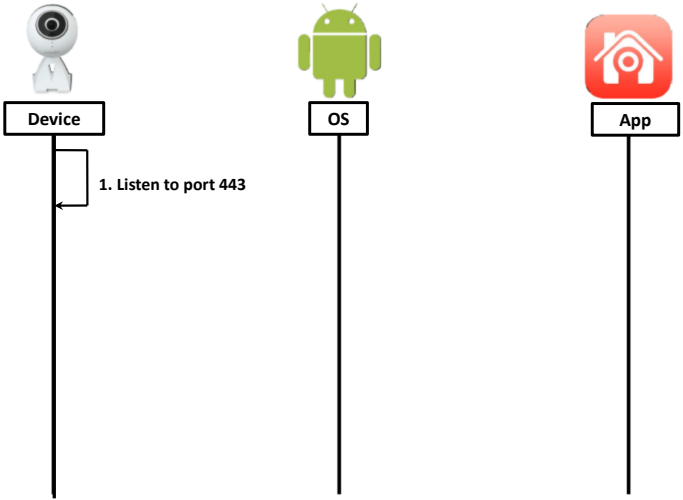
Annual Bluetooth Location Service Device Shipments



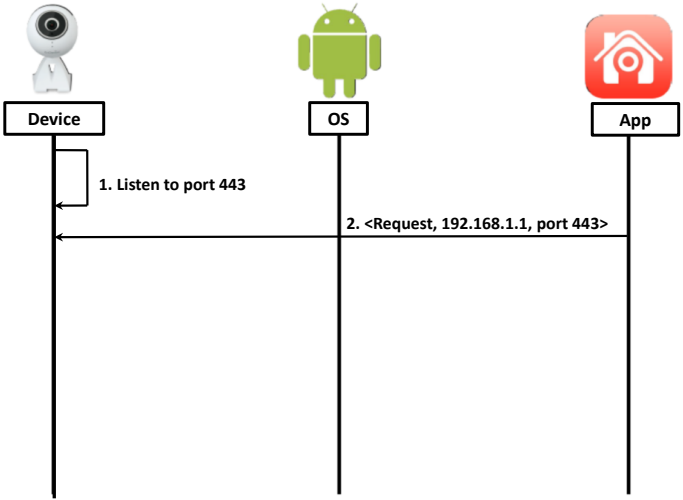
The General Workflow of Device Communication in TCP/IP Setting



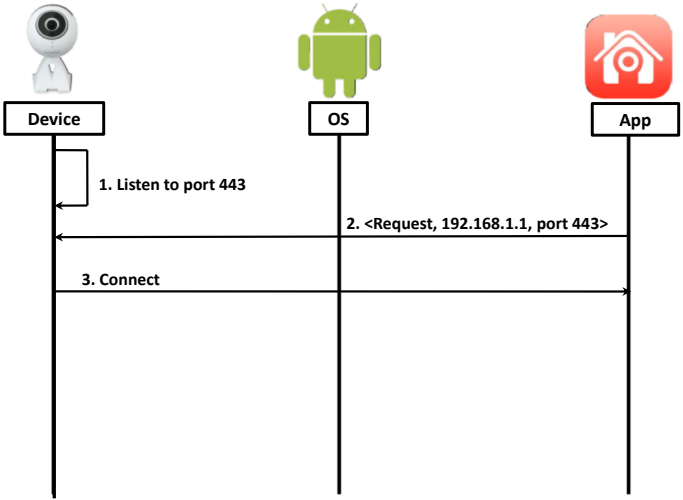
The General Workflow of Device Communication in TCP/IP Setting



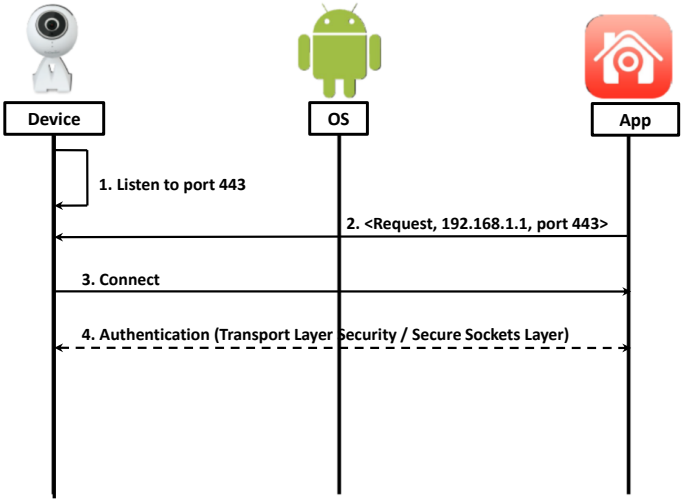
The General Workflow of Device Communication in TCP/IP Setting



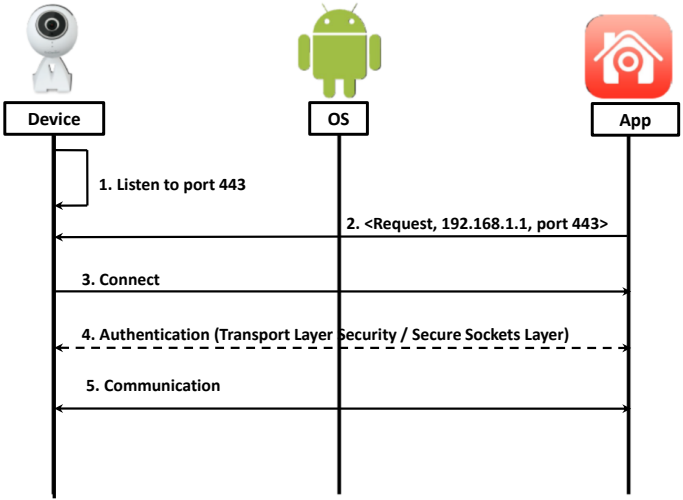
The General Workflow of Device Communication in TCP/IP Setting



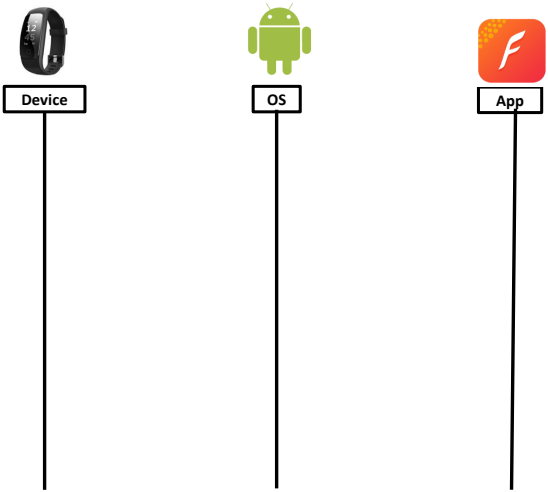
The General Workflow of Device Communication in TCP/IP Setting



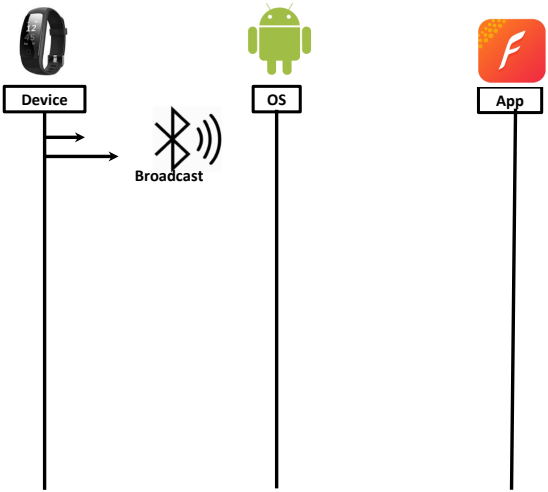
The General Workflow of Device Communication in TCP/IP Setting



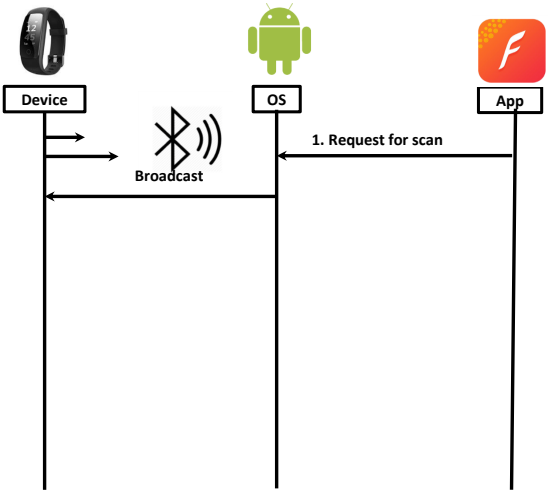
The General Workflow of Device Communication in TCP/IP Setting



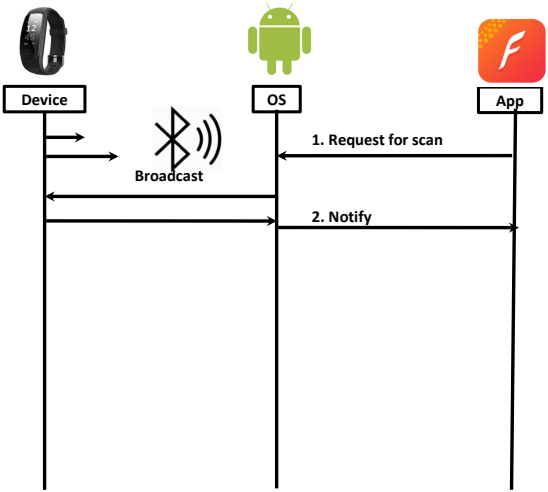
The General Workflow of BLE IoT Devices and Companion Apps



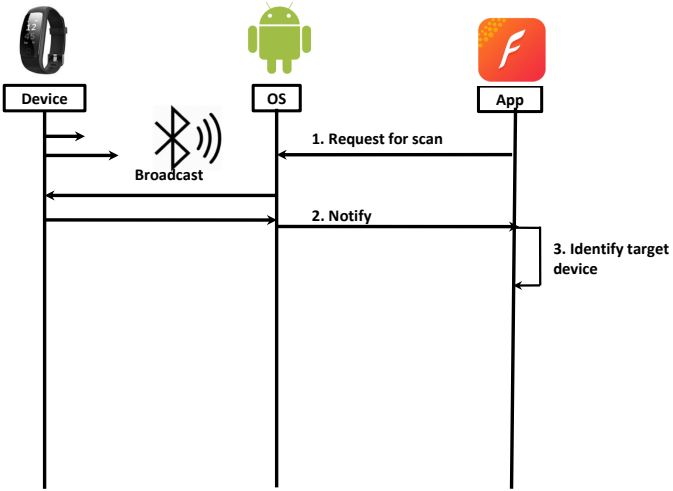
The General Workflow of BLE IoT Devices and Companion Apps



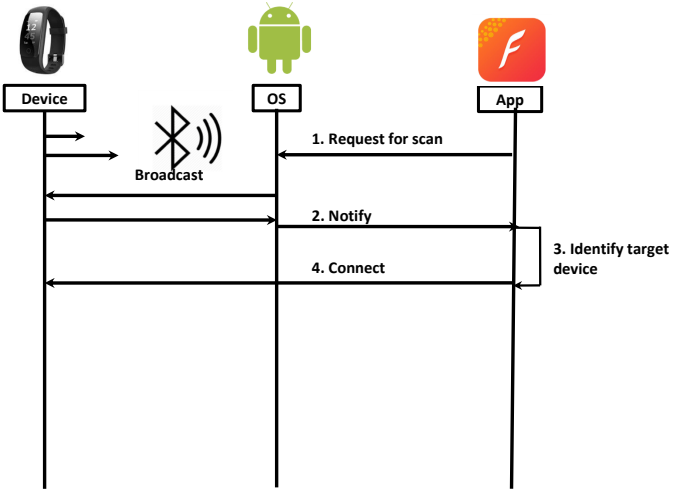
The General Workflow of BLE IoT Devices and Companion Apps



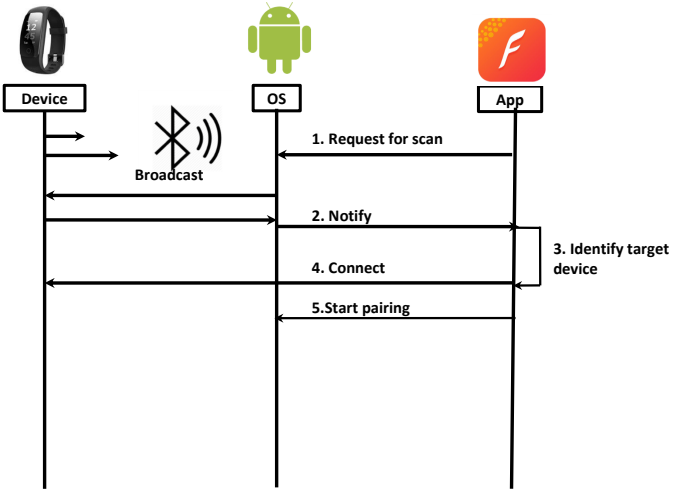
The General Workflow of BLE IoT Devices and Companion Apps



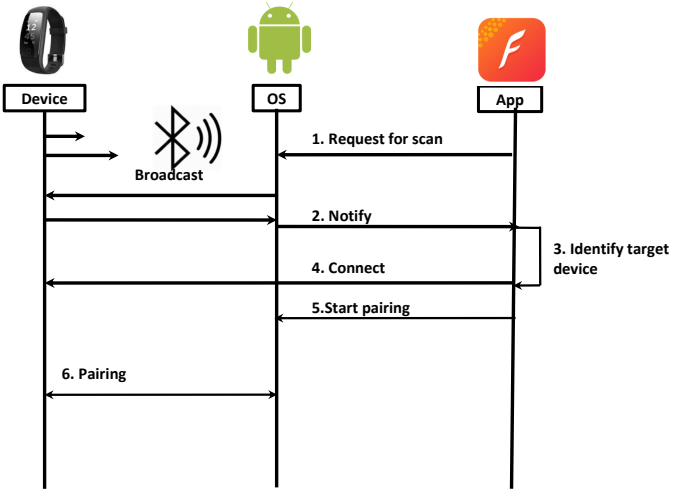
The General Workflow of BLE IoT Devices and Companion Apps



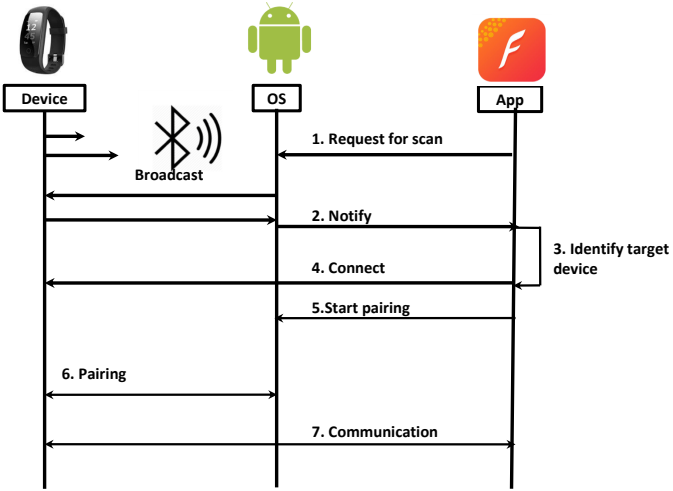
The General Workflow of BLE IoT Devices and Companion Apps



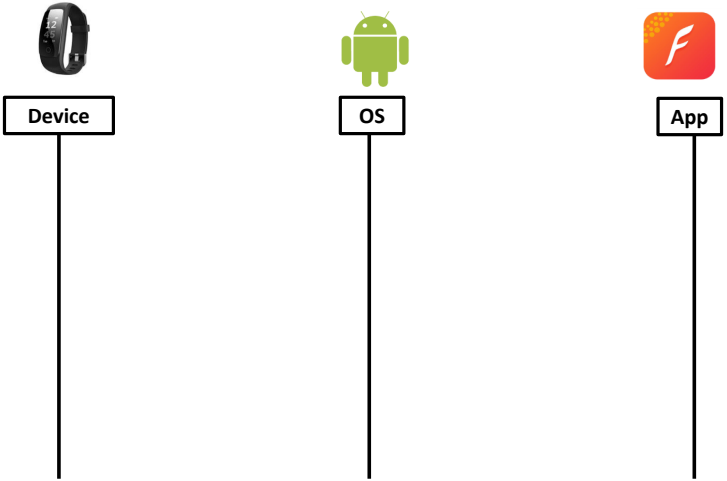
The General Workflow of BLE IoT Devices and Companion Apps



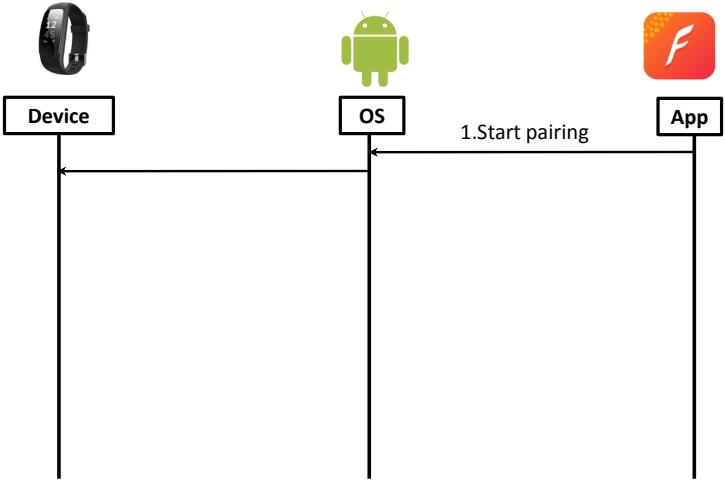
The General Workflow of BLE IoT Devices and Companion Apps



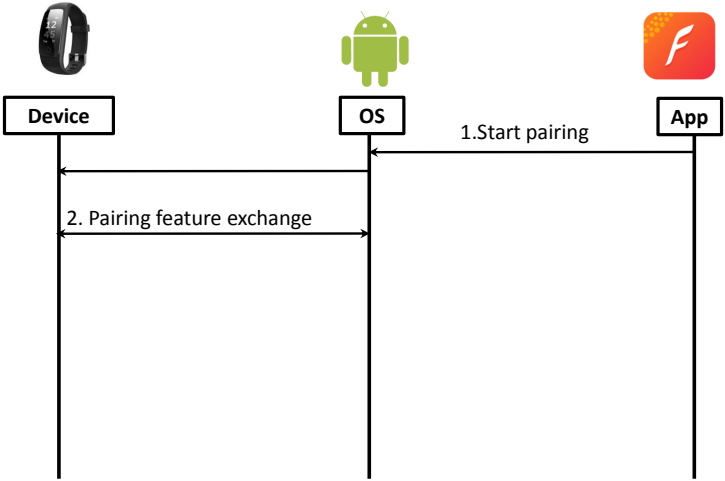
Pairing Workflow



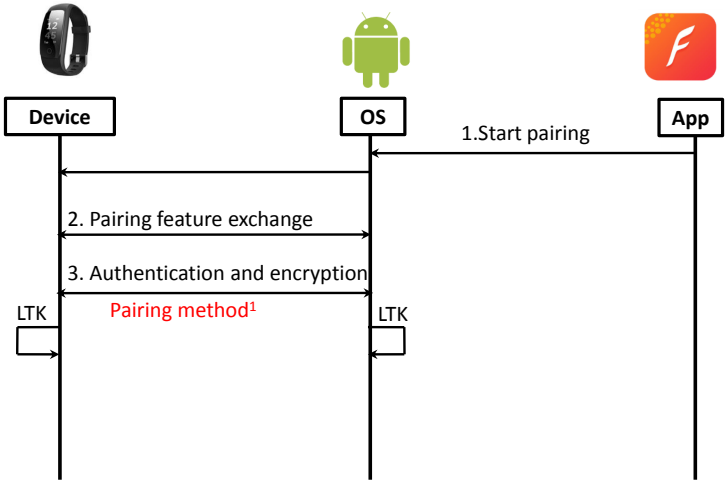
Pairing Workflow



Pairing Workflow



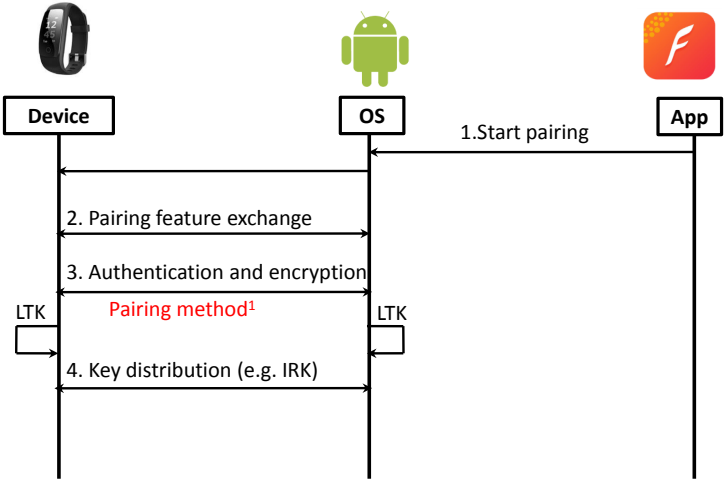
Pairing Workflow



Pairing Methods

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

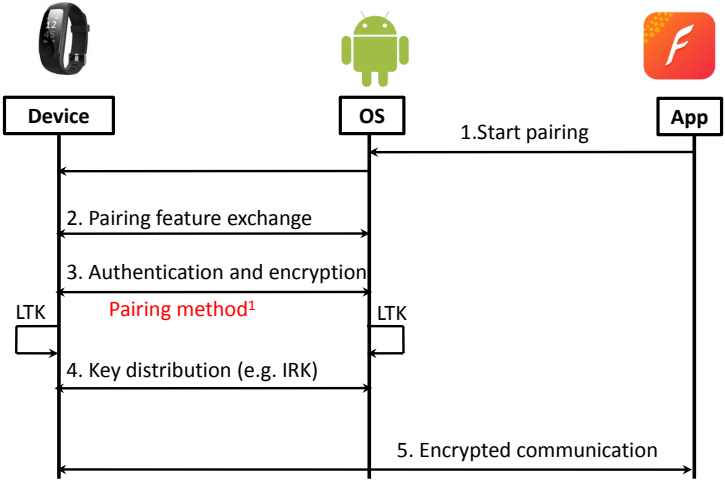
Pairing Workflow



Pairing Methods

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

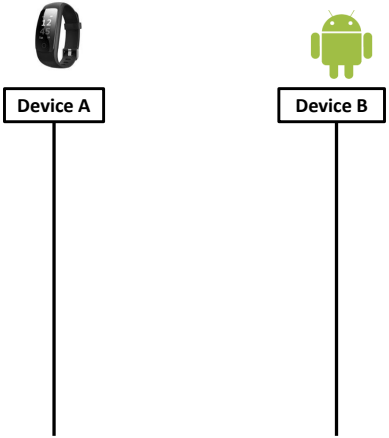
Pairing Workflow



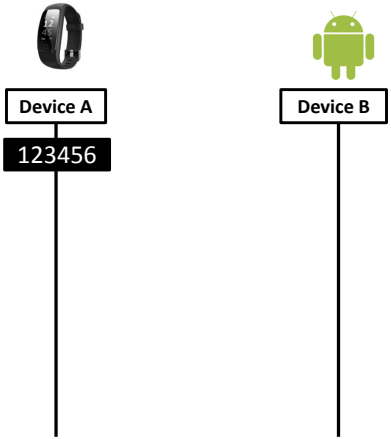
Pairing Methods

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

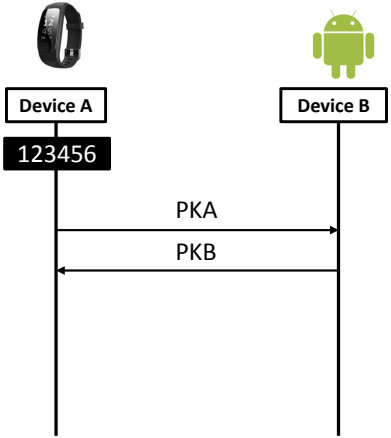
Workflow of Passkey Entry



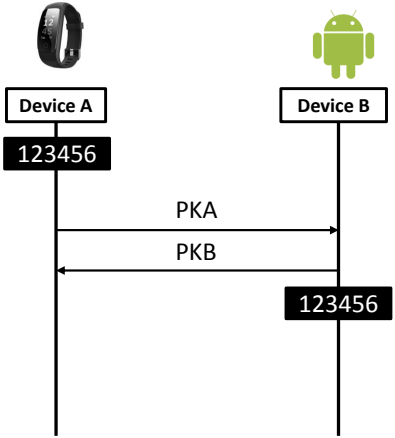
Workflow of Passkey Entry



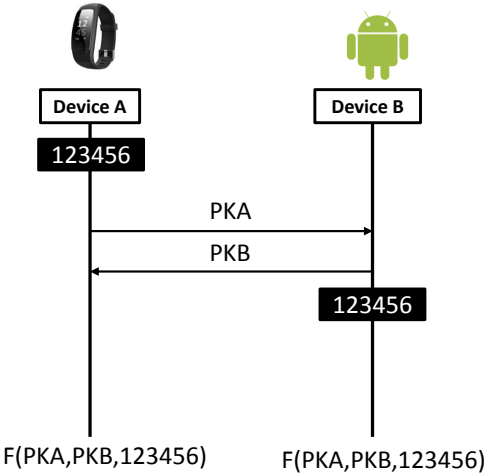
Workflow of Passkey Entry



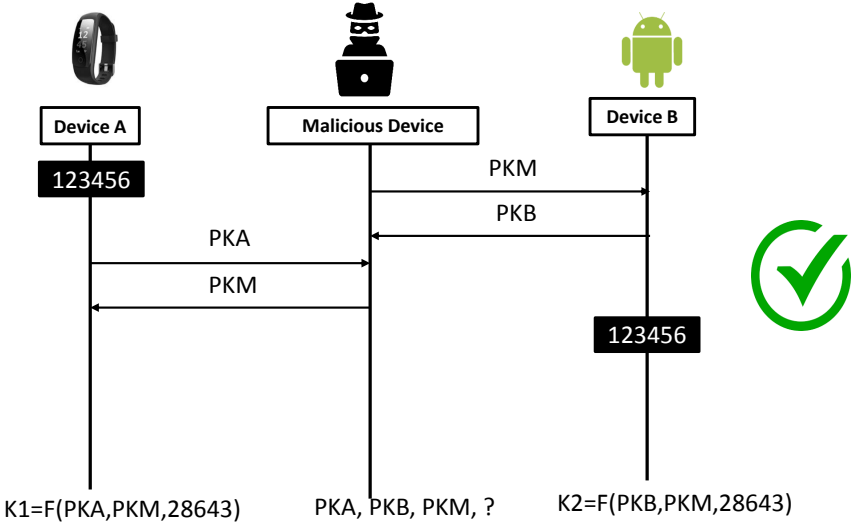
Workflow of Passkey Entry



Workflow of Passkey Entry

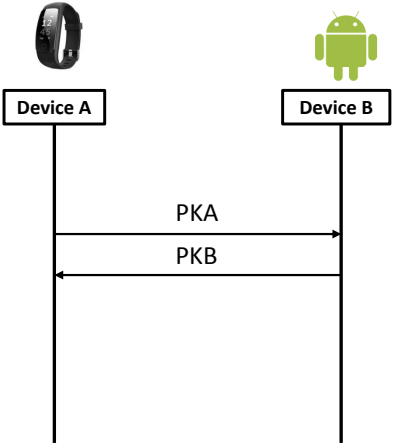


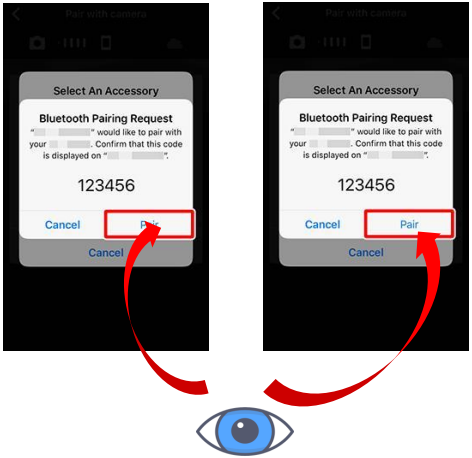
Workflow of Passkey Entry



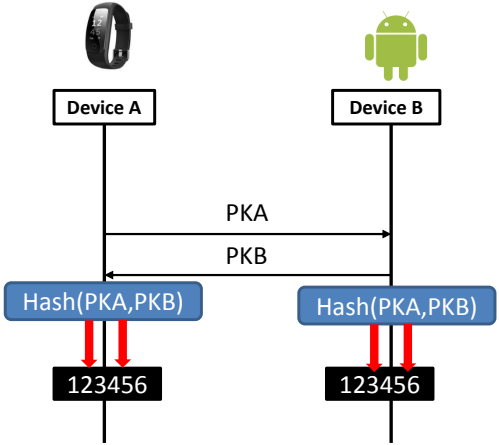
Workflow of Numeric Comparison

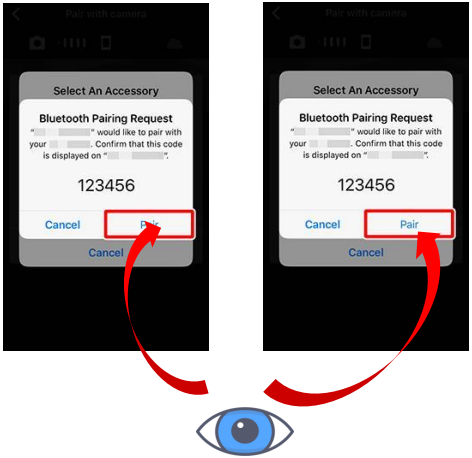
Workflow of Numeric Comparison



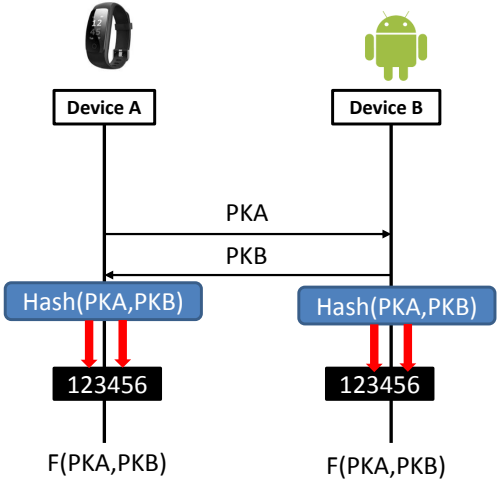


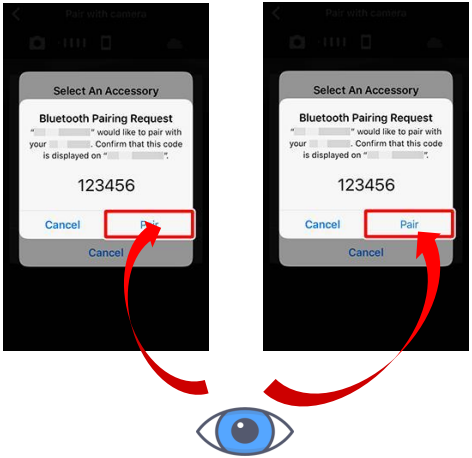
Workflow of Numeric Comparison



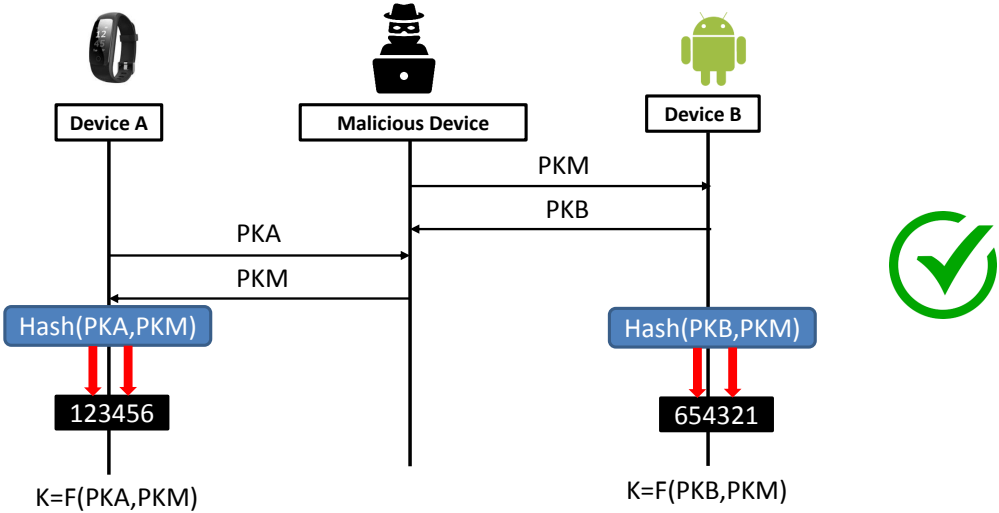


Workflow of Numeric Comparison

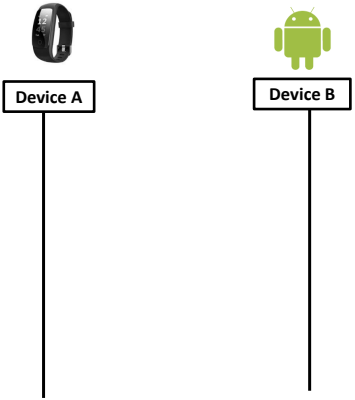




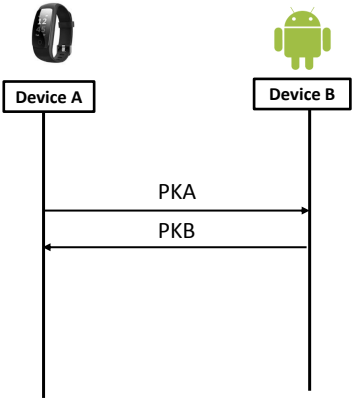
Workflow of Numeric Comparison



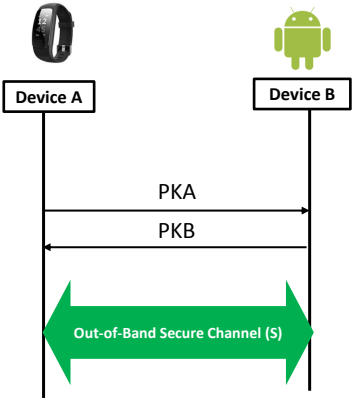
Workflow of Out of Band



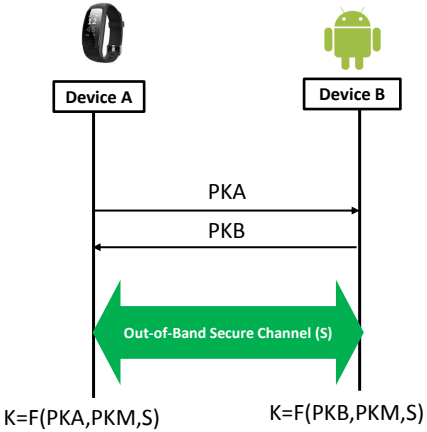
Workflow of Out of Band



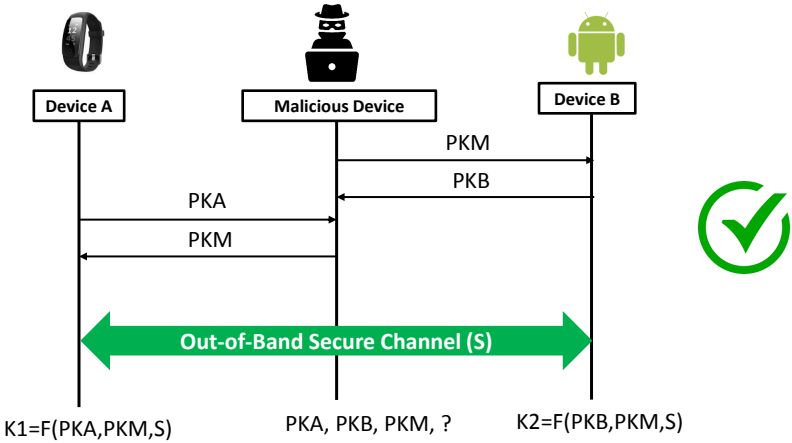
Workflow of Out of Band



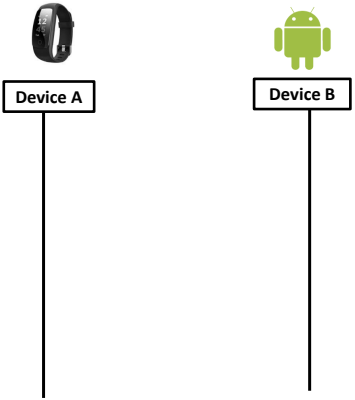
Workflow of Out of Band



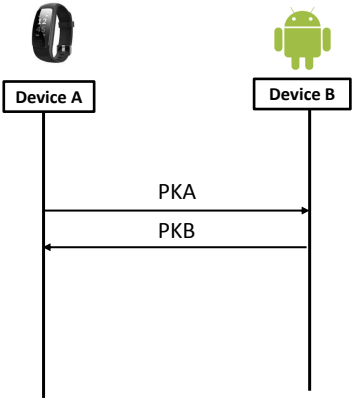
Workflow of Out of Band



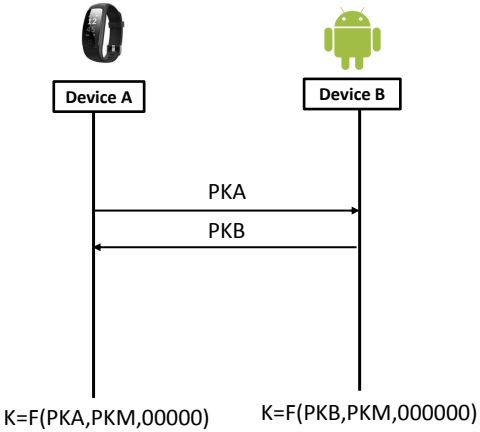
Workflow of Justworks



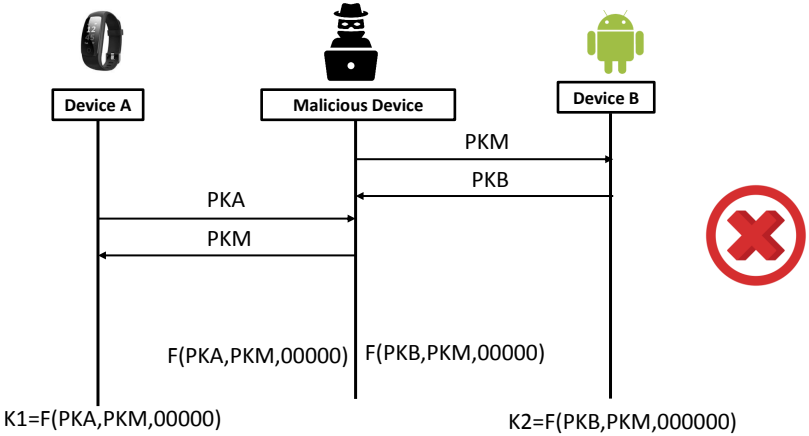
Workflow of Justworks



Workflow of Justworks



Workflow of Justworks



Bluetooth Security Levels and SCO mode

1. **Level 1:** Plaintext (None)
2. **Level 2:** Encrypted (Just Works)
3. **Level 3:** Authenticated (Passkey, Entry, Numeric Comparison, and Out of Band)

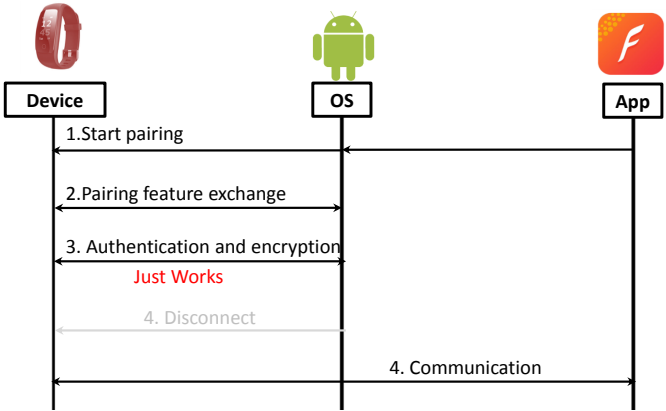
Bluetooth Security Levels and SCO mode

1. **Level 1:** Plaintext (None)
2. **Level 2:** Encrypted (Just Works)
3. **Level 3:** Authenticated (Passkey, Entry, Numeric Comparison, and Out of Band)
4. **Secure Connection Only (SCO) mode**: Enforced Passkey, Numeric Comparison, and Out of Band

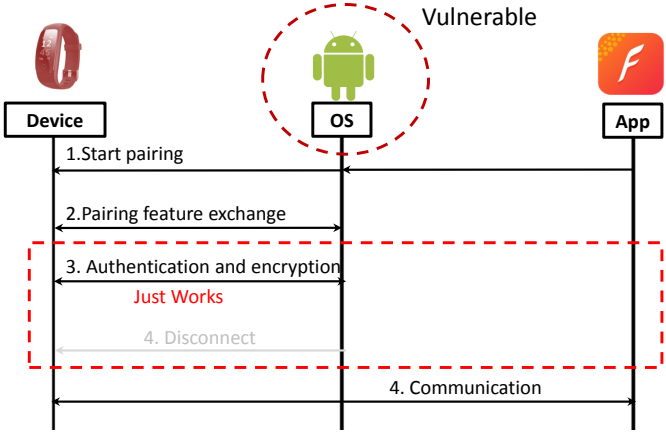
Our Observation

Although BLE specifies the SCO mode for a peripheral that provides services, it does not explicitly define (or require) the SCO mode for a master, which is also the pairing initiator.

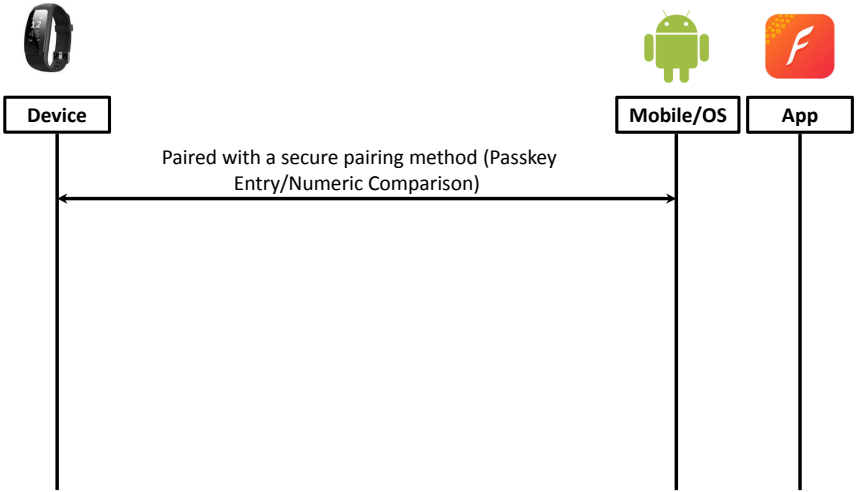
Root Cause


Device
OS
App
1.Start pairing
2.Pairing feature exchange
3. Authentication and encryption
Just Works
4. Disconnect
4. Communication

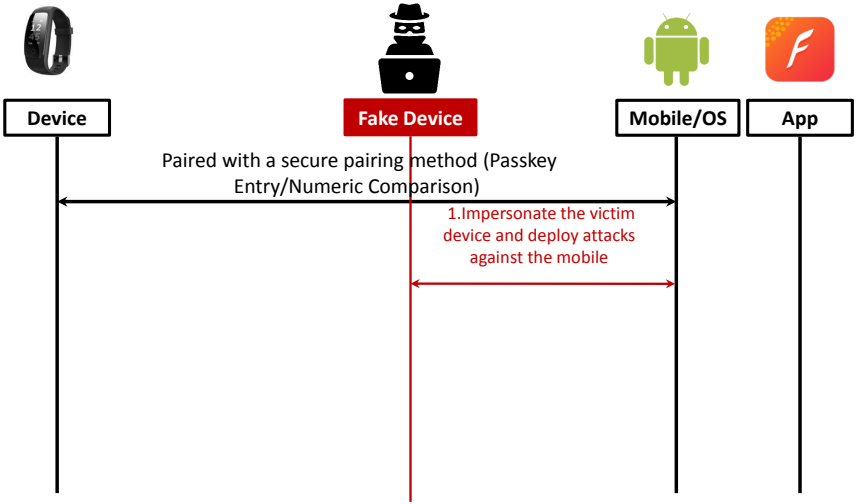
Root Cause


Vulnerable
Device
OS
App
1.Start pairing
2.Pairing feature exchange
3. Authentication and encryption
Just Works
4. Disconnect
4. Communication

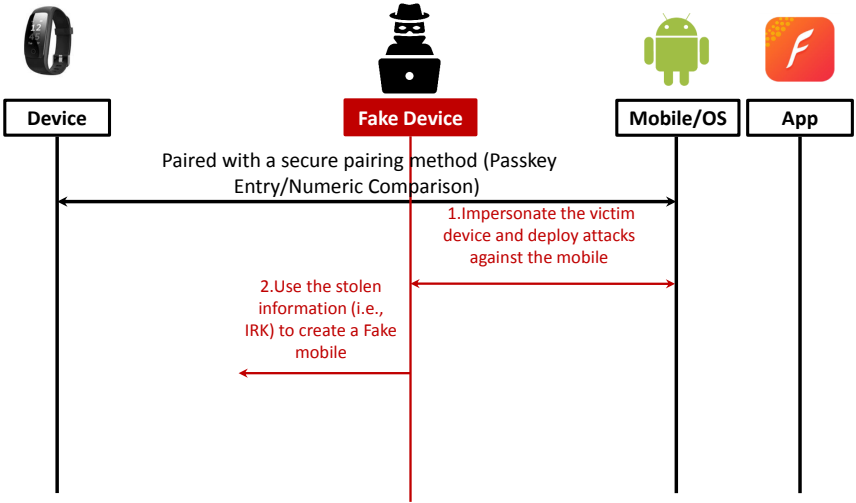
Downgrade Attacks



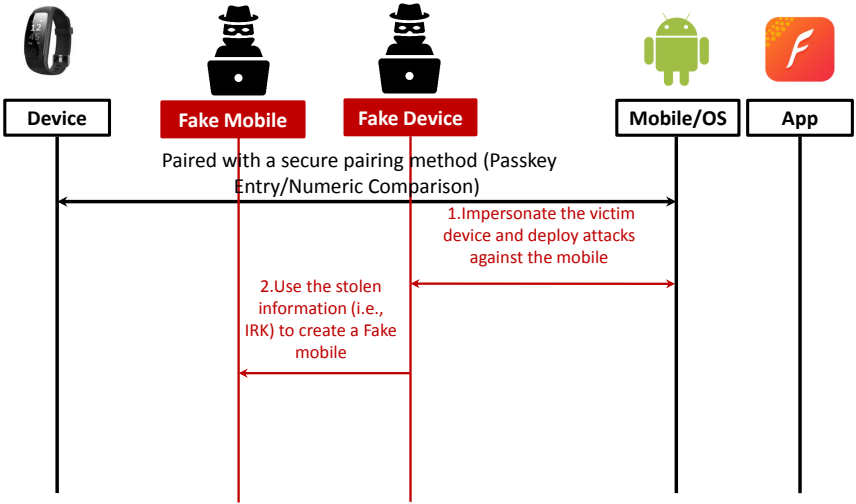
Downgrade Attacks



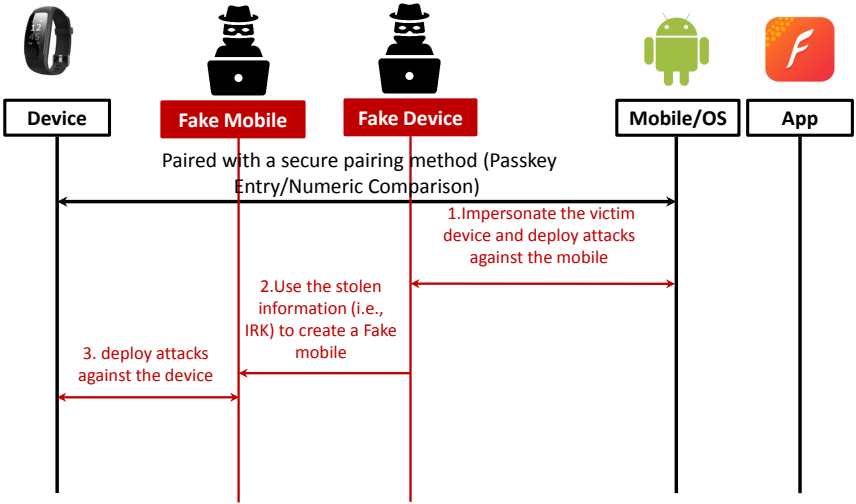
Downgrade Attacks



Downgrade Attacks

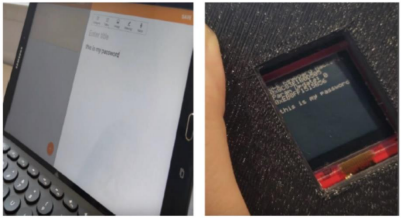


Downgrade Attacks



Downgrade Attacks

The Tested BLE devices

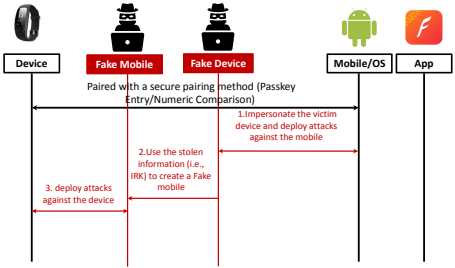


User Attacker

MITM attack against BLE keyboards

CVE-2020-9770

Downgrade Attacks

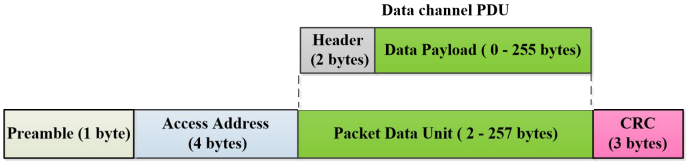


"Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks", Yue Zhang, Jian Weng, Rajib Dey, Yier Jin, Zhiqiang Lin, and Xinwen Fu. *In Proceedings of the 29th USENIX Security Symposium*, Boston, MA. August 2020

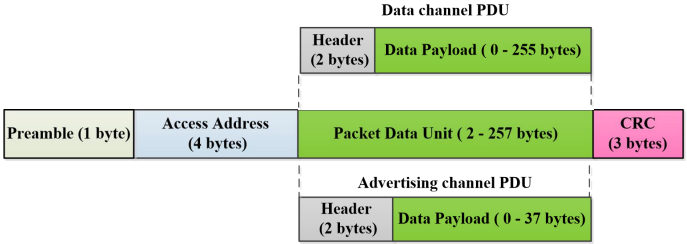
The Format of A Bluetooth Packet

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

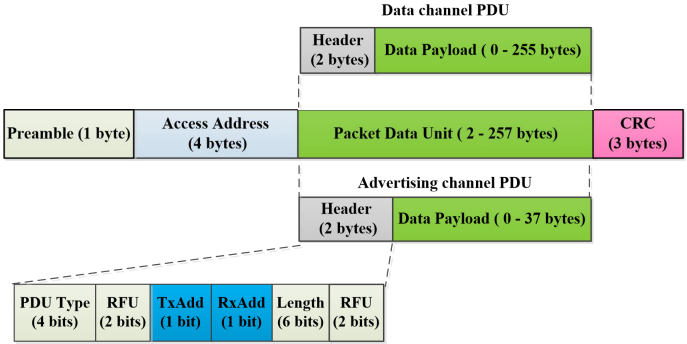
The Format of A Bluetooth Packet



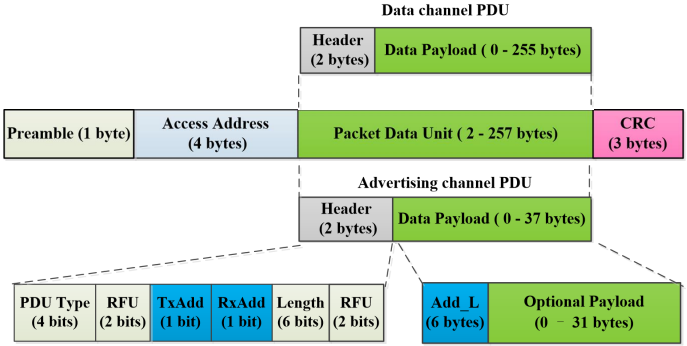
The Format of A Bluetooth Packet



The Format of A Bluetooth Packet



The Format of A Bluetooth Packet



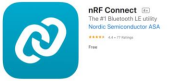
Bluetooth Sniffers

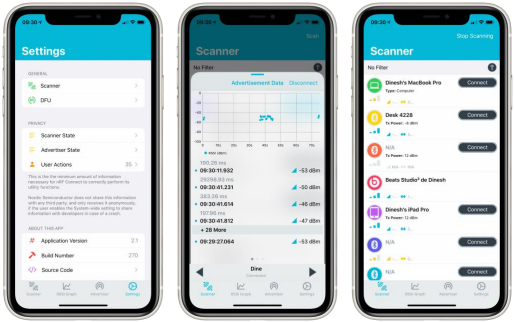
Ubertooth One Sniffer

125 USD

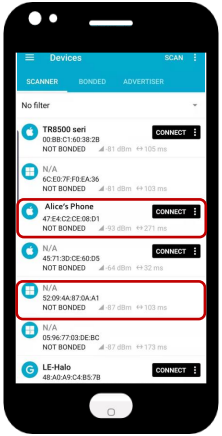
Adafruit LE sniffer

25 USD





Bluetooth Sniffers

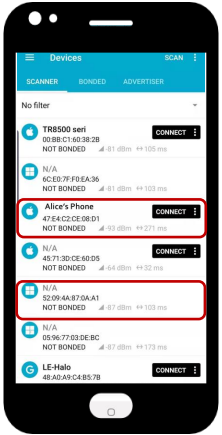


Alice's phone

Bob's phone

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

Bluetooth Sniffers



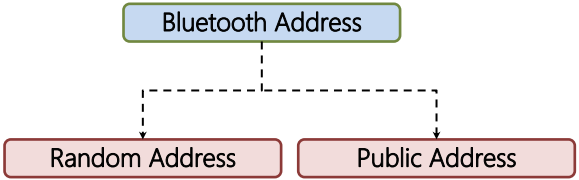
Alice's phone

Bob's phone

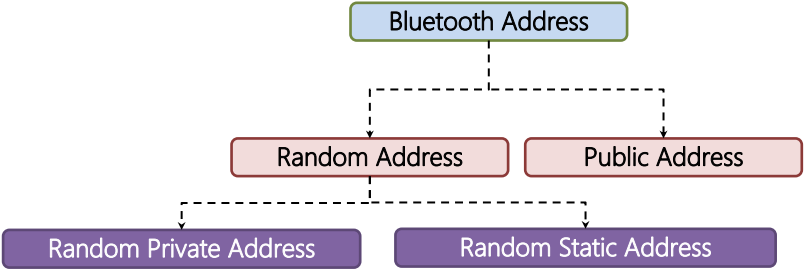
T1: 52:09:4A:87:0A:A1

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

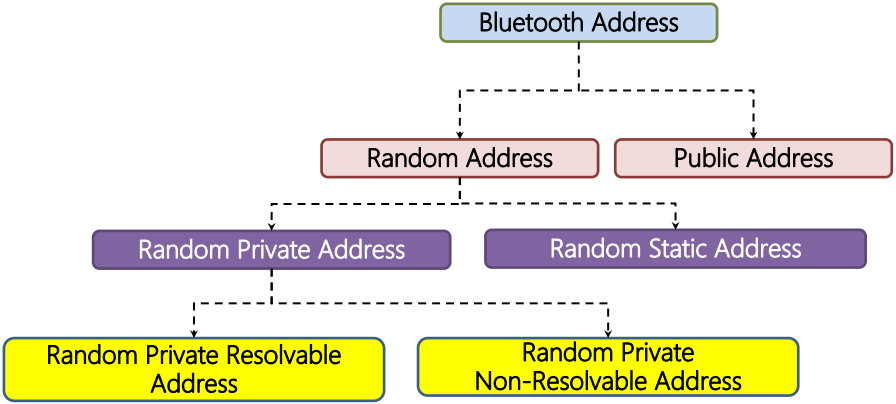
Bluetooth Address Types



Bluetooth Address Types



Bluetooth Address Types



How to Avoid Being Tracked: MAC Address Randomization

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

How to Avoid Being Tracked: MAC Address Randomization

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

(I) RPA Generation

How to Avoid Being Tracked: MAC Address Randomization

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

(I) RPA Generation

Resolvable Private Address (RPA)

rand = prand + type

hash = H(IRK, rand)

Type	prand	Hash
01 (2bits)	0x00...3 (22bits)	0x00...04 (24bits)

How to Avoid Being Tracked: MAC Address Randomization

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

(I) RPA Generation

Resolvable Private Address (RPA)

(II) RPA Resolution

rand = prand + type

hash = H(IRK, rand)

Type	prand	Hash
01 (2bits)	0x00...3 (22bits)	0x00...04 (24bits)

How to Avoid Being Tracked: MAC Address Randomization

I. Advertising filter policy

Only allows its allowlisted central to connect (e.g., Smart Earbuds)

II. Advertising filter policy

Automatically connects its allowlisted peripherals (e.g., Smart Earbuds)

Allowlist creates a one-to-one /one to multiple relationship between devices

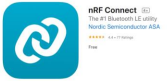
Allowlist

Ubertooth One Sniffer

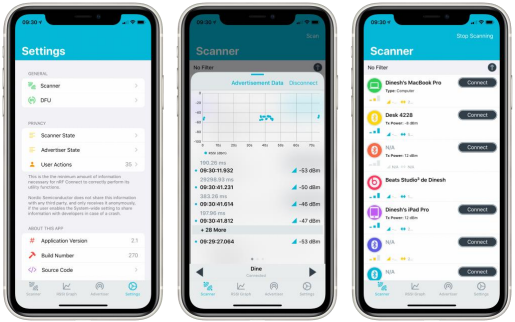
125 USD

Adafruit LE sniffer

25 USD



nRF Connect 4+
The #1 Bluetooth LE utility
Nordic Semiconductor ASA
4.4 • 17 Ratings
Free



Our Insights (I) — Allowlist Side Channel

58:D7:8E:C7:8e:31

NO.	Time	Source	Destination	TYPE
1	00:00:04	58:D7:8E:C7:8e:31	Broadcast	ADV_IND

Our Insights (I) — Allowlist Side Channel

58:D7:8E:C7:8e:31

7e:D7:8E:C7:8e:51

NO.	Time	Source	Destination	TYPE
1	00:00:04	58:D7:8E:C7:8e:31	Broadcast	ADV_IND
2	00:00:08	7e:D7:8E:C7:8e:51	58:D7:8E:C7:8e:31	SCAN_REQ
3	00:00:12	58:D7:8E:C7:8e:31	Broadcast	SCAN_RSP

Our Insights (I) — Allowlist Side Channel

NO.	Time	Source	Destination	TYPE
1	00:00:04	58:D7:8E:C7:8e:31	Broadcast	ADV_IND
2	00:00:08	7e:D7:8E:C7:8e:51	58:D7:8E:C7:8e:31	SCAN_REQ
3	00:00:12	58:D7:8E:C7:8e:31	Broadcast	SCAN_RSP
4	00:00:16	4f:b7:8E:C7:8e:38	58:D7:8E:C7:8e:31	SCAN_REQ
5	00:00:24	58:D7:8E:C7:8e:31	Broadcast	ADV_IND

Our Insights (I) — Allowlist Side Channel

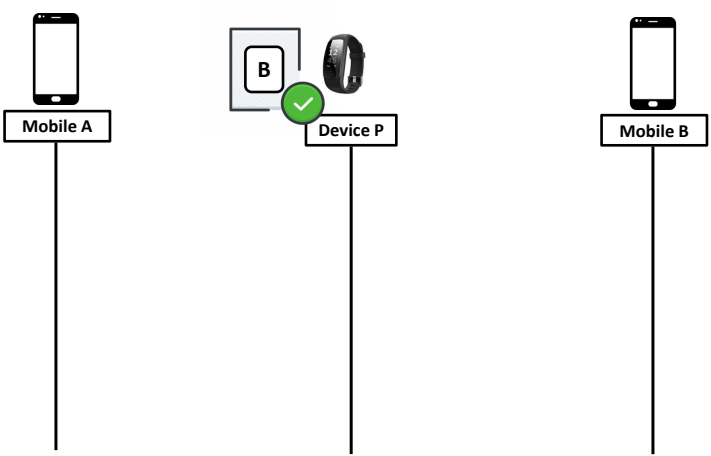
58:D7:8E:C7:8e:31

7e:D7:8E:C7:8e:51

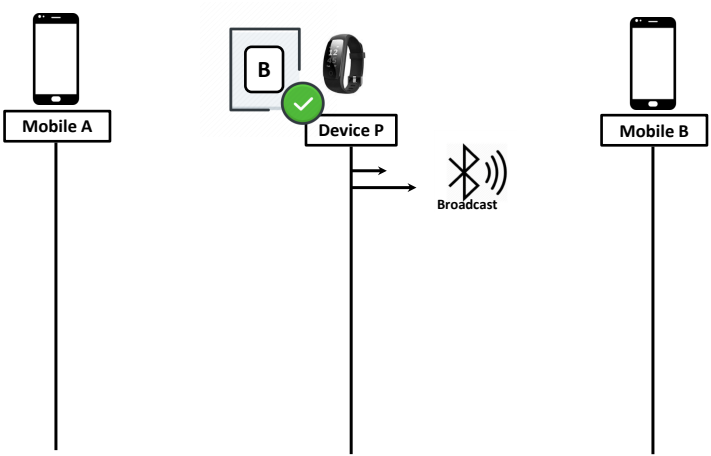
4f:b7:8E:C7:8e:38

NO.	Time	Source	Destination	TYPE
1	00:00:04	58:D7:8E:C7:8e:31	Broadcast	ADV_IND
2	00:00:08	7e:D7:8E:C7:8e:51	58:D7:8E:C7:8e:31	SCAN_REQ
3	00:00:12	58:D7:8E:C7:8e:31	Broadcast	SCAN_RSP
4	00:00:16	4f:b7:8E:C7:8e:38	58:D7:8E:C7:8e:31	SCAN_REQ
5	00:00:24	58:D7:8E:C7:8e:31	Broadcast	ADV_IND
.....				
200	00:15:08	73:D7:8E:C7:8e:45	58:D7:8E:C7:8e:31	SCAN_REQ
201	00:15:12	58:D7:8E:C7:8e:31	Broadcast	SCAN_RSP

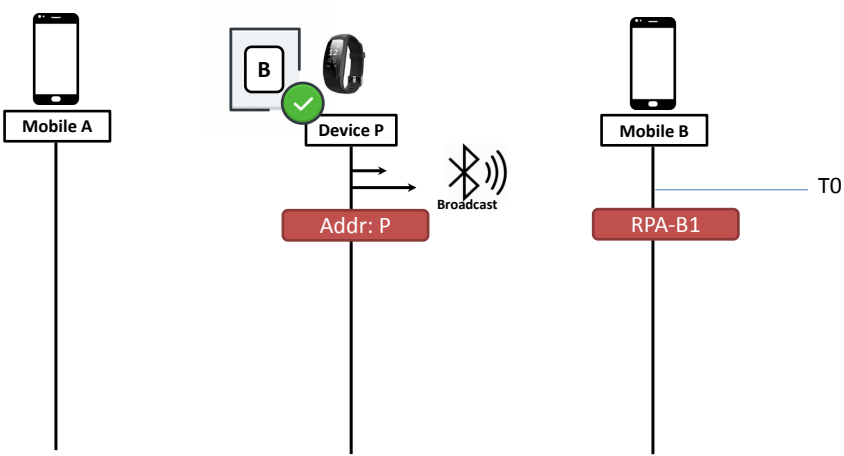
Our Insights (I) — Allowlist Side Channel



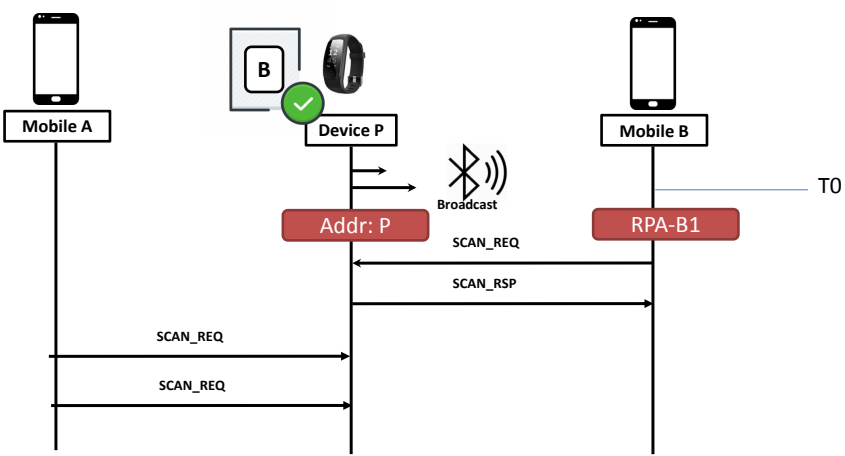
Our Insights (I) — Allowlist Side Channel



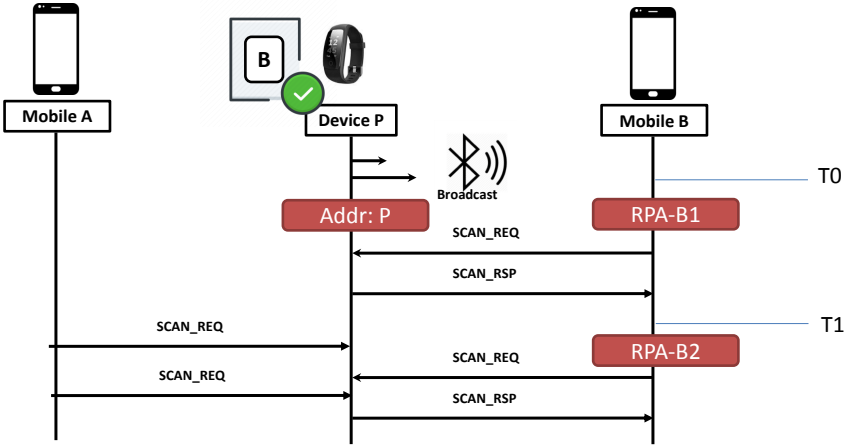
Our Insights (I) — Allowlist Side Channel



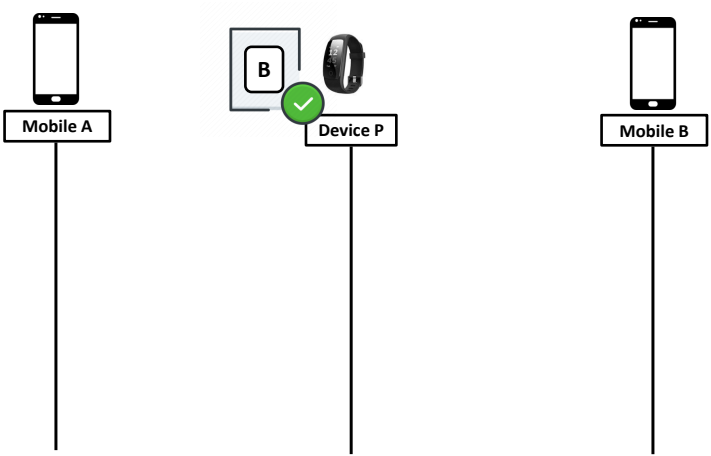
Our Insights (I) — Allowlist Side Channel



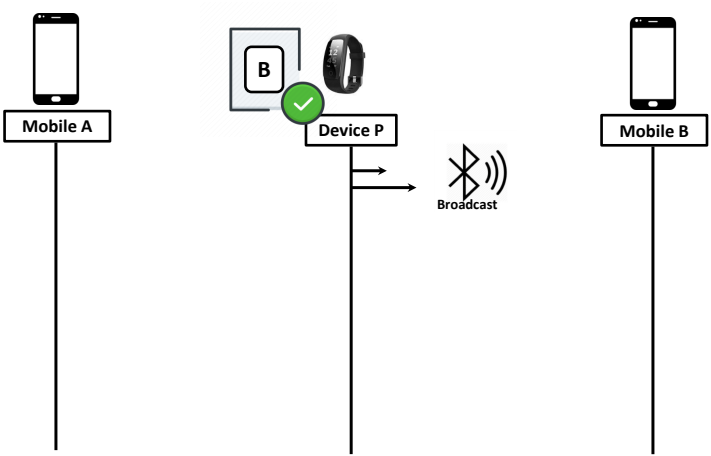
Our Insights (I) — Allowlist Side Channel



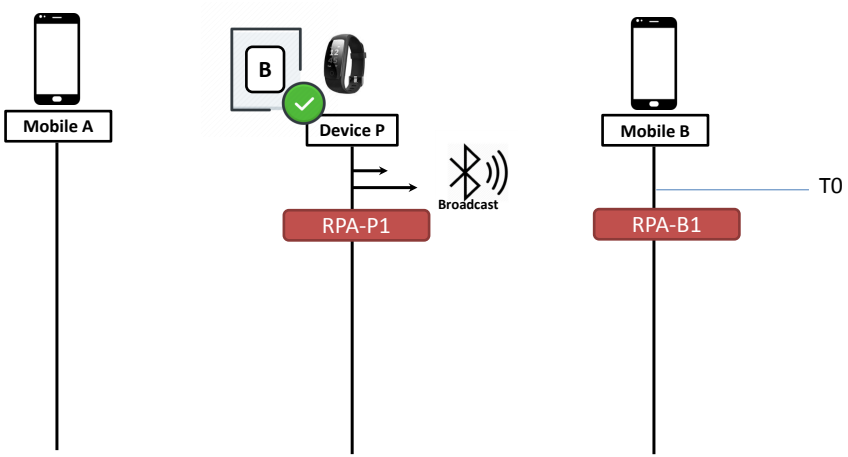
Passive Bluetooth Address Tracking (BAT) Attacks



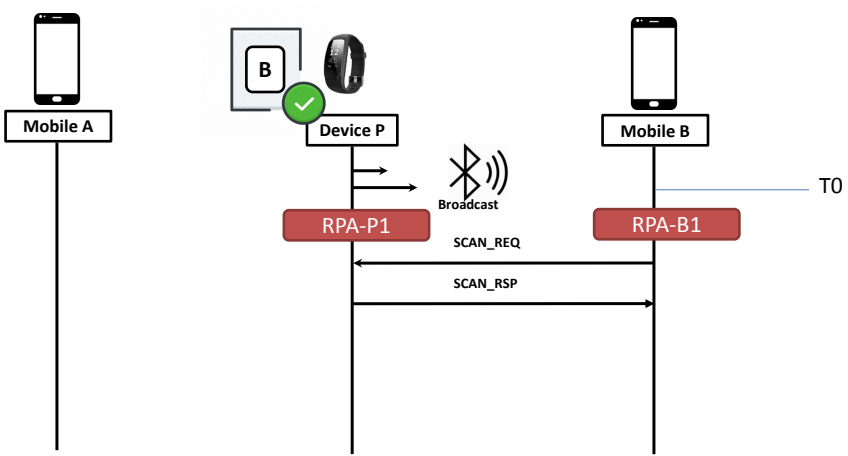
Passive Bluetooth Address Tracking (BAT) Attacks



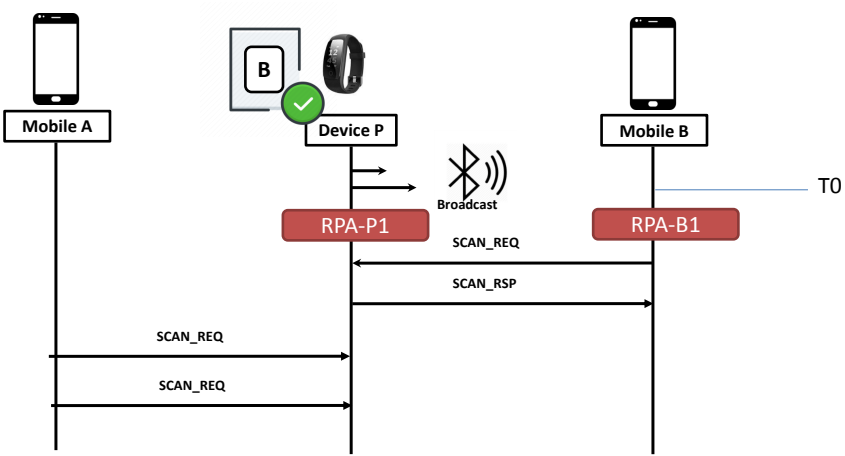
Passive Bluetooth Address Tracking (BAT) Attacks



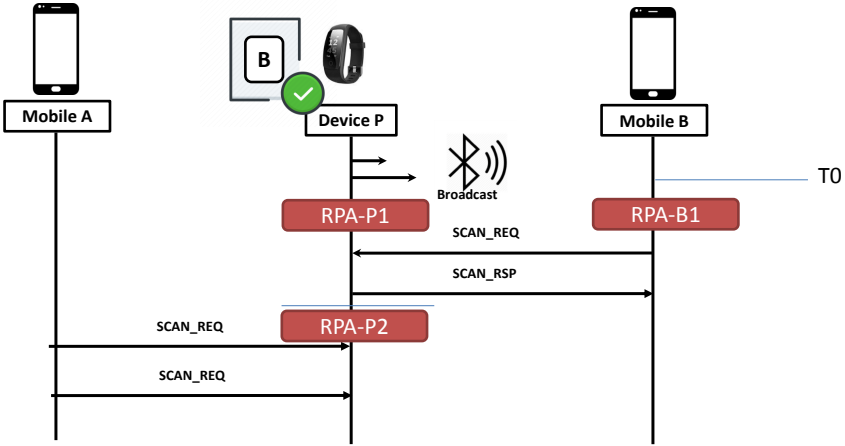
Passive Bluetooth Address Tracking (BAT) Attacks



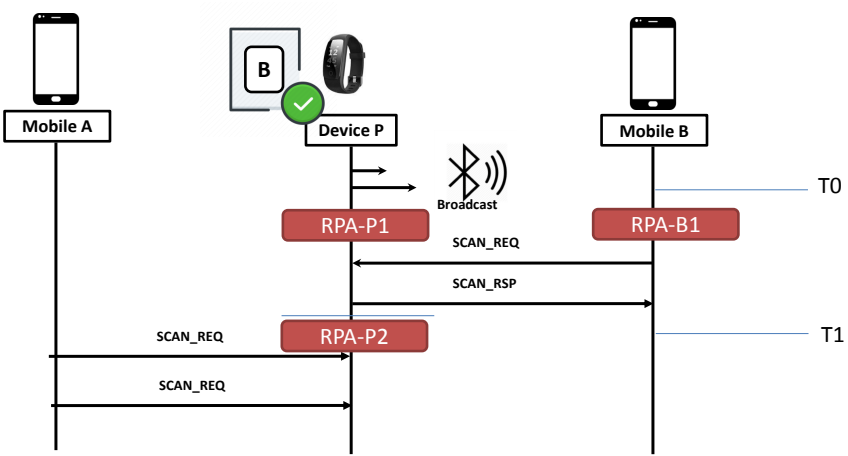
Passive Bluetooth Address Tracking (BAT) Attacks



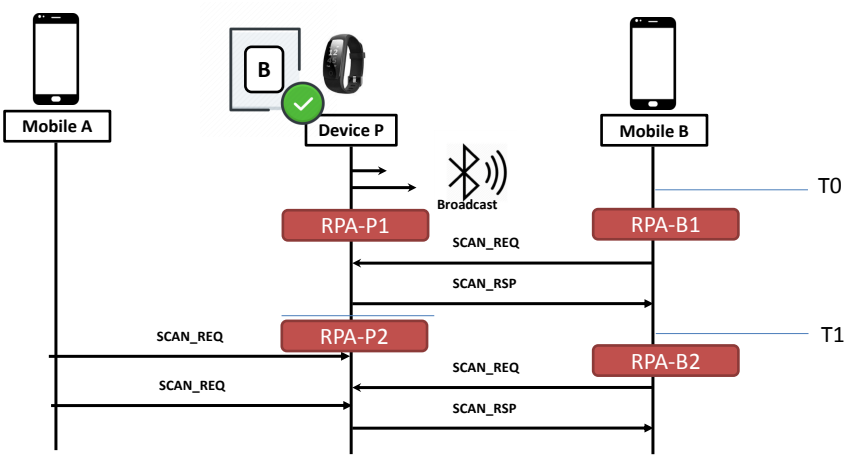
Passive Bluetooth Address Tracking (BAT) Attacks



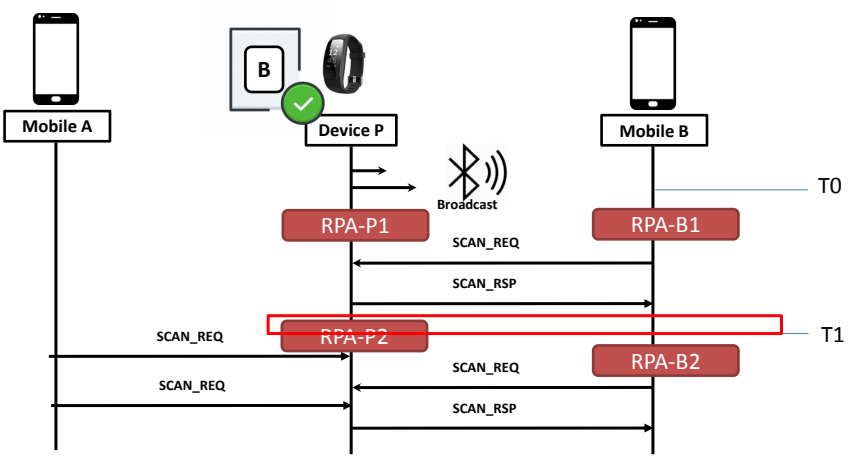
Passive Bluetooth Address Tracking (BAT) Attacks



Passive Bluetooth Address Tracking (BAT) Attacks



Passive Bluetooth Address Tracking (BAT) Attacks



Our Insights (II) — MAC Address Replay

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

Our Insights (II) — MAC Address Replay

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

(I) RPA Generation

Our Insights (II) — MAC Address Replay

Identity Resolving Key (IRK)

Identity Resolving Key (IRK)

(I) RPA Generation

Resolvable Private Address (RPA)

(II) RPA Resolution

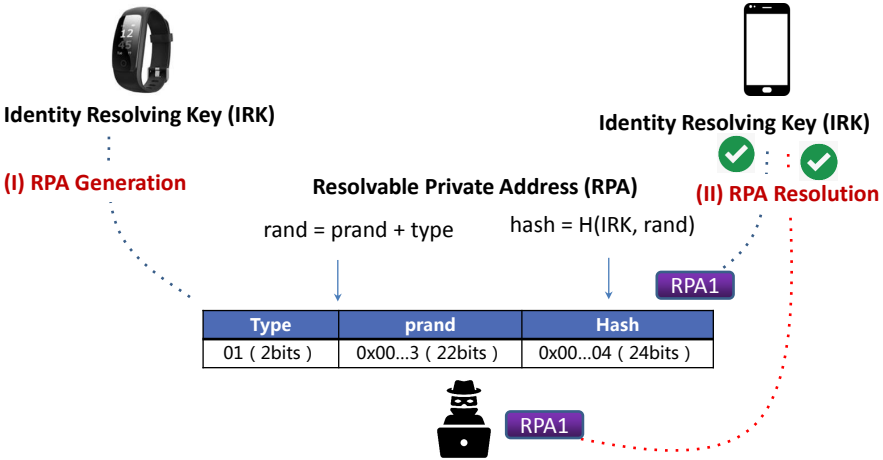
rand = prand + type

hash = H(IRK, rand)

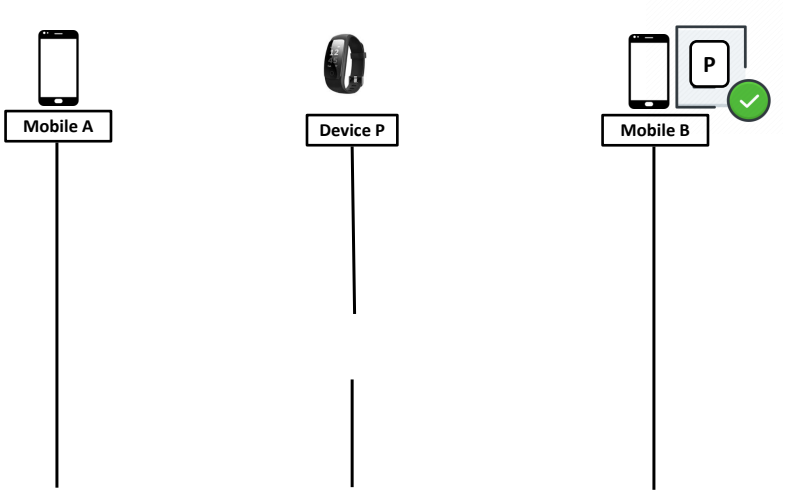
RPA1

Type	prand	Hash
01 (2bits)	0x00...3 (22bits)	0x00...04 (24bits)

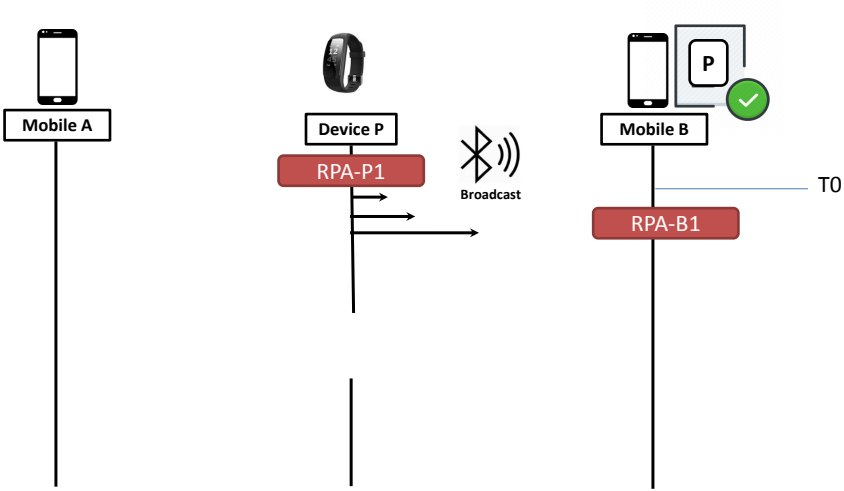
Our Insights (II) — MAC Address Replay



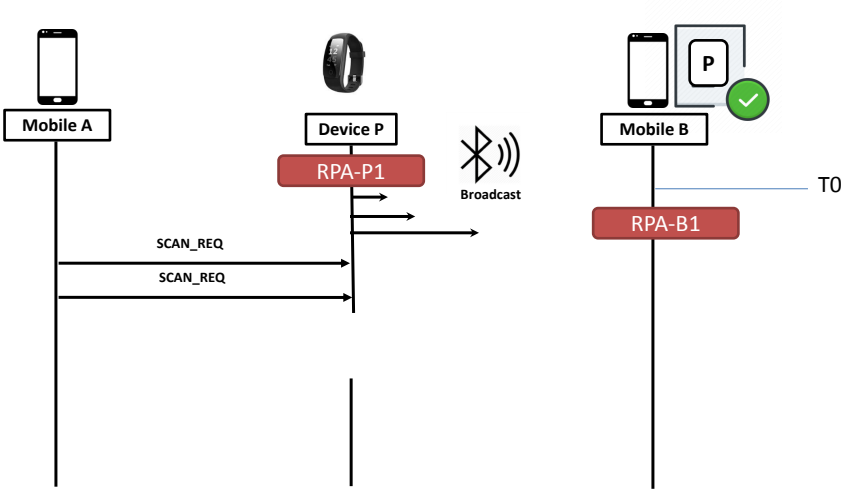
Active Bluetooth Address Tracking (BAT) Attacks



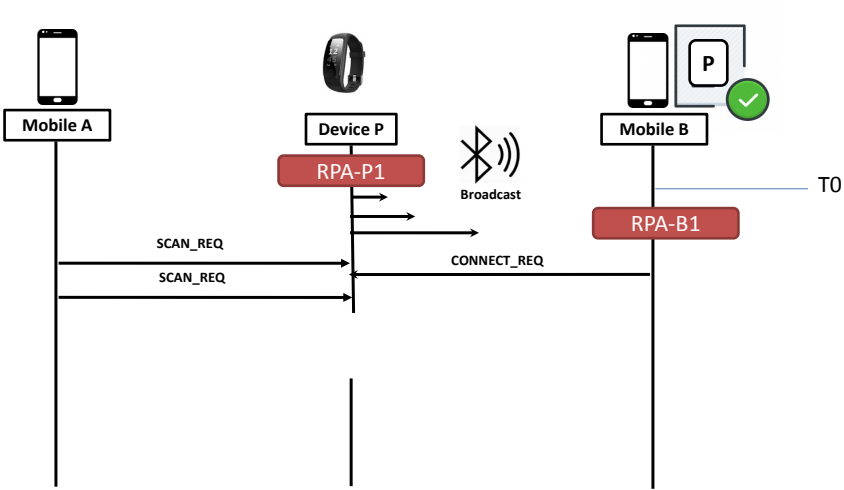
Active Bluetooth Address Tracking (BAT) Attacks



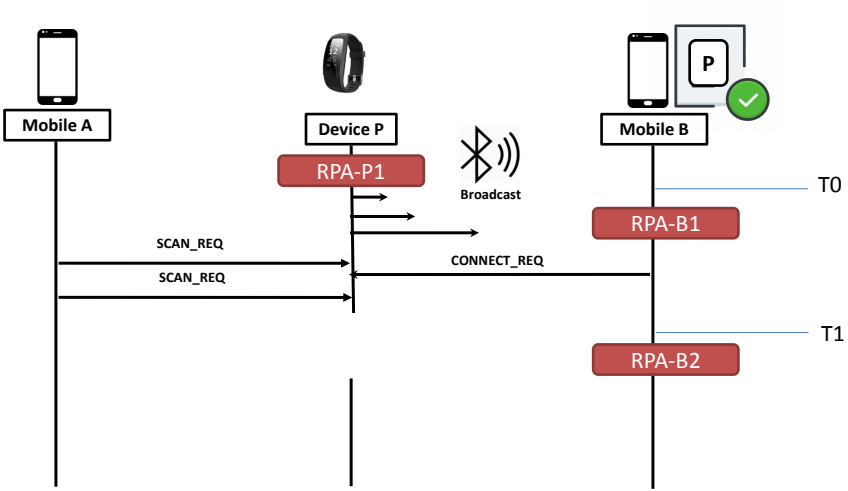
Active Bluetooth Address Tracking (BAT) Attacks



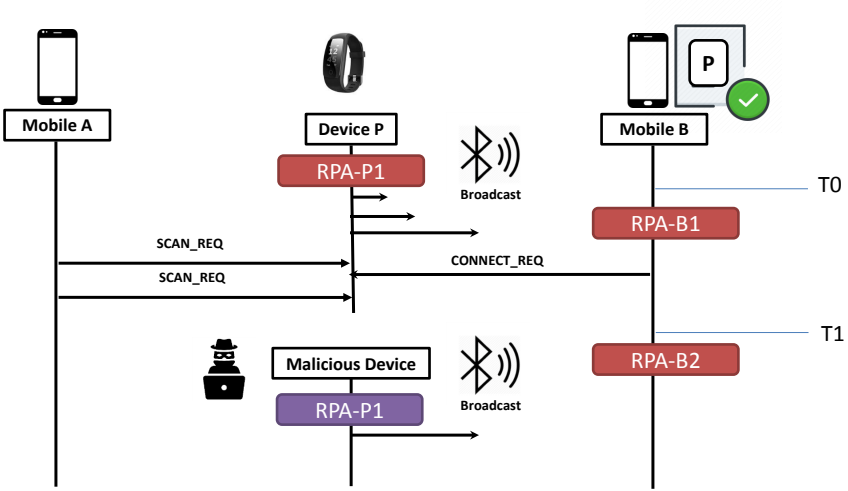
Active Bluetooth Address Tracking (BAT) Attacks



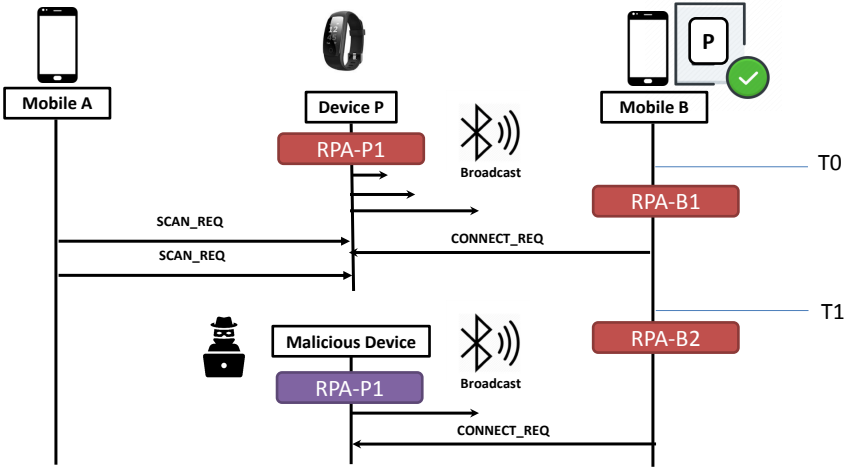
Active Bluetooth Address Tracking (BAT) Attacks



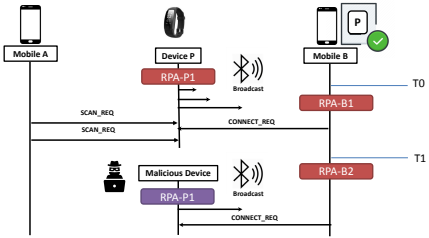
Active Bluetooth Address Tracking (BAT) Attacks



Active Bluetooth Address Tracking (BAT) Attacks

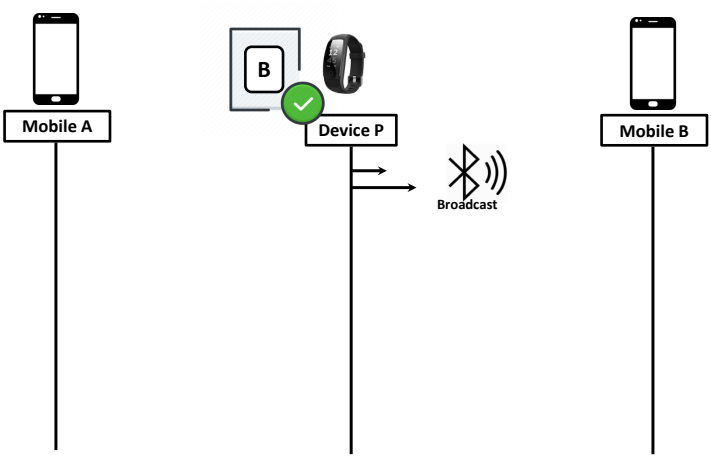


Active Bluetooth Address Tracking (BAT) Attacks

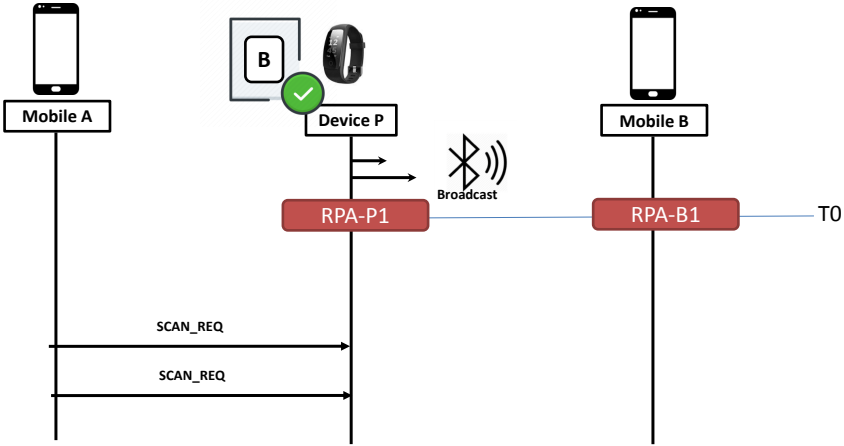


"When Good Becomes Evil: Tracking Bluetooth Low Energy Devices via Allowlist-based Side Channel and Its Countermeasure". Yue Zhang, and Zhiqiang Lin. *In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS 2022).* November 2022

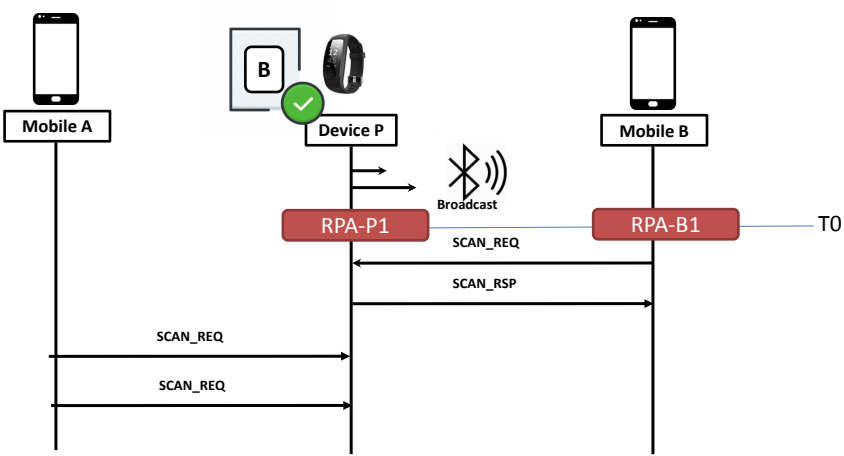
SABLE — Passive Defense



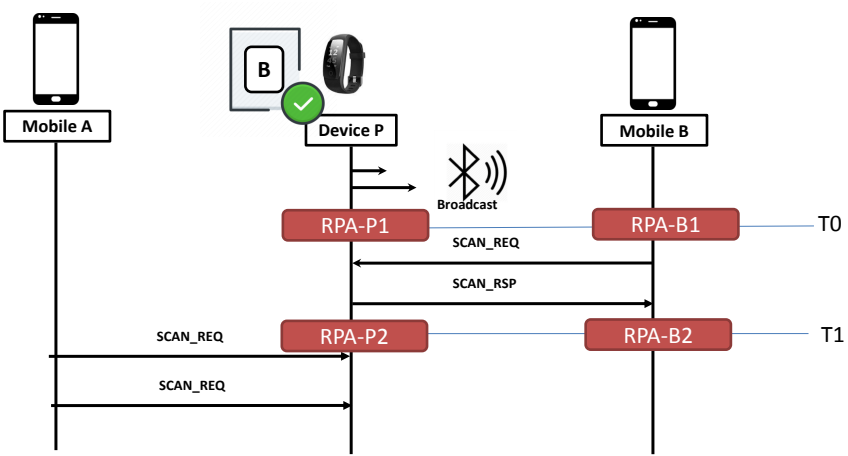
SABLE — Passive Defense



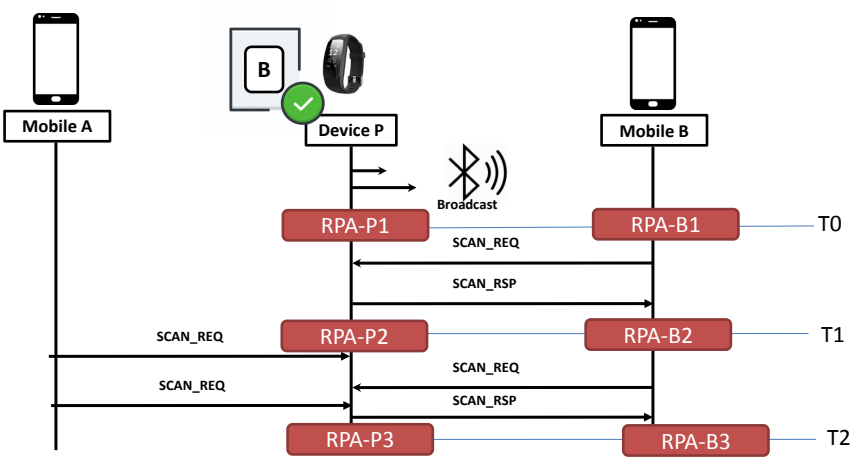
SABLE — Passive Defense



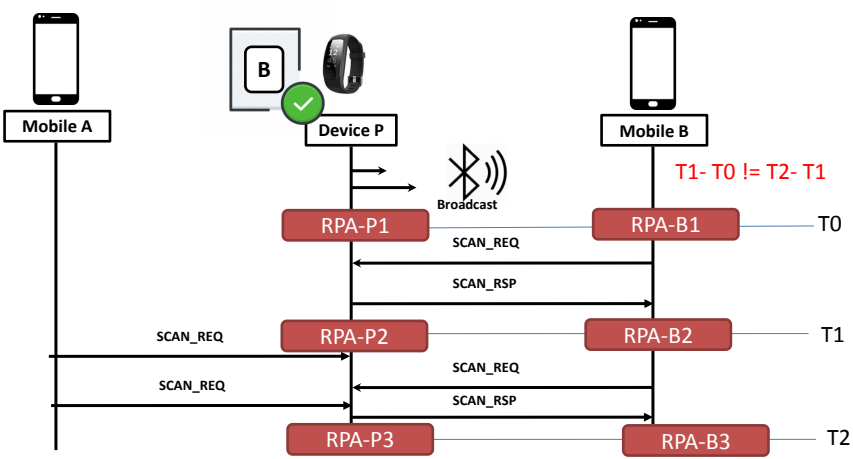
SABLE — Passive Defense



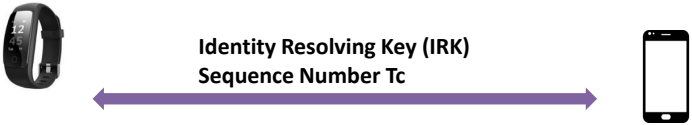
SABLE — Passive Defense



SABLE — Active Defense



SABLE — Active Defense



SABLE — Active Defense

Identity Resolving Key (IRK)
Sequence Number Tc

(I) RPA Generation

Resolvable Private Address (RPA)

rand = prand + type

hash = H(IRK, rand, Tc)

Type	prand	Hash
01 (2bits)	0x00...3 (22bits)	0x00...04 (24bits)

SABLE — Active Defense

Identity Resolving Key (IRK)
Sequence Number Tc

(I) RPA Generation

Resolvable Private Address (RPA)

(II) RPA Resolution

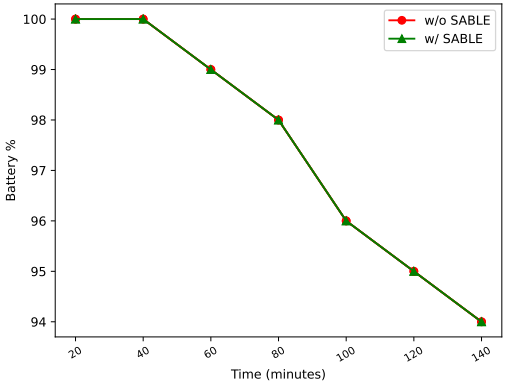
rand = prand + type

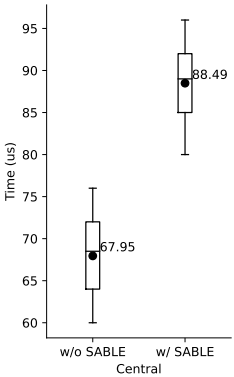
hash = H(IRK, rand, Tc)

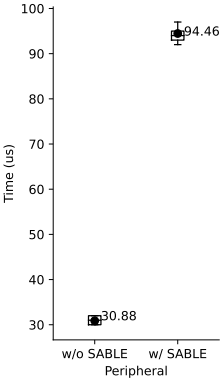
RPA1

Type	prand	Hash
01 (2bits)	0x00...3 (22bits)	0x00...04 (24bits)

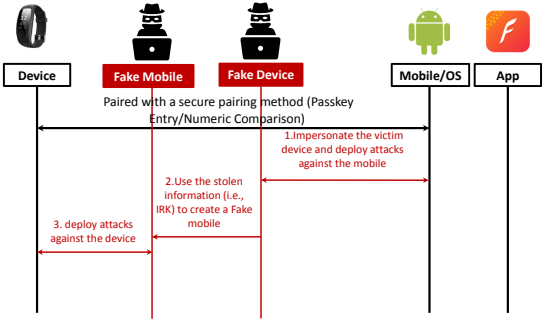
Performance of SABLE





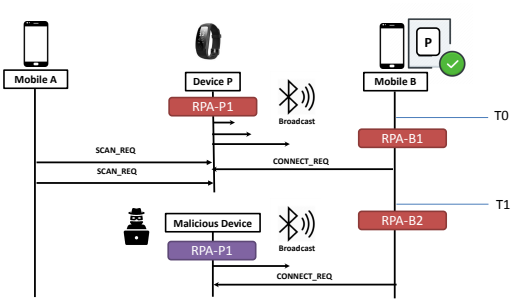


Lesson Learned (1/3): Bluetooth Communication Can Be Downgraded



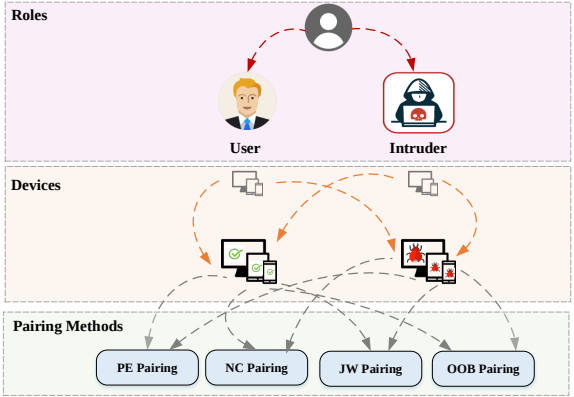
- Bluetooth protocol can be downgraded
- There are many stages that are not part of the pairing protocol, but they are, in fact, closely related to pairing security.
- A systematic analysis of different stages (other than pairing), including the error handling of BLE communication, is needed.

Lesson Learned (2/3): New Features Need More Investigation



- BLE introduces multiple new features (e.g., Allow-list)
- Those new features need to be understood and investigated. 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 is often confusing and not consistent across chapters.
- The confusion may lead to the fact that different vendors implement BLE protocols in quite different ways, for example, for error handling, and IRK use.
- Converting the Bluetooth specification to formal model (e.g., using NLP), and formally verify the entire protocol would help.
- See our NDSS'23 paper.