Bluetooth® Seminar Series

Tools, Techniques, and Trends

Privacy Protection Mechanisms in Bluetooth Technology

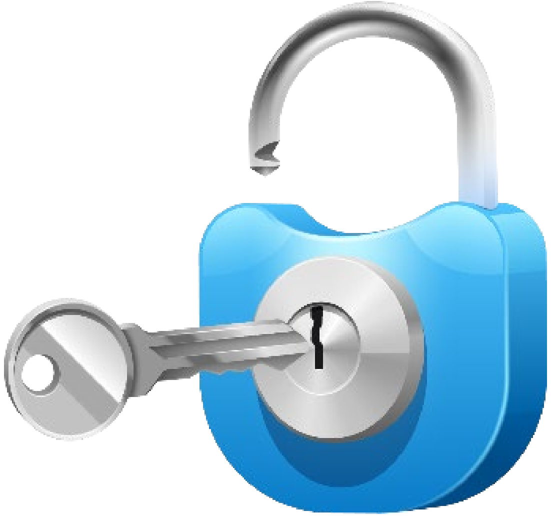
Tim Wei | Senior Application Engineer | Ellisys

The Concern

- Being tracked without your awareness
- Tracking is achieved by linking you to a unique identity:
  - The International Mobile Equipment Identity (IMEI) of your phone/watch
  - The MAC Address of Wi-Fi®
  - The MAC Address of Bluetooth

The Solution (1)

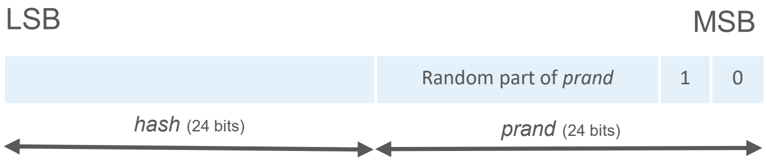
- Resolvable Private Address
  - A Bluetooth Address changes from time to time
  - Default 15 min, can be from 1 s to about 11.5 hours
- After the Bluetooth Address changes, it looks like a different device
- Only trusted devices know that it's the same device
  - Identity Resolving Key (IRK)
  - Identity Address
- Introduced with Bluetooth LE at Bluetooth 4.0 and enhanced in later versions



11:22:33:44:55:66

The Solution (2)

Resolvable Private Address



$$\mathit{hash} = \mathit{ah}(\mathrm{IRK}, \mathit{prand})$$

A hash function is any function that can be used to map data of arbitrary size to fixed-size values

ah is a hash function

Resolving List

Local IRK1	Peer IRK1	Peer Device Identity Address1	Address Type1
Local IRK2	Peer IRK2	Peer Device Identity Address2	Address Type2
Local IRK3	Peer IRK3	Peer Device Identity Address3	Address Type3
Local IRK4	Peer IRK4	Peer Device Identity Address4	Address Type4

$$\mathit{localHashX} = \mathit{ah}(\mathrm{Peer\ IRKX}, \mathit{prand})$$

If localHashX = hash, the address is resolved, and the identity address of the peer device is Peer Device Identity AddressX

Bluetooth Address Types

- Public Address (Address Type = 0x00)
- Random Address (Address Type = 0x01)
  - Static Address

LSB	Random part of *static address*	1	1	MSB

  - Private Address
    - Non-resolvable private address

LSB	Random part of *non-resolvable address*	0	0	MSB

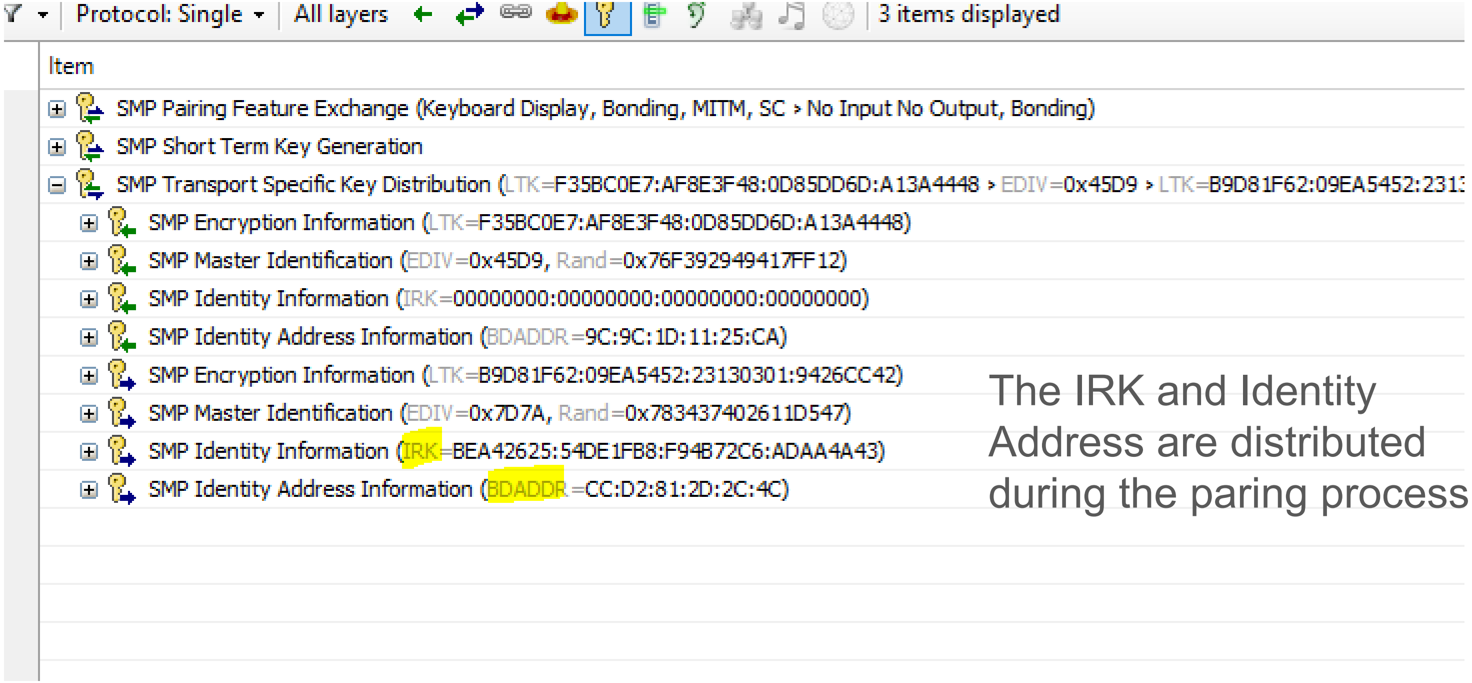
    - Resolvable private address

LSB		Random part	1	0	MSB
	hash (24 bits)	*prand* (24 bits)			

Only public address and static address can be used as identity address

If a Non-resolvable private address is used, the device doesn't want anybody know who it is

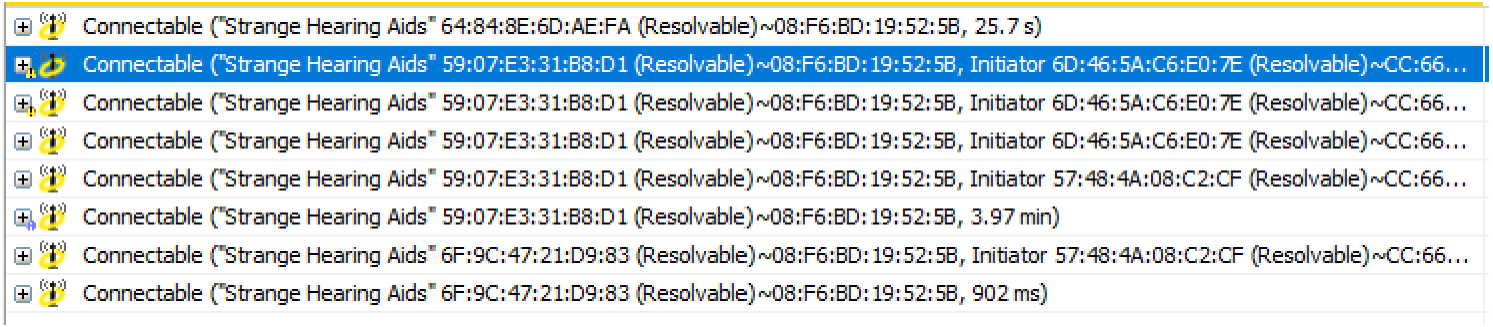
Example (1)



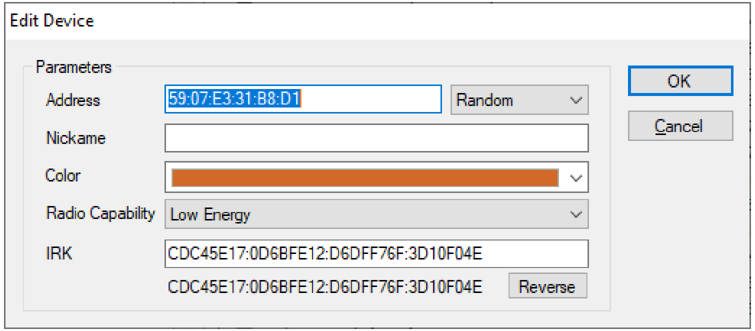
```
⊞ SMP Pairing Feature Exchange (Keyboard Display, Bonding, MITM, SC › No Input No Output, Bonding)
⊞ SMP Short Term Key Generation
⊟ SMP Transport Specific Key Distribution (LTK=F35BC0E7:AF8E3F48:0D85DD6D:A13A4448 › EDIV=0x45D9 › LTK=B9D81F62:09EA5452:2313
    ⊞ SMP Encryption Information (LTK=F35BC0E7:AF8E3F48:0D85DD6D:A13A4448)
    ⊞ SMP Master Identification (EDIV=0x45D9, Rand=0x76F392949417FF12)
    ⊞ SMP Identity Information (IRK=00000000:00000000:00000000:00000000)
    ⊞ SMP Identity Address Information (BDADDR=9C:9C:1D:11:25:CA)
    ⊞ SMP Encryption Information (LTK=B9D81F62:09EA5452:23130301:9426CC42)
    ⊞ SMP Master Identification (EDIV=0x7D7A, Rand=0x783437402611D547)
    ⊞ SMP Identity Information (IRK=BEA42625:54DE1FB8:F94B72C6:ADAA4A43)
    ⊞ SMP Identity Address Information (BDADDR=CC:D2:81:2D:2C:4C)
```

The IRK and Identity Address are distributed during the paring process

Example (2)



```
Connectable ("Strange Hearing Aids" 64:84:8E:6D:AE:FA (Resolvable)~08:F6:BD:19:52:5B, 25.7 s)
Connectable ("Strange Hearing Aids" 59:07:E3:31:B8:D1 (Resolvable)~08:F6:BD:19:52:5B, Initiator 6D:46:5A:C6:E0:7E (Resolvable)~CC:66...
Connectable ("Strange Hearing Aids" 59:07:E3:31:B8:D1 (Resolvable)~08:F6:BD:19:52:5B, Initiator 6D:46:5A:C6:E0:7E (Resolvable)~CC:66...
Connectable ("Strange Hearing Aids" 59:07:E3:31:B8:D1 (Resolvable)~08:F6:BD:19:52:5B, Initiator 6D:46:5A:C6:E0:7E (Resolvable)~CC:66...
Connectable ("Strange Hearing Aids" 59:07:E3:31:B8:D1 (Resolvable)~08:F6:BD:19:52:5B, Initiator 57:48:4A:08:C2:CF (Resolvable)~CC:66...
Connectable ("Strange Hearing Aids" 59:07:E3:31:B8:D1 (Resolvable)~08:F6:BD:19:52:5B, 3.97 min)
Connectable ("Strange Hearing Aids" 6F:9C:47:21:D9:83 (Resolvable)~08:F6:BD:19:52:5B, Initiator 57:48:4A:08:C2:CF (Resolvable)~CC:66...
Connectable ("Strange Hearing Aids" 6F:9C:47:21:D9:83 (Resolvable)~08:F6:BD:19:52:5B, 902 ms)
```



Edit Device

Parameters

Address: 59:07:E3:31:B8:D1 Random

Nickame:

Color: 🟧

Radio Capability: Low Energy

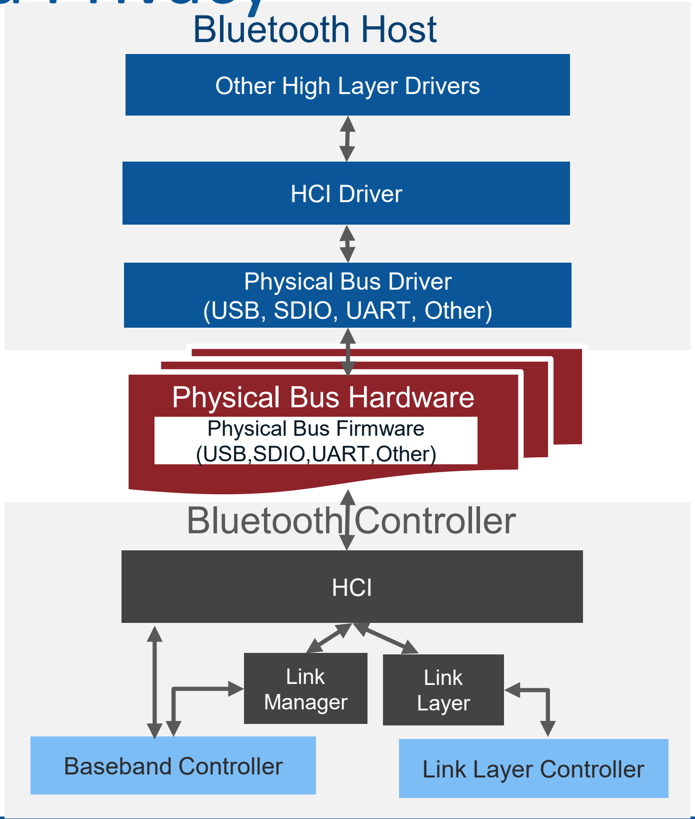
IRK: CDC45E17:0D6BFE12:D6DFF76F:3D10F04E

CDC45E17:0D6BFE12:D6DFF76F:3D10F04E

Looks like 3 devices are advertising, but with the IRK and a resolving list, the sniffer knows it's just one device

Host-based and Controller-based Privacy

- Two types of implementation choices
  - Just Host-based privacy
  - Host-based and Controller-based privacy
- When Controller-based privacy is supported
  - Address resolution can be done in the controller
  - Commands and events can refer to the peer device by identity address
  - The identity address can be used in the White List (which is not possible with Just host based privacy if the other side has Privacy enabled)



Two Modes of Privacy

- Device Privacy Mode
  - Only concerned about its own privacy
  - If the peer device has distributed its IRK

Resolvable Private Address	Accept
Identity Address	Accept

- Network Privacy Mode
  - Concerned about the privacy of the network
  - If the peer device has distributed its IRK

Resolvable Private Address	Accept
Identity Address	Reject

Device Privacy Mode

Network Privacy Mode

Summary

- Bluetooth Privacy Feature protects you from being tracked
  - Resolvable Private Address
  - Identity Resolving Key (IRK)
  - Identity Address
  - Resolving List
- Host-based and Controller-based Privacy
- Two modes of privacy
  - Device Privacy Mode
  - Network Privacy Mode

Thank you!

Questions?

Contact Information

Name:	Tim Wei
Email:	tim.wei@ellisys.com
Phone:	866.724.9185
Web:	www.ellisys.com