物聯網 BLE 認證機制設計的挑戰

以 Gogoro Smart Scooter 為例

GD、CSC

台灣科技大學 資管所

隱私與風險管理實驗室

講師介紹

G D

- 台灣科技大學 資管所 碩士生
- Team T5 CTO ~~(Chief Food Officer)~~
- CHROOT Member
- 曾任
  - 到處打零工
  - 好學生乖小孩
- 數位鑑識、事件處理、威脅情資整合
- 走在路上偶爾踢到一些漏洞
  去年 Synology 送我一台 NAS
  ~~希望 Gogoro 也能這麼 nice XD~~

CSC

- 台灣科技大學 資管所 副教授
- 夠麻吉股份有限公司 獨立董事
- 台灣大學 資訊管理 博士
- 曾任
  - 資誠企業管理顧問股份有限公司協理
  - 意藍科技股份有限公司資深顧問
- 具有 CISSP、CCFP、CSSLP、CISM 等多張國際資安認證。
- 近年來除了從事資安研究，發表多篇國際期刊與會議論文外，也曾協助多家政府單位與企業，建立資訊安全管理制度，或發掘系統資安漏洞。

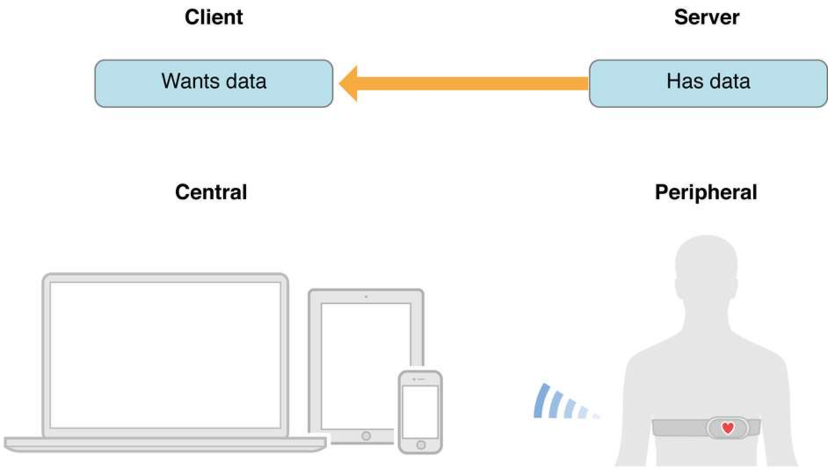
大綱

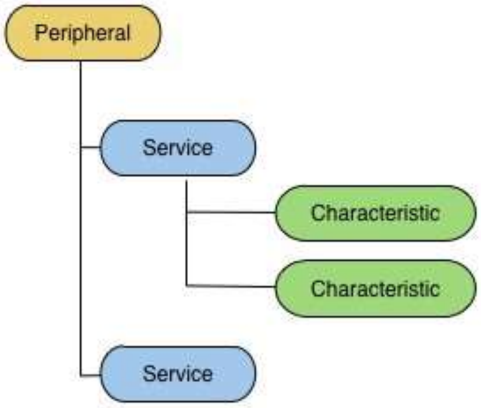
1. 介紹 Bluetooth Low Energy、安全性分析流程
2. Smartphone 透過 BLE 控制 IoT 裝置，需要一套認證機制
3. BLE 4.0 配對有許多限制，許多廠商選擇不配對另設計認證機制
4. 重視消費者隱私下，硬體識別元(Identifier)受限、亂數化
5. 未配對裝置無法取得硬體識別元，設計認證機制遇到的挑戰
6. 提出一種更好的認證機制：雙計數器強化認證

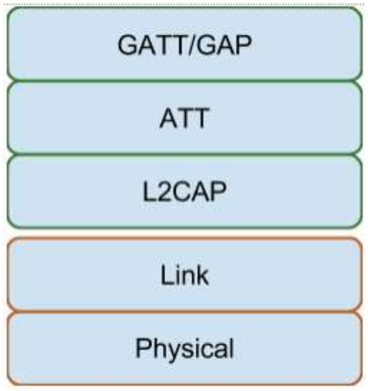
Bluetooth 4.0 有三種

High Speed	Classic	Low Energy
用 WiFi 傳資料	最常見的藍牙	原名 Wibree 協定
建立持續連線	可建立持續連線	不建立持續連線
高耗電	中耗電	低耗電
高頻寬	中頻寬	低頻寬
短距離	中距離	長距離
(我沒用過)	耳機、鍵盤、滑鼠	溫度計、手環、IoT 裝置

Bluetooth 4.0 Low Energy







類似 HTTP：session-less 並有七種 method

Method	方向	功能
Request	Central -> Peripheral	一般發送訊息
Response	Peripheral -> Central	回覆 Request 用
Commands	Central -> Peripheral	不用 Response
Notifications	Peripheral -> Central	不用 Confirm
Indications	Peripheral -> Central	需要 Confirm
Confirmations	Central -> Peripheral	回覆 Indication 用

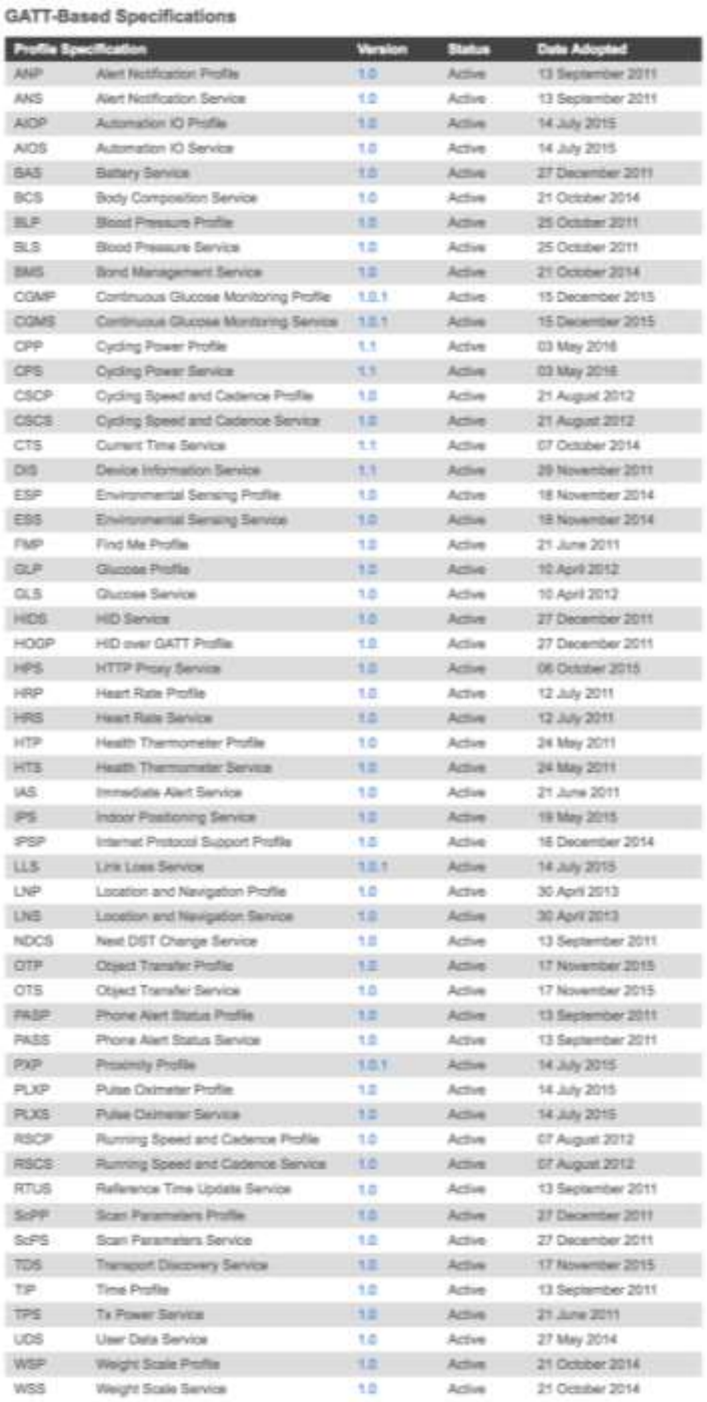
通常電量大的是 Client、電量小的是 Server (僅在收到 request 時供電運作) Fig. Ref: Stanfy Inc, 2015

BLE 廣泛應用在 IoT 健康家電產品

長輩有言「幹壞事是進步最大的原動力」
好奇手養「到底在傳輸什麼碗糕封包？」

內建許多 Profile

- 時間、溫度、電源
- 體重、用戶資料
- 血壓、血糖、體脂
- 心跳、脈搏、跑步
- 速度、方向、室內定位

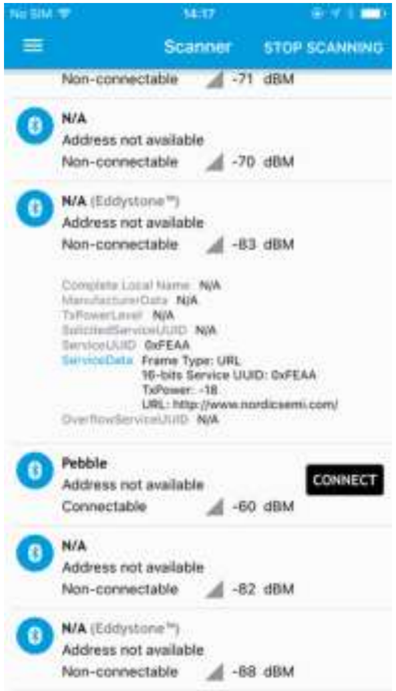


GATT-Based Specifications

Profile Specification		Version	Status	Date Adopted
ANP	Alert Notification Profile	1.0	Active	13 September 2011
ANS	Alert Notification Service	1.0	Active	13 September 2011
AIOP	Automation IO Profile	1.0	Active	14 July 2015
AIOS	Automation IO Service	1.0	Active	14 July 2015
BAS	Battery Service	1.0	Active	27 December 2011
BCS	Body Composition Service	1.0	Active	21 October 2014
BLP	Blood Pressure Profile	1.0	Active	25 October 2011
BLS	Blood Pressure Service	1.0	Active	25 October 2011
BMS	Bond Management Service	1.0	Active	21 October 2014
CGMP	Continuous Glucose Monitoring Profile	1.0.1	Active	15 December 2015
CGMS	Continuous Glucose Monitoring Service	1.0.1	Active	15 December 2015
CPP	Cycling Power Profile	1.1	Active	03 May 2016
CPS	Cycling Power Service	1.1	Active	03 May 2016
CSCP	Cycling Speed and Cadence Profile	1.0	Active	21 August 2012
CSCS	Cycling Speed and Cadence Service	1.0	Active	21 August 2012
CTS	Current Time Service	1.1	Active	07 October 2014
DIS	Device Information Service	1.1	Active	29 November 2011
ESP	Environmental Sensing Profile	1.0	Active	18 November 2014
ESS	Environmental Sensing Service	1.0	Active	18 November 2014
FMP	Find Me Profile	1.0	Active	21 June 2011
GLP	Glucose Profile	1.0	Active	10 April 2012
GLS	Glucose Service	1.0	Active	10 April 2012
HIDS	HID Service	1.0	Active	27 December 2011
HOGP	HID over GATT Profile	1.0	Active	27 December 2011
HPS	HTTP Proxy Service	1.0	Active	06 October 2015
HRP	Heart Rate Profile	1.0	Active	12 July 2011
HRS	Heart Rate Service	1.0	Active	12 July 2011
HTP	Health Thermometer Profile	1.0	Active	24 May 2011
HTS	Health Thermometer Service	1.0	Active	24 May 2011
IAS	Immediate Alert Service	1.0	Active	21 June 2011
IPS	Indoor Positioning Service	1.0	Active	19 May 2015
IPSP	Internet Protocol Support Profile	1.0	Active	16 December 2014
LLS	Link Loss Service	1.0.1	Active	14 July 2015
LNP	Location and Navigation Profile	1.0	Active	30 April 2013
LNS	Location and Navigation Service	1.0	Active	30 April 2013
NDCS	Next DST Change Service	1.0	Active	13 September 2011
OTP	Object Transfer Profile	1.0	Active	17 November 2015
OTS	Object Transfer Service	1.0	Active	17 November 2015
PASP	Phone Alert Status Profile	1.0	Active	13 September 2011
PASS	Phone Alert Status Service	1.0	Active	13 September 2011
PXP	Proximity Profile	1.0.1	Active	14 July 2015
PLXP	Pulse Oximeter Profile	1.0	Active	14 July 2015
PLXS	Pulse Oximeter Service	1.0	Active	14 July 2015
RSCP	Running Speed and Cadence Profile	1.0	Active	07 August 2012
RSCS	Running Speed and Cadence Service	1.0	Active	07 August 2012
RTUS	Reference Time Update Service	1.0	Active	13 September 2011
ScPP	Scan Parameters Profile	1.0	Active	27 December 2011
ScPS	Scan Parameters Service	1.0	Active	27 December 2011
TDS	Transport Discovery Service	1.0	Active	17 November 2015
TIP	Time Profile	1.0	Active	13 September 2011
TPS	Tx Power Service	1.0	Active	21 June 2011
UDS	User Data Service	1.0	Active	27 May 2014
WSP	Weight Scale Profile	1.0	Active	21 October 2014
WSS	Weight Scale Service	1.0	Active	21 October 2014

BLE 很容易玩

- Nordic nRF App



No SIM 14:17

Scanner STOP SCANNING

Non-connectable -71 dBM

N/A
Address not available
Non-connectable -70 dBM

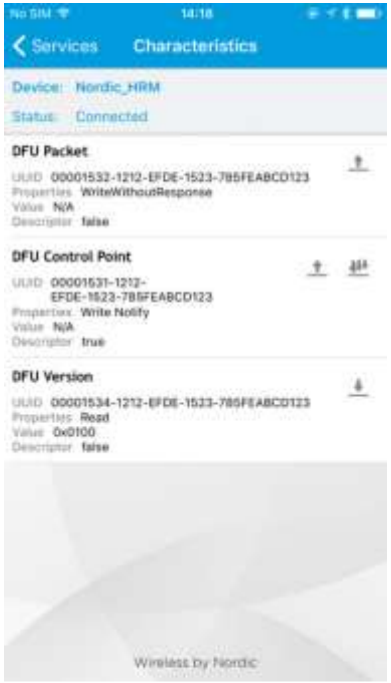
N/A (Eddystone™)
Address not available
Non-connectable -83 dBM

Complete Local Name N/A
ManufacturerData N/A
TxPowerLevel N/A
SolicitedServiceUUID N/A
ServiceUUID 0xFEAA
ServiceData Frame Type: URL
16-bits Service UUID: 0xFEAA
TxPower: -18
URL: http://www.nordicsemi.com/
OverflowServiceUUID N/A

Pebble
Address not available
Connectable -60 dBM
CONNECT

N/A
Address not available
Non-connectable -82 dBM

N/A (Eddystone™)
Address not available
Non-connectable -88 dBM



No SIM 14:18

Services Characteristics

Device: Nordic_HRM
Status: Connected

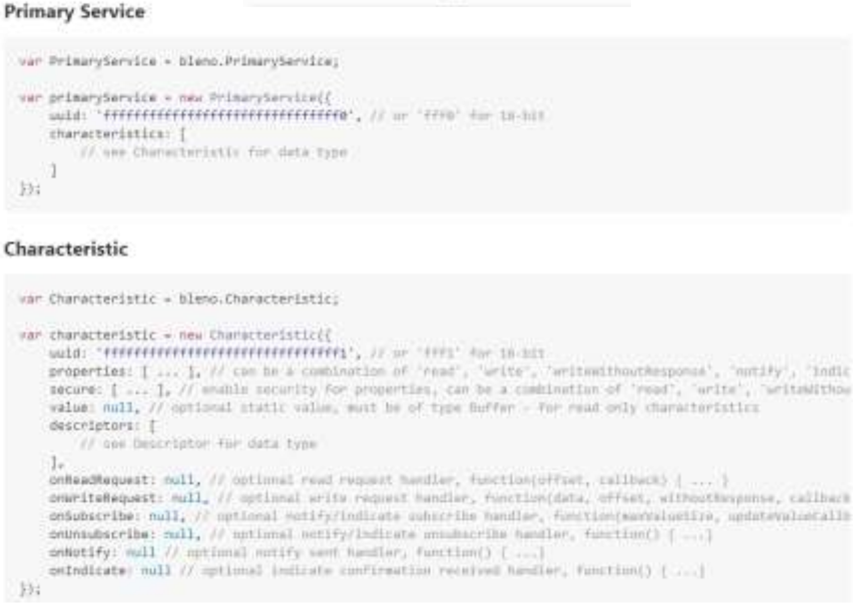
DFU Packet
UUID 00001532-1212-EFDE-1523-785FEABCD123
Properties WriteWithoutResponse
Value N/A
Descriptor false

DFU Control Point
UUID 00001531-1212-EFDE-1523-785FEABCD123
Properties Write Notify
Value N/A
Descriptor true

DFU Version
UUID 00001534-1212-EFDE-1523-785FEABCD123
Properties Read
Value 0x0100
Descriptor false

Wireless by Nordic

- bleno Node.js



Primary Service

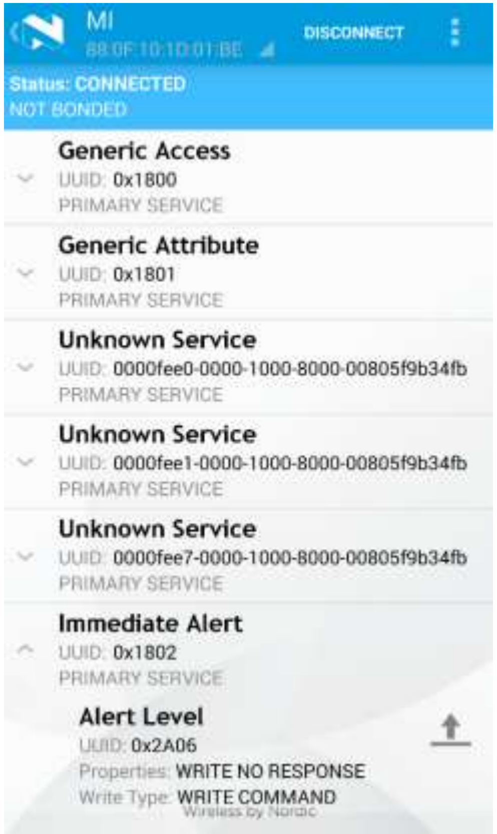
```
var PrimaryService = bleno.PrimaryService;

var primaryService = new PrimaryService({
    uuid: 'fffffffffffffffffffffffffffffff0', // or 'fff0' for 16-bit
    characteristics: [
        // see Characteristic for data type
    ]
});
```

Characteristic

```
var Characteristic = bleno.Characteristic;

var characteristic = new Characteristic({
    uuid: 'fffffffffffffffffffffffffffffff1', // or 'fff1' for 16-bit
    properties: [ ... ], // can be a combination of 'read', 'write', 'writeWithoutResponse', 'notify', 'indic
    secure: [ ... ], // enable security for properties, can be a combination of 'read', 'write', 'writeWithou
    value: null, // optional static value, must be of type Buffer - for read only characteristics
    descriptors: [
        // see Descriptor for data type
    ],
    onReadRequest: null, // optional read request handler, function(offset, callback) { ... }
    onWriteRequest: null, // optional write request handler, function(data, offset, withoutResponse, callback
    onSubscribe: null, // optional notify/indicate subscribe handler, function(maxValueSize, updateValueCallb
    onUnsubscribe: null, // optional notify/indicate unsubscribe handler, function() { ...}
    onNotify: null // optional notify sent handler, function() { ...}
    onIndicate: null // optional indicate confirmation received handler, function() { ...}
});
```

BLE 也很容易惡搞控制

- 在捷運上讓旁邊的小米手環一直震動



MI
88:0F:10:10:01:BE
DISCONNECT

Status: CONNECTED
NOT BONDED

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Unknown Service
UUID: 0000fee0-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

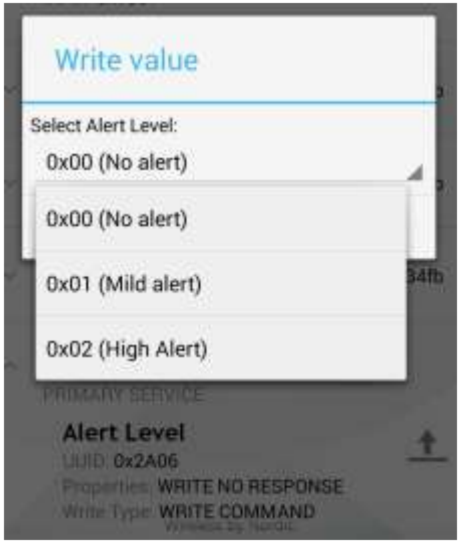
Unknown Service
UUID: 0000fee1-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Unknown Service
UUID: 0000fee7-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Immediate Alert
UUID: 0x1802
PRIMARY SERVICE

Alert Level
UUID: 0x2A06
Properties: WRITE NO RESPONSE
Write Type: WRITE COMMAND

Wireless by Nordic



Write value

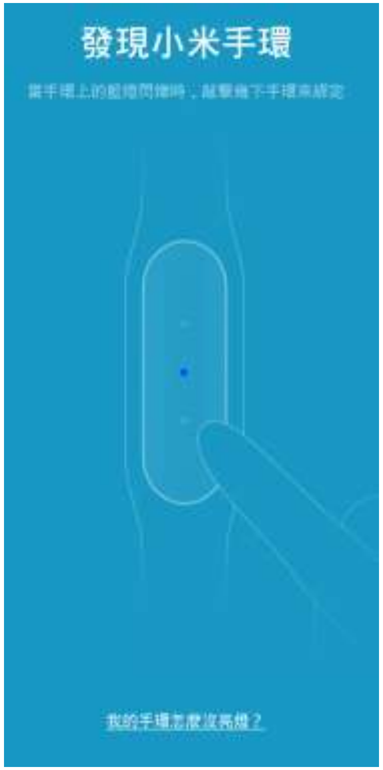
Select Alert Level:
0x00 (No alert)

0x00 (No alert)
0x01 (Mild alert)
0x02 (High Alert)

PRIMARY SERVICE

Alert Level
UUID: 0x2A06
Properties: WRITE NO RESPONSE
Write Type: WRITE COMMAND

Wireless by Nordic



發現小米手環

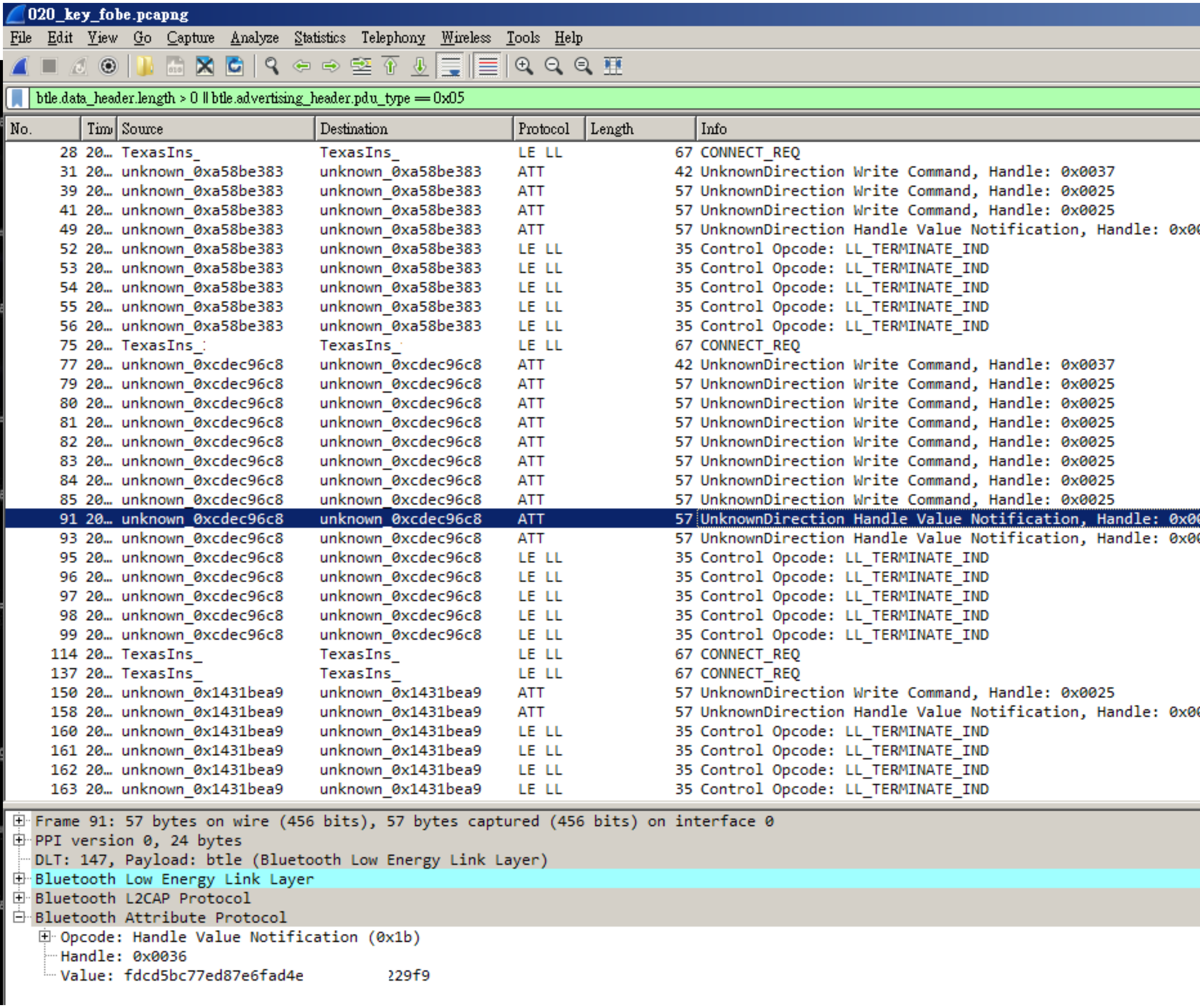
當手環上的藍燈閃爍時，敲擊幾下手環來綁定

我的手環怎麼沒亮燈？

Le IoT 想想物聯網 blog 有很不錯的教學

BLE Sniffer 錄封包 都是明文？！

```
CAP continua
56e delta_t=
CAP continua
81 delta_t=
    Channel Index: 17
    LLID: 1 / LL Data PDU / empty or L2CAP continua
    NESN: 0  SN: 1  MD: 0

    Data:
    CRC:   d1 00 65

systime=1441512979 freq=2440 addr=8d651b4d delta_t=
86 9e d1 00 65 92 86 01 5d 3e 0e 5e 65 e0 61 9a 7d
 c8 8f 67 02 f5 4f a7 f5
Data / AA 8d651b4d (valid) / 30 bytes
    Channel Index: 17
    LLID: 2 / LL Data PDU / L2CAP start
    NESN: 1  SN: 0  MD: 0

    Data:  d1 00 65 92 86 01 5d 3e 0e 5e 65 e0 61 9
f5 cc c8 8f 67 02 f5
    CRC:   4f a7 f5

systime=1441512979 freq=2440 addr=72f844df delta_t=
01 00 9b 72 68
Data / AA 72f844df (valid) /  0 bytes
    Channel Index: 17
    LLID: 1 / LL Data PDU / empty or L2CAP continua
    NESN: 0  SN: 0  MD: 0

    Data:
    CRC:   9b 72 68
```



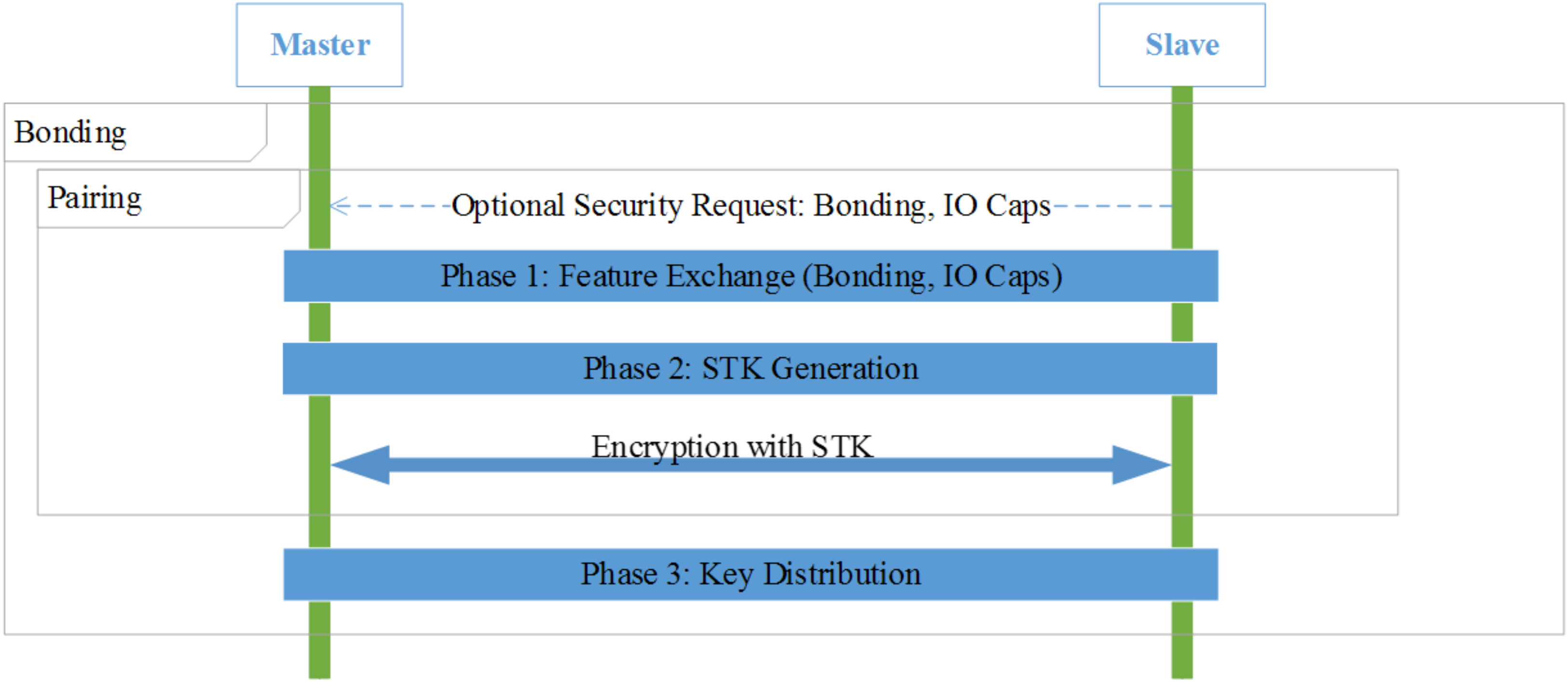
020_key_fobe.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
btle.data_header.length > 0 || btle.advertising_header.pdu_type == 0x05

No.  Tim Source              Destination         Protocol Length Info
  28 20… TexasIns_           TexasIns_           LE LL        67 CONNECT_REQ
  31 20… unknown_0xa58be383  unknown_0xa58be383  ATT          42 UnknownDirection Write Command, Handle: 0x0037
  39 20… unknown_0xa58be383  unknown_0xa58be383  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  41 20… unknown_0xa58be383  unknown_0xa58be383  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  49 20… unknown_0xa58be383  unknown_0xa58be383  ATT          57 UnknownDirection Handle Value Notification, Handle: 0x0
  52 20… unknown_0xa58be383  unknown_0xa58be383  LE LL        35 Control Opcode: LL_TERMINATE_IND
  53 20… unknown_0xa58be383  unknown_0xa58be383  LE LL        35 Control Opcode: LL_TERMINATE_IND
  54 20… unknown_0xa58be383  unknown_0xa58be383  LE LL        35 Control Opcode: LL_TERMINATE_IND
  55 20… unknown_0xa58be383  unknown_0xa58be383  LE LL        35 Control Opcode: LL_TERMINATE_IND
  56 20… unknown_0xa58be383  unknown_0xa58be383  LE LL        35 Control Opcode: LL_TERMINATE_IND
  75 20… TexasIns_           TexasIns_           LE LL        67 CONNECT_REQ
  77 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          42 UnknownDirection Write Command, Handle: 0x0037
  79 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  80 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  81 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  82 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  83 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  84 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  85 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Write Command, Handle: 0x0025
  91 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Handle Value Notification, Handle: 0x0
  93 20… unknown_0xcdec96c8  unknown_0xcdec96c8  ATT          57 UnknownDirection Handle Value Notification, Handle: 0x0
  95 20… unknown_0xcdec96c8  unknown_0xcdec96c8  LE LL        35 Control Opcode: LL_TERMINATE_IND
  96 20… unknown_0xcdec96c8  unknown_0xcdec96c8  LE LL        35 Control Opcode: LL_TERMINATE_IND
  97 20… unknown_0xcdec96c8  unknown_0xcdec96c8  LE LL        35 Control Opcode: LL_TERMINATE_IND
  98 20… unknown_0xcdec96c8  unknown_0xcdec96c8  LE LL        35 Control Opcode: LL_TERMINATE_IND
  99 20… unknown_0xcdec96c8  unknown_0xcdec96c8  LE LL        35 Control Opcode: LL_TERMINATE_IND
 114 20… TexasIns_           TexasIns_           LE LL        67 CONNECT_REQ
 137 20… TexasIns_           TexasIns_           LE LL        67 CONNECT_REQ
 150 20… unknown_0x1431bea9  unknown_0x1431bea9  ATT          57 UnknownDirection Write Command, Handle: 0x0025
 158 20… unknown_0x1431bea9  unknown_0x1431bea9  ATT          57 UnknownDirection Handle Value Notification, Handle: 0x0
 160 20… unknown_0x1431bea9  unknown_0x1431bea9  LE LL        35 Control Opcode: LL_TERMINATE_IND
 161 20… unknown_0x1431bea9  unknown_0x1431bea9  LE LL        35 Control Opcode: LL_TERMINATE_IND
 162 20… unknown_0x1431bea9  unknown_0x1431bea9  LE LL        35 Control Opcode: LL_TERMINATE_IND
 163 20… unknown_0x1431bea9  unknown_0x1431bea9  LE LL        35 Control Opcode: LL_TERMINATE_IND

⊞ Frame 91: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface 0
⊞ PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
⊞ Bluetooth Low Energy Link Layer
⊞ Bluetooth L2CAP Protocol
⊟ Bluetooth Attribute Protocol
    ⊞ Opcode: Handle Value Notification (0x1b)
      Handle: 0x0036
      Value: fdcd5bc77ed87e6fad4e        229f9
```

很多 IoT 裝置 BLE 其實沒有加密

Security Manager Protocol

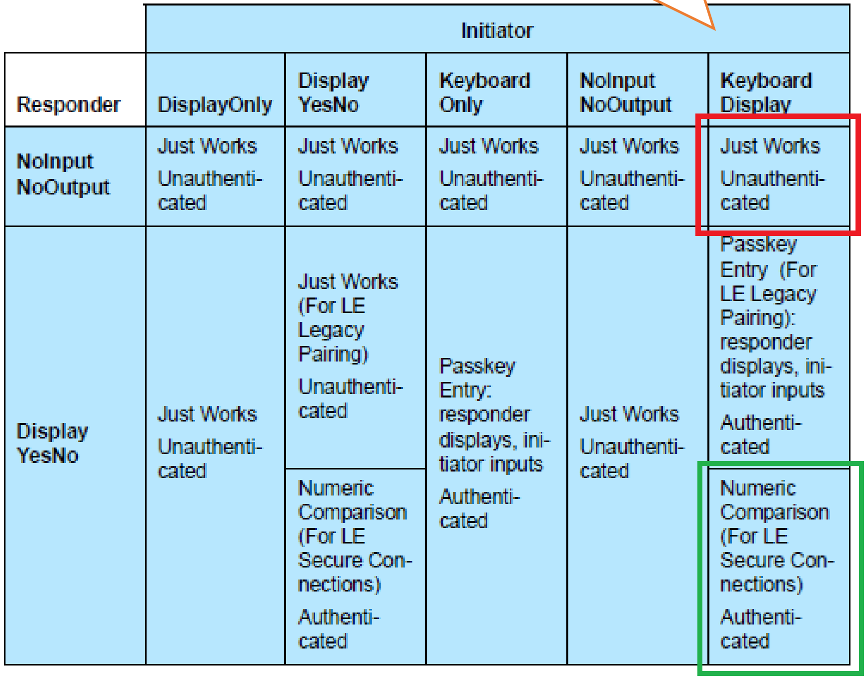
Pairing	Bonding	Re-establishment
Short Term Key	Permanent Key	Permanent Key


Master
Slave
Bonding
Pairing
Optional Security Request: Bonding, IO Caps
Phase 1: Feature Exchange (Bonding, IO Caps)
Phase 2: STK Generation
Encryption with STK
Phase 3: Key Distribution

BLE 4.0 SMP 配對方式

Pairing方法	MitM 攻擊難度	方便性
Just Works	沒有保護	最方便，但沒有辦法驗證裝置
Passkey Entry	簡單，暴力猜出PIN	一方要有螢幕、一方要有鍵盤
Out-Of-Band	困難，走獨立通道	用NFC 等其他方式交換key

Just Works 無法驗證裝置



	Initiator				
Responder	DisplayOnly	Display YesNo	Keyboard Only	NoInput NoOutput	Keyboard Display
NoInput NoOutput	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated	Just Works Unauthenticated
Display YesNo	Just Works Unauthenticated	Just Works (For LE Legacy Pairing) Unauthenticated Numeric Comparison (For LE Secure Connections) Authenticated	Passkey Entry: responder displays, initiator inputs Authenticated	Just Works Unauthenticated	Passkey Entry (For LE Legacy Pairing): responder displays, initiator inputs Authenticated Numeric Comparison (For LE Secure Connections) Authenticated

BLE 4.2 六位數字比對(需有螢幕)

許多廠商選擇不配對的原因：

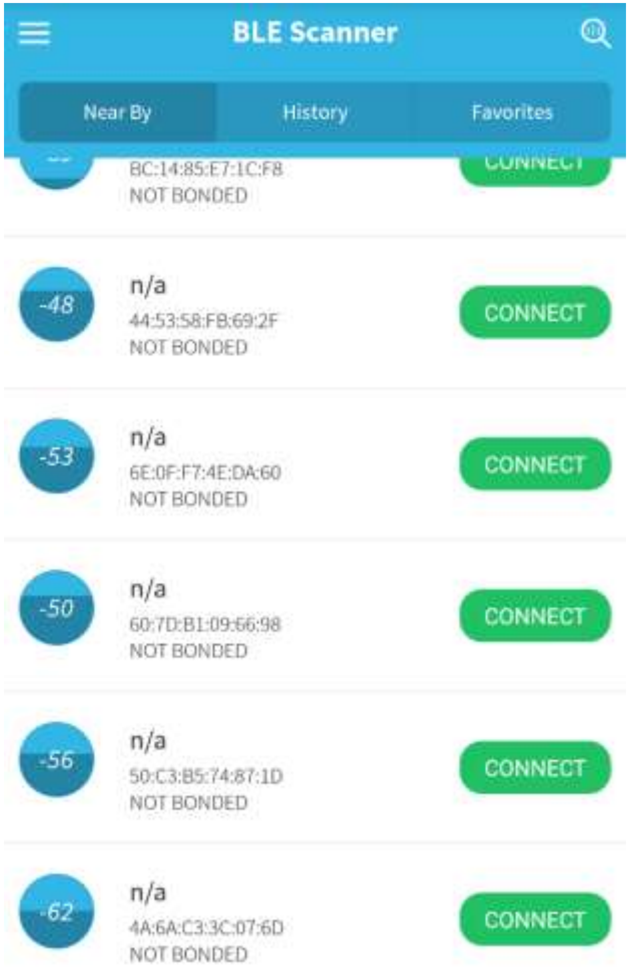
1. 使用前需要花費時間配對，不方便
2. 有已知安全弱點，配對不一定比較安全
3. 沒有螢幕顯示，則無法進行數字比對

BLE 4.0 隱私保護

- 硬體識別元 讀取限制
  - 防止 App 追蹤用戶
  - MAC Address 讀出來是 020000000000000

- 硬體識別元 亂數化
  - 防止附近設備掃描追蹤用戶
  - MAC Address 每次重開都不同
  - 配對過的裝置可用 IRK 解出固定 MAC

- 無硬體識別元，增加驗證機制設計的困難



BC:14:85:E7:1C:F8
NOT BONDED

-48
n/a
44:53:58:FB:69:2F
NOT BONDED

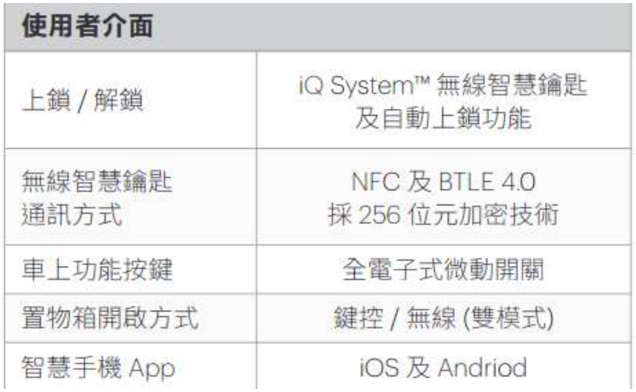
-53
n/a
6E:0F:F7:4E:DA:60
NOT BONDED

-50
n/a
60:7D:B1:09:66:98
NOT BONDED

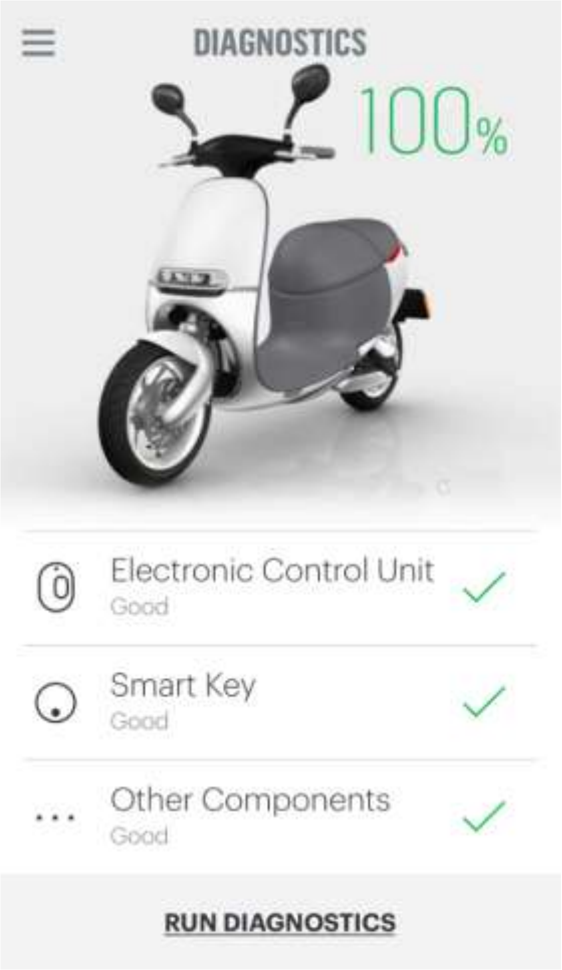
-56
n/a
50:C3:B5:74:87:1D
NOT BONDED

-62
n/a
4A:6A:C3:3C:07:6D
NOT BONDED

Gogoro Smart Scooter



使用者介面	
上鎖 / 解鎖	iQ System™ 無線智慧鑰匙 及自動上鎖功能
無線智慧鑰匙 通訊方式	NFC 及 BTLE 4.0 採 256 位元加密技術
車上功能按鍵	全電子式微動開關
置物箱開啟方式	鍵控 / 無線 (雙模式)
智慧手機 App	iOS 及 Andriod

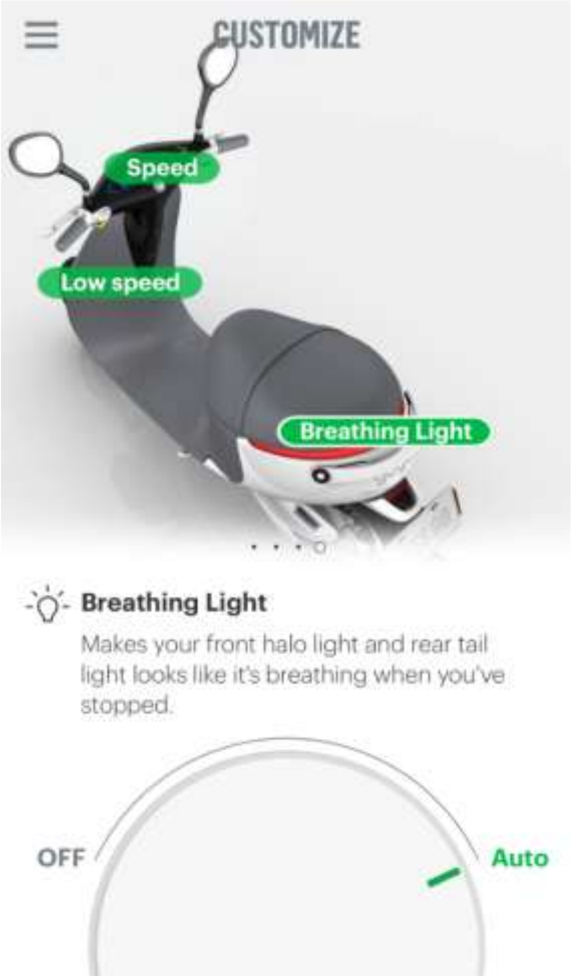


DIAGNOSTICS

100%

Electronic Control Unit Good	✓
Smart Key Good	✓
Other Components Good	✓

RUN DIAGNOSTICS



CUSTOMIZE

Breathing Light

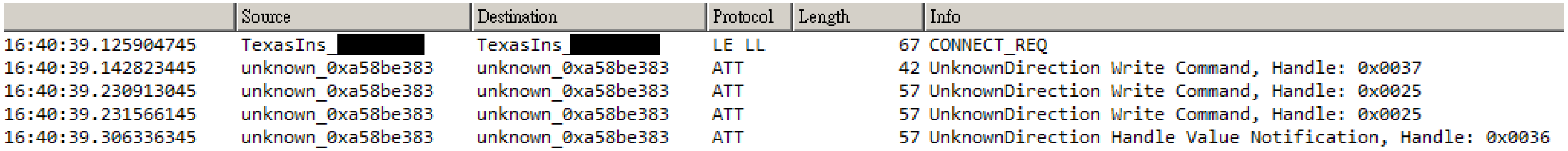
Makes your front halo light and rear tail light looks like it's breathing when you've stopped.

OFF

Auto

Key Fob Unlock (BLE)

(better than Keeloq)

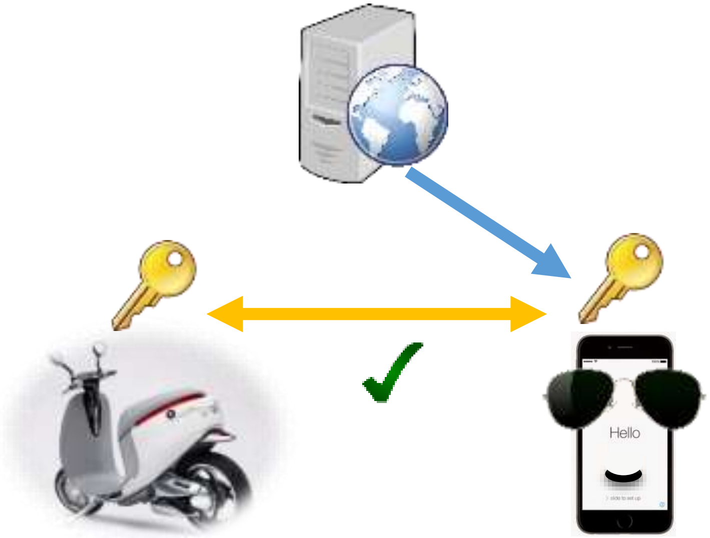


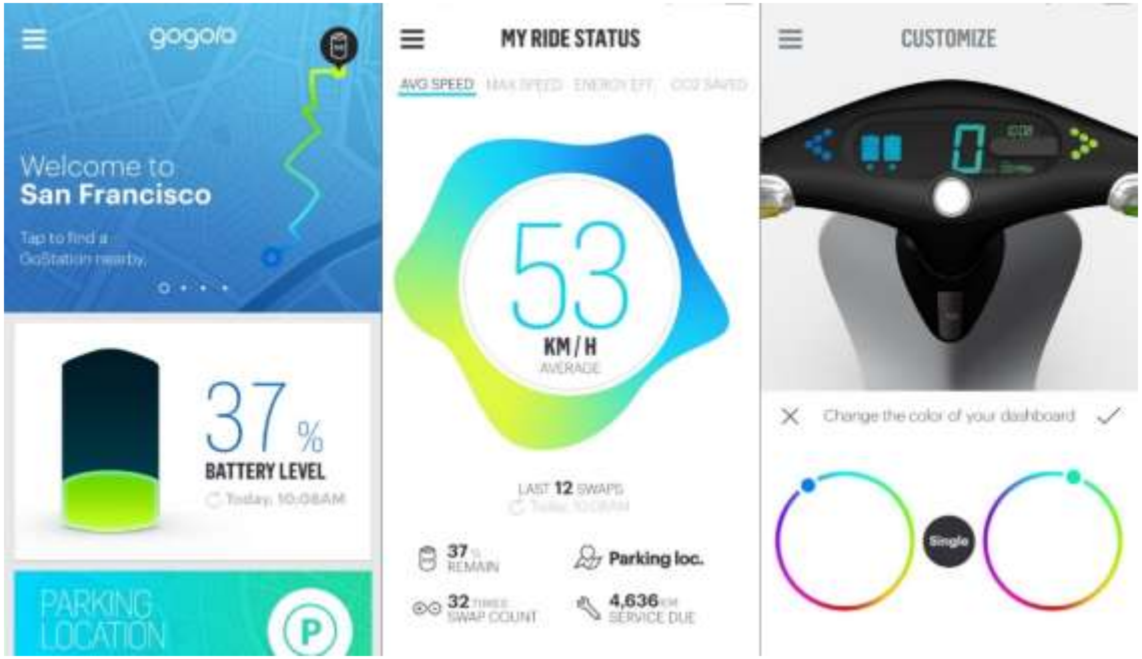
```
                    Source              Destination         Protocol  Length  Info
16:40:39.125904745  TexasIns_[redacted]  TexasIns_[redacted]  LE LL         67 CONNECT_REQ
16:40:39.142823445  unknown_0xa58be383  unknown_0xa58be383  ATT           42 UnknownDirection Write Command, Handle: 0x0037
16:40:39.230913045  unknown_0xa58be383  unknown_0xa58be383  ATT           57 UnknownDirection Write Command, Handle: 0x0025
16:40:39.231566145  unknown_0xa58be383  unknown_0xa58be383  ATT           57 UnknownDirection Write Command, Handle: 0x0025
16:40:39.306336345  unknown_0xa58be383  unknown_0xa58be383  ATT           57 UnknownDirection Handle Value Notification, Handle: 0x0036
```

Origin	Handle	Value	推測用途
鑰匙		CONNECT_REQ	開始連線
車子	0x37	01 00	Command ID
車子	0x25	c2 e7 20 bf d2 99 9d 43 68 c6 2d 65 39 3d 72 c9 f3	亂數Challenge
鑰匙	0x36	d2 25 57 33 19 18 51 fd ae 7d 1b ed 85 e0 10 78 e2	簽章Response
車子		LL_TERMINATE_IND	結束連線

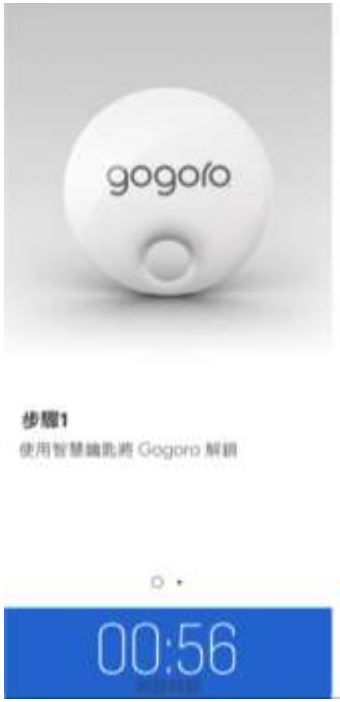
Mobile App (Gateway)

- 交車設定 My Gogoro 帳號
- App 登入下載 Scooter 資訊





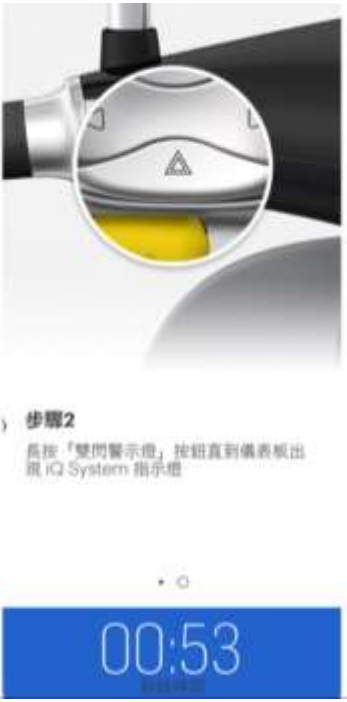
Mobile App Pairing & Unlock



步驟1

使用智慧鑰匙將 Gogoro 解鎖

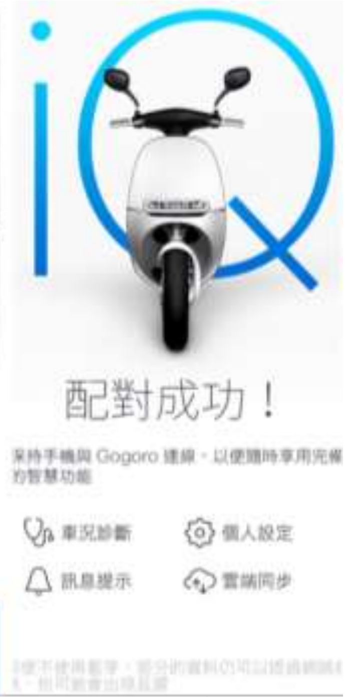
00:56



步驟2

長按「雙閃警示燈」按鈕直到儀表板出現 iQ System 指示燈

00:53



配對成功！

保持手機與 Gogoro 連線，以便隨時享用完備的智慧功能

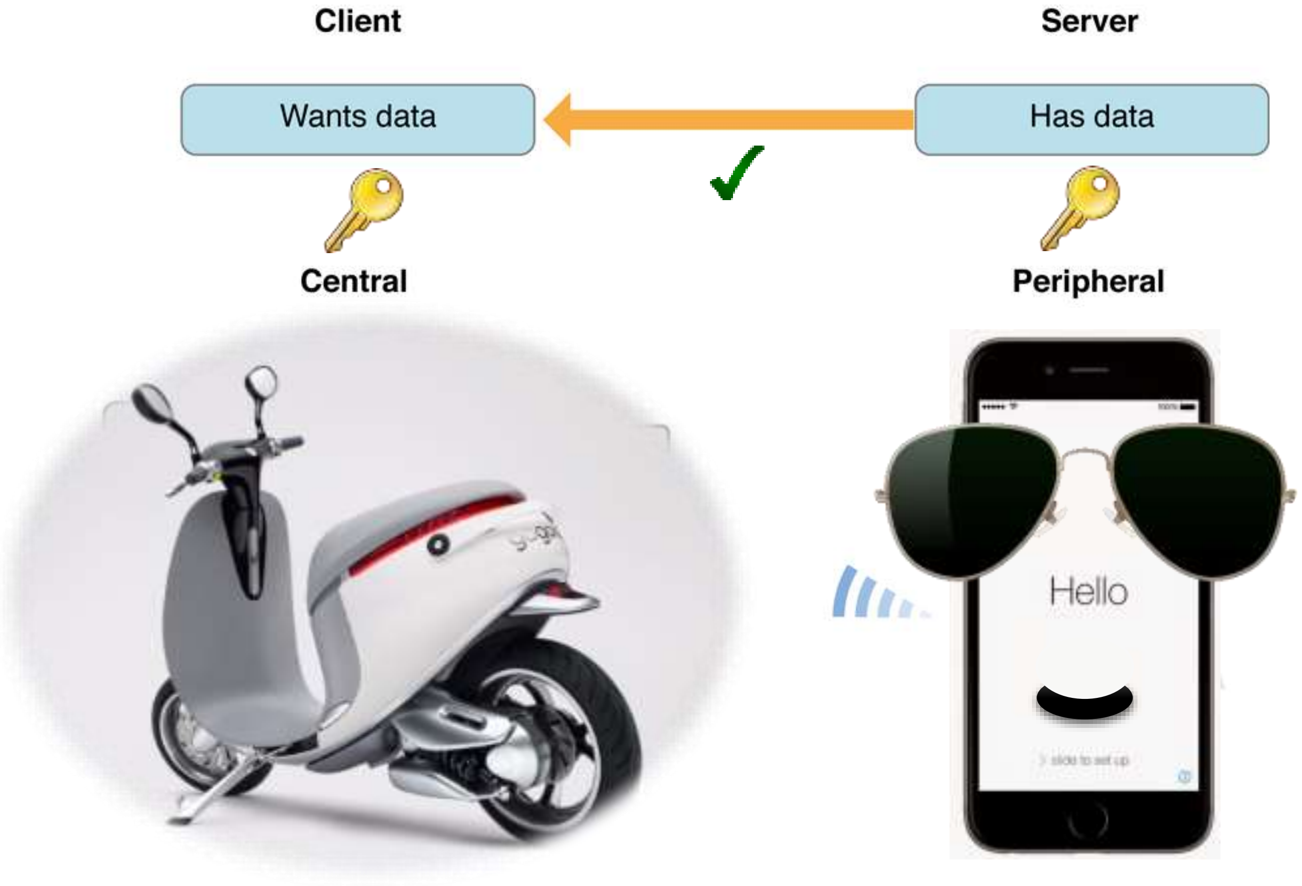
車況診斷　個人設定

訊息提示　雲端同步

僅 ATT 讀寫資訊、無 BLE 配對綁定

問題定義

- BLE 末配對，無硬體識別元，如何設計認證機制？



Client

Server

Wants data

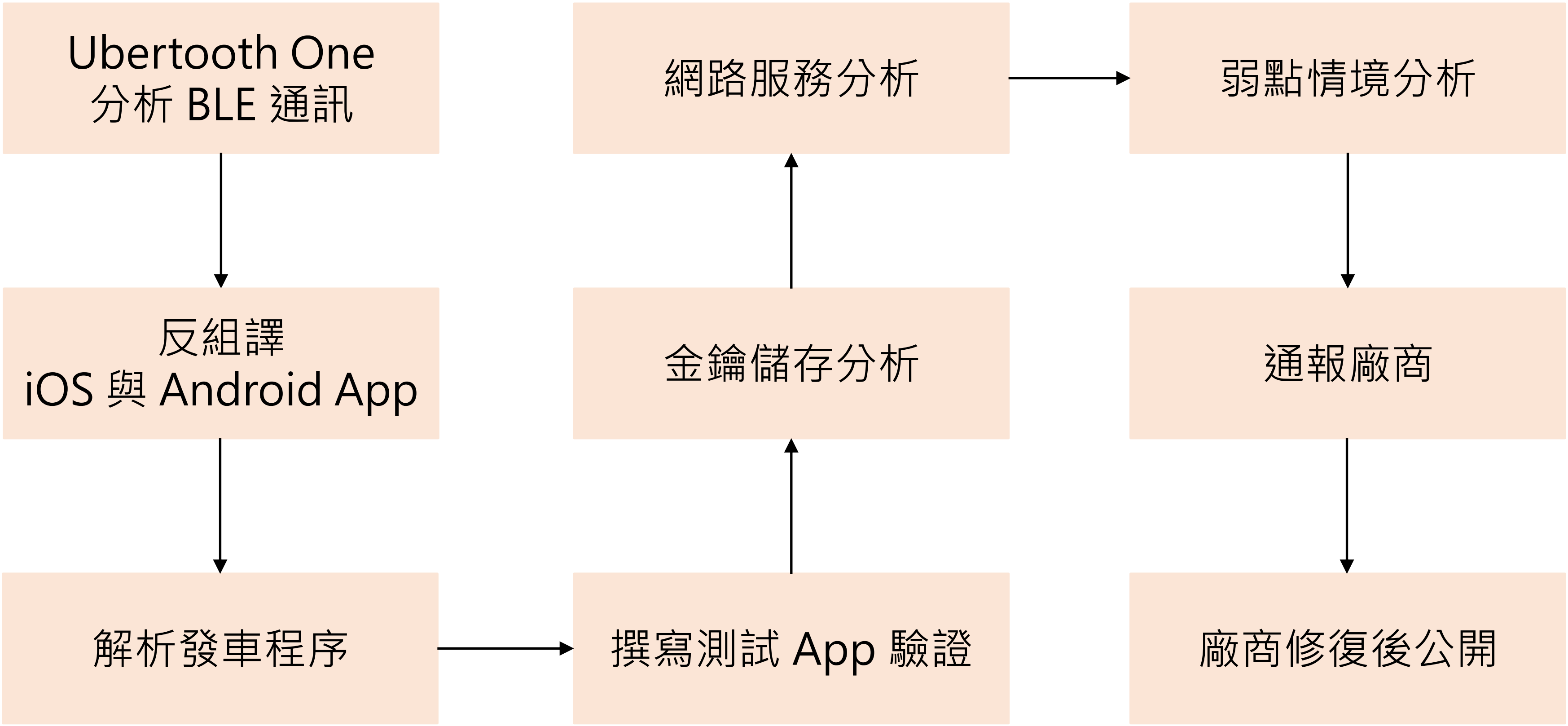
Has data

✓

Central

Peripheral

分析方法



Ubertooth One
分析 BLE 通訊

反組譯
iOS 與 Android App

解析發車程序

撰寫測試 App 驗證

金鑰儲存分析

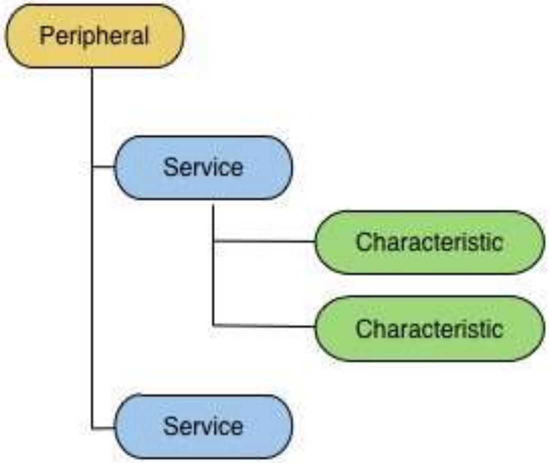
網路服務分析

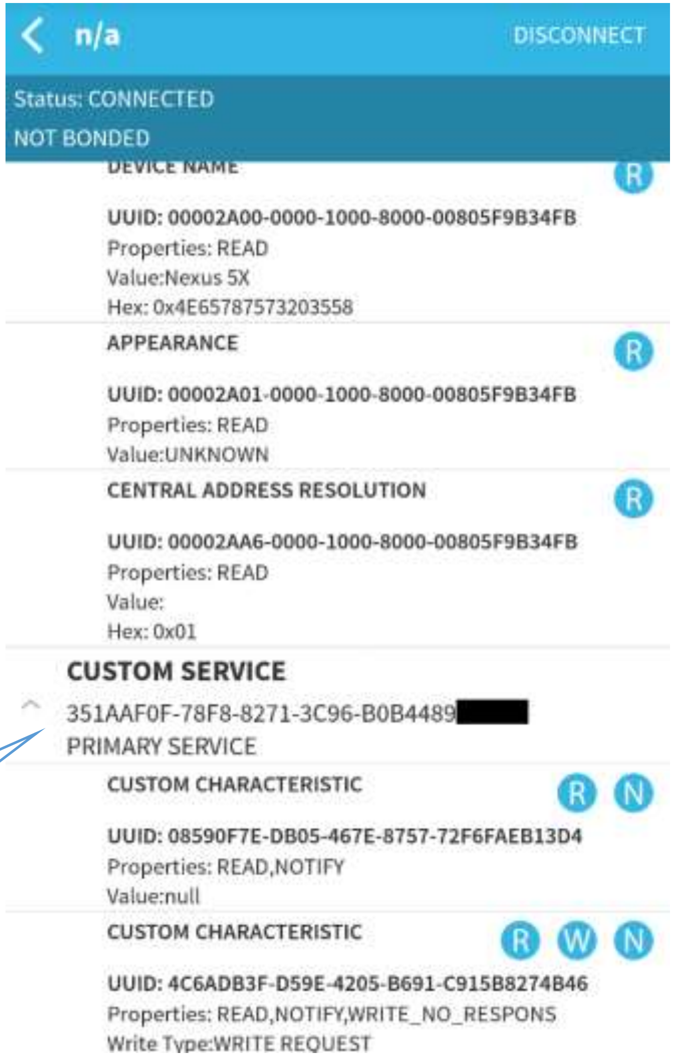
弱點情境分析

通報廠商

廠商修復後公開

BLE Gogoro Service





Status: CONNECTED
NOT BONDED

DEVICE NAME

UUID: 00002A00-0000-1000-8000-00805F9B34FB
Properties: READ
Value:Nexus 5X
Hex: 0x4E65787573203558

APPEARANCE

UUID: 00002A01-0000-1000-8000-00805F9B34FB
Properties: READ
Value:UNKNOWN

CENTRAL ADDRESS RESOLUTION

UUID: 00002AA6-0000-1000-8000-00805F9B34FB
Properties: READ
Value:
Hex: 0x01

CUSTOM SERVICE
351AAF0F-78F8-8271-3C96-B0B4489[redacted]
PRIMARY SERVICE

CUSTOM CHARACTERISTIC

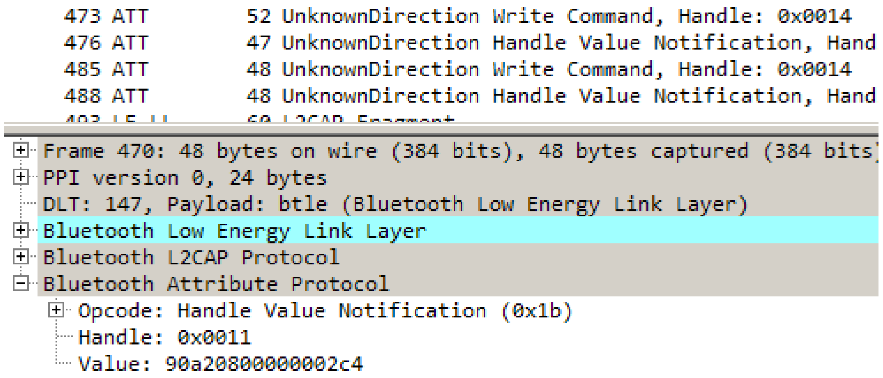
UUID: 08590F7E-DB05-467E-8757-72F6FAEB13D4
Properties: READ,NOTIFY
Value:null

CUSTOM CHARACTERISTIC

UUID: 4C6ADB3F-D59E-4205-B691-C915B8274B46
Properties: READ,NOTIFY,WRITE_NO_RESPONS
Write Type:WRITE REQUEST

Service UDID 末 8 byte
為 Scooter MAC Address

App Protocol 分析



```
   473 ATT          52 UnknownDirection Write Command, Handle: 0x0014
   476 ATT          47 UnknownDirection Handle Value Notification, Hand
   485 ATT          48 UnknownDirection Write Command, Handle: 0x0014
   488 ATT          48 UnknownDirection Handle Value Notification, Hand
   493 LE LL        60 L2CAP Fragment
⊞ Frame 470: 48 bytes on wire (384 bits), 48 bytes captured (384 bits
⊞ PPI version 0, 24 bytes
  DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
⊞ Bluetooth Low Energy Link Layer
⊞ Bluetooth L2CAP Protocol
⊟ Bluetooth Attribute Protocol
   ⊞ Opcode: Handle Value Notification (0x1b)
     Handle: 0x0011
     Value: 90a20800000002c4
```

90 **A2** 08 00 00 00 **02** C4 (hex)
90: Header, **A2**: Command, 08: Length,
02: Parameter, C4: Checksum

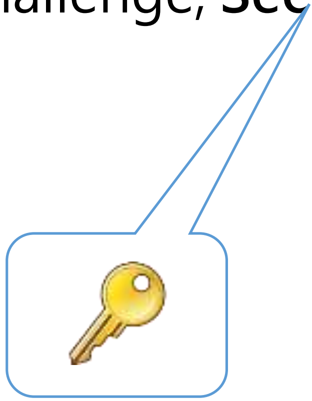
A開頭 一般資訊查詢

Origin	Cmd	Function
App	A0	GetScooterSettingWithType
App	A1	GetScooterErrors
App	A2	GetScooterInfo
App	A3	SetScooterSetting
Scooter	A4	ScooterGetSettingStatus
Scooter	A5	ScooterErrorStatus
Scooter	A6	ScooterInfoState
Scooter	A7	ScooterSetSettingStatus
Scooter	A8	NotifyScooterError
Scooter	A9	NotifyInfo
Scooter	AE	PurchasedStatus
Scooter	AF	ScooterInfoState
Scooter	B0	ECU Challenge nonce
App	B1	ECU Response digest
Scooter	B2	ECU unknown
Scooter	B3	ECU Error
App	B4	ECU Cmd (Lock, Unlock, Open Trunk)

B開頭 ECU Challenge Response

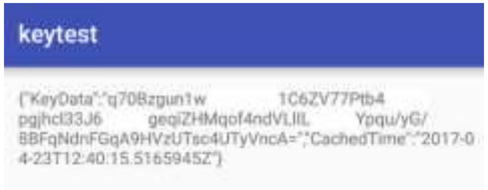
Gogoro Unlock 流程

1. Scooter 掃描附近Peripheral 是否有 GATT Gogoro 服務
UUID 351AAF0F-末8 byte 同Scooter MAC Address才連上
2. Mobile App 讀取 Scooter 目前狀態，啟用解鎖按鈕
按下按鈕後送出 ECU_Cmd(0xB4) Value 上鎖0x00、解鎖0x01
3. Scooter 發出 ECU_Challenge (0xB0)
隨機產生的亂數 256 bit nonce
4. Mobile App 回覆 ECU_Response (0xB1)
ECU_Response =SHA256(ECU_Challenge, **Security_Key**)
5. Scooter 比對 ECU_Response 無誤
執行 ECU_Cmd 完成解鎖通電。



車鑰匙 Security_Key

- ECU_Response =SHA256(ECU_Challenge, **Security_Key**)
- 早期版本 Security_Key 就放在 Document 目錄下(有稍微加密)
  - iOS MobileAppProp.plist 中 ScooterSKey
  - Android Settings.xml 中 AppSettings_DefScooter/encryptedkey2
  - 解密方式法 AES-256, CBC/PKCS7Padding, IV=UserId, Key = ScooterUUID
- iTunes 或 Android 備份程式預設會拷走
  - 插上傳輸線 Juicy Attack、從 PC iTunes 備份、各種方式
  - AndroidManifest.xml 中 allowBackup 目前是 true
- 從 WebAPI 取得
  - Try 出 My Gogoro 密碼（帳單、論壇、App）
  - 偷出 Cookie (Web_Token 也存在 MobileAppProp.plist)
  - https://mobile-pro.gogoroapp.com/WebService/Web/GetKey



```
{"KeyData":"q70Bzgun1w          1C6ZV77Ptb4
pgjhcl33J6       geqiZHMqof4ndVLIIL       Ypqu/yG/
8BFqNdnFGqA9HVzUTsc4UTyVncA=","CachedTime":"2017-0
4-23T12:40:15.5165945Z"}
```

Insecure App Data Storage

- Token, Certificate 應該放在加密儲存區
  - 未使用中 是加密狀態、使用中 管制 Timeout
  - 限制 user、限制 process、限制 export

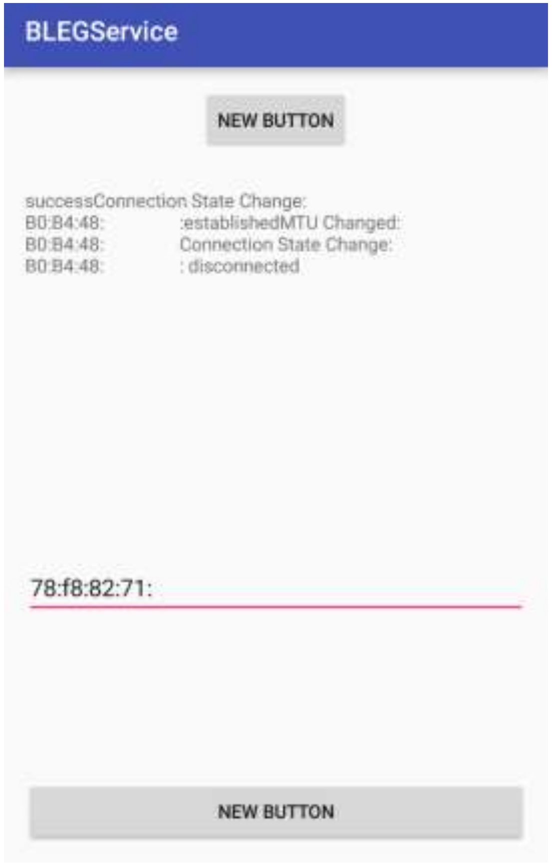
- 各大作業系統都有提供
  - Apple iOS/macOS Keychain
    - iPhone 6~ Secure Enclave
  - Android Keystore
    - Samsung S6~ KNOX
  - Windows Protected Storage
    - HSM Such as UbiKey

Unlock 模擬程式

- 依照上述分析結果，我們撰寫 Android App 可 Unlock 已知 Security_Key 的 Scooter
- Live Demo

因此得知：

1. 攻擊者只要取得 Security_Key 就可把車發動
2. Security_Key 可被轉移到其他手機使用
3. Scooter 無法驗證Mobile App 硬體識別元



```
successConnection State Change:
B0:B4:48:            :establishedMTU Changed:
B0:B4:48:            Connection State Change:
B0:B4:48:            : disconnected
```

78:f8:82:71:

Gogoro 分析結果

- 裝置識別元 隱私保護 → 提高驗證設計難度
    - 實驗證明，IoT 裝置在無法驗證裝置識別元下，只能依靠金鑰
    - 保護好 Security_Key 是唯一方法
- Insecure App Data Storage 弱點
    - Gogoro Mobile App 把 Security_Key 存在 Document 目錄
    - 應存到加密儲存區 Keychain/Keystore ，可避免備份外流
- 其他可能威脅
    - 取 Security_Key API 沒有 SSL Cert Pining 可能被中間人攻擊
    - Challenge-Response 可能被Rely-Attack (類似車用遙控器)

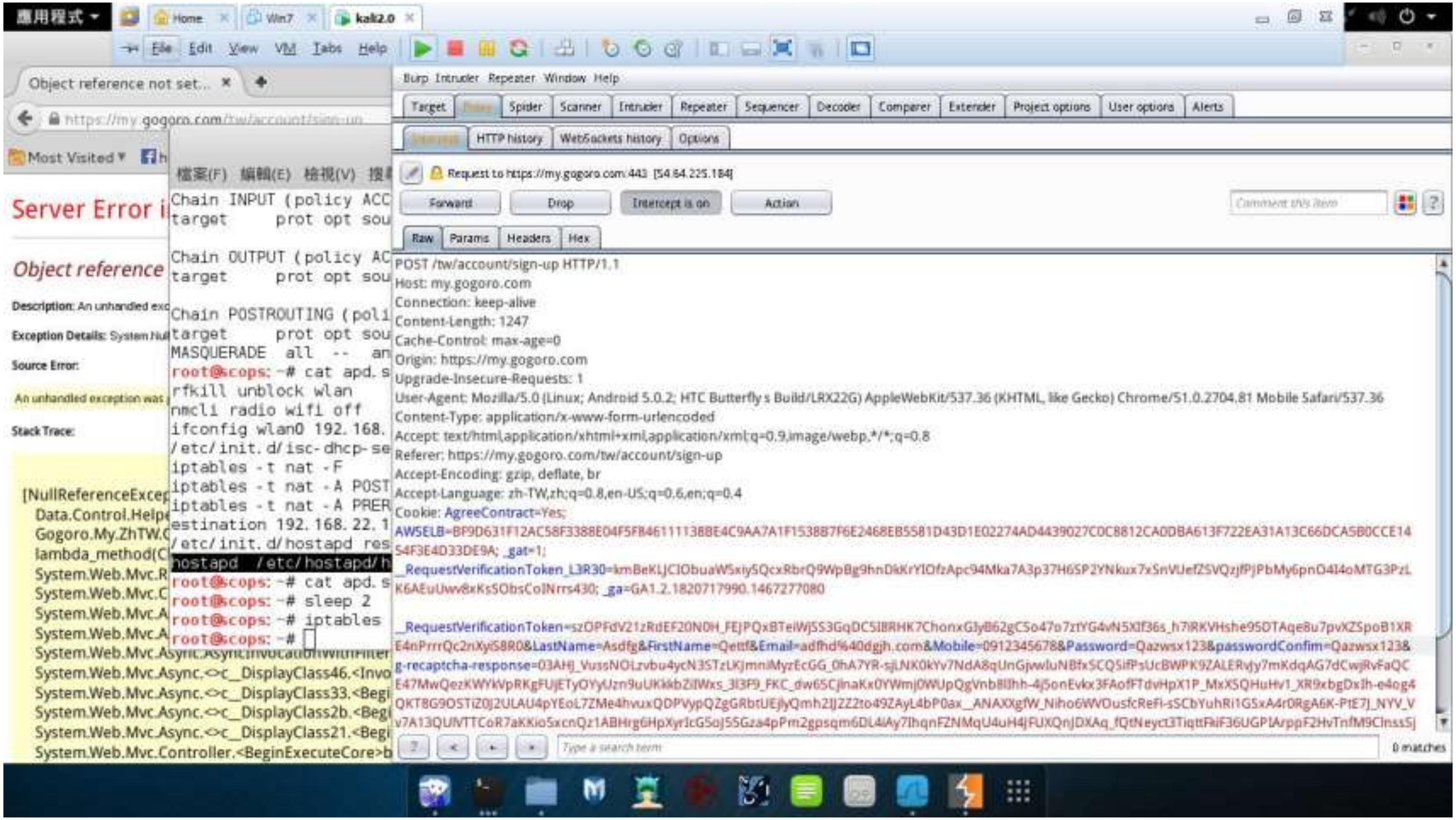
大體來說 Gogoro 系統設計是安全的

- 藍牙傳輸雖然沒有配對與加密，但是傳輸的是一次性的 Challenge/ Response
- 在手機端，金鑰基本上是綁手機，除非手機有自己做破解，而且被安裝後門程式，不然不易直接從手機取得金鑰 Security Key
- 但從網路中取得金鑰資訊這段，目前沒有綁憑證 cert pining，也沒有 MyGogoro 帳號 username/password 以外認證機制

威脅情境

- 使用者手機被植入木馬、電腦備份檔被偷走
- 使用者在不安全的網路環境中啟動手機 App 並登入 Gogoro 系統
    - 可以利用中間人攻擊取得 Key
- 使用 BLE 掃描取得服務的 UUID

- 接下來就可以到使用者的車子旁邊，送出解鎖指令並回應 Challenge，然後就可以發車了


應用程式
Home
Win7
kali2.0
File Edit View VM Tabs Help
Object reference not set...
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches
Most Visited
檔案(F) 編輯(E) 檢視(V) 搜

https://my.gogoro.com/tw/account/sign-up

Server Error i

Object reference

Description: An unhandled exc

Exception Details: System.Nul

Source Error:

An unhandled exception was

Stack Trace:

```
[NullReferenceExcep
   Data.Control.Helpe
   Gogoro.My.ZhTW.C
   lambda_method(C
   System.Web.Mvc.R
   System.Web.Mvc.C
   System.Web.Mvc.A
   System.Web.Mvc.A
   System.Web.Mvc.Async.AsyncInvocationWithFilter
   System.Web.Mvc.Async.<>c__DisplayClass46.<Invo
   System.Web.Mvc.Async.<>c__DisplayClass33.<Begi
   System.Web.Mvc.Async.<>c__DisplayClass2b.<Begi
   System.Web.Mvc.Async.<>c__DisplayClass21.<Begi
   System.Web.Mvc.Controller.<BeginExecuteCore>b
```

```
Chain INPUT (policy ACC
target     prot opt sou

Chain OUTPUT (policy AC
target     prot opt sou

Chain POSTROUTING (poli
target     prot opt sou
MASQUERADE  all  --  an
root@scops:~# cat apd.s
rfkill unblock wlan
nmcli radio wifi off
ifconfig wlan0 192.168.
/etc/init.d/isc-dhcp-se
iptables -t nat -F
iptables -t nat -A POST
iptables -t nat -A PRER
estination 192.168.22.1
/etc/init.d/hostapd res
hostapd  /etc/hostapd/h
root@scops:~# cat apd.s
root@scops:~# sleep 2
root@scops:~# iptables
root@scops:~# 
```

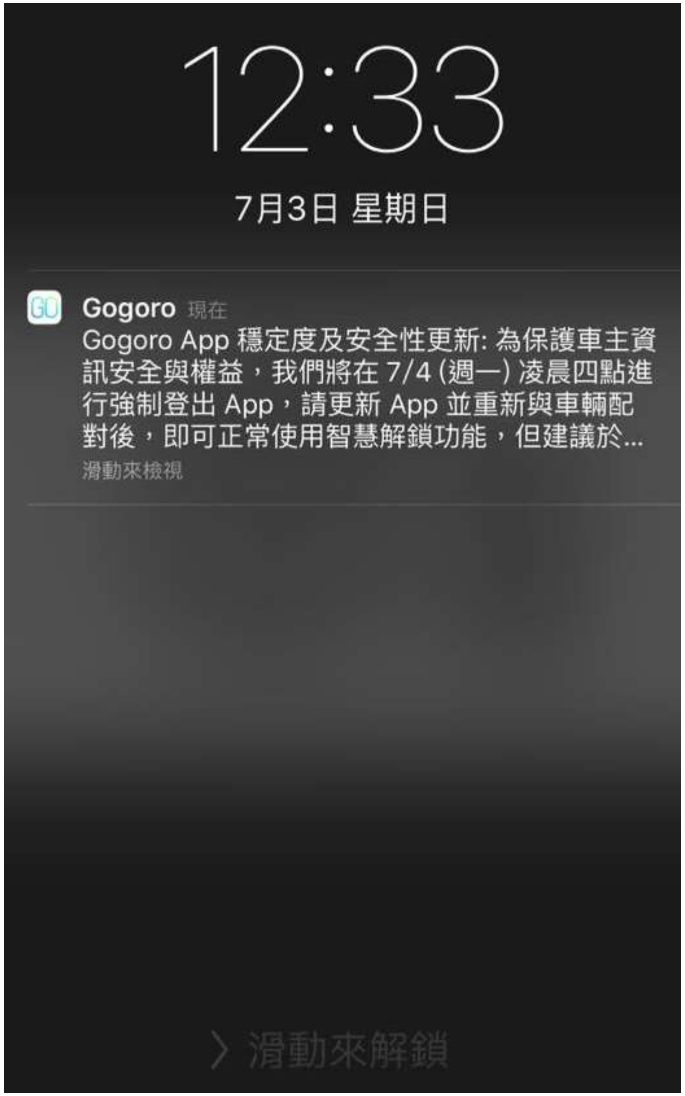
Request to https://my.gogoro.com:443 [54.64.225.184]

```
POST /tw/account/sign-up HTTP/1.1
Host: my.gogoro.com
Connection: keep-alive
Content-Length: 1247
Cache-Control: max-age=0
Origin: https://my.gogoro.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 5.0.2; HTC Butterfly s Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.81 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://my.gogoro.com/tw/account/sign-up
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: AgreeContract=Yes;
AWSELB=BF9D631F12AC58F3388E04F5F84611113BBE4C9AA7A1F153887F6E2468EB5581D43D1E02274AD4439027C0C8812CA0DBA613F722EA31A13C66DCA5B0CCE14
54F3E4D33DE9A; _gat=1;
__RequestVerificationToken_L3R30=kmBeKLJCIObuaW5xiy5QcxRbrQ9WpBg9hnDkKrYIOfzApc94Mka7A3p37H6SP2YNkux7xSnVUefZSVQzjfPjPbMy6pnO4I4oMTG3PzL
K6AEuUwv8xKsSObsCoINrrs430; _ga=GA1.2.1820717990.1467277080

__RequestVerificationToken=szOPFdV21zRdEF20N0H_FEJPQxBTeiWjSS3GqDC5I8RHK7ChonxGJyB62gC5o47o7ztYG4vN5XIf36s_h7iRKVHshe95DTAqe8u7pvXZSpoB1XR
E4nPrrrQc2nXyiS8R0&LastName=Asdfg&FirstName=Qettf&Email=adfhd%40dgjh.com&Mobile=0912345678&Password=Qazwsx123&passwordConfim=Qazwsx123&
g-recaptcha-response=03AHJ_VussNOLzvbu4ycN3STzLKjmniMyzEcGG_0hA7YR-sjLNK0kYv7NdA8qUnGjwwIuNBfxSCQSifPsUcBWPK9ZALERvjy7mKdqAG7dCwjRvFaQC
E47MwQezKWYkVpRKgFUjETyOYyUzn9uUKkkbZiIWxs_3I3F9_FKC_dw65CjlnaKx0YWmj0WUpQgVnb8Ihh-4j5onEvkx3FAofFTdvHpX1P_MxXSQHuHv1_XR9xbgDxIh-e4og4
QKT8G9OSTiZ0J2ULAU4pYEoL7ZMe4hvuxQDPVypQZgGRbtUEjlyQmh2JJ2Z2to49ZAyL4bP0ax__ANAXXgfW_Niho6WVOusfcRefi-sSCbYuhRi1G5xA4r0RgA6K-PtE7J_NYV_V
v7A13QUNTTCoR7aKKio5xcnQz1ABHrg6HpXyrIcG5oJ55Gza4pPm2gpsqm6DL4iAy7IhqnFZNMqU4uH4JFUXQnJDXAq_fQtNeyct3TiqttFkiF36UGPIArppF2HvTnfM9CInssSj
```

弱點通報廠商

- 2016/02 App 開始支援 BLE 解鎖
- 2016/04 發現弱點並通報廠商
- 2016/04 增強 Security Key 保護
- 2016/07 增強 SSL Cert 驗證
- 2016/07 強制登出更新

We will keep investing on security area and have more frequently release for security improvement in the future.



12:33

7月3日 星期日

Gogoro 現在

Gogoro App 穩定度及安全性更新: 為保護車主資訊安全與權益，我們將在 7/4 (週一) 凌晨四點進行強制登出 App，請更新 App 並重新與車輛配對後，即可正常使用智慧解鎖功能，但建議於...

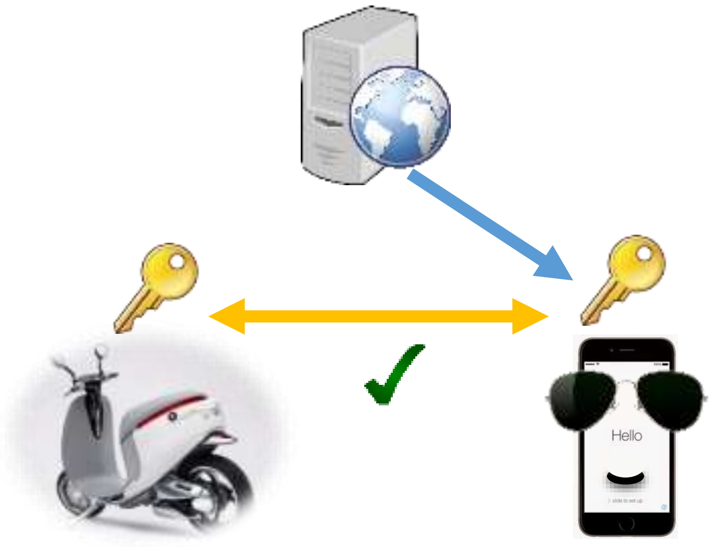
滑動來檢視

〉滑動來解鎖

IoT 裝置認證設計的挑戰

- 無法讀取裝置識別元
  - IoT 裝置事先不認識手機
  - IoT 裝置事先　認識金鑰
  - 藉由 Server 把金鑰給手機

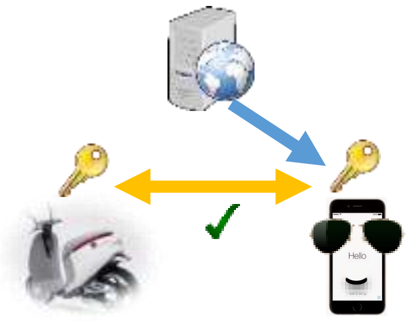
- 防止金鑰被複製？
  - BLE 4.2 Secure Connections
  - 金鑰 + 手機裝置識別元
  - 金鑰 Secure Element 儲存
  - 金鑰 + SMS OTP
  - 金鑰 + Dual HOTP 認證



認證機制 解法比較

認證方法	優點	缺點
金鑰 Server Provision	IoT裝置不需事先認識手機	金鑰複製容易、盜用察覺難
BLE 4.2 Secure Connections	防MITM、傳輸加密、防複製	雙方都需要數字顯示螢幕
金鑰 + 手機裝置識別元	可驗證手機、防止複製	隱私衝突、Root還是可拷
金鑰 Secure Element 儲存	加密保護、拷出困難	不是每隻手機都有 SE
金鑰 + Server SMS OTP 發送	綁門號、不用綁定手機	SMS要錢、需要電信門號 IoT 裝置需跟 Server 同步
金鑰 + 雙計數器強化認證	綁定手機、可察覺金鑰盜用	未必能阻擋金鑰盜用

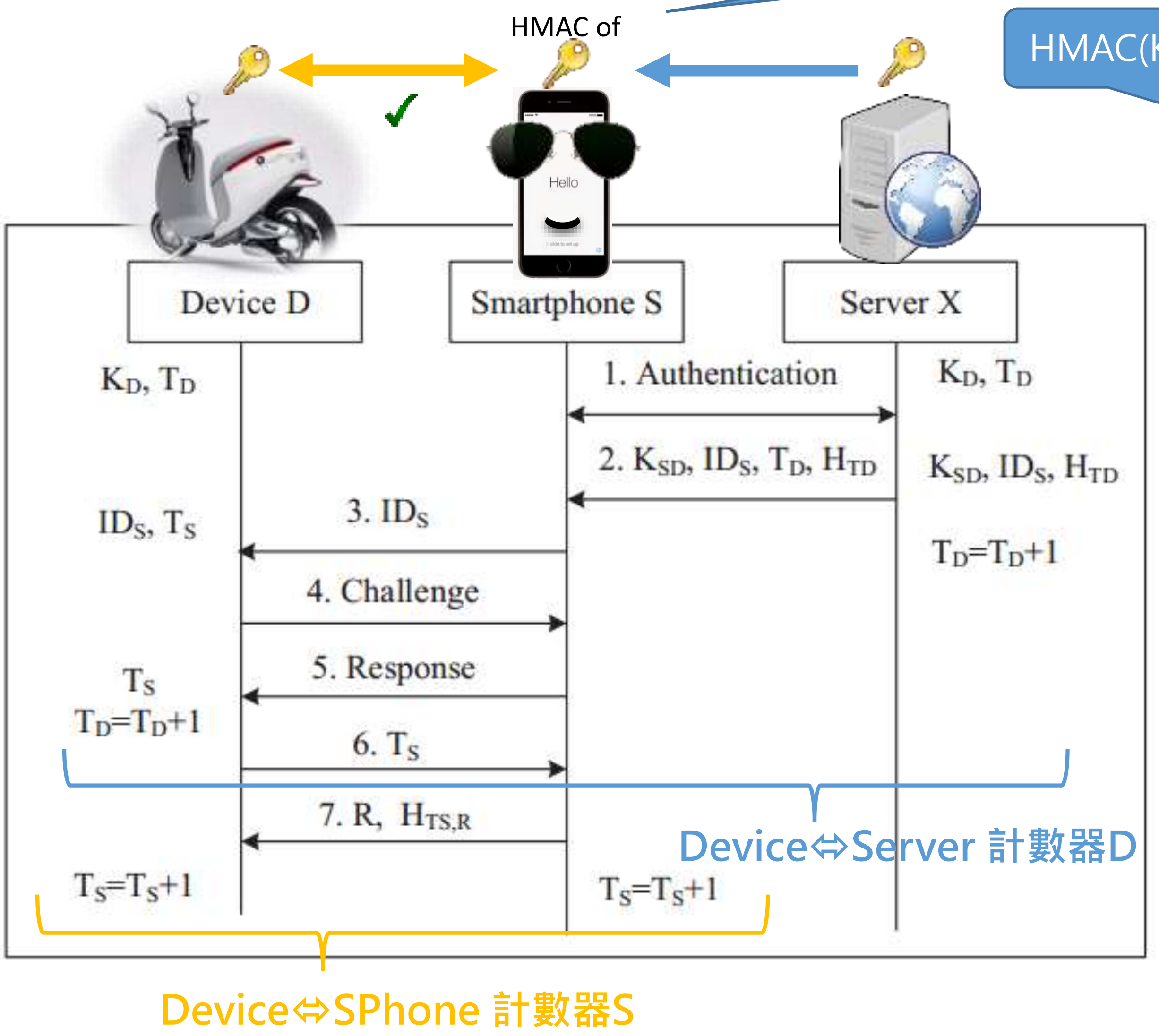
勝



雙計數器強化認證

若手機遺失可 revoke HMAC(Key)

HMAC(Key) 被偷用會 desync計數器



Device⇔Server

K_D 永久共有金鑰

T_D 計數器D

ID_S 身分證

K_{SD} HMAC(K_D, ID_S) 臨時

H_{TD} HMAC(K_D, T_D) 臨時

Device⇔SPhone

Cha. RAND()

Res. HMAC(K_{SD}, H_{TD}, T_D)

T_S 計數器S

R Request Cmd

$H_{TS,R}$ HMAC(K_{SD}, T_S, R)

若金鑰被複製使用
計數器會不一致
可讓使用者察覺問題

結論

1. 介紹 Bluetooth Low Energy、安全性分析流程
2. Smartphone 透過 BLE 控制 IoT 裝置，需要一套認證機制
3. BLE 4.0 配對有許多限制，許多廠商選擇不配對另設計認證機制
4. 重視消費者隱私下，硬體識別元(Identifier)受限、亂數化
5. 未配對裝置無法取得硬體識別元，設計認證機制遇到的挑戰
6. 提出一種更好的認證機制：雙計數器強化認證

未來展望

- Key Fob 晶片演算法研究
- Challenge nonce 亂數強度
- 是否可從ECU Firmware 或其他管道取得 Security_Key
- Relay-Attack 在什麼樣的環境下可達成

特別致謝

- CSC 老師指導、參與研究、提供設備
- Gogoro 設計這台 Smart Scooter 還不錯騎
- Hiraku (皮樂姐姐) 幫忙 dump iOS app
- Lab 同學各種支援

Q&A

- 物聯網 Security or Nothing
- 謝謝大家、敬請指教

References

- Bluetooth SIG, Bluetooth Smart (Low Energy) Security. Bluetooth SIG, 2016
https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx
- Bluetooth SIG, Bluetooth Specification Version 4.0, Bluetooth SIG, 2010
- Andrew Garkavyi, Bluetooth Low Energy. Essentials for Creating Software with Device to Smartphone Connectivity, Stanfy Inc, 2015
https://medium.com/@stanfy/bluetooth-low-energy-essentials-for-creating-software-with-device-to-smartphone-connectivity-5164c71963e7
- Mike Ryan, Bluetooth: With Low Energy comes Low Security, iSEC Partners, USENIX WOOT, 2013.
- Mike Ryan, Hacking Bluetooth Low Energy: I Am Jack's Heart Monitor, ToorCon 14, 2012.
- Lindell, A. Y. Attacks on the pairing protocol of bluetooth v2.1, BlackHat US, 2008.
- Samy Kamkar, Drive It Like You Hacked It, Defcon 23, 2015
http://samy.pl/defcon2015/2015-defcon.pdf
- Gogoro, Gogoro Smart Scooter 規格書, 睿能創意股份有限公司, 2015.
http://images.gogoroapp.com/download/PDF/tw/Gogoro-Smartscooter-Spec-Sheet-2015-06-17-02-Chinese.pdf
- Google, Android Physical Identifier Privacy, Google, 2016.
- https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html#behavior-hardware-id
- Apple, iOS Physical Identifier Privacy, Apple, 2016.
https://developer.apple.com/library/ios/documentation/UIKit/Reference/UIDevice_Class
- N. Gupta, Inside Bluetooth Low Energy. Artech House, 2013.
- Le IoT 想想物聯網 Blog, 2016
https://thinkingiot.blogspot.tw/