BLE authentication design challenges on smartphone controlled IoT devices: analyzing Gogoro Smart Scooter

Is Smart Phone a secure key for vehicle?

 $\mathsf{GD} \mathrel{\scriptstyle{\scriptstyle \wedge}} \mathsf{CSC}$

Privacy and Risk Management Lab IM, NTUST, Taiwan



Speakers

G D



- Graduate Student at NTUST IM
- CHROOT/HITCON Coordinator
- Team T5 CTO
 - Digital Forensics & Incident Response
 - Threat Intelligence Program & Plat.
- Research on Foods, plays CTFs
- Occasionally got vulnerabilities
 - Synology Bounty Program (2015)



CSC



- Associate Professor at NTUST IM
- Ph.D., Dept of IM, NTU
- Gomaji (TW.8472) Board member
- CISSP, CCFP, CSSLP, CISM, PMP
- Published many practical security papers on journals. Helped many private and public sectors to establish info security policy.

HITCON



- CTF Team
 - DEF CON 2nd Place
- CTF Event
 - DEF CON Qualifier



- Community Conf
- Enterprise Conf
- Girls Conf



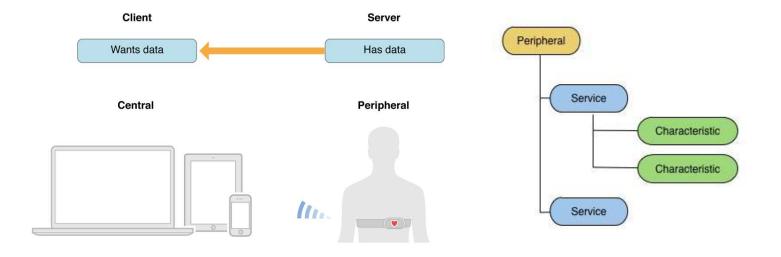
Table of content

- **1. Introduction** to Bt Low Energy, Security Manager Protocol, Smartphone authentications to controls IoT devices via BLE.
- 2. BLE 4.0 has many **privacy features**, restricting vendor powers, Hardware identifiers are either limited or randomized.
- 3. Challenges when designing auth methods, many vendors giving up **SMP pairing**, using just plaintext transmissions.
- 4. How to **analyze BLE protocols**, we exaimed many health and IoT devices, including Gogoro Smart Scooter vehicle.
- 5. Without SMP pairing, these vendor-designed authentications are sometimes **flawed**, so we are able to ignite other Gogoro.
- 6. We propose a **better auth protocol**: Dual-counter enhanced.

Bluetooth 4.0

High Speed	Classic	Low Energy
WiFi mixed BT	Most common BT	Originally "Wibree"
Persistent connections	Persistent connections	Non-persistent
High power consump.	Mid power consump.	Low power consump.
High bandwidth	Mid bandwidth	Low bandwidth
Short range	Mid range	Long range
(never tried)	Headphones, Keyboards, Mouse	Health wrists, Temp. sensors, IoT devices

Bluetooth 4.0 Low Energy



GATT/GAP	
ATT	
L2CAP	
Link	
Physical	

BLE is session-less, 7 methods, similar to HTTP

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

Usually Server has smaller battery and operates only when requested. Fig. Ref: Stanfy Inc, 2015

BLE widely adopted in Health & IoT



Curiosity to understand how it works.

BLE built-in profiles

- Time, Temp, Energy
- Weight, User profile
- Blood pressure, glucose
- Body mass, heart rate
- Speed, direction, location

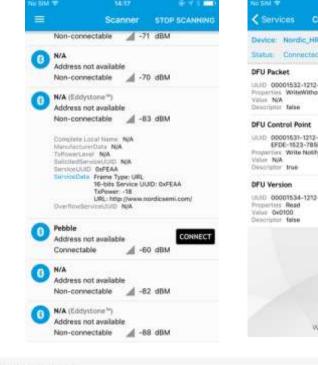
GATT-Based Specifications

Profile Sp	editation .	Version	Status	Date Adopted
ANP	Alert Notification Profile	1.0	Attive	13 September 2011
NNS .	Alert Notification Service	1.0	Active .	13 September 2011
HOP	Automation IO Profile	12	Active	14 July 2015
NOS	Automation 10 Service	1.0	Active	14 July 2018
SAS .	Battery Service	10	Attive	27 December 2011
ics .	Body Composition Service	1.0	Active	21 October 2014
LP.	Bood Pressure Profile	12	Attre	25 October 2011
LS.	Blood Pressure Service	1.0	Active	25 Octuber 2011
MS .	Bond Management Service	1.0	Active	21 October 2014
GMP	Continuous Glucose Monitoring Profile	10.1	Active :	15 December 2015
SWD	Continuous Glucose Montoring Service	121	Active	15 December 2015
pp -	Cycling Power Profile	1.1	Active	03 May 2016
PS	Oyding Power Service	13	Active	03 May 2016
SCP	Oyding Bpeed and Cadence Profile	1.0	Active	21 August 2012
SCS :	Cycling Speed and Cadence Service	1.0	Active :	21 August 2012
75	Current Time Service	1.1	Active	07 Octuber 2014
10	Device Information Service	1.1	Active	29 November 2011
se	Environmental Sensing Profile	1.0	Active	18 November 2014
95	Environmental Sensing Service	10	Active	18 November 2014
up.	Find Me Profile	1.2	Active	21 June 2011
(P	Glucose Profile	32	Active	10 April 2012
15	Glucose Service	1.0	Active	10 April 2012
OS .	HID Service	10	Active	27 December 2011
OGP	HD over GATT Profile	1.0	Active	27 December 2011
PS	HTTP Proxy Service	10	Active	06 October 2015
RP	Heart Rate Profile	1.0	Active	12 July 2011
RS	Heat Rate Service	10	Active	12 July 2011
12	Health Thermometer Profile	10	Active	24 May 2011
15	Health Thermumeter Service	12	Active	24 May 2011
s.	Immediate Alert Service	10	Active	21 June 2011
	Indoor Postoning Service	12	Active	19 May 2015
SP	Internet Protocol Subport Profile	1.5	Active	16 December 2014
8	Line Loss Service	12.1	Active	14 July 2018
NP.	Location and Navigation Profile	10	Active	30 April 2013
NS	Loostion and Nevigation Service	1.0	Active	30 April 2013
DCS	Next DST Change Service	1.0	Active	13 Sectember 2011
TP	Object Transfer Profile	1.0	Active	17 November 2015
175	Object Transfer Service	10	Active	17 November 2015
458	Phone Aiert Status Profile	1.0	Active	13 September 2011
ASS	Phone Alert Status Service	1.0	Active	13 September 2011
P	Proximity Profile	1.0.1	Active	14 July 2015
UP	Pulse Oximater Profile	1.2	Active	14 July 2015
LOS	Pulse Ostnetor Prote	10	Active	14 July 2015
SCP		1.0		
SCP SCS	Running Speed and Cadence Profile	10	Active	C7 August 2012
	Running Speed and Cadence Service		Active	07 August 2012
TUS	Reference Time Update Service	1.0	Active	13 September 2011
PP .	Scart Parameters Profile	10	Active	37 December 2011
cPS	Scan Parameters Service	1.0	Active :	27 December 2011
06	Transport Discovery Service	1.0	Active	17 November 2015
P	Time Profile	1.0	Active	13 September 2011
PS	Ts Power Service	1.2	Altive	21 June 2011
CS.	User Data Service	1.0	Active	27 May 2014
	Weight Scale Profile		Active	21 Octuber 2014
WSP	Weight Scale Profile Weight Scale Service	1.0	Active Active	21 October 20 21 October 20

BLE playgrounds

• Nordic nRF App

• Node.js bleno



Primary Service

var PrimaryService - blenc.PrimaryService; var primaryService - mex PrimaryService({ auid: 'freeffeetfeetfeetfeetfeetfeetee', // ar 'free' data is-bit characteristics { // see Characteristic for data type 1 };;

Device: Nordic_HRM Statu: Connected DFU Packet ULU 00001532-1212-EFDE-1523-785FEABC0123 Properties WinkWithouResponse You NA Description: the DFU Control Point ULU 00001531-1212-EFDE-1523-785FEABC0123 Properties: Withe Notify You NA Description: The DFU Version ULU 00001534-1212-EFDE-1533-785FEABC0123 Properties: Read You Solid Description: Table

Characteristics

.

Wireless by Northc

-

Characteristic

BLE is easy to hijack



• Sending vibrate message to nearby MI wristbands

Stat	SEOF TO TO TO THE A
401	BONDED
Ŷ	Generic Access UUID: 0x1800 PRIMARY SERVICE
R	Generic Attribute UUID: 0x1801 PRIMARY SERVICE
¢.	Unknown Service UUID: 0000fee0-0000-1000-8000-00805f9b34fb PRIMARY SERVICE
~	Unknown Service UUID: 0000fee1-0000-1000-8000-00805f9b34ft PRIMARY SERVICE
<u>.</u>	Unknown Service UUID: 0000fee7-0000-1000-8000-00805f9b34ft PRIMARY SERVICE
~	Immediate Alert UUID: 0x1802 PRIMARY SERVICE
	Alert Level UEID: 0x2A06 Properties: WRITE NO RESPONSE Write Type: WRITE COMMAND Winders by Nords

write	value	
Select Alert	: Level:	
0x00 (N	o alert)	
0x00 (N	o alert)	
0x01 (M	ild alert)	32
0x02 (Hi	igh Alert)	
PRIMARY	SERVICE	
Alert		
UUID: 0	2A06 WRITE NO RESPO	and the second s

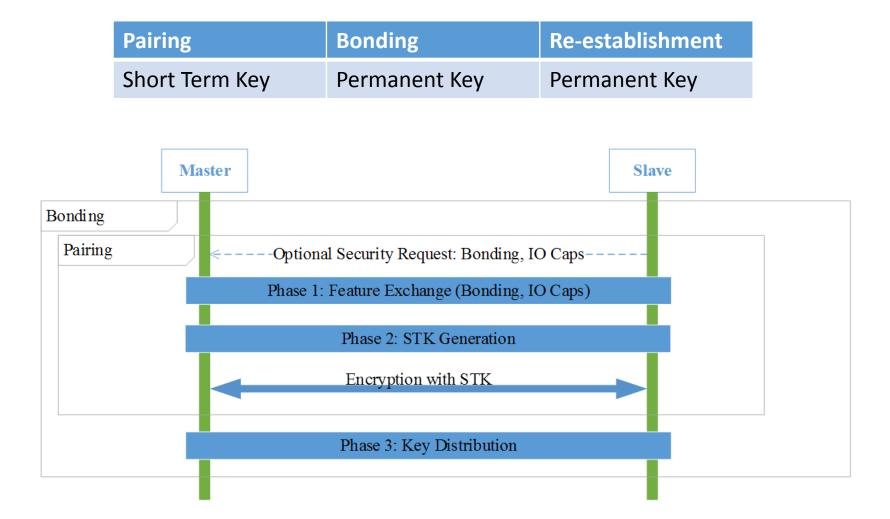


Ref: "Le IoT 想想物聯網 blog"

All BLE sniffer got is in plaintext ?!

	020_key_fobe.pcapng	Antistics Talanhany Mimless	Teele Help	
	File Edit View Go Capture Analyze St			
	🚄 🔳 🖉 💿 🕌 🛅 🗙 🖻 🍳 🗢		ચિલ્લ 😐	
	btle.data_header.length > 0 btle.advertising	_header.pdu_type == 0x05		
CAP continue	¹⁶ No. Tim Source	Destination	Protocol Length	
	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
1. 92210	41 20 unknown_0xa58be383	unknown_0xa58be383	ATT	57 UnknownDirection Write Command, Handle: 0x0025
560 delta te	49 20 unknown_0xa58be383	unknown_0xa58be383	ATT	57 UnknownDirection Handle Value Notification, Handle: 0x00
	52 20 unknown_0xa58be383	unknown_0xa58be383	LE LL	35 Control Opcode: LL_TERMINATE_IND
and the second	53 20 unknown_0xa58be383	unknown_0xa58be383	LE LL	35 Control Opcode: LL_TERMINATE_IND
The second secon	54 20 unknown_0xa58be383	unknown_0xa58be383	LE LL	35 Control Opcode: LL_TERMINATE_IND
CAP continue	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
Bl delta_t=	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
Channel Index: 17	84 20 unknown_0xcdec96c8	unknown_0xcdec96c8	ATT	57 UnknownDirection Write Command, Handle: 0x0025
LLID: 1 / LL Data PDU / empty or L2CAP continue	85 20 unknown_0xcdec96c8	unknown_0xcdec96c8	ATT	57 UnknownDirection Write Command, Handle: 0x0025
NESN: 0 SN: 1 MD: 0	91 20 unknown_0xcdec96c8	unknown_0xcdec96c8	ATT	57 UnknownDirection Handle Value Notification, Handle: 0x00
	93 20 unknown_0xcdec96c8	unknown_0xcdec96c8	ATT	57 UnknownDirection Handle Value Notification, Handle: 0x00
Data: CRC: d1 00 65	95 20 unknown_0xcdec96c8	unknown_0xcdec96c8	LE LL	35 Control Opcode: LL_TERMINATE_IND
UNU1 01 00 05	96 20 unknown_0xcdec96c8	unknown_0xcdec96c8	LE LL	35 Control Opcode: LL_TERMINATE_IND
systime=1441512979 freg=2440 addr=8d651b4d delta t=	97 20 unknown_0xcdec96c8	unknown_0xcdec96c8	LE LL	35 Control Opcode: LL_TERMINATE_IND
86 9e d1 00 65 92 86 01 5d 3e 8e 5e 65 e0 61 9a 7d	98 20 unknown_0xcdec96c8	unknown_0xcdec96c8	LE LL	35 Control Opcode: LL_TERMINATE_IND
c8 8f 67 62 f5 4f a7 f5	99 20 unknown_0xcdec96c8	unknown_0xcdec96c8	LE LL	35 Control Opcode: LL_TERMINATE_IND
Data / AA 8d651b4d (valid) / 30 bytes	114 20 TexasIns_	TexasIns_	LE LL	67 CONNECT_REQ
Channel Index: 17	137 20… TexasIns_	TexasIns_	LE LL	67 CONNECT_REQ
LLID: 2 / LL Data PDU / L2CAP start	150 20 unknown_0x1431bea9	unknown_0x1431bea9	ATT	57 UnknownDirection Write Command, Handle: 0x0025
NESN: 1 SN: 0 MD: 0	158 20 unknown_0x1431bea9	unknown_0x1431bea9	ATT	57 UnknownDirection Handle Value Notification, Handle: 0x00
	160 20 unknown_0x1431bea9	unknown_0x1431bea9	LE LL	35 Control Opcode: LL_TERMINATE_IND
Data: d1 00 65 92 86 01 5d 3e 0e 5e 65 e0 61 9	161 20 unknown_0x1431bea9	unknown_0x1431bea9	LE LL	35 Control Opcode: LL_TERMINATE_IND
f5 cc c8 8f 67 02 f5	162 20 unknown_0x1431bea9	unknown_0x1431bea9	LE LL	35 Control Opcode: LL_TERMINATE_IND
CRC: 4f a7 f5	163 20 unknown_0x1431bea9	unknown_0x1431bea9	LE LL	35 Control Opcode: LL_TERMINATE_IND
systime=1441512979 freq=2440 addr=72f844df delta t:	🕀 Frame 91: 57 bytes on wire (45	6 bits), 57 bytes capt	tured (456 bits)	on interface 0
01 00 9b 72 68	🕀 PPI version 0, 24 bytes			
Data / AA 72f844df (valid) / 8 bytes	DLT: 147, Payload: btle (Bluet	Yooth Low Energy Link /	Layer)	
Channel Index: 17	🕀 Bluetooth Low Energy Link Laye			
LLID: 1 / LL Data PDU / empty or L2CAP continue	Bluetooth L2CAP Protocol Second			
NESN: 0 SN: 0 MD: 0	🗄 Bluetooth Attribute Protocol			
Picany, W. Wix, W. Fizz, W.	Opcode: Handle Value Notifi	cation (0x1b)		
Data:	Handle: 0x0036			
CRC: 9b 72 68	Value: fdcd5bc77ed87e6fad4e	229f9		
	4			
	4			

Security Manager Protocol



BLE 4.0 SMP pairing

Just Works is Un-authed

Pairing Mtd.	MitM attacks	Usability
Just Works	Vulnerable	Convenient, Un-authed
Passkey Entry	If you brute-PIN	Needs screen & Keyboard
Out-Of-Band	Secure via NFC	Needs NFC transceivers

Why vendors did not use SMP pairing:

- 1. Pairing takes time and effort
- 2. Paired does not always means secure
- 3. No screen for numeric comparison

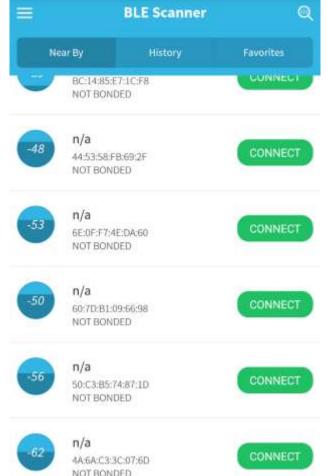


Initiator Display Keyboard NoInput Keyboard Responder DisplayOnly YesNo Only NoOutput Display Just Works Just Works Just Works Just Works Just Works NoInput Unauthenti-Unauthenti-Unauthenti-Unauthenti-Unauthenti-NoOutput cated cated cated cated cated Passkey Entry (For Just Works LE Legacy (For LE Pairing): Legacy responder Pairing) Passkey displays, ini-Unauthenti-Entry: tiator inputs cated Just Works responder Just Works Authenti-Display displays, ini-Unauthenti-Unauthenticated YesNo tiator inputs cated cated Numeric Numeric Authenti-Comparison Comparison cated (For LE (For LE Secure Con-Secure Connections) nections) Authenti-Authenticated cated

BLE 4.2 screen numb. comp.

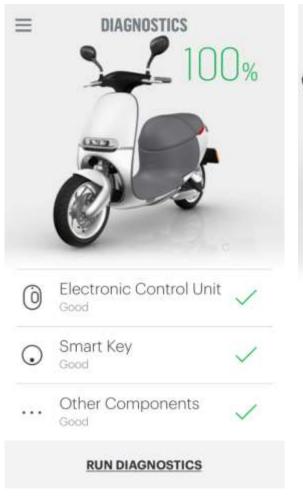
BLE 4.0 privacy features

- HW Identifier Read Limitations
 - Prevents App/Ads tracking user
 - MAC Address always 020000000000
- HW Identifier Randomization
 - Prevents AP tracking/nearby scanning
 - MAC Address different per power-cycle
 - SMP paired device gets fixed MAC via IRK



• How to authenticate device without HW identifier?

Gogoro Smart Scooter





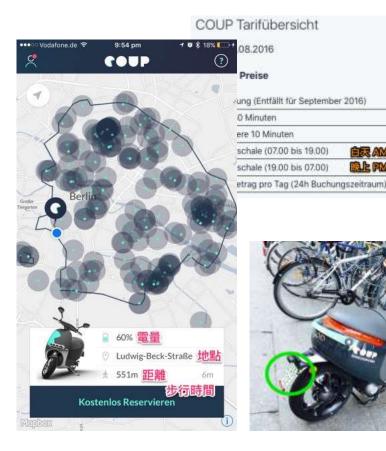
-`____` Breathing Light

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





Public Rental in Berlin



Our current research is based on Taiwan Gogoro. Berlin Gogoro might work different from Taiwan's.

Gogoro's awesome electric scooter is coming to Europe next year, Amsterdam first

By Clem Zegler in Sveniller 11, 1971-1970 - In: # Deal? # Spenier

30 € 3 €

1€

20 €

10 €

30 €

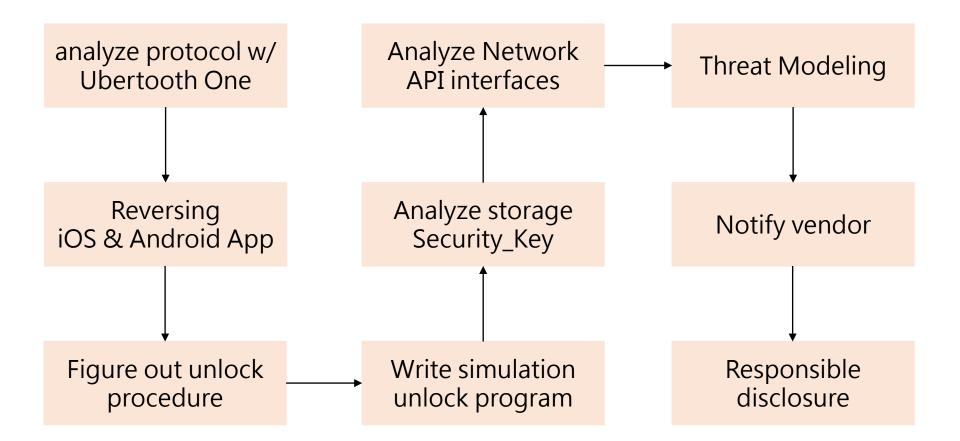


Bosch Teams Up with Gogoro to Bring Electric Scooter-Sharing to Berlin

by Kinder Korosec - Elizabeticensec - ALX2.001 4, 2016, 1.51 AM EDT



Analyzing method



Key Fob Unlock (BLE)







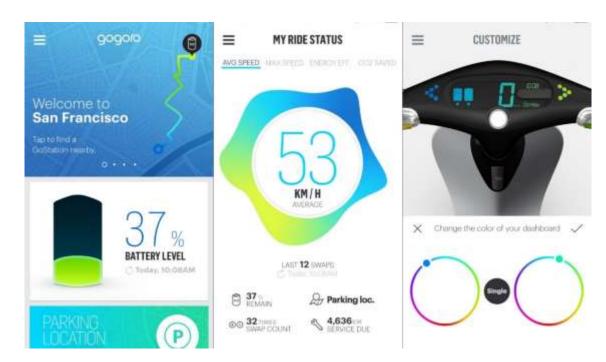
	Source	Destination	Protocol	Length	Info
16:40:39.125904745	TexasIns	TexasIns	LE LL	67	CONNECT_REQ
16:40:39.142823445	unknown_0xa58be383	unknown_0xa58be383	ATT	42	UnknownDirection Write Command, Handle: 0x0037
16:40:39.230913045	unknown_0xa58be383	unknown_0xa58be383	ATT	57	' UnknownDirection Write Command, 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	Function
Key Fob		CONNECT_REQ	Init connection
Scooter	0x37	01 00	Command ID
Scooter	0x25	c2 e7 20 bf d2 99 9d 43 68 c6 2d 65 39 3d 72 c9 f3	Rand. Challenge
Key Fob	0x36	d2 25 57 33 19 18 51 fd ae 7d 1b ed 85 e0 10 78 e2	Signed. Response
Scooter		LL_TERMINATE_IND	Ends connection

(this is much better than widely adopted Keeloq protocol)

Mobile App (Gateway)

- My Gogoro single-sign-on
- App gets scooter information





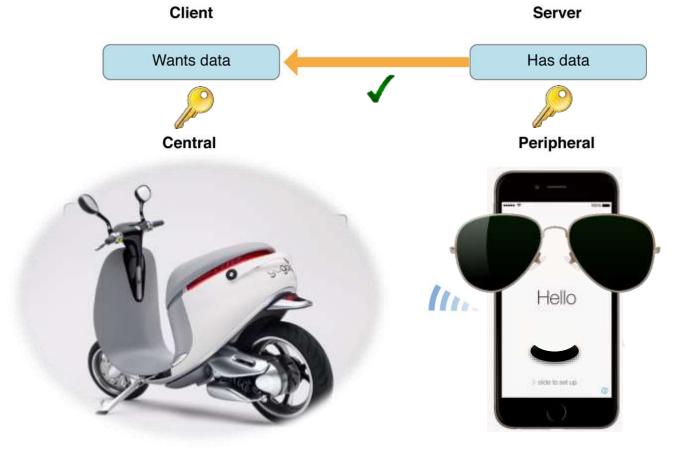
LOG IN

Mobile App Pairing & Unlock

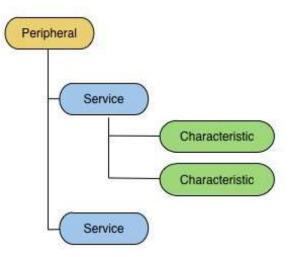


Vendor's challenge

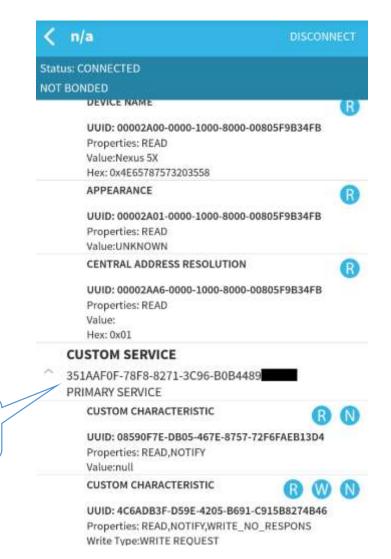
• How to design authentication protocol when we did not BLE pairing and have no HW identifier?



BLE Gogoro Service



BLE Service UDID last 6-bytes must be Scooter MAC Address



Gogoro App Protocol

A-prefix: querying information

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
105 15 11	60 LOCAD Engrant

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

Origin	Cmd	Function
Арр	A0	GetScooterSettingWithType
Арр	A1	GetScooterErrors
Арр	A2	GetScooterInfo
Арр	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	BO	ECU Challenge nonce
Арр	B1	ECU Response digest
Scooter	B2	ECU unknown
Scooter	B3	ECU Error
Арр	B4	ECU Cmd (Lock, Unlock, Open Trunk)

B-prefix: ECU Challenge Response

Gogoro Unlock flow

- 1. Scooter scans nearby peripheral for GATT Gogoro Service And if UUID {351AAF0F-}last 6-bytes matches its MAC Address
- 2. Mobile App reads GATT Scooter status, enable unlock button. Click to send ECU_Cmd(0xB4): 00 Lock, 01 Unlock, 02 Op Truck
- 3. Scooter writes ECU_Challenge (0xB0), a random 256 bit nonce
- 4. Mobile App notify ECU_Response (0xB1), also 256 bits ECU_Response = SHA256(ECU_Challenge, **Security_Key**)
- 5. Scooter compares ECU_Response if correct then ECU_Cmd will be executed, Unlocked.





the Security_Key



- ECU_Response = SHA256(ECU_Challenge, Security_Key)
- Early App put Security_Key in Document folder (slightly encrypted)
 - iOS MobileAppProp.plist has ScooterSKey
 - Android Settings.xml has AppSettings_DefScooter/encryptedkey2
 - Decrypting: AES-256, CBC/PKCS7Padding, IV=UserId, Key = ScooterUUID
- Document folder can be backed-up via iTunes / Android adb
 - Various methods: cable Juicy Attack, iTunes backup folder extraction etc.
 - AndroidManifest.xml has allowBackup flag set to true
- Security_Key can be retrieved from WebAPI
 - Attacker can brute My Gogoro membership
 - App Cookie can be stolden (MobileAppProp.plist has Web_Token)
 - <u>https://mobile-pro.gogoroapp.com/WebService/Web/GetKey</u>

kevtest

["KeyData":"q70Bzgun1w 1C6ZV77Ptb4 pgjhcl33J6 geqiZHMqof4ndVLIII, Ypqu/yG/ 8BFqNdnFGqA9HVzUTsc4UTyVncA=","CachedTime":"2017-0 4-23T12:40:15.51659452"]

Insecure App Data Storage

- Token, Certificate should be stored encrypted
 - Manages Timeout, Password Tamper etc.
 - Limits user, process access and key export
- Most OS platforms has secure storage zone
 - Apple iOS/macOS Keychain
 - iPhone 6~ Secure Enclave
 - Android Keystore
 - Samsung S6~ KNOX
 - Windows Protected Storage
 - HSM Such as UbiKey

Unlock code generator

• We wrote our Android App to generate ECU_Response and unlocked scooters successfully if Security_Key is known.

• Demo

Via this experiment we proved:

- 1. Security_Key is necessary to unlock scooter.
- 2. Security_Key can be cloned or transferred.
- 3. Gogoro Scooter cannot identify Mobile App hardware.

successConnection State Change: 80:84:48: :establishedMTU Changed: 80:84:48: Connection State Change: 80:84:48: : disconnected 78:f8:82:71:
78:f8:82:71:
i en ere ere ere ere ere ere ere ere ere

Gogoro Analysis Summary

- HW identifier privacy makes authentication difficult
 - IoT device trusts Security_Key rather than your Mobile Phone
 - Protect your Security_Key hard !!!
- Insecure App Data Storage vulnerable
 - Security_Key should not be stored in Document folder
 - Should be stored at Keychain / KeyStore
- Other possible weakness
 - WebAPI should do SSL Cert Pining to prevent MitM
 - Relay-Attack for Challenge-Response might be possible
 - Dumping Security_Key from Key Fob MCU or Scooter ECU?

Gogoro system is generally safe...

- Although BLE SMP pairing is not adapted, Challenge/Response is better than Keeloq OTP
- Obtaining Security_Key from mobile phone is possible only when malware infected/jailbroken.
- Obtaining Security_Key from PC backup folder still needs to infect PC and decrypt slightly AES.
- Obtaining Security_Key from WebAPI might be the easiest way if username / password can be retrieved, brute-force or from other leaked database.

How to steal a Gogoro Scooter

- Infect the owner's phone or backup PC
 - Obtain and decrypt Security_Key from plist
- Owner open App to check fuel in Public Wifi
 - Do SSL MitM to get his cookie
 - Ask WebAPI for Security_Key
- Simulate the BLE Gogoro Service
 - With target scooter's MAC UUID
 - Approach target scooter and do ECU Challenge Response
 - Rode away as soon as possible.
- But you still cannot exchange battery :-(
 - Gogoro Battery has NFC authentication.

SSL MitM to retrieve Security_Key

Image: And your you bus sets Image: And your you bus sets Image: And your your your your your your your your	周田提式 - 😫 全Home × 🗇 Win7 × 📦 kaki	10 ×	- 🛛 🗉 🖉 🐨 🗸 •
Operative Network Processor Target Spart <	Ele Edit View VM Iabs Hel	+ 🕨 🛢 🐻 Q H D O Q D 🛏 🗶 🦷 🗖	- D - F
Multiple//my gegono.com/mulacecom/files/um Most Vailed * Th	Object reference not set × +	Burp Intruder Repeater Window Help	-11
Most Vaited * Th Exp(r) ##(c) ##(c	B https://my.goggeo.com/tw/account/sine-un		12
Server Errori Prot opt sou Image: Prot opt sou Image: Prot opt sou Object reference Chain OUTPUT (policy AC target prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net arget prot opt sou Post //w/account/sign-up HTP/1.1 Headers: System.Net Argent Nonlina's 0.10, Unit, android 5.0.2; HTC Butterfly's Build/LRX22G) AppleWebRU537.36 (KHTML, like Gecko) Chrome/51.0.2704, 81 Mobile Safaru/537.36 Gogoro: MY/ATW Infoll and on 192. 168. Gogoro: MY/ATW Post Best in art - F System.Web.MvcC Post Best in art - A System.Web.MvcC Post Best in att - A Post Best in att - I Post Best in att - A System.Web.MvcC Post Best in att - A Post Best in att - I Post Best in att - A System.Web.MvcC Post Best in		- Community Schusser (1995) and a second schuse of schus	
Object reference copyon Description: An unhandled scape chain POSTROUTING (pc) 1 copyon Description: An unhandled scape chain POSTROUTING (pc) 1 copyon Description: An unhandled scape chain POSTROUTING (pc) 1 content.target prot op scou MASQUERADE all an mucli radio wifil off fronting with and point this://my.gogoro.com Upgrade.insecure.Requests: 1 unhandled scapes arc at apds. - frkill unblock with mucli radio wifil off fronting with and point this://my.gogoro.com Upgrade.insecure.Requests: 1 uncli radio wifil off fronting with and point this://my.gogoro.com/ Upgrade.insecure.Requests: 1 uncli radio wifil off fronting with and point this://my.gogoro.com/ Upgrade.insecure.Requests: 1 uncli radio wifil off fronting with and point this://my.gogoro.com/ Upgrade.insecure.Requests: 1 upgrade.insecure.Requests: 1 u			Caminent this item
	Description: An unhandled exc Exception Details: System.twi Source Error: An unhandled exception was Source Error: An unhandled exception was Stack Trace: [NullReferenceExcer Data.Control.Helpe Bata.Control.Helpe System.Web.Mvc.R System.Web.Mvc.R System.Web.Mvc.A System.Web.Mvc.A System.Web.Mvc.Async.⇔c_DisplayClass20. <bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.⇔c_DisplayClass20.<bet System.Web.Mvc.Async.</bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet </bet 	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: Mozillar/S.0 (Linux; Android S.0.2; HTC Butterfly's Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2 Content-Type: application/x-www-form-urlencoded Accept text/html,application/xhtmi+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=BP9D631F12AC58F3388E04F5F846111138BE4C9AA7A1F1538B7F6E2468EB5581D43D1E02274AD4439027C0C8812CA0DBA613 S4F3Ed033DE94; gat=1; RequestVerificationToken_L3R3D=kmBeKLJC1ObuaW5kiySQcxRbrQ9WpBg9hnDikKrY1OfzApc94Mka7A3p37H65P2YNkux7xSmVUef2S K6AEuUw&RxS50bsColNrrs430 ga=GA1.2, 1820717990.1467277080 RequestVerificationToken=sz0PFdV21zRidEF20NDH_FEJPQxBTeiWJ5S3GQDC5IBRHK7ChonxGbj862gC5o47o7ztYG4wN5XIf36s, h7iRKV E4nPrrrQc2nXyiSBR0&LastName=Asdfg&FirstName=Qettl&Email=adfid540dgih.com&Mobile=0912345678&Pasword=Qazwisx1238 g=recaptcha=response=03AHg_VusNOLzvbu4ycN357zLKjmmIMyzEcG6_0hA7YR-sjLNXKYV7NA8qUnGpwUNBB/SCQ5iP3UCBWPK92 E47MwQezKWYWpRKgFUJETyOYyJzn9uUKkbb2IWxs_313F9_FKC_dw65CJinaKx0YWmJ0WUpQgYnbBlbh-4j5onEvkx3FAofFTdvHpXTP_M QKT8G905Ti20J2ULAU4pYEoL7ZMe4hvuxQ0PVypQ2gGRbtUEJ)YQmh2JJ2Z2to492AyL&PDex_ANAXgfW_Niho6WVOusfcReFi-SCDYu VA13QUIVTTC67aXkio5xcnQz1ABHrg6HpXyrLcG50J55Gza4pPrr2gpsgm6DL4Ay7IhqnF2NMqU4uH4JFUXQnJDXAq_IQtNeyct3TigtFi	3F722EA31A13C66DCA5B0CCE14 VQzJ/PjPbMy6pnO4I4oMTG3PzL Alshe950TAqe8u7pvX25po81XR ApasswordConfim=Qazwsx1238 ALERvjy7mKdqAG7dCwjRvFaQC AxX5QHuHV1_XR9xbgDx3h-e4og4 uhR11G5xA4r0RgA6K-PtE7J_NYV_V kiF36UGPIArppF2HvTnfM9CInss5j
	system regulation of the segment of the		

Responsible disclosure

- 2016/02 App supports BLE unlock
- 2016/04 We notified Gogoro Vendor
- 2016/04 Fixed Security Key store
- 2016/07 Fixed SSL Cert verification
- 2016/07 Issued force logout update
- 2016/12 Full Recall / Replace ECU
- Better Bluetooth Pairing Function



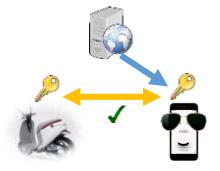
improvement in the future.

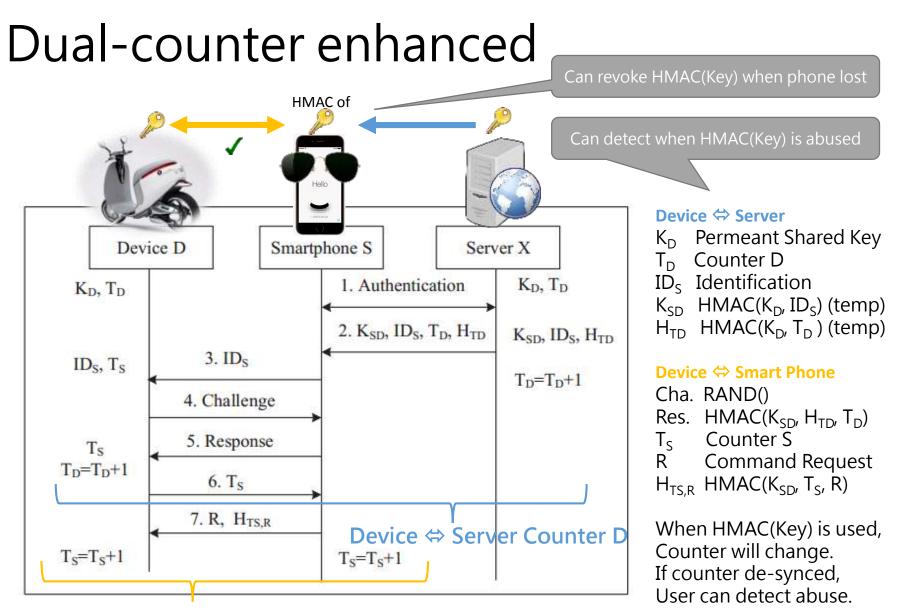
Designing good IoT-phone authentication

- Device does not know each other
 - IoT device does not know phone
 - IoT device knows secret key
 - IoT server provision secret key to phone
- Preventing Security_Key cloning
 - BLE 4.2 SMP Secure Connections
 - Phone has hardware identifier
 - store it in Secure Element
 - use OOB OTP such as SMS
 - add dual-counter to detect

Auth Methods Comparisons

Method	Advantage	Disadvantage
Server Provision Secret Key	Phone device independent	Easy to steal, hard to detect
BLE 4.2 Secure Connections	Prevents MITM and clone.	Need a numeric display
Hardware Identifier	ID device. Prevents clone.	Privacy concern
Store in Secure Element	Encrypted, difficult to clone	Not every phone has SE
OOB OTP such as SMS	Trusting phone number.	OOB Channel cost (SMS)
Dual-counter detection	Can easily detect abuse.	Cannot prevent abuse.





Device ⇔ S. Phone Counter S

Conclusion

- 1. introduction to Bt Low Energy, Security Manager Protocol, Smartphone authentications to controls IoT devices via BLE.
- 2. BLE 4.0 has many privacy features, restricting vendor powers, Hardware identifiers are either limited or randomized.
- 3. Challenges when designing auth methods, many vendors giving up SMP pairing, using just plaintext transmissions.
- 4. How to analyze BLE protocols, we examined many health and IoT devices, including Gogoro Smart Scooter vehicle.
- 5. Without SMP pairing, these vendor-designed authentications are sometimes flawed, so we are able to ignite other Gogoro.
- 6. We propose a better auth protocol: Dual-counter enhanced.

Future research

- Hardware hacking
 - Dump Security_Key from Key Fob MCU (TI CC2540)
 - Dump Security_Key from Scooter ECU (Atmel)
- Cryptography analysis
 - Challenge nonce randomization strength?
 - Challenge response acceptance timeframe?
- Relay-Attack on challenge responses
 - Attacker A approach Owner
 - Attacker B approach Scooter
 - A & B Relay challenge response over internet

Special thanks to

- Professor CSC's guidance and research
- Gogoro designed a BLE Smart Scooter
- Hiraku help dumping iOS app
- Support from lab and company colleagues



- IoT is Security or Nothing
- Any questions?
 - GD@TeamT5.org

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 <u>http://samy.pl/defcon2015/2015-defcon.pdf</u>
- 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/