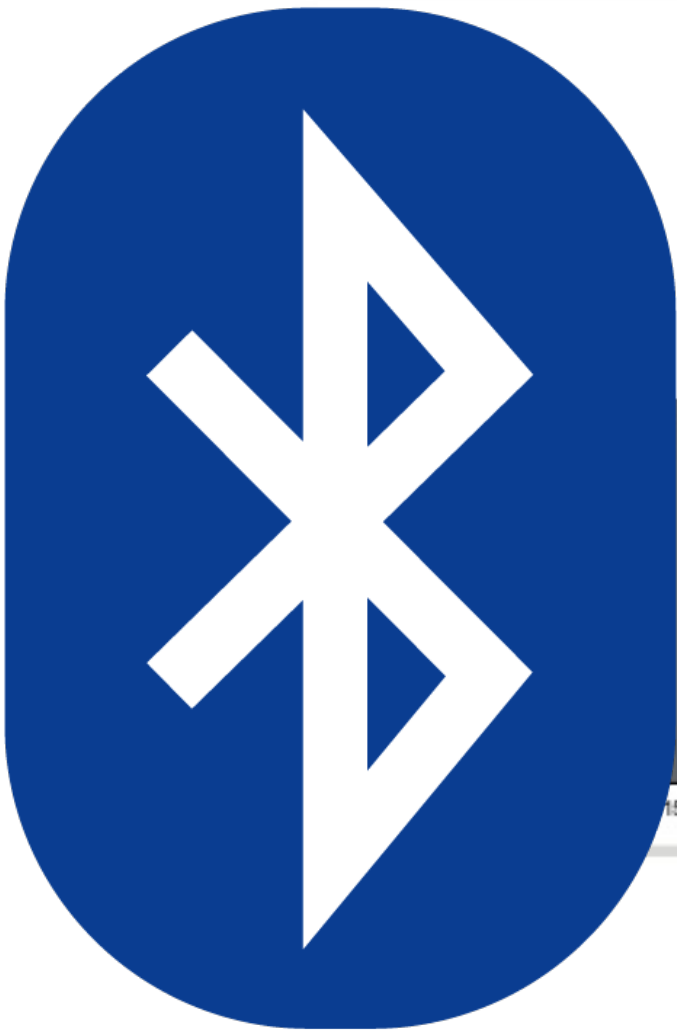


Bluetooth Hacking: Tools and Techniques

ICE9
CONSULTING

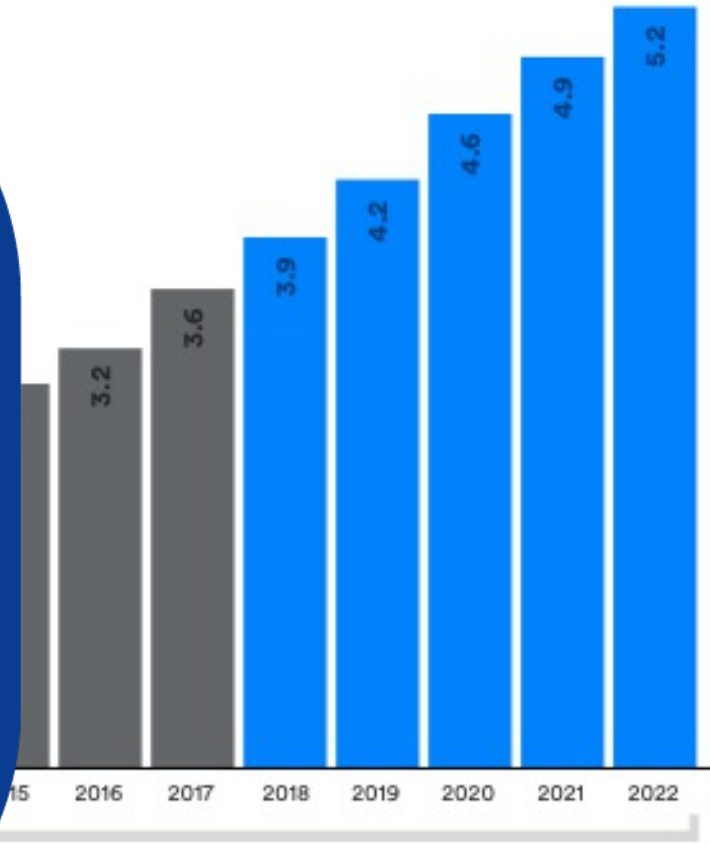
Mike Ryan

Founder
ICE9 Consulting
@mpeg4codec



Total Bluetooth Device Shipments

numbers in billions



12%

compound annual growth rate
(CAGR) over 10 years



Who is this talk for?

Bluetooth device developers

Penetration testers

Managers

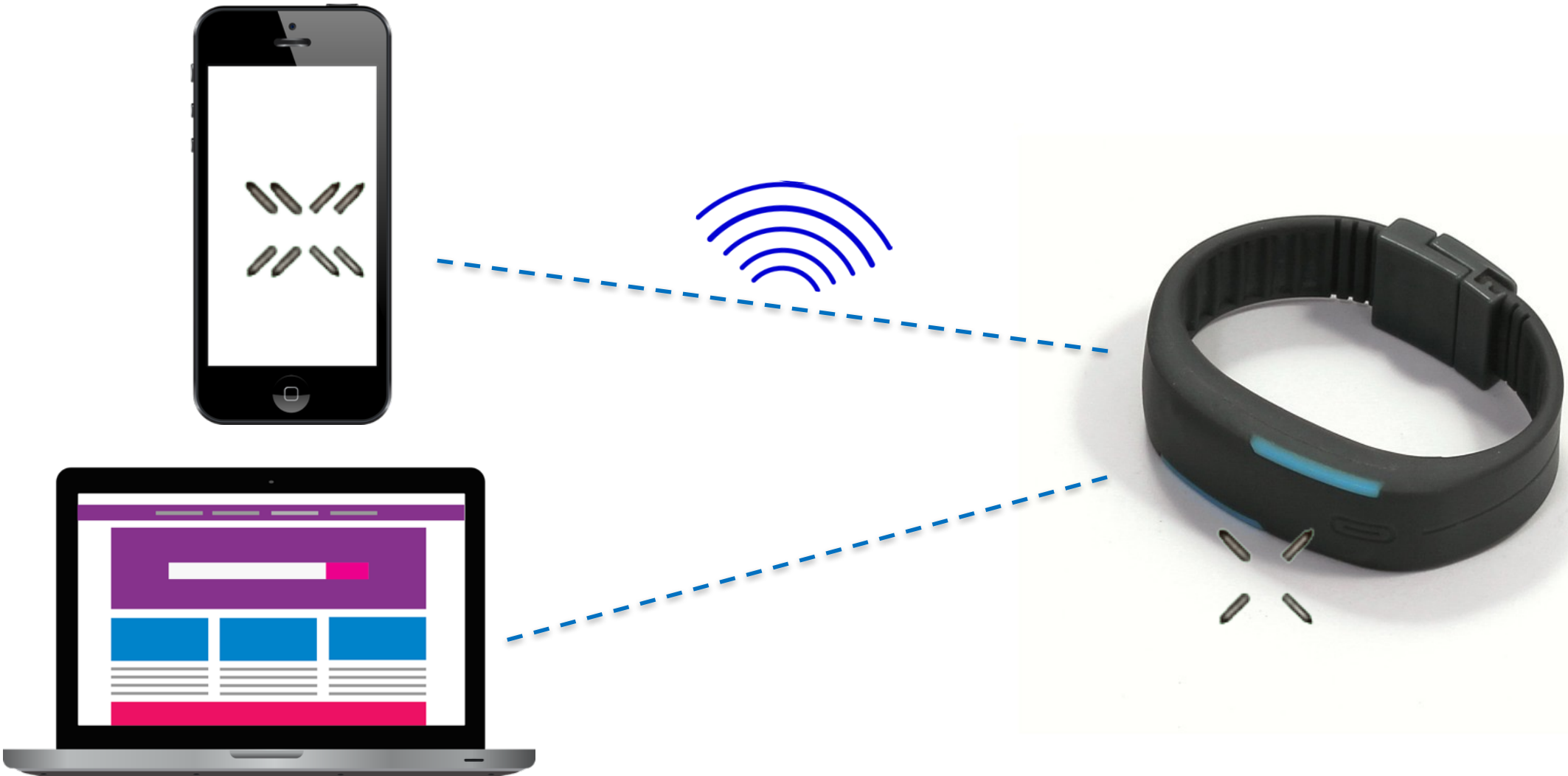
Structure of the Talk

Overview of Bluetooth

RE Process and Tools

Case Studies

Bluetooth and the Reverse Engineering Process



Reverse Engineering Process

1. Do something with the device and app
2. Capture the data sent via Bluetooth
3. Analyze

???

Sniffing Bluetooth is **Hard**





Pros: 100% reliable

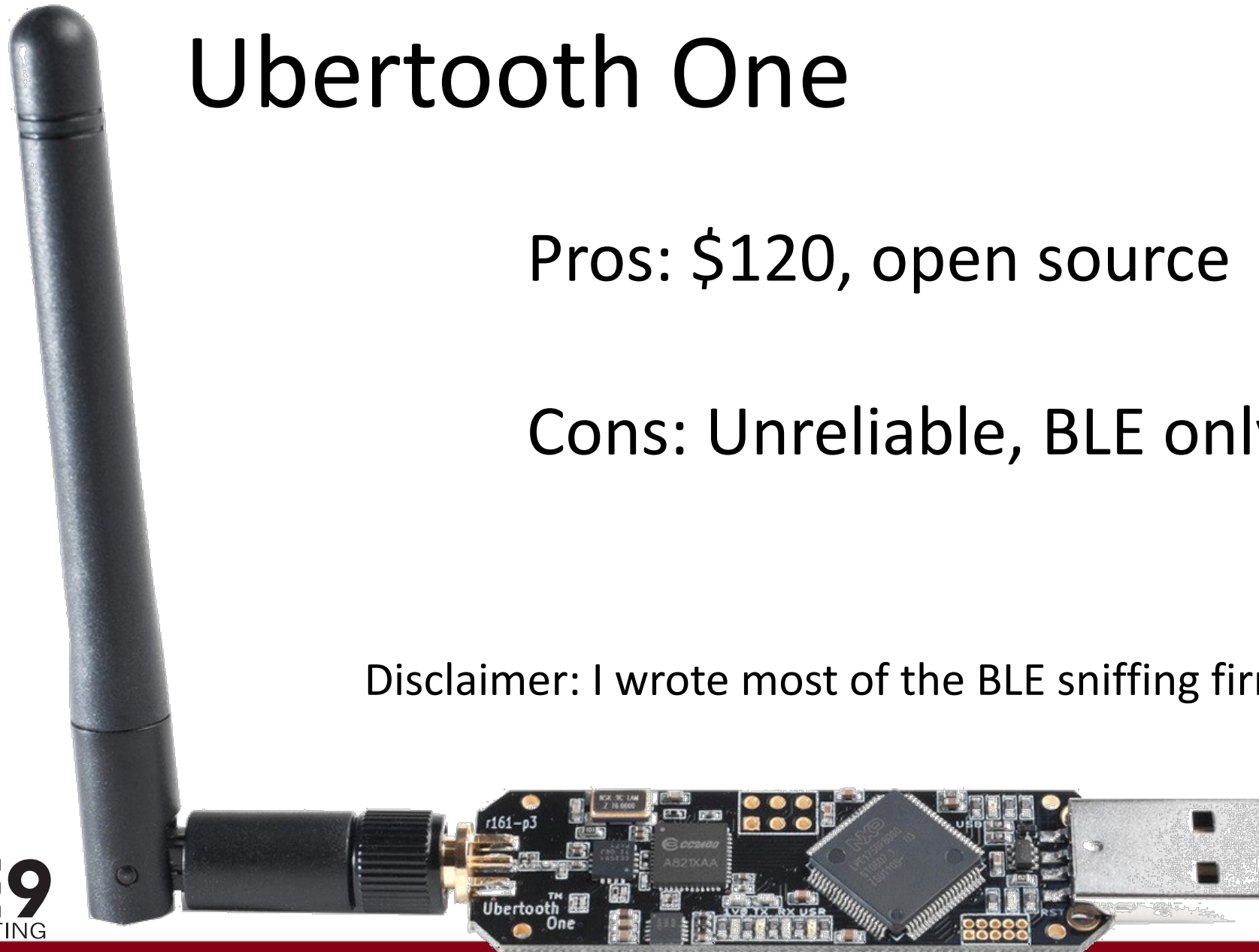
Cons: \$20,000

Ubertooth One

Pros: \$120, open source

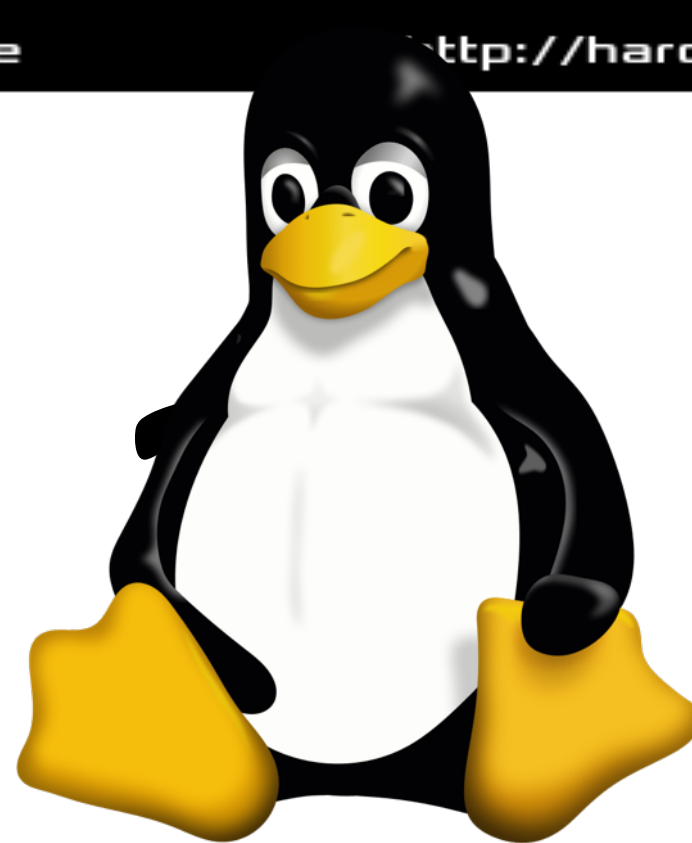
Cons: Unreliable, BLE only

Disclaimer: I wrote most of the BLE sniffing firmware

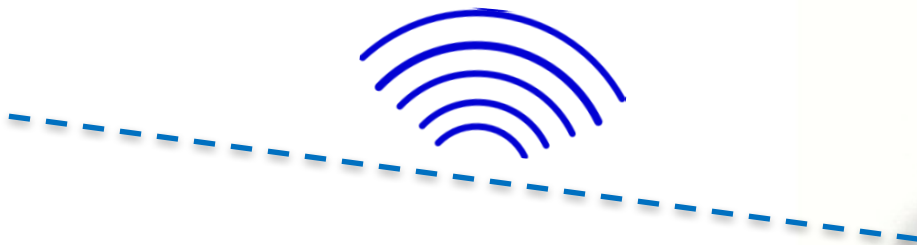




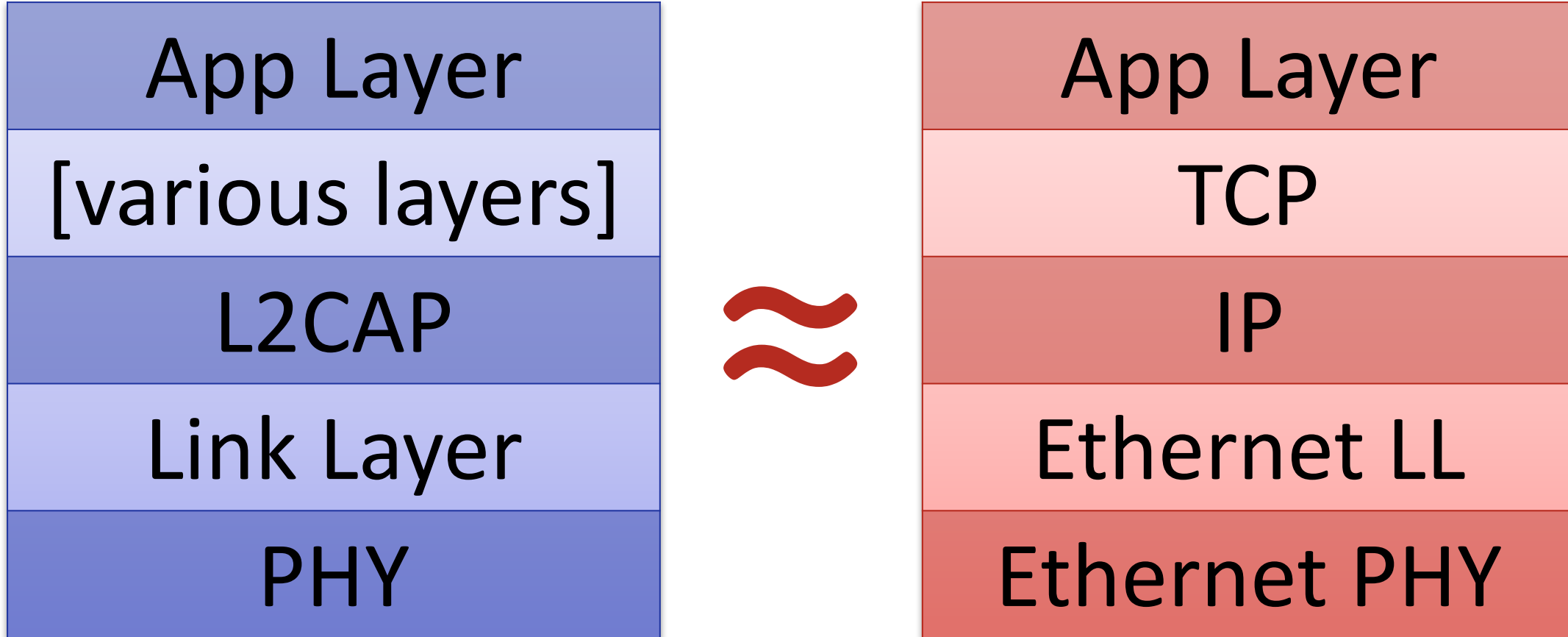
There is



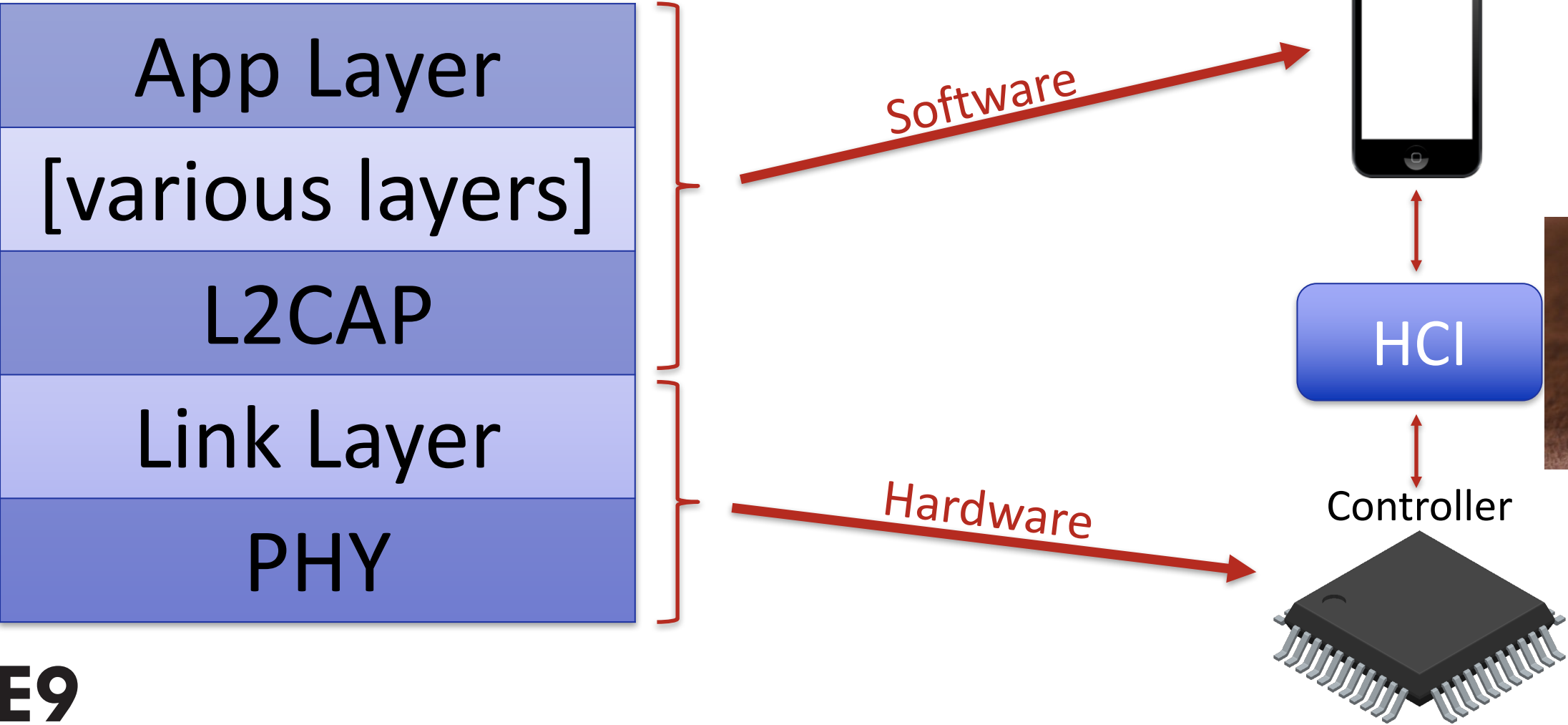
BeOS X!ay!



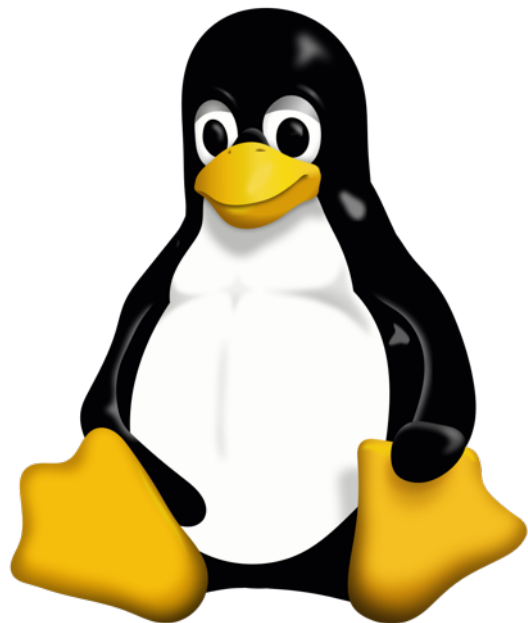
Bluetooth Overview



Bluetooth Overview



Logging HCI



OSX



Developer options

On

Take bug report

Desktop backup password
Desktop full backups aren't currently protected

Stay awake
Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Capture all bluetooth HCI packets in a file

Running services
View and control currently running services

Debugging

USB debugging
Debug mode when USB is connected

OS X packet logger

Stop

Clear

Priorities

Throughput

Packet Types

A2DP Control

ACLDecoder

ATTDecoder

ATTDecoder:Error

AVCTP

Error

HCI Command:Accept Connection Request

HCI Command:Authentication Requested

HCI Command:Change Connection Packet Type

HCI Command:Change Local Name

HCI Command:Create Connection

HCI Command:Create Connection Cancel

HCI Command>Delete Stored Link Key

HCI Command:Disconnect

HCI Command:HCI Inquiry

HCI Command:HCI Inquiry Cancel

HCI Command:LE Add Device To White List

HCI Command:LE Clear White List

HCI Command:LE Connection Update

Priority Set

Default

Audio

HID

LE

Kernel

Priori...

6

5

5

10

5

10

5

6

5

5

9

9

8

9

6

6

9

5

5

Unfiltered Hand...

ACL Filter

Find

Filter

Decode Packets

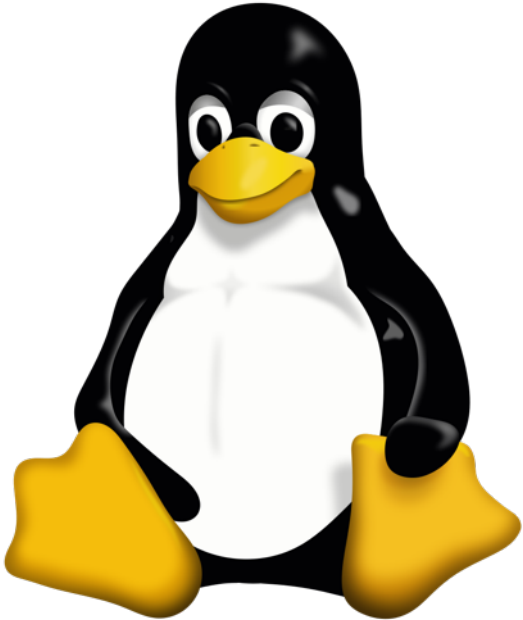
64990 total (3 Err / 5731 HCI / 7727 ACL / 0 SCO / 11448 Misc)

Type	Handle	Decoded Packet
NOTE		**** [IOBluetoothHostControllerUSBTransport][BulkOutWriteCompleteAction] --
HII receive	0x000B	▶HID Interrupt: [A1] Trackpad (Button:0 Timestamp 4141211)[28] Event Data [
HCI EVENT	0x000C	▶Number of Completed Packets - Connection Handle: 0x000C - Packets: 0x0001
KERNEL DEBUG		▶**** [IOBluetoothHostController][ProcessNumberOfCompletedPacketsEvent] --
NOTE		**** [IOBluetoothDevice][decrementNumberOfOutstandingPacketsBy] -- Handle
KERNEL DEBUG		▶**** [IOBluetoothHostController][ProcessNumberOfCompletedPacketsEvent] --
KERNEL DEBUG		▶**** [IOBluetoothHostController][DecrementOutstandingACLPackets] - decreme
HII receive	0x000B	▶HID Interrupt: [A1] Trackpad (Button:0 Timestamp 4141222)[28] Event Data [
KERNEL DEBUG		▶**** [IOBluetoothHostControllerUSBTransport][BulkOutWrite] -- add Bulk Out
KERNEL DEBUG		▶**** [IOBluetoothHostController][SendACLData] -- Handle 0x000c -- Before s
KERNEL DEBUG		▶**** [IOBluetoothHostController][SendACLData] -- Connection Handle 0x000c
AVDTP SEND	0x000C	▶SBC Audio Data - Sequence 13305 - Size: 603 (0x25B) - Frames: 5 - Bitpool:
KERNEL DEBUG		▶**** [IOBluetoothHostController][TransferACLPacketToHW] -- Handle 0x000C -
NOTE		**** [IOBluetoothHostControllerUSBTransport][BulkOutWriteCompleteAction] --
HCI EVENT	0x000C	▶Number of Completed Packets - Connection Handle: 0x000C - Packets: 0x0001
KERNEL DEBUG		▶**** [IOBluetoothHostController][ProcessNumberOfCompletedPacketsEvent] --
NOTE		**** [IOBluetoothDevice][decrementNumberOfOutstandingPacketsBy] -- Handle
KERNEL DEBUG		▶**** [IOBluetoothHostController][ProcessNumberOfCompletedPacketsEvent] --
KERNEL DEBUG		▶**** [IOBluetoothHostController][DecrementOutstandingACLPackets] - decreme
HII receive	0x000B	▶HID Interrupt: [A1] Trackpad (Button:0 Timestamp 4141233)[28] Event Data [
KERNEL DEBUG		▶**** [IOBluetoothHostControllerUSBTransport][BulkOutWrite] -- add Bulk Out
KERNEL DEBUG		▶**** [IOBluetoothHostController][SendACLData] -- Handle 0x000c -- Before s
KERNEL DEBUG		▶**** [IOBluetoothHostController][SendACLData] -- Connection Handle 0x000c
AVDTP SEND	0x000C	▶SBC Audio Data - Sequence 13306 - Size: 603 (0x25B) - Frames: 5 - Bitpool:
KERNEL DEBUG		▶**** [IOBluetoothHostController][TransferACLPacketToHW] -- Handle 0x000C -
NOTE		**** [IOBluetoothHostControllerUSBTransport][BulkOutWriteCompleteAction] --

ICE9
CONSULTING

by payatu

Linux Logging



```
$ sudo btmon -w logfile.log
```

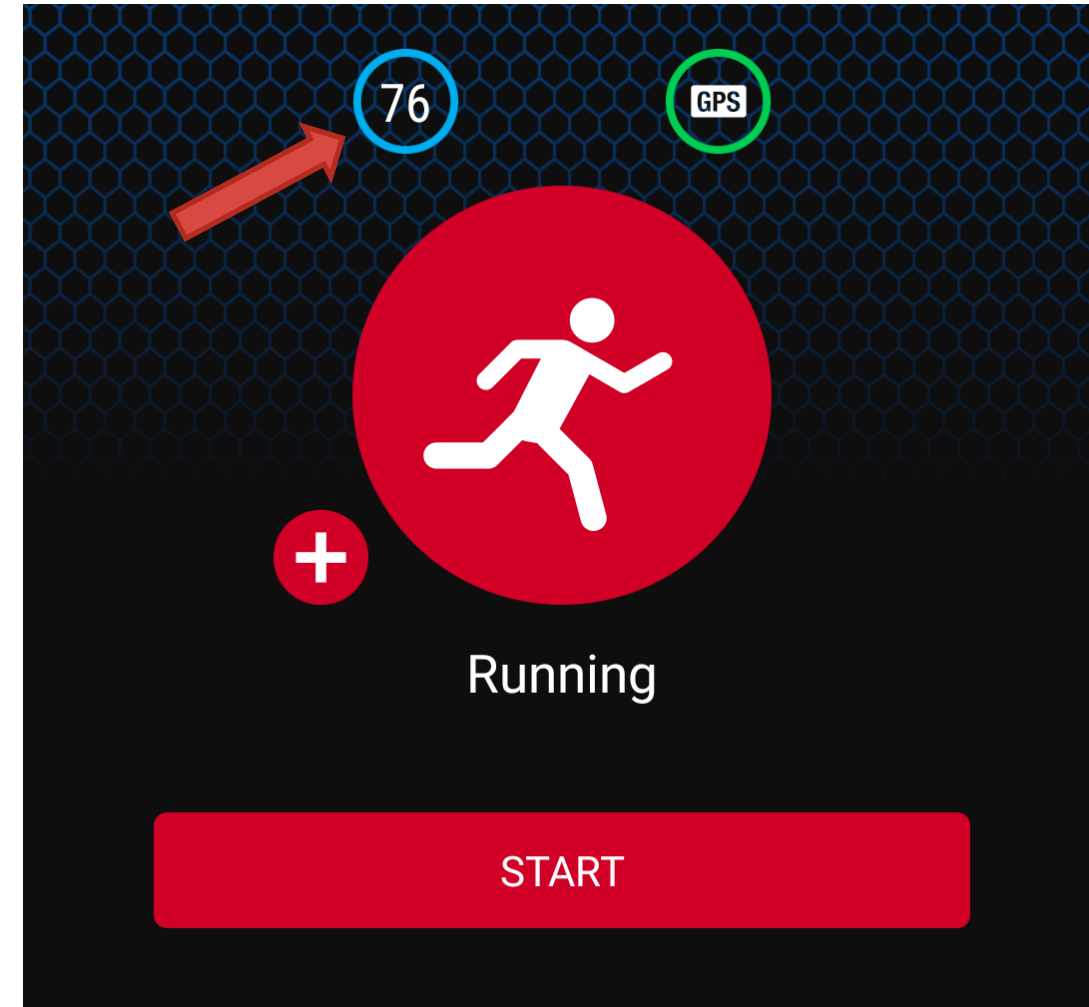

Reverse Engineering Process

1. Do something with the device and app
2. Capture the data sent via Bluetooth
3. Analyze



Case Studies

Case Study 1: BLE Heart Rate Monitor



01_hrm.log

btatt

No.	Time	Source	Destination	Protocol	Length	Info
1517	0.990614		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1518	0.992877		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1532	0.977430		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1552	1.483901		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1553	0.496208		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1554	0.999473		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1555	0.990111		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1556	0.989773		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1557	0.990310		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1558	1.485342		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1559	0.494066		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1560	0.990667		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1561	0.989790		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1562	0.990521		_00:0...	localhost...	ATT	16 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
1576	0.980326		_00:0...	localhost...	ATT	18 Rcvd Handle Value Notification, Handle: 0x0011 (Heart Rate: Heart Rate Measurement)

▶ Bluetooth HCI H4

▶ Bluetooth HCI ACL Packet

▶ Bluetooth L2CAP Protocol

▼ Bluetooth Attribute Protocol

- ▶ Opcode: Handle Value Notification (0x1b)
 - ▶ Handle: 0x0011 (Heart Rate: Heart Rate Measurement)
 - ▶ Flags: 0x16, RR Interval, Sensor Support, Sensor Contact Value: 82
 - ▼ RR Intervals [count = 1]
 - RR Interval: 729

01_hrm

82

btatt

bthci_cmd.le_long_tem_key

No encryption

Case Study 1: Conclusions

- Wireshark is incredible
- Getting Bluetooth logs is practical


```
# gatttool -b 00:18:00:00:00:7E --primary
attr handle = 0x0001, end grp handle = 0x000b
uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle = 0x000c, end grp handle = 0x000e
uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle = 0x000f, end grp handle = 0x0014
uuid: 0000180d-0000-1000-8000-00805f9b34fb
attr handle = 0x0015, end grp handle = 0x0023
uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle = 0x0024, end grp handle = 0x0026
uuid: 0000180f-0000-1000-8000-00805f9b34fb
attr handle = 0x0027, end grp handle = 0xffff
uuid: 6217ff49-ac7b-547e-eecf-016a06970ba9
```

Case Study 2: BLE Blood Pressure Monitor



02_bpmon.log

btatt.value

No.	Time	Source	Destination	Protocol	Length	Info
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x000e (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0016 (Unknown)
...	0.0...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x0015 (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
→	0.0...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x000d (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
...	0.1...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x000d (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)

▶ Frame 460: 29 bytes on wire (232 bits), 29 bytes captured (232 bits)

▶ Bluetooth

▶ Bluetooth HCI H4

▶ Bluetooth HCI ACL Packet

▶ Bluetooth L2CAP Protocol

▶ Bluetooth Attribute Protocol

▶ Opcode: Handle Value Indication (0x1d)

▶ Handle: 0x000d (Peripheral Preferred Connection Parameters: Unknown)

Value: 3e75005100000062535510610001000001

[Response in Frame: 461]

0000 02 06 20 18 00 14 00 04 00 1d 0d 00 3e 75 00 51 ..>u.Q

0010 00 00 00 62 53 55 10 61 00 01 00 00 01 ...bSU.a

Value (btatt.value), 17 bytes

Packets: 508 · Displayed: 17 (3.3%) · Load time: 0:0.36

Profile: Default

Protocol Specifications

GATT Specifications

- GATT Overview
- GATT Characteristics
- GATT Declarations
- GATT Descriptors
- GATT Services**
- Mesh GATT Services XML
- Available Schemas

Errata Service Releases

Qualification Test Requirements

Assigned Numbers

Specifications in Development

Interoperable Prototype Test Events (IOP)

Name	Uniform Type Identifier	Assigned Number	Specification
Generic Access	org.bluetooth.service.generic_access	0x1800	GSS
Alert Notification Service	org.bluetooth.service.alert_notification	0x1811	GSS
Automation IO	org.bluetooth.service.automation_io	0x1812	GSS
Battery Service	org.bluetooth.service.battery_service	0x181F	GSS
Blood Pressure	org.bluetooth.service.blood_pressure	0x182B	GSS
Body Composition	org.bluetooth.service.body_composition	0x182C	GSS
Bond Management Service	org.bluetooth.service.bond_management	0x182E	GSS
Continuous Glucose Monitoring	org.bluetooth.service.continuous_glucose_monitoring	0x1831	GSS
Current Time Service	org.bluetooth.service.current_time	0x1832	GSS
Cycling Power	org.bluetooth.service.cycling_power	0x183E	GSS
Cycling Speed and Cadence	org.bluetooth.service.cycling_speed_and_cadence	0x183F	GSS
Device Information	org.bluetooth.service.device_information	0x183A	GSS
HTTP Proxy	org.bluetooth.service.http_proxy	0x1823	GSS



Write characteristic: Phone → Device

Notify characteristic: Device → Phone

02_bpmon.log

btatt.value

No.	Time	Source	Destination	Protocol	Length	Info
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x000e (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0016 (Unknown)
...	0.0...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x0015 (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
→	0.0...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x000d (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)
...	0.1...	e7:59:...	loca...	A...	...	Rcvd Handle Value Indication, Handle: 0x000d (Unknown)
...	0.0...	localh...	e7:5...	A...	...	Sent Write Request, Handle: 0x0013 (Unknown)

▶ Frame 460: 29 bytes on wire (232 bits), 29 bytes captured (232 bits)

▶ Bluetooth

▶ Bluetooth HCI H4

▶ Bluetooth HCI ACL Packet

▶ Bluetooth L2CAP Protocol

▼ Bluetooth Attribute Protocol

▶ Opcode: Handle Value Indication (0x1d)

▶ Handle: 0x000d (Peripheral Preferred Connection Parameters: Unknown)

Value: 3e75005100000062535510610001000001

[\[Response in Frame: 461\]](#)

0000	02 06 20 18 00 14 00 04	00 1d 0d 00 3e 75 00 51>u.Q
0010	00 00 00 62 53 55 10 61	00 01 00 00 01	...bSU.a

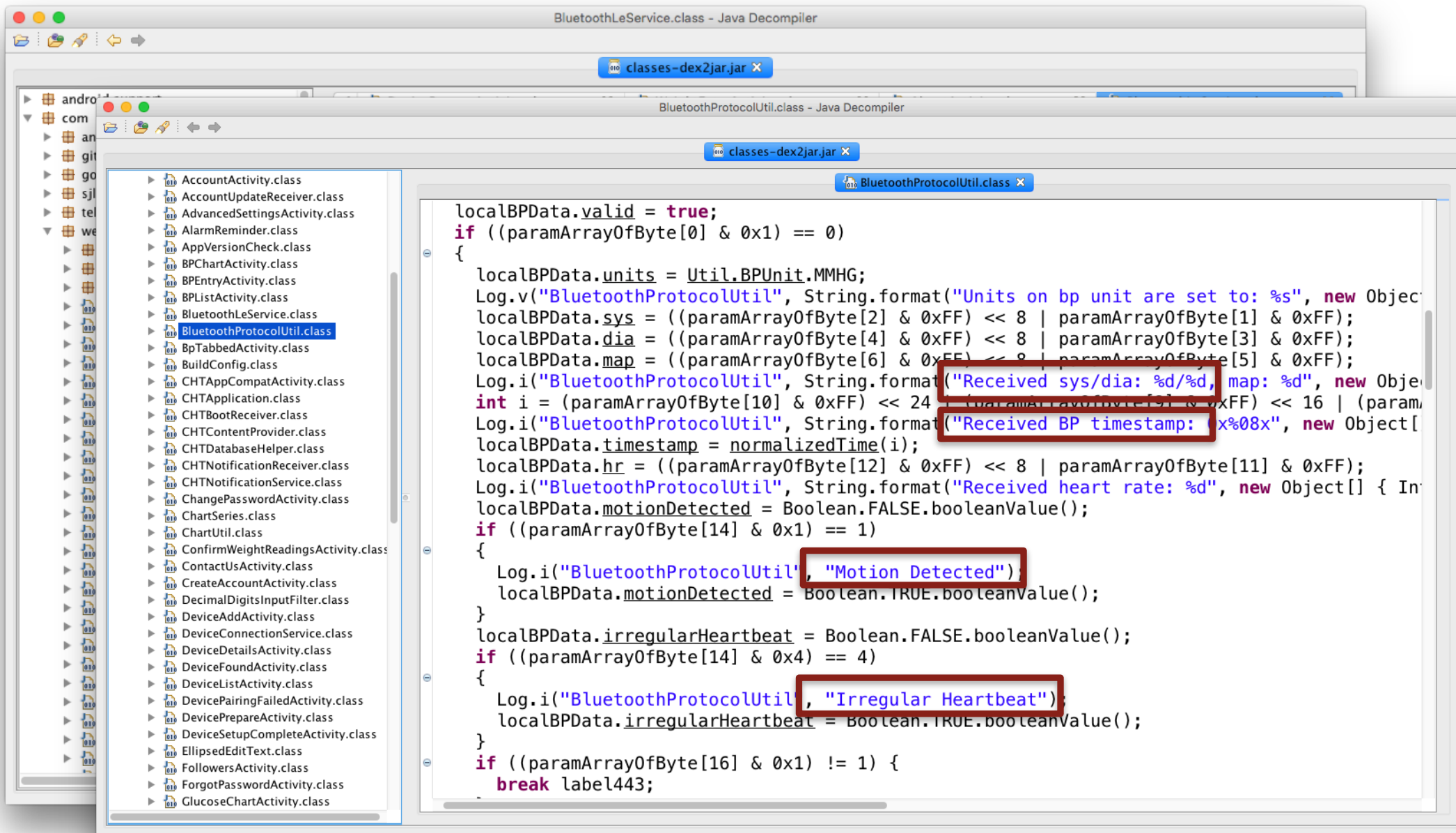
Value (btatt.value), 17 bytes

Packets: 508 · Displayed: 17 (3.3%) · Load time: 0:0.36

Profile: Default

75 00 51 00

117 / 81

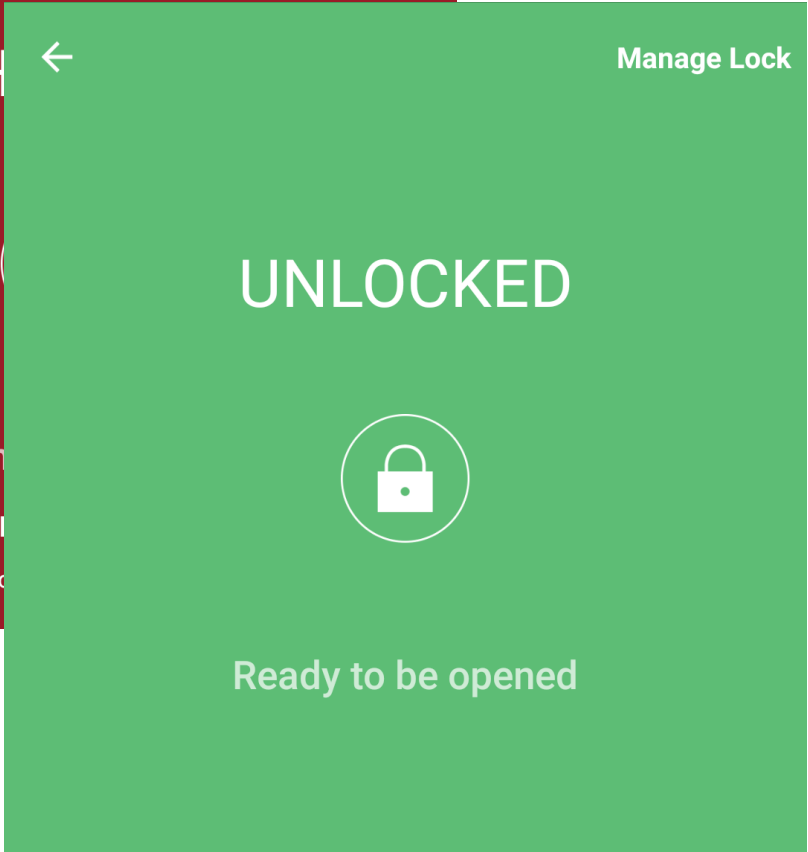
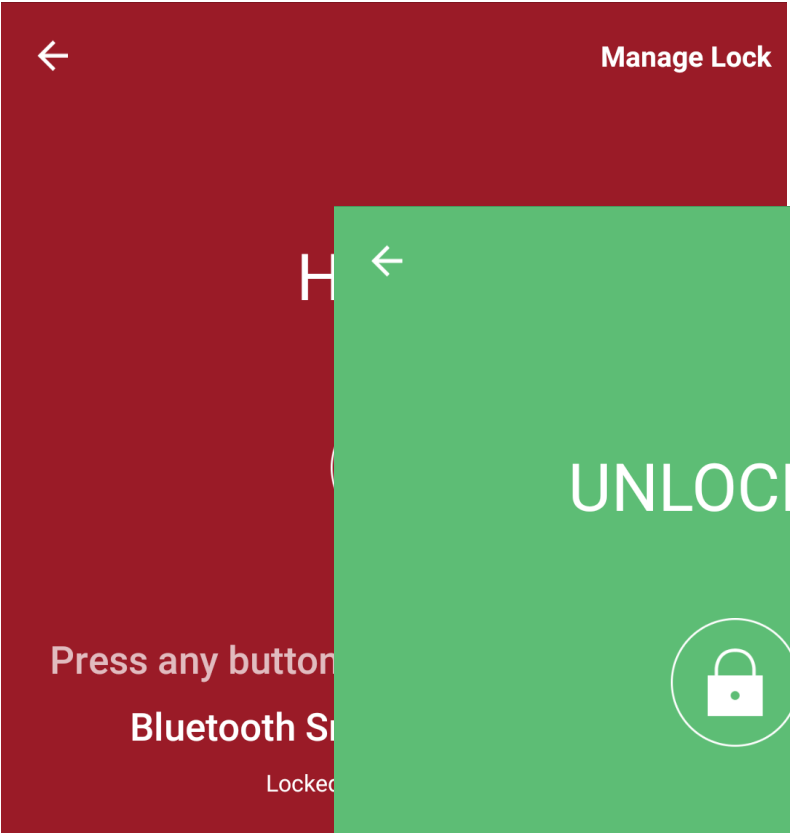


Conclusions: BP Monitor

- “Hidden” serial port
- Normal binary protocol reverse engineering
- Look in the app

Once again – No Encryption
Firmware Update Service

Case Study 3: BLE Padlock



btatt.value && !btatt.opcode == 0x17

No.	Time	Source	Destination	Protocol	Length	Info
...	0.0...	TexasI...	loca...	A...	...	Rcvd Read Blob Response, Handle: 0x000d (Unknown)
...	0.0...	localh...	Texa...	A...	...	Sent Prepare Write Request, Handle: 0x000d (Unknown), Offse
...	0.0...	localh...	Texa...	A...	...	Sent Prepare Write Request, Handle: 0x000d (Unknown), Offse
...	0.1...	TexasI...	loca...	A...	...	Rcvd Handle Value Notification, Handle: 0x000d (Unknown)
...	0.0...	TexasI...	loca...	A...	...	Rcvd Read Response, Handle: 0x000d (Unknown)
...	0.1...	localh...	Texa...	A...	...	Sent Prepare Write Request, Handle: 0x000d (Unknown), Offse
→ ...	0.0...	localh...	Texa...	A...	...	Sent Prepare Write Request, Handle: 0x000d (Unknown), Offse
...	0.1...	TexasI...	loca...	A...	...	Rcvd Handle Value Notification, Handle: 0x000d (Unknown)
...	0.0...	localh...	Texa...	A...	...	Sent Write Command, Handle: 0x000d (Unknown)

Frame 454: 18 bytes on wire (144 bits), 18 bytes captured (144 bits)

- Bluetooth
- Bluetooth HCI H4
- Bluetooth HCI ACL Packet
- Bluetooth L2CAP Protocol
- Bluetooth Attribute Protocol
 - Opcode: Prepare Write Request (0x16)
 - Handle: 0x000d (Unknown)
 - Offset: 18
 - Value: 8aa5f5a4

[Response in Frame 456]

0000 02 09 00 0d 00 09 00 04 00 16 0d 00 12 00 8a a5

0010 f5 a4 ..

Value (btatt.value), 4 bytes

Packets: 502 · Displayed: 79 (15.7%) · Load time: 0:0.11 · Profile: Default

- Open ⌘O
- Open Recent ▶
- Merge...
- Import from Hex Dump...
- Close ⌘W
- Save ⌘S
- Save As... ⌥⌘S
- File Set ▶
- Export Specified Packets...
- Export Packet Dissections ▶
- Export Packet Bytes... ⌥⌘X
- Export PDUs to File...
- Export SSL Session Keys...
- Export Objects ▶
- Print... ⌘P

01_bpmo

← → → ↕

Source

host

controller

post

- As Plain Text...
- As CSV...
- As "C" Arrays...
- As PSML XML...
- As PDML XML...
- As JSON...

```
> 00808ce41b91c80036cec999ac3b3c28 .....6....;<(  
8a59 .Y  
> 6734e9599d67aeb9872a2d4b53be37e g4.Y.g...r...;~  
ce27 .'  
> a85ee6a4473b75bb5d728fe4ebfd27f4 .^..G;u.]r....'.  
fd4b .K  
> ca320ac80767c32b841ef0929ea5c18c .2...g.+.....  
< 00000000000083000194d8e91bb0c96b .....k  
d444 .D  
> 010002ad84a3d26928e0ed4172 .....i(..Ar...  
< 000002ea7d3f471955503efa55 .....}?G.UP>.U...  
> 010002b06544063fe042eaa7d7 .....eD.?.B.....  
< 0000015e4811134b373fb3e4 ...^H..K7?.....  
> 0100024221a30f917f9d19ceea ...B!.....  
> 0118 .....  
> 0100 .....  
> 00808ce41b91c80036cec999ac3b3c28 .....6....;<(  
8a59 .Y  
> 6734e9599d67aeb9872a2d4b53be37e g4.Y.g...r...;~  
ce27 .'  
> a85ee6a4473b75bb5d728fe4ebfd27f4 .^..G;u.]r....'.  
fd4b .K  
> ca320ac80767c32b841ef0929ea5c18c .2...g.+.....  
< 0000000000008a00016f436989f42194 .....oCi...!.
```

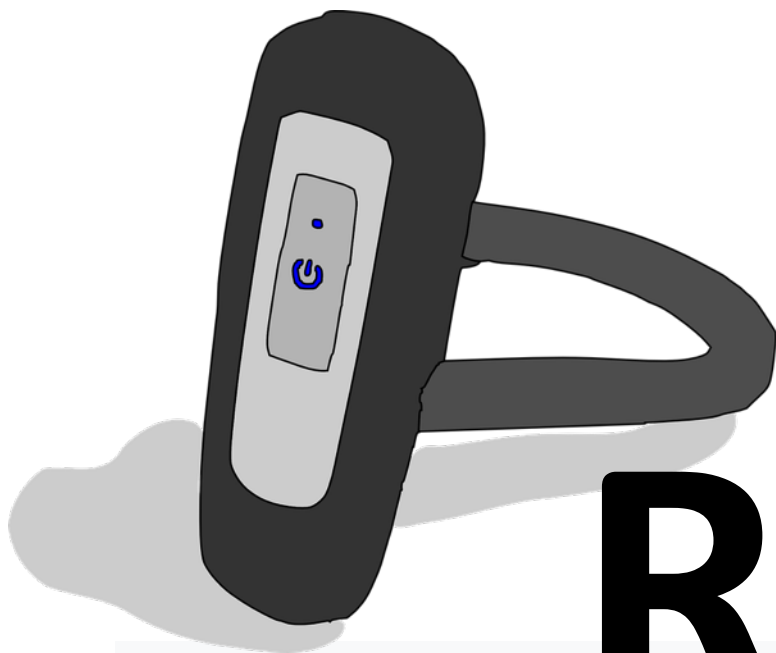
```
< 0000fc471c5c1af03acce70b6ec3ccf5 ...G.\...:...n...
598df50e Y...
< 0000fc471c5c1af03acce70b6ec3ccf5 ...G.\...:...n...
598df50ee3eb Y.....
< 950160f487ea7a466ad695bdf5449e84 ..`...zFj....D..
a4dcf6caf107 .....
< 12cbbcbcbcbaddf6a63490de5cccfb06e .....jcI.....n
8131b9837d59 .1..}Y
< 4913c26fa48a3a4f4ad0749d8008b354 I..o...:0J.t....T
47f268342f1a G.h4/.
< 9e744503851202bdf9325d70c4e5289c .tE.....2]p..(.
41b23b3ef53e A.;>.>
< 303d998fc096bab541302735f0b5b31e 0=.....A0'5....
dd5025648464 .P%d.d
< ec077985c022bee9147b9eef05cbe206 ..y.."...{.....
8655136b2a11 .U.k*.
< 6b5904fea330e3f6b5f5b9cf9c41ecc8 kY...0.....A..
23a2cfddace1 #.....
< dd634cf217bb94425130c536688526e4 .cL....BQ0.6h.&.
5675584537f3 VuXE7.
< 6e4b2bee8cbeb78b617058d21bfca6b3 nK+.....apX.....
bf17fd3d84d3 ...=..
< f8d186e94f0a6910d58ee27d651050a7 ....0.i....}e.P.
167dbb8d3dad .}..=.
```

Conclusions: Padlock

- Developers were security-minded
- Home-grown crypto is fraught with peril

Intermission

Case Study 4: Classic Bluetooth Headset



~~A2DP? HFP?~~

Reasons

- 29 Proximity Profile (PP)
- 30 Serial Port Profile (SPP)
- 31 Service Discovery Application Pr
- 32 SIM Access Profile (SAP, SIM, r



data							Expression...	
No.	Time	Source	Destination	Protocol	Length	Info		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	23	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	23	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	localh...	Bang...	RFCOMM	664	Sent UIH Channel=1		
...	0.0...	BangAn...	loca...	RFCOMM	29	Rcvd UIH Channel=1		

▶ Frame 206: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits)

▶ Bluetooth

▶ Bluetooth HCI H4

▶ Bluetooth HCI ACL Packet

▶ Bluetooth L2CAP Protocol

▶ Bluetooth RFCOMM Protocol

▼ Data (650 bytes)

Data: 0048ff16010cff70fffb00c3ff0f005e0010ffbf00beff7b...

[Length: 650]

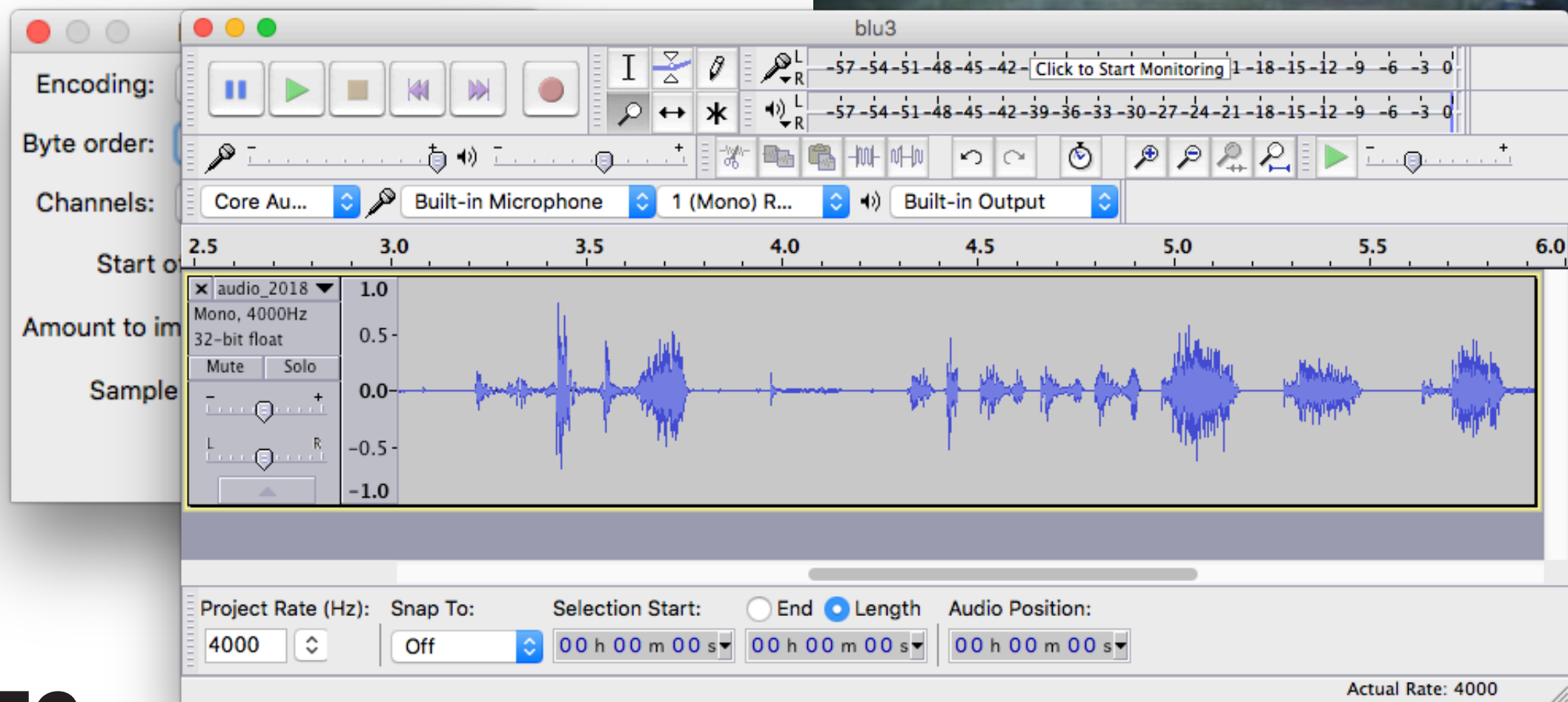
0000	02 0c 00 93 02 8f 02 44 00 0b ef 14 05 00 48 ffDH.
0010	16 01 0c ff 70 ff fb 00 c3 ff 0f 00 5e 00 10 ffp... ..^...

80	77	DD	AF	magic number
XX				opcode
YY				sequence number
ZZ	ZZ			length (16 bit little endian)
...				data
CC	CC			checksum

```
< [81] 80807f7f .....
< [85] 03000c80000300011000 .....
> [08] 01000000 .....
< [88] 00120008 .....
< [8b] ffffffffaffe0ffe8000fffc40006001c .....
      ffa9001effcbffc7003bffc5001c0010 .....;.....
      ffd001dffb20003ffd7ffb8ffefffc5 .....
      ffe2ffeaffcb0008000affef0019fff2 .....
      00000008001000130006fffa001d001c .....
      ffccffa0003ffcafff20005ffc9000b .....
      fffaaffec003effc7fffe0021ffe30032 .....>.....!...2
      00040022000bffe003dffe1001efffc ..."......=.
      d2f4 .....
< [8b] ffdc003cffe7000a0015ffd90019ffe4 ...<.....
      fff10024ffaa0013000effcd0007ffe0 ...$.
      ffeaffcfff9ffe5ffc7ffe0ffccffa1 .....
      ffedffcaffb8ffdbffa4ffd7ffd7ffd6 .....
      ffd5ffaaffbfff3ffe1ffc6ff9dffec .....
      ffd7ffa1ffd7ffc1ffc8ffdaffdffea .....
      ffc4fff8ffc6ffcbfff1ffccffecffd2 .....
      ffecffecfffd001dffcbffdfccbfdd5 .....
      af76 .....v.....
< [8b] 0006ffe9000dffffdffe40006fff40004 .....
      0013fffe0008fff3ffeaffef000affef .....
```



Audacity®



Conclusions: Headset

- The techniques apply equally well to BR and BLE
- Ultimately boils down to basic RE

Case Study 5: BLE Credit Card



What is a Bluetooth credit card?



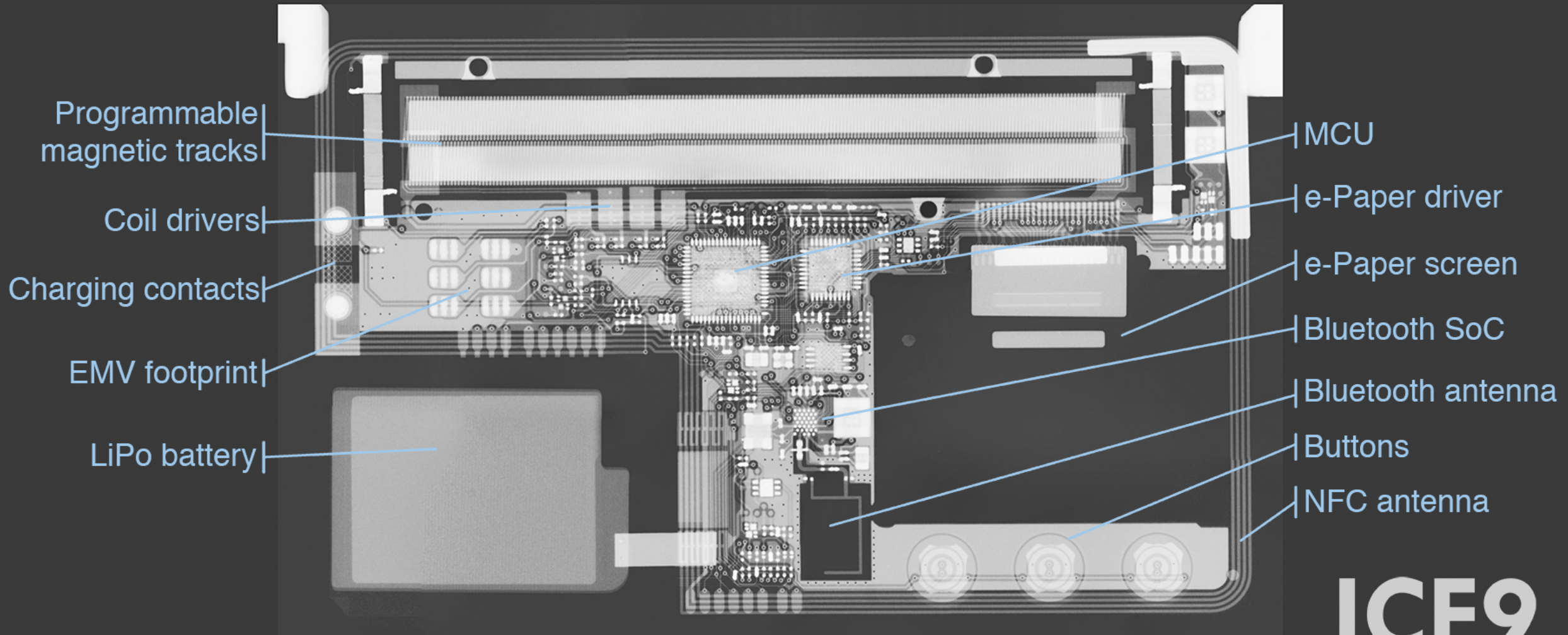
+



=



Bluetooth credit card



X-ray by John McMaster (@johndmcmaster)

ICE9
CONSULTING
<https://ice9.us/>

delete.log

bthci_cmd.le_long_tem_key

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
→ ...	0.0...	host	cont...	HCI_C...	32	Sent LE Start Encryption

▶ Frame 778: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)

▶ Bluetooth

▶ Bluetooth HCI H4

▼ Bluetooth HCI Command – LE Start Encryption

- ▶ Command Opcode: LE Start Encryption (0x2019)
Parameter Total Length: 28
Connection Handle: 0x0002
Random Number: 0000000000000000
Encrypted Diversifier: 0x0000
Long Term Key: 8dfa9078fe07e28c8c68fe142adf1d37
[\[Pending in frame: 779\]](#)
[Command-Pending Delta: 15.089ms]

0010 8d fa 90 78 fe 07 e2 8c 8c 68 fe 14 2a df 1d 37 ...x.... .h..*..7

Long Term Key (bthci_cmd.le_long_tem_key), 16 bytes

Packets: 1350 · Displayed: 1 (0.1%) · Load time: 0:0.15

Profile: Default

ICE9
CONSULTING

by payatu

- XX – opcode
- YY – total number of messages
- ZZ – current message
- WW – checksum

Conclusions: Credit Card

- HCI logging allows us to see encrypted data
- Encryption isn't a silver bullet

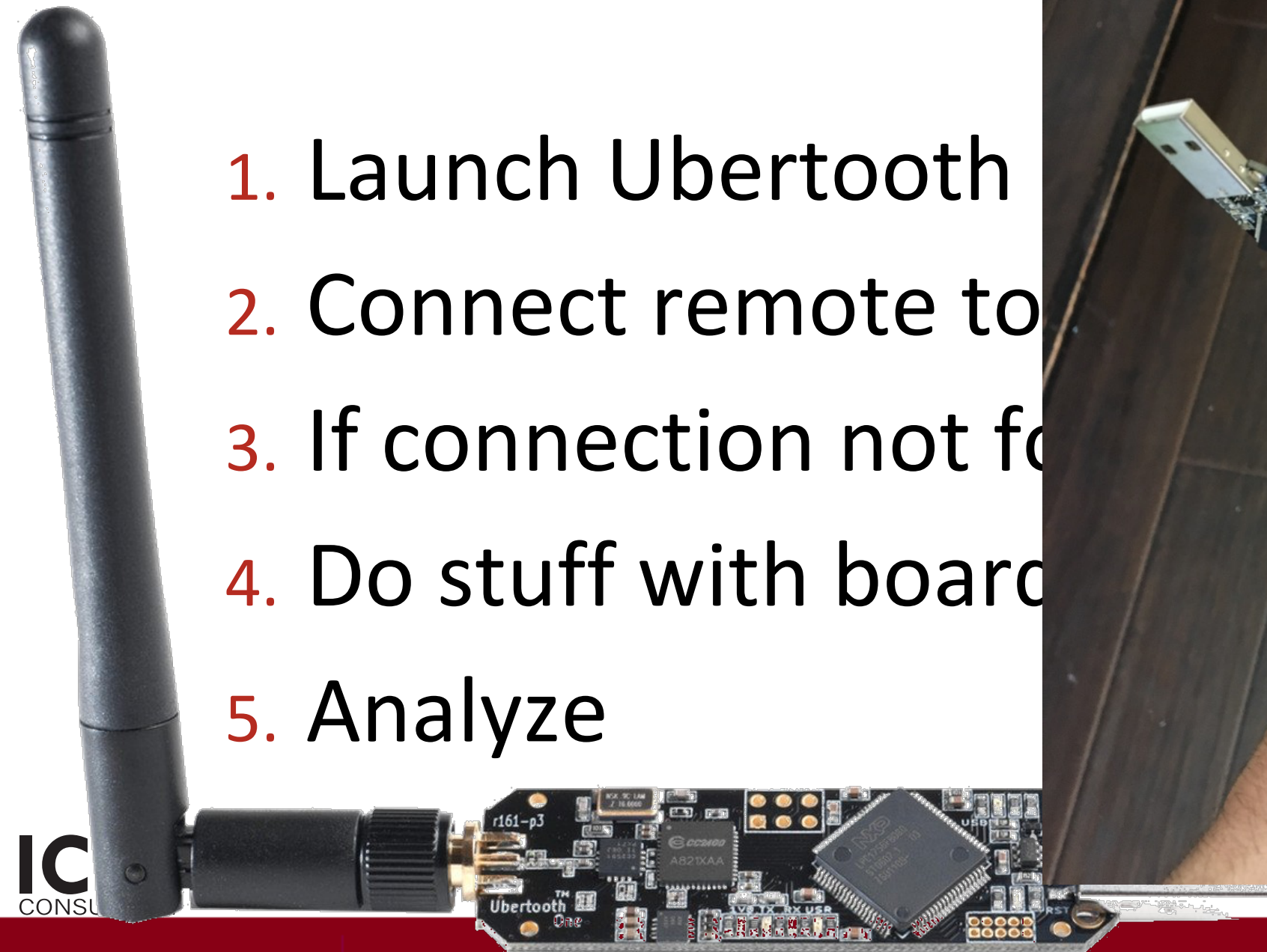
Case Study 6: BLE Electric Skateboard



No App!



1. Launch Ubertooth
2. Connect remote to
3. If connection not fo
4. Do stuff with board
5. Analyze

IC
CONS

01_connection.pcapng

(btatt.opcode == 0x1d) || (btatt.handle == 0x0013)

No.	Time	Source	Destination	Protocol	Length	Info
1830	0.015483	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1844	0.067138	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1850	0.029968	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1856	0.030261	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1862	0.029887	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
→ 1870	0.030028	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1878	0.029732	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1884	0.030005	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
1891	0.030530	Unknown_0x6477b343	Unknown_0...	ATT	48	UnknownDirection Write Request, Handle: 0x001a (Unknown)
						0x001a (Unknown)
						0x001a (Unknown)
						0x001a (Unknown)
						0x001a (Unknown)
						0x001a (Unknown)
						0x001a (Unknown)

Frame 1870 (48 bytes) on interface (blue...)

PPI

DLT: Bluetooth

Blue...

Blue...

Bluetooth Attribute Protocol

▶ Opcode: Write Request (0x12)

Handle: 0x001a (Unknown)

Value: 524330323332370d

[\[Response in Frame: 1874\]](#)

0000 00 00 18 00 93 00 00 00 36 75 0c 00 00 7e 09 00 6u...~..

0010 22 b9 4b 7b 80 7f 00 00 43 b3 77 64 0e 0f 0b 00 ".K{...Gnd..."

0020 04 00 12 1a 00 52 43 30 32 33 32 37 0d bd a8 be ... RC0 2327. ...

Opcode (btatt.opcode), 1 byte

Packets: 2821 - Displayed:

No Encryption



RC00000

idle

RC02002

dead man's trigger

RC02327

RC027D6

RC02AA6

RC032F4

increasing throttle



Conclusions: Skateboard

- Ubertooth is much harder to use than HCI logging
- If using encryption, have to crack

Parting Thoughts

Most Common Security Problems

- No encryption
- Problems with home made encryption
- Debug interfaces left behind
- Incomplete threat modeling

Conclusions

Affordable

RE Process and Tools

Case Studies

Call to Action

Go forth and hack some Bluetooth

Bluetooth Hacking: Tools and Techniques

<https://ice9.us/>

mike@ice9.us

ICE9
CONSULTING