Security of *Bluetooth* Network Data Traffic

Michael Grant Williams
DoD Contractor
Iowa State University
Ph.D. Student,
IEEE Student Member

Agenda

- About the author
- Security Issue or Vulnerability
- Bluetooth Threats
- Introduction on project
- Background of project
  - Tools used
  - Test method
  - Test results
  - Mitigation solutions
- Future research
- Questions
- References

About The Author

- Employed by the Garrett Group
  - DoD contractor – J84 GSIN Team
- IT Certifications
  - CISSP
  - CEH
  - Cisco – CCNA / Security / Wireless
  - Microsoft – MCSE / MSITP / MCP
  - CompTia – A+ / Network + / Security+
  - ITIL Foundations

- Education
  - Ph.D. student at Iowa State University (ISU)
    - Computer Networking Systems / Secure and Reliable Computing
  - University of Nebraska at Omaha
    - Masters in MIS / Grad certification in Information Assurance
    - Bachelors in MIS
    - Bachelors in Banking and Finance
  - Rock Valley Community College
    - Associates in Aviation Maintenance (Airframe and Power-plant certified)

All Bluetooth Versions (Ref 23)	**Security Issue or Vulnerability**	Remarks
18	Link keys can be stored improperly.	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls
19	Strengths of the pseudo-random number generators (PRNG) are not known.	The Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the security mechanisms. Bluetooth implementations should use strong PRNGs based on NIST standards.
20	Encryption key length is negotiable.	The v3.0 and earlier specifications allow devices to negotiate encryption keys as small as one byte. Bluetooth LE requires a minimum key size of seven bytes. NIST strongly recommends using the full 128-bit key strength for both BR/EDR (E0) and LE (AES-CCM).
21	No user authentication exists.	Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer.
22	End-to-end security is not performed.	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls.
23	Security services are limited.	Audit, non-repudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.
24	Discoverable and/or connectable devices are prone to attack.	Any device that must go into discoverable or connectable mode to pair or connect should only do so for a minimal amount of time. A device should not be in discoverable or connectable mode all the time.

Bluetooth Threats (Ref 23)

Bluesnarfing BTLE is NA	Enables attackers to gain access to a Bluetooth-enabled device by exploiting a **firmware flaw in older devices**. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device including the device's international mobile equipment identity (IMEI).
Bluejacking	Is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they may entice the user to respond in some fashion or add the new contact to the device's address book
Bluebugging BTLE is NA	Exploits a **security flaw in the firmware of some older Bluetooth devices** to gain access to the device and its commands. This attack uses the commands of the device without informing the user
Car Whisperer NA within **Wearable Tech**	Is a software tool developed by European security researchers that exploits a key implementation issue in hands-free Bluetooth car kits installed in automobiles. The Car Whisperer software allows an attacker to send to or receive audio from the car kit.
Denial of Service	Bluetooth **is susceptible to DoS attacks**. Impacts include making a device's **Bluetooth interface unusable and draining the device's battery**. These types of attacks are not significant and, because of the proximity required for Bluetooth use, can usually be easily averted by simply moving out of range.
Fuzzing Attacks **Future Research Project**	Fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. If a **device's operation is slowed or stopped by these attacks, a serious vulnerability potentially exists in the protocol stack**
Pairing Eavesdropping **Current Research Project**	PIN/Legacy Pairing (Bluetooth 2.0 and earlier) and LE Pairing (Bluetooth 4.0) are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s) given sufficient time, which allows trusted device impersonation and active/passive data decryption.
Secure Simple Pairing Attacks	A number of techniques can force a remote device to use **Just Works SSP and then exploit its lack of MITM protection (e.g., the attack device claims that it has no input/output capabilities**). Further, fixed passkeys could allow an attacker to perform MITM attacks as well.

Introduction

- This research project focused on the security of the *Microsoft Band 2* fitness tracker.
- This project is to investigation how secure data is when transmitted via *Bluetooth* to and from a wearable device.
- This project answered three research questions; (1) Is the pairing key transmitted in the clear
- (2) Is Bluetooth traffic transmitted in the clear
- (3) Could a Man in The Middle Attack (MITMA) take place.

Introduction

- *MS Band 2* has been available for purchase since November 1, 2015, so it is relativity new
- MS Band 3 is schedule for release November 2016
- Conducted literature regarding wearable technology and various findings in device security, vulnerabilities, threats, weaknesses, and viable mitigation solutions. (see reference section)
- Similar research was done on a Fitbit by Cyr, B., Horn, W., Miao, D., & Specter, M. At Massachusetts Institute of Technology Security Analysis of Wearable Fitness Devices (Fitbit) (2014) – Ref 06.

Background – Tools used

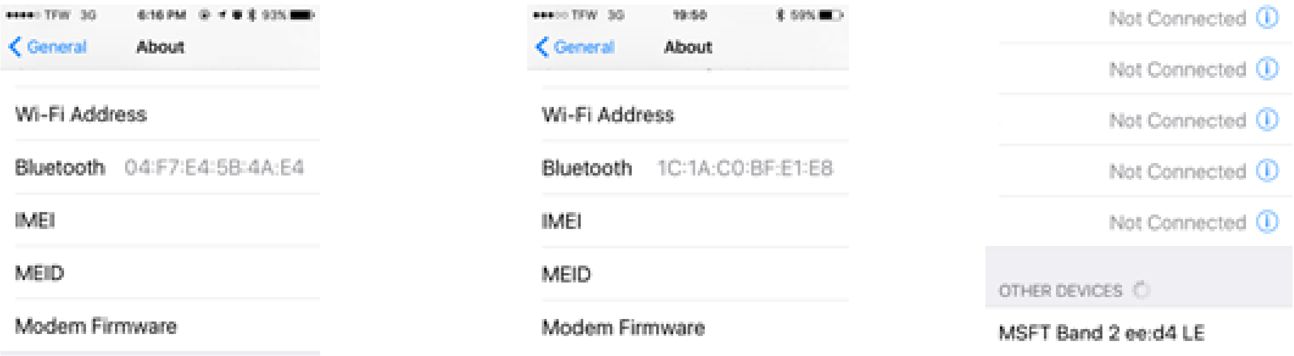
- Original Research Project
  - Kali Linux (VM Ware & Flash drive)
  - Ubertooth One (Linux only)
  - Wireshark
  - Texas Instrument
    - Bluetooth Low Energy Software Stack
    - CC2540 USB Dongle
  - Nordic Semiconductor
    - nRF Sniffer software (works in conjunction with Wireshark)
    - nRF51822 USB Dongle
  - 2 IPhones - most recent IOS – 9.2.1
  - MS Band 2 fitness tracker & mobile app

Background Test Method

- Issues / Trouble with System configuration
  - Kali Linux - Not operating in virtual environment
    - Kismet would operate for a few minutes then crash
  - USB Kali Linux
    - Ubertooth One using Kismet not all detecting Bluetooth devices
    - Wireshark provide invalid data due to devices not being detected
- Opted to use other tools since Kali Linux and Ubertooth was not functioning correctly
  - Texas Instrument products provided unreliable results
  - Nordic Semiconductor products was inconsistent results
    - Results to be discussed later

Background Test Method

- Research project configuration



TFW 3G 6:16 PM 93%

< General About

Wi-Fi Address

Bluetooth 04:F7:E4:5B:4A:E4

IMEI

MEID

Modem Firmware

TFW 3G 19:50 59%

< General About

Wi-Fi Address

Bluetooth 1C:1A:C0:BF:E1:E8

IMEI

MEID

Modem Firmware

Not Connected

Not Connected

Not Connected

Not Connected

Not Connected

OTHER DEVICES

MSFT Band 2 ee:d4 LE

Figure 3:

Primary *IPhone* Secondary *IPhone* *MS Band 2*

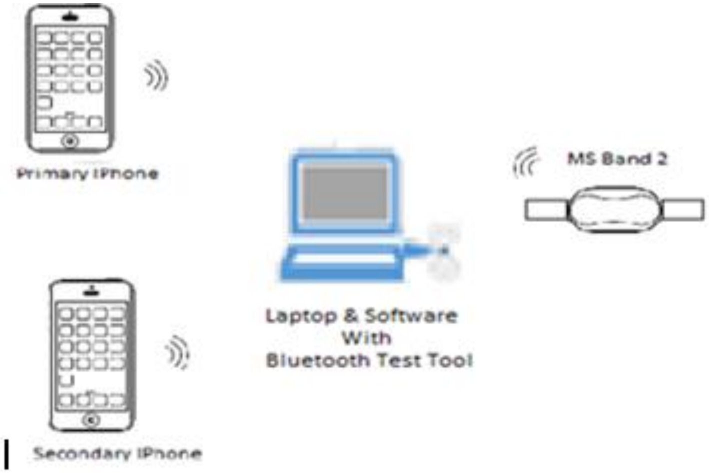
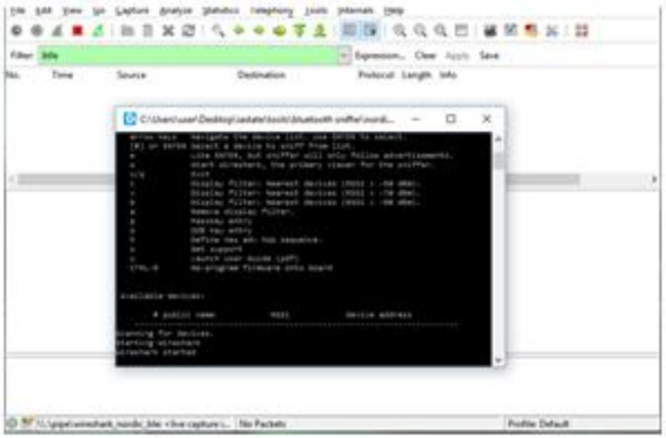


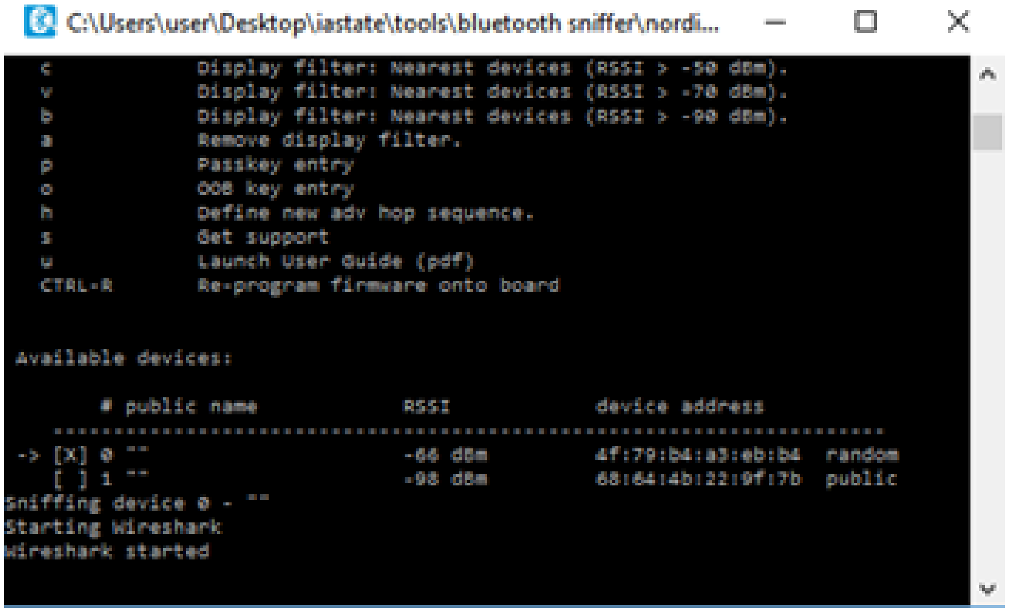
Figure 4: Overview of the controlled lab environment

Background Test Method

- Research project configuration
- Bluetooth Device Address
  - Public Address
    - Known static address
  - Random Address
    - Unknown dynamic address
    - Offer better security



```
C:\Users\user\Desktop\iastate\tools\bluetooth sniffer\nordi...
  arrow keys   Navigate the device list, use ENTER to select.
  [X] or ENTER Select a device to sniff from list.
  a            Like ENTER, but sniffer will only follow advertisements.
  w            Start Wireshark, the primary viewer for the sniffer.
  q/Q          Exit
  c            Display filter: Nearest devices (RSSI > -50 dBm).
  v            Display filter: Nearest devices (RSSI > -70 dBm).
  b            Display filter: Nearest devices (RSSI > -90 dBm).
  a            Remove display filter.
  p            Passkey entry
  o            OOB key entry
  h            Define new adv hop sequence.
  s            Get support
  u            Launch User Guide (pdf)
  CTRL-R       Re-program firmware onto board

Available devices:

      # public name          RSSI          device address
   -----------------------------------------------------------------
Scanning for devices.
Starting Wireshark
Wireshark started
```

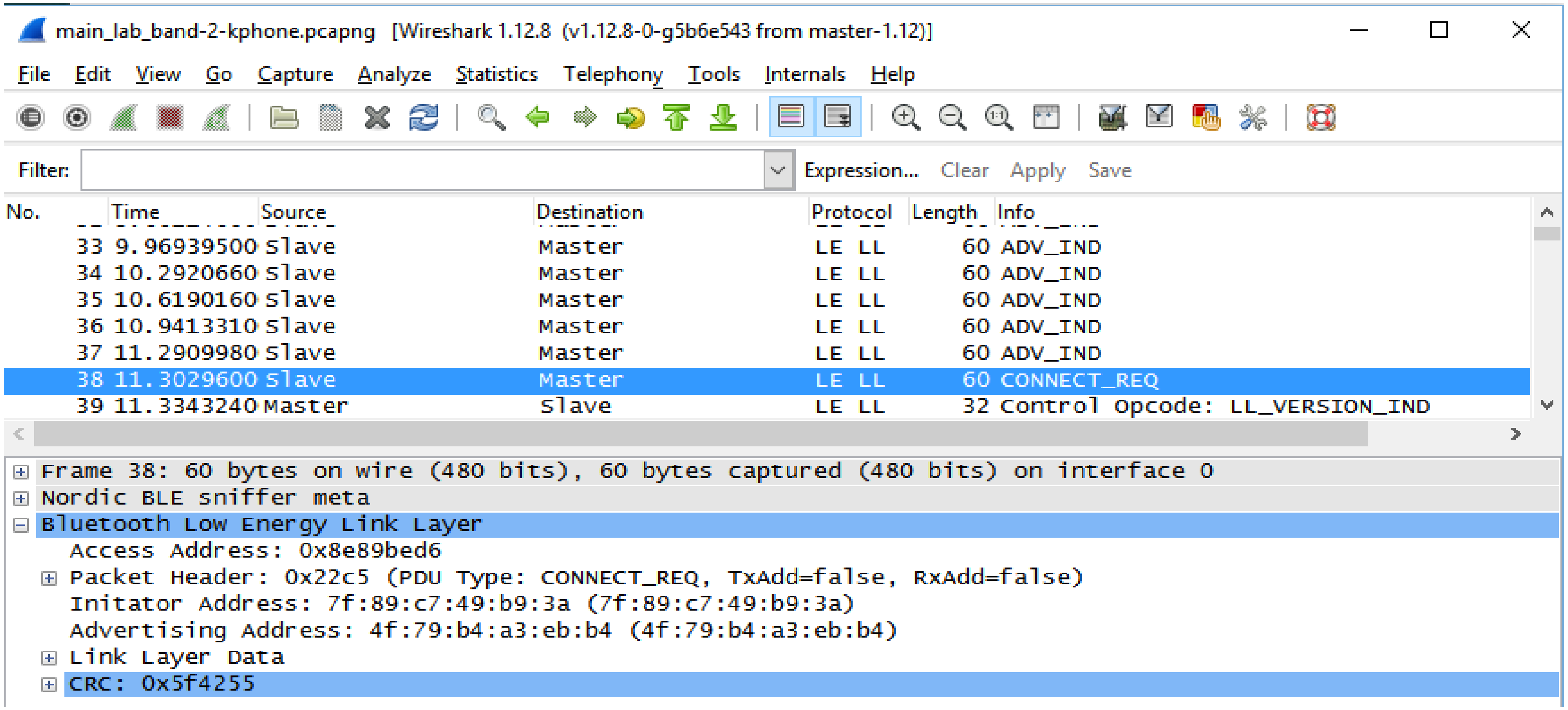


```
C:\Users\user\Desktop\iastate\tools\bluetooth sniffer\nordi...
  c            Display filter: Nearest devices (RSSI > -50 dBm).
  v            Display filter: Nearest devices (RSSI > -70 dBm).
  b            Display filter: Nearest devices (RSSI > -90 dBm).
  a            Remove display filter.
  p            Passkey entry
  o            OOB key entry
  h            Define new adv hop sequence.
  s            Get support
  u            Launch User Guide (pdf)
  CTRL-R       Re-program firmware onto board


 Available devices:

       # public name            RSSI           device address
    -----------------------------------------------------------------
 -> [X] 0 ""                    -66 dBm        4f:79:b4:a3:eb:b4  random
    [ ] 1 ""                    -98 dBm        68:64:4b:22:9f:7b  public
Sniffing device 0 - ""
Starting Wireshark
Wireshark started
```

Diagram 4 Screenshot of Public and Random MAC Address

Background Test Method

- Nordic Semiconductor test results



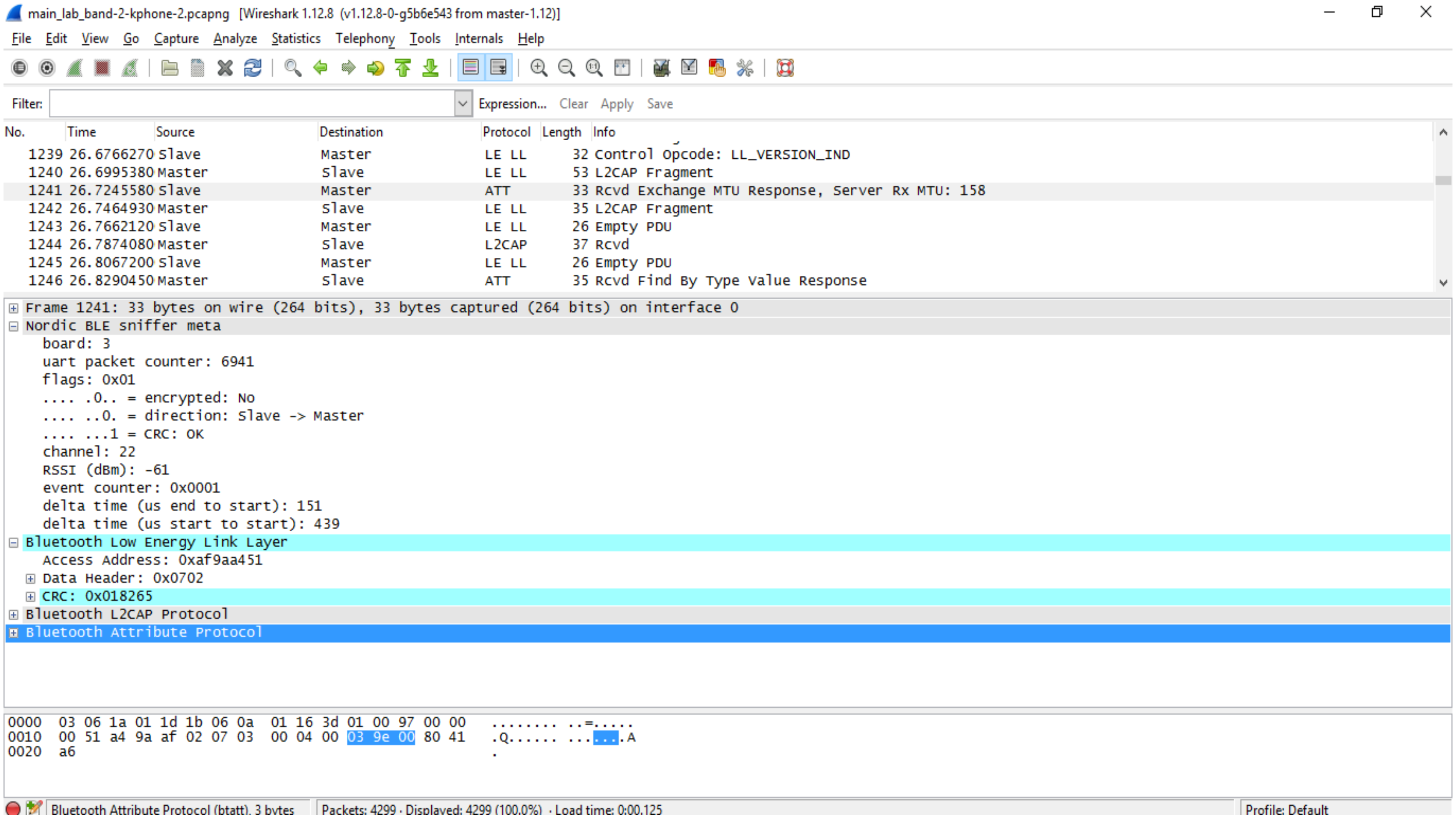
```
No.  Time        Source   Destination  Protocol  Length  Info
  33 9.96939500  Slave    Master       LE LL         60  ADV_IND
  34 10.2920660  Slave    Master       LE LL         60  ADV_IND
  35 10.6190160  Slave    Master       LE LL         60  ADV_IND
  36 10.9413310  Slave    Master       LE LL         60  ADV_IND
  37 11.2909980  Slave    Master       LE LL         60  ADV_IND
  38 11.3029600  Slave    Master       LE LL         60  CONNECT_REQ
  39 11.3343240  Master   Slave        LE LL         32  Control Opcode: LL_VERSION_IND
```

```
⊞ Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Nordic BLE sniffer meta
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊞ Packet Header: 0x22c5 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
    Initator Address: 7f:89:c7:49:b9:3a (7f:89:c7:49:b9:3a)
    Advertising Address: 4f:79:b4:a3:eb:b4 (4f:79:b4:a3:eb:b4)
  ⊞ Link Layer Data
  ⊞ CRC: 0x5f4255
```

- Show the connection request for MS Band 2
  - Random Address = 4F:79:C7:49:EB:B4 (from slide 9)
  - Advertising Address = 4F:79:C7:49:EB:B4 (above)

Background Test Method

- Nordic Semiconductor test results



```
No.   Time       Source   Destination   Protocol  Length  Info
 1239 26.6766270 Slave    Master        LE LL       32 Control Opcode: LL_VERSION_IND
 1240 26.6995380 Master   Slave         LE LL       53 L2CAP Fragment
 1241 26.7245580 Slave    Master        ATT         33 Rcvd Exchange MTU Response, Server Rx MTU: 158
 1242 26.7464930 Master   Slave         LE LL       35 L2CAP Fragment
 1243 26.7662120 Slave    Master        LE LL       26 Empty PDU
 1244 26.7874080 Master   Slave         L2CAP       37 Rcvd
 1245 26.8067200 Slave    Master        LE LL       26 Empty PDU
 1246 26.8290450 Master   Slave         ATT         35 Rcvd Find By Type Value Response
```

```
⊞ Frame 1241: 33 bytes on wire (264 bits), 33 bytes captured (264 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 6941
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 22
    RSSI (dBm): -61
    event counter: 0x0001
    delta time (us end to start): 151
    delta time (us start to start): 439
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9aa451
  ⊞ Data Header: 0x0702
  ⊞ CRC: 0x018265
⊞ Bluetooth L2CAP Protocol
⊞ Bluetooth Attribute Protocol
```

```
0000  03 06 1a 01 1d 1b 06 0a  01 16 3d 01 00 97 00 00   ........ ..=.....
0010  00 51 a4 9a af 02 07 03  00 04 00 03 9e 00 80 41   .Q...... .......A
0020  a6                                                 .
```

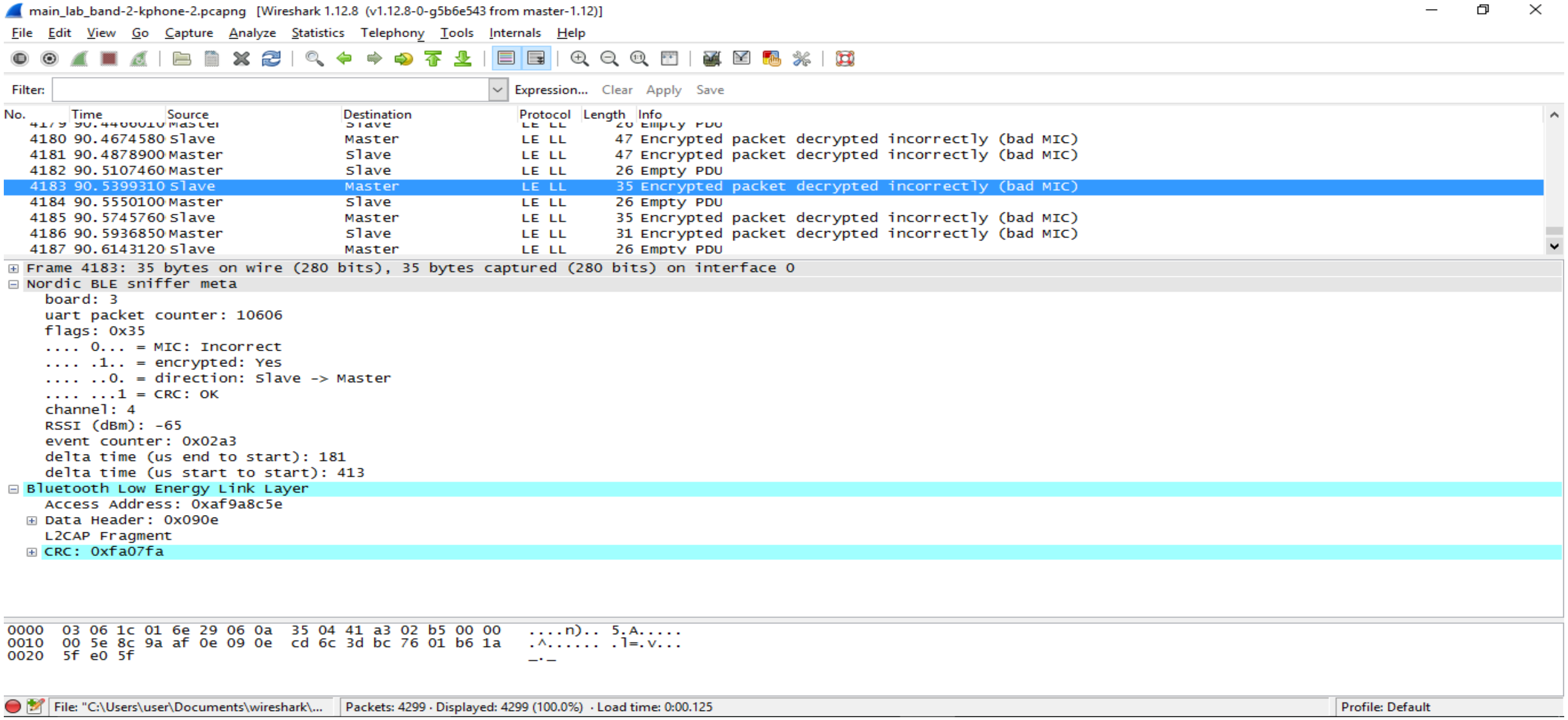
Bluetooth Attribute Protocol (btatt), 3 bytes | Packets: 4299 · Displayed: 4299 (100.0%) · Load time: 0:00.125 | Profile: Default

Shows traffic is send unencrypted

but will switch be being encrypted as shown in slide 12

Background Test Method

- Nordic Semiconductor test results


main_lab_band-2-kphone-2.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source   Destination  Protocol Length Info
4179 90.4466010 Master   Slave        LE LL    26 Empty PDU
4180 90.4674580 Slave    Master       LE LL    47 Encrypted packet decrypted incorrectly (bad MIC)
4181 90.4878900 Master   Slave        LE LL    47 Encrypted packet decrypted incorrectly (bad MIC)
4182 90.5107460 Master   Slave        LE LL    26 Empty PDU
4183 90.5399310 Slave    Master       LE LL    35 Encrypted packet decrypted incorrectly (bad MIC)
4184 90.5550100 Master   Slave        LE LL    26 Empty PDU
4185 90.5745760 Slave    Master       LE LL    35 Encrypted packet decrypted incorrectly (bad MIC)
4186 90.5936850 Master   Slave        LE LL    31 Encrypted packet decrypted incorrectly (bad MIC)
4187 90.6143120 Slave    Master       LE LL    26 Empty PDU
```

```
⊞ Frame 4183: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 10606
    flags: 0x35
    .... 0... = MIC: Incorrect
    .... .1.. = encrypted: Yes
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 4
    RSSI (dBm): -65
    event counter: 0x02a3
    delta time (us end to start): 181
    delta time (us start to start): 413
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9a8c5e
  ⊞ Data Header: 0x090e
    L2CAP Fragment
  ⊞ CRC: 0xfa07fa
```

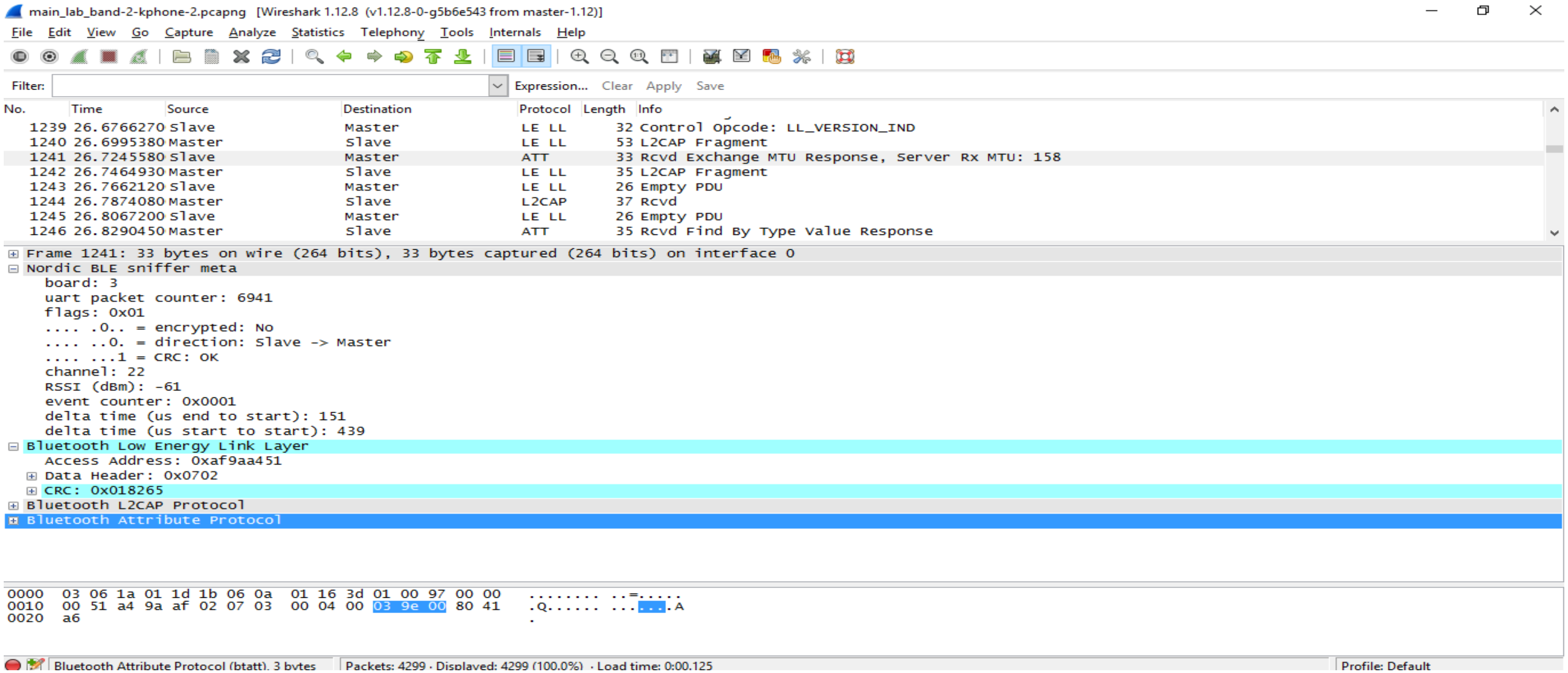
```
0000  03 06 1c 01 6e 29 06 0a  35 04 41 a3 02 b5 00 00   ....n).. 5.A.....
0010  00 5e 8c 9a af 0e 09 0e  cd 6c 3d bc 76 01 b6 1a   .^...... .l=.v...
0020  5f e0 5f                                           _._
```

File: "C:\Users\user\Documents\wireshark\... Packets: 4299 · Displayed: 4299 (100.0%) · Load time: 0:00.125 Profile: Default

- Was un-encrypted as shown in slide 11
- Shows traffic is send encrypted
  - But not decrypted properly
  - Show empty PDU

Background Test Method

- Nordic Semiconductor test results



main_lab_band-2-kphone-2.pcapng [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source  Destination  Protocol Length Info
1239 26.6766270  Slave   Master       LE LL     32 Control Opcode: LL_VERSION_IND
1240 26.6995380  Master  Slave        LE LL     53 L2CAP Fragment
1241 26.7245580  Slave   Master       ATT       33 Rcvd Exchange MTU Response, Server Rx MTU: 158
1242 26.7464930  Master  Slave        LE LL     35 L2CAP Fragment
1243 26.7662120  Slave   Master       LE LL     26 Empty PDU
1244 26.7874080  Master  Slave        L2CAP     37 Rcvd
1245 26.8067200  Slave   Master       LE LL     26 Empty PDU
1246 26.8290450  Master  Slave        ATT       35 Rcvd Find By Type Value Response
```

```
⊞ Frame 1241: 33 bytes on wire (264 bits), 33 bytes captured (264 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 6941
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 22
    RSSI (dBm): -61
    event counter: 0x0001
    delta time (us end to start): 151
    delta time (us start to start): 439
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9aa451
  ⊞ Data Header: 0x0702
  ⊞ CRC: 0x018265
⊞ Bluetooth L2CAP Protocol
⊞ Bluetooth Attribute Protocol
```

```
0000  03 06 1a 01 1d 1b 06 0a  01 16 3d 01 00 97 00 00   ........ ..=.....
0010  00 51 a4 9a af 02 07 03  00 04 00 03 9e 00 80 41   .Q...... .......A
0020  a6                                                  .
```

Bluetooth Attribute Protocol (btatt), 3 bytes | Packets: 4299 · Displayed: 4299 (100.0%) · Load time: 0:00.125 | Profile: Default

- Shows Bluetooth L2CAP Protocol
  - L2CAP is the layer that text transmitted
  - fragment packet should contain text

Background – Tools used

- Encountered issues
  - Not able to locate the plain text
  - Packets being un-encrypted then switches to being encrypted
- Revised Research Project
  - Perytons
    - *Bluetooth Smart Protocol Analyzers (BSPA)*
    - Hardware used with the *BSPA* software
      - 3 *Texas Instruments (TI) CC2540* Smart USB dongles
      - 1 *Bluegiga BLED112 Bluetooth* Smart USB dongle for time synchronization only
      - 4 port USB hub
  - 2 IPhones - most recent IOS – 9.2.1
  - MS Band 2 fitness tracker & mobile app
  - Wireshark - Secondary method to analyze the packets

Background – Revised Tools

- System configuration
  - Laptop *Windows* 10 with *PBSA* 5.4
    - Used to analyze the *Bluetooth* data traffic
  - *Texas Instrument* USB Dongle
    - Used capture BTLE 4.0 packets
  - *Bluegiga* BLED112
    - Time synchronization
  - *IPhone* 5
    - Most recent IOS – 9.2.1

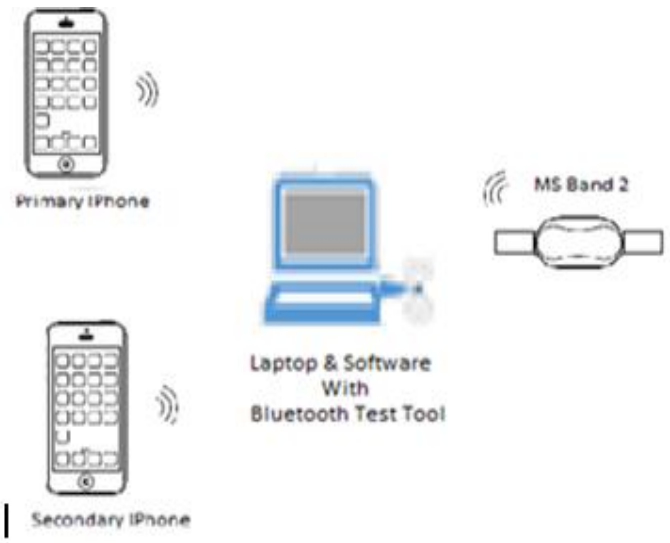
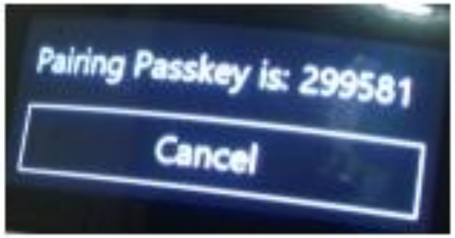


Figure 4: Overview of the controlled lab environment

Background Test Method

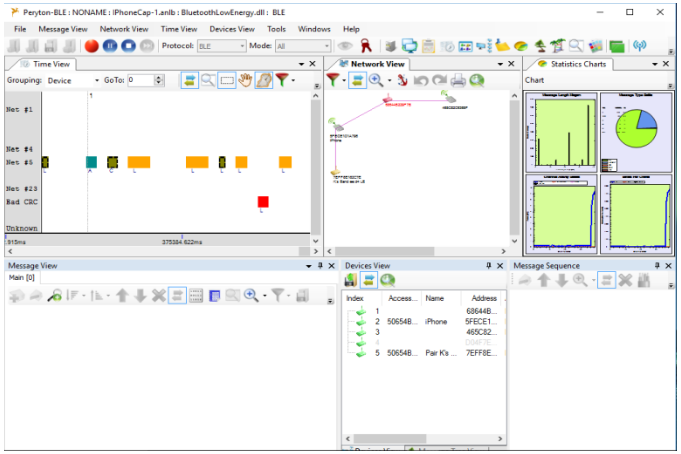
- Peryton test results
  - Shows the Bluetooth Pairing Code used



Pairing Passkey is: 299581

Figure 7: The pairing code of the *MS Band 2*

  - Show the two devices are paired and communicating



Peryton-BLE : NONAME : IPhoneCap-1.anlb : BluetoothLowEnergy.dll : BLE

Protocol: BLE

Mode: All

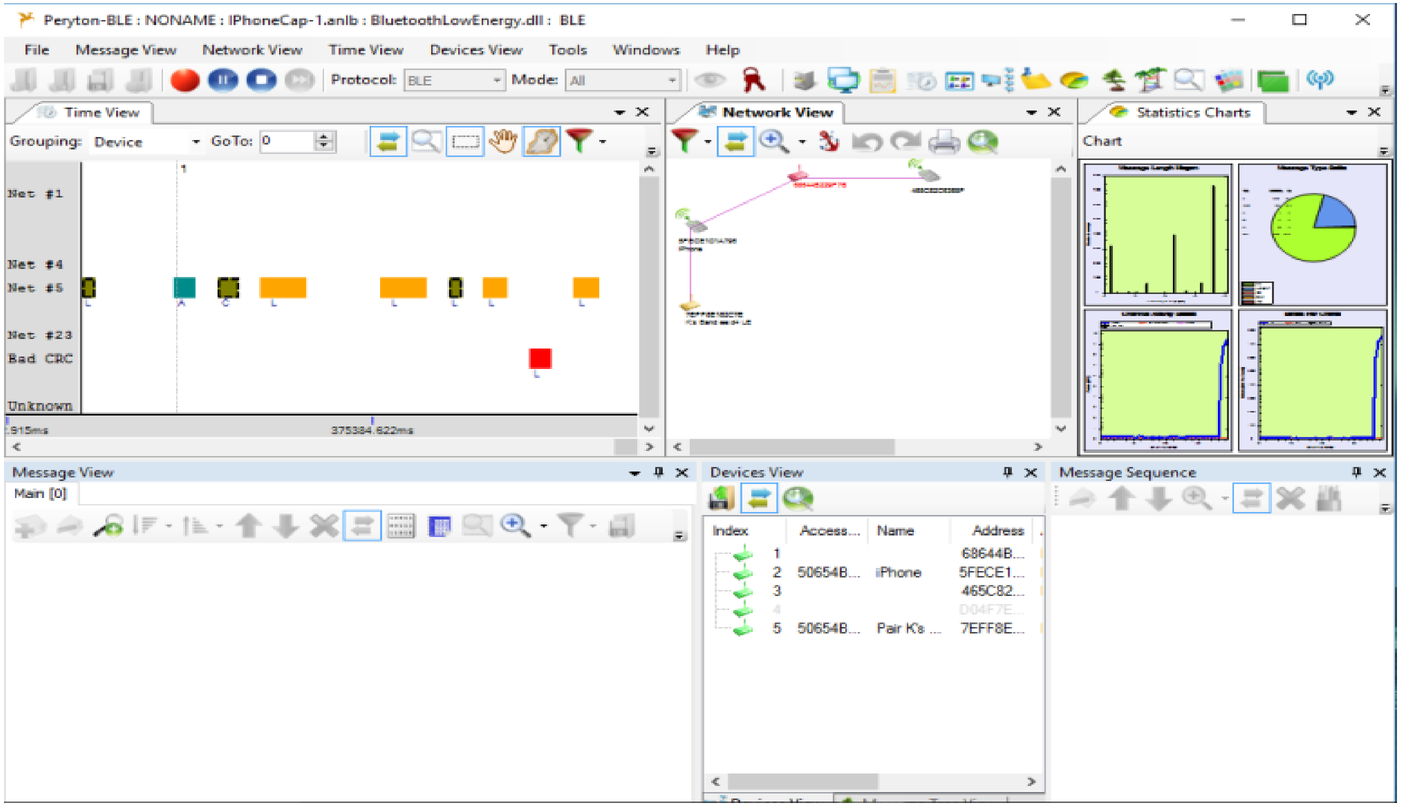
Grouping: Device

GoTo: 0

Index	Access...	Name	Address
1			68644B...
2	50654B...	iPhone	5FECE1...
3			465C82...
4			D04F7E...
5	50654B...	Pair K's ...	7EFF8E...

Background Test Method

- Show the two devices are paired and communicating
  - Passing packets between the two devices



Peryton-BLE : NONAME : IPhoneCap-1.anlb : BluetoothLowEnergy.dll : BLE

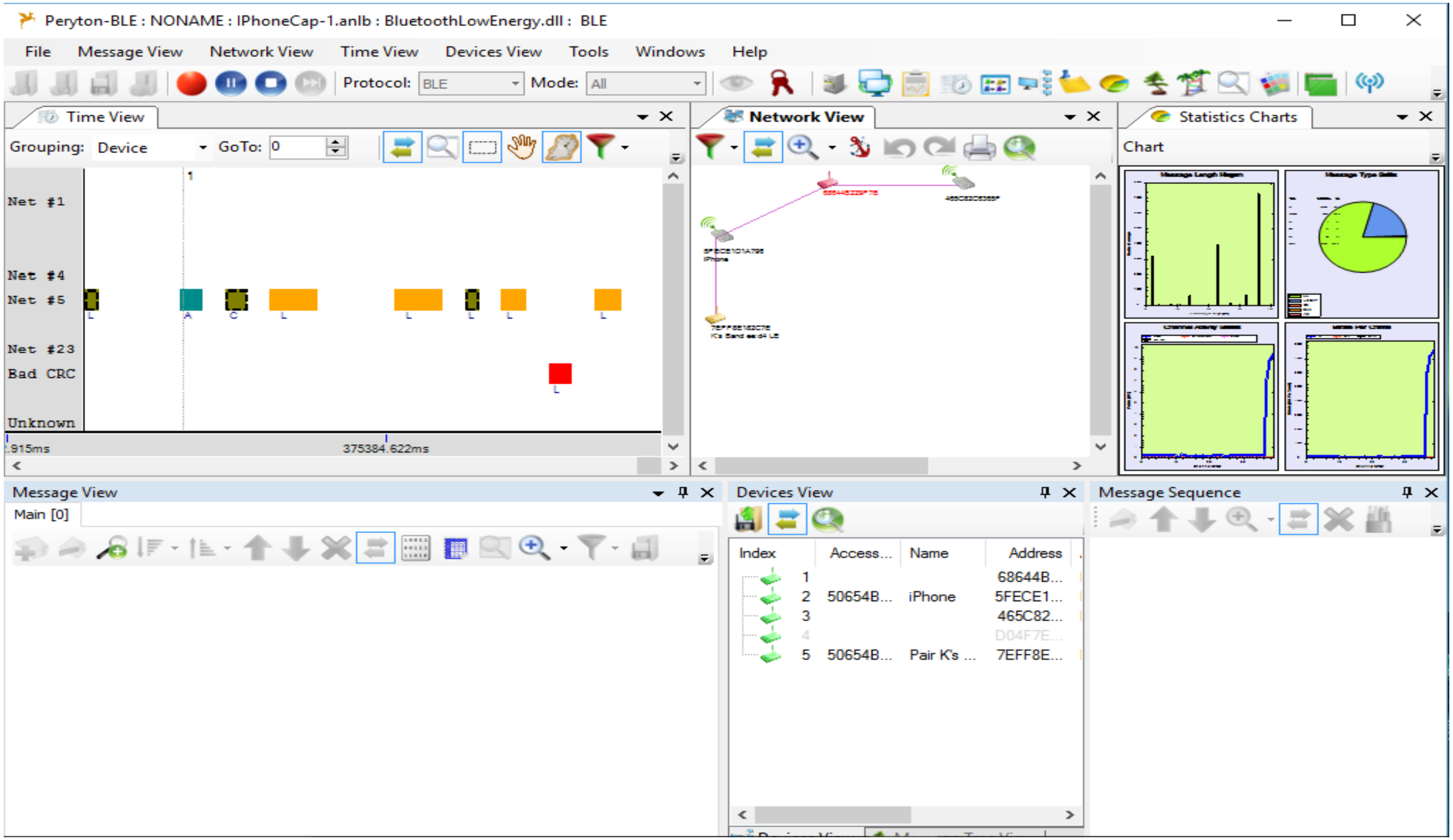
Protocol: BLE Mode: All

Grouping: Device GoTo: 0

Index	Access...	Name	Address
1			68644B...
2	50654B...	iPhone	5FECE1...
3			465C82...
4			D04F7E...
5	50654B...	Pair K's ...	7EFF8E...

Background Test Method

- Peryton test results
  - Show encrypted Bluetooth with L2CAP traffic
    - The red icon indicates the traffic is encrypted



Peryton-BLE : NONAME : IPhoneCap-1.anlb : BluetoothLowEnergy.dll : BLE

Protocol: BLE

Mode: All

Grouping: Device

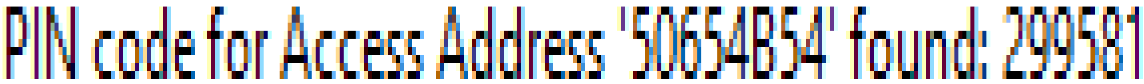
GoTo: 0

Main [0]

Index	Access...	Name	Address
1			68644B...
2	50654B...	iPhone	5FECE1...
3			465C82...
4			D04F7E...
5	50654B...	Pair K's ...	7EFF8E...

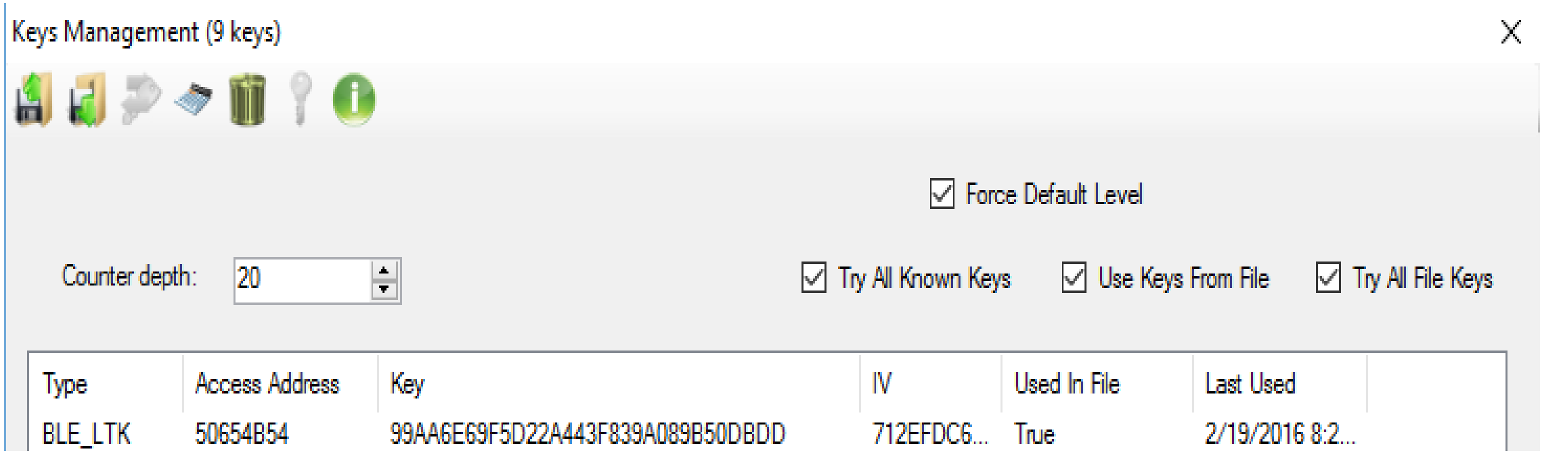
Background Test Method

- Peryton test results
  - Shows the recovered Bluetooth Pairing Code



PIN code for Access Address '50654B54' found: 299581

    - Peryton software was able to recovery the Bluetooth Pairing Code with Brute-force under 20 seconds
    - Addition to discovering the encryption key
  - Shows encryption key used to decrypt packets



Keys Management (9 keys)

☑ Force Default Level

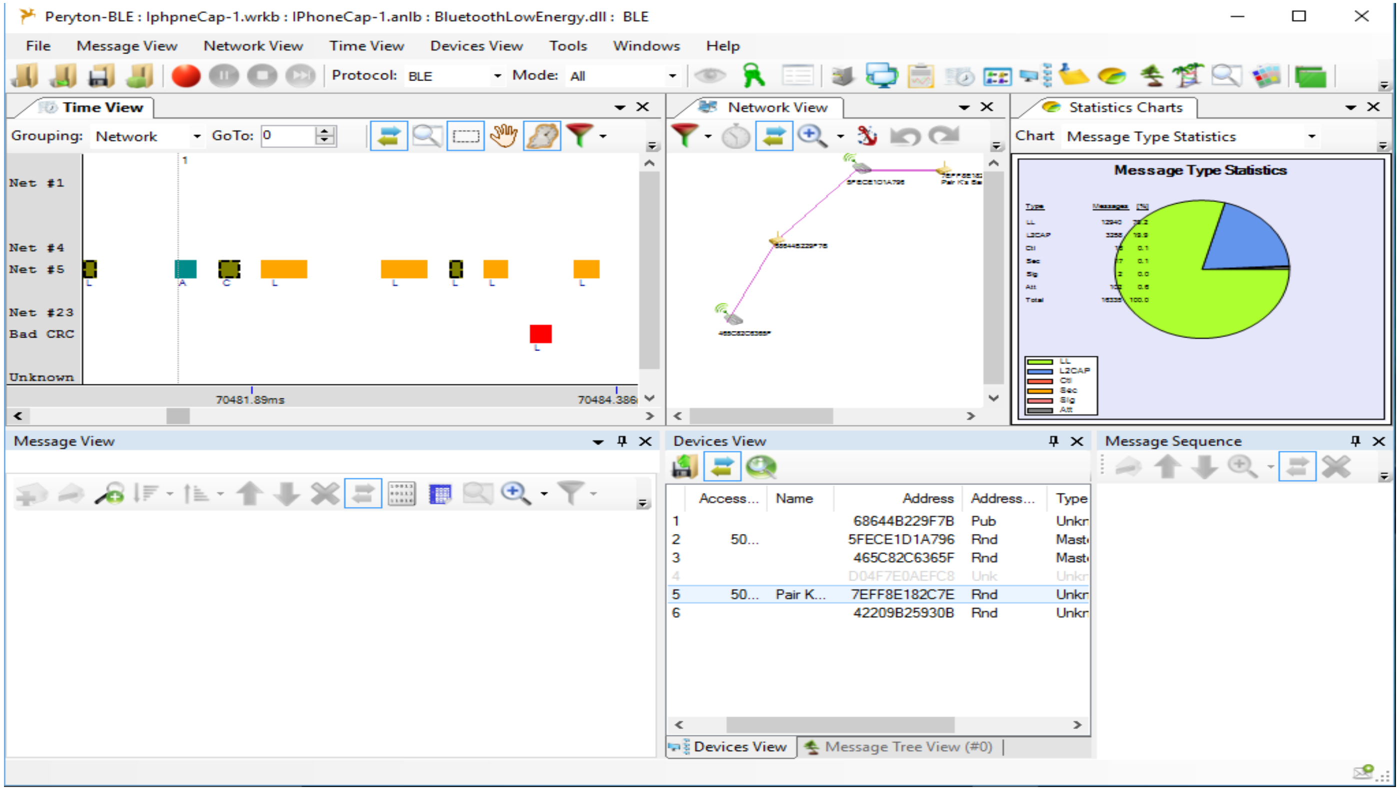
Counter depth: 20

☑ Try All Known Keys ☑ Use Keys From File ☑ Try All File Keys

Type	Access Address	Key	IV	Used In File	Last Used
BLE_LTK	50654B54	99AA6E69F5D22A443F839A089B50DBDD	712EFDC6...	True	2/19/2016 8:2...

Background Test Method

- Peryton test results
  - Show decrypted Bluetooth with L2CAP traffic
    - The green icon indicates traffic is decrypted
      - The blue shaded pie is the L2CAP traffic



Peryton-BLE : IphpneCap-1.wrkb : IPhoneCap-1.anlb : BluetoothLowEnergy.dll : BLE

Protocol: BLE

Mode: All

Grouping: Network

GoTo: 0

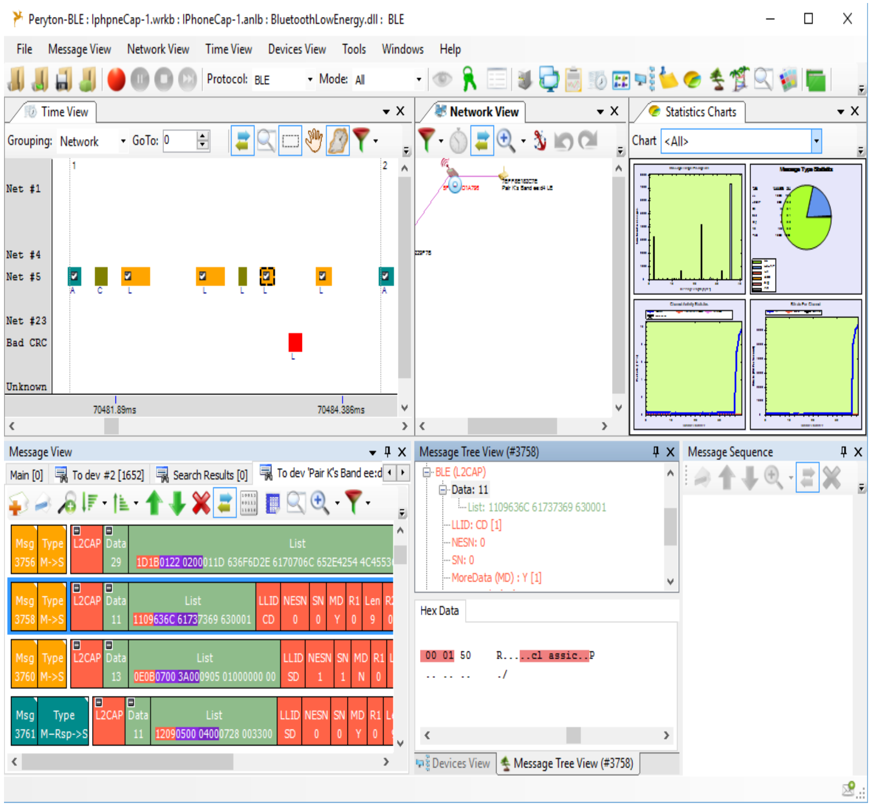
Chart Message Type Statistics

Devices View

	Access...	Name	Address	Address...	Type
1			68644B229F7B	Pub	Unkr
2	50...		5FECE1D1A796	Rnd	Mast
3			465C82C6365F	Rnd	Mast
4			D04F7E0AEFC8	Unk	Unkr
5	50...	Pair K...	7EFF8E182C7E	Rnd	Unkr
6			42209B25930B	Rnd	Unkr

Background Test Method

- Peryton test results
  - Show decrypted Bluetooth L2CAP traffic in plain text
  - The green icon indicates traffic is decrypted
  - The blue shaded pie is the L2CAP traffic



Peryton-BLE : IphpneCap-1.wrkb : IPhoneCap-1.anlb : BluetoothLowEnergy.dll : BLE

Protocol: BLE · Mode: All

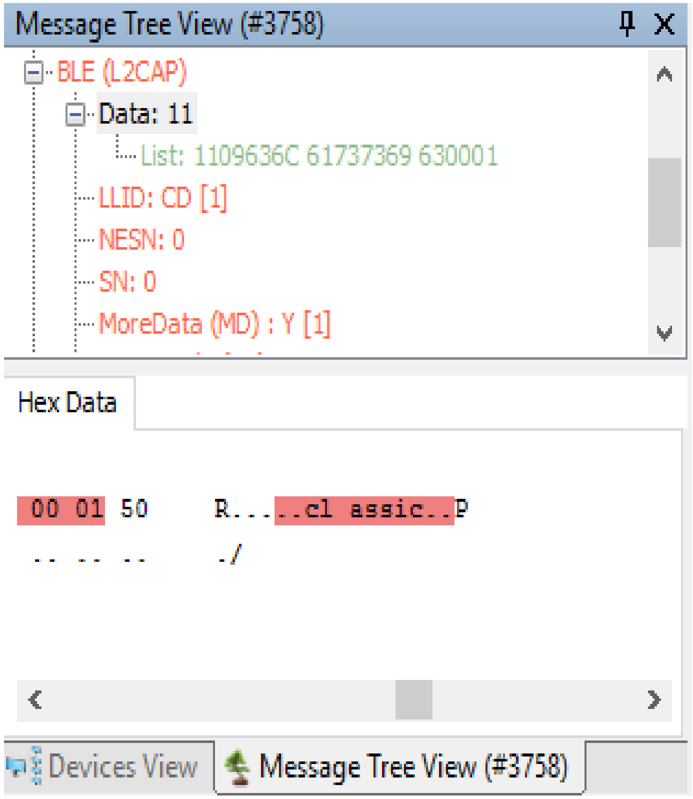
Grouping: Network · GoTo: 0

Chart <All>

```
Msg 3756 | Type M->S | L2CAP | Data 29 | List 1D1B0122 0200011D 636F6D2E 6170706C 652E4254 4C4553
Msg 3758 | Type M->S | L2CAP | Data 11 | List 1109636C 61737369 630001 | LLID CD | NESN 0 | SN 0 | MD Y | R1 0 | Len 9 | R2 0
Msg 3760 | Type M->S | L2CAP | Data 13 | List 0E0B0700 3A000905 01000000 00 | LLID SD | NESN 1 | SN 1 | MD N | R1 0
Msg 3761 | Type M-Rsp->S | L2CAP | Data 11 | List 12090500 04000728 003300 | LLID SD | NESN 0 | SN 0 | MD Y | R1 0
```

```
BLE (L2CAP)
  Data: 11
    List: 1109636C 61737369 630001
  LLID: CD [1]
  NESN: 0
  SN: 0
  MoreData (MD) : Y [1]
```

```
00 01 50      R.....cl assic..P
.. .. ..      ./
```



```
BLE (L2CAP)
  Data: 11
    List: 1109636C 61737369 630001
  LLID: CD [1]
  NESN: 0
  SN: 0
  MoreData (MD) : Y [1]
```

```
00 01 50      R.....cl assic..P
.. .. ..      ./
```

Test Results

- The test results show the following
  - The Bluetooth Pairing Code was encrypted during transmission
  - The fitness tracker data was security send over the Bluetooth network
  - Man in The Middle Attack can take place on fitness tracking devices
  - Encryption packets was successful decrypted

Mitigation solutions

- These solutions are based on Bluetooth Security Standards and Industry best practices
  - **Vendors / Manufactures**
    - Minimum PIN length of 8 [11]
    - Dynamic random MAC addresses [23]
    - Dynamic *Bluetooth* pairing key [23]
    - Use an advanced encryption standard counter with CBC-MAC. “AES-CCM is used in *Bluetooth* LE to provide confidentiality as well as per-packet authentication and integrity. [23]”
    - Use “[n]ew cryptographic keys called the Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK) [23]”
    - Use Security Mode 1 level 3. “NIST considers this the most secure of these modes/levels and strongly recommends its use for all LE connections [23]”
    - Use maximum allowable key sizes (128b) [23]

Mitigation Solutions (Continued)

- **Corporates**
  - Implement security awareness and training [11]
  - Establish and enforce device configuration guidelines and security policies [11]
  - Disable / turn off services [11]
- **End Users**
  - Switch the Bluetooth device to use the hidden or non-discoverable mode [11]
  - Only activate Bluetooth only when it is needed. Turn on airplane mode [11]
  - Disable / turn off GPS tracking location services [11]
  - Ensure device firmware is up-to-date [11]
  - Modify / change default configurations and passwords [11]

Future Research Project

- Conduct Fuzzing on IPhone Wi-Fi hardware
  - Analyze weakness in hardware and Firmware

- Capture Wi-Fi data between IPhone Health app web site
  - Determine if data can be decrypted over Wi-Fi
  - Determine what additional data is being send
  - Determine if GPS data can be interpreted and analyzed to determine user location

Questions & Answers

References

- Adafruit Learning System, " Introducing the Adafruit BlueFruit LE Sniffer", (2015) https://learn.adafruit.com/introducing-the-adafruit-bluefruit-le-sniffer
- Austen, Kat. "The Trouble with Wearables." (2015): 22-24.
- Bluetooth, S. I. G. "Specification of the Bluetooth System: Covered Core Package version: 4.0." (2010).
- Brink, Deborah Silvia. *Affecting user attitudes: Mobile devices and Bluetooth security*. Diss. The University of Alabama In Huntsville, 2015.
- Bouhenguel, Redjem, Imad Mahgoub, and Mohammad Ilyas. "Bluetooth security in wearable computing applications." *High Capacity Optical Networks and Enabling Technologies, 2008. HONET 2008. International Symposium on*. IEEE, 2008
- Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security Analysis of Wearable Fitness Devices (Fitbit). Massachusetts Institute of Technology.
- Clausing, D. I. E., Schiefer, M., Lösche, U., & Morgenstern, D. I. M. (2015). Security Evaluation of nine Fitness Trackers.
- Creasy, Hank and Knoespel. "The New Generation of Electronic Health Records: What Health Apps Know About You" Virginia Lawyer, Health Law (2015), 24-25.
- Gehrmann, Christian, and Kaisa Nyberg. "Enhancements to Bluetooth Baseband Security." Proceedings of Nordsec. Vol. 2001. 2001.
- Hale, Matthew L., et al. "Secu Wear: An Open Source, Multi-component Hardware/Software Platform for Exploring Wearable Security." *Mobile Services (MS), 2015 IEEE International Conference on*. IEEE, 2015.
- Hall, J. B. "Brush up on Bluetooth". *Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC), Research Project, Version 1.4 b*. (2003) 1-14
- Hassler, Susan. "You in Your Internet of Things [Spectral lines]." Spectrum, IEEE 52.4 (2015): 8-8.
- Hughes, Alan. *Threat assessment of wearable technology*. Diss. Utica College, 2014.
- Hunter, Philip. "Is now the time to define a mobile security policy?" *Computer Fraud & Security* 2007.6 (2007): 10-12.
- Jakobson, Markus, and Susanne Wetzel. "Security weaknesses in Bluetooth." Topics in Cryptology—CT-RSA 2001. Springer Berlin Heidelberg, 2001. 176-191.
- King, Christopher, Jonathan Chu, and Andrew Mellinger. "Emerging Technology Domains Risk Survey." (2015).
- Kitsos, Paraskevas, et al. "Hardware implementation of Bluetooth security." IEEE Pervasive Computing 1 (2003): 21-29.
- Li, Andrew M., and Sharon F. Terry. "Linking Personal Health Data to Genomic Research." Genetic testing and molecular biomarkers 19.1 (2015): 1-2.
- Lin, Ying-Dar, et al. "Mobile Application Security." *Computer* 47.6 (2014): 21-23.

References

- Migicovsky, Alex, et al. "Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2014. 89-96.
- Niem, T. C. "Bluetooth and its inherent security issues". *Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC), Research Project, Version 1.4 b*. (2003) 1-29
- Nigel, Davies, et al. "Security and privacy implications of pervasive memory augmentation." Pervasive Computing, IEEE 14.1 (2015): 44-53.
- Padgette, John, Karen Scarfone, and Lily Chen. "Guide to bluetooth security." *NIST Special Publication* 800.121 (2012): 25.
- Paul, Greig, and James Irvine. "Privacy Implications of Wearable Health Devices." *Proceedings of the 7th International Conference on Security of Information and Networks*. ACM, 2014.
- Pauli, D. "'10-second' theoretical hack could jog Fitbits into malware-spreading mode (Wristputer-pusher disputes claims from Fortinet)" The Register Oct 2015, (2015) http://www.theregister.co.uk/2015/10/21/fitbit_hack/
- Rahman, Mahmudur, Bogdan Carbunar, and Madhusudan Banik. "Fit and vulnerable: Attacks and defenses for a health monitoring device." arXiv preprint arXiv:1304.5672 (2013).
- Rahman, M., Carbunar, B., & Topkara, U. Step Towards Better Security: Attacks and Defenses for Low Power Fitness Trackers.
- Roque, Rob. "Technology Trends to Prepare for in 2015." Government Finance Review (2015).
- SANS Institute Policy Team "Bluetooth Baseline Requirements Policy" Consensus Policy Resource Community, SANS Institute, (2014) https://www.sans.org/security-resources/policies/network-security/pdf/bluetooth-baseline-requirements-policy
- Tan, Margaret, and Kathrine Aguilar Masagca. "An investigation of Bluetooth security threats." *Information Science and Applications (ICISA), 2011 International Conference on*. IEEE, 2011.
- Thierer, Adam D. "the internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation." *Rich. JL & Tech.* 21 (2015): 6-15.
- Toorani, Mohsen. "On vulnerabilities of the security association in the IEEE 802.15. 6 standard." *arXiv preprint arXiv:1501.02601* (2015).
- Vainio, Juha T. "Bluetooth security." Department of Computer Science and Engineering, Helsinki University of Technology, Available at website http://www.niksula.cs.hut.fi/~jiitv/bluesec.html (2000).
- Xu, Y. "Swot Analysis of Domestic Market of Wearable Sports Equipment Based on Internet of Things Technology." *2015 International Conference on Artificial Intelligence and Industrial Engineering*. Atlantis Press, 2015.
- Yan, Tong, Yachao Lu, and Nan Zhang. "Privacy Disclosure from Wearable Devices." *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing*. ACM, 2015.
- Zhou, Wei, and Selwyn Piramuthu. "Security/privacy of wearable fitness tracking IoT devices." *Information Systems and Technologies (CISTI), 2014 9th Iberian Conference on*. IEEE, 2014.